ABSTRACT

Title of Thesis:	A SYSTEMS MODELING DESIGN UTILIZING AN OBJECT-ORIENTED APPROACH CONCERNING INFORMATION RISK MANAGEMENT
Degree candidate:	Noriaki Suzuki
Degree and year:	Master of Science in Systems Engineering, 2005 Fall
Thesis directed by:	Nelson X. Liu, Assistant Research Scientist, Institute for Systems Research

Adopting advanced information technologies within the present broad application fields requires precise security. However, security problems regarding information privacy have occurred frequently over the last 5 years despite the contribution of these technologies. To respond to the need for securing information privacy, the Information Privacy Law was enacted on April 1, 2005 in Japan. One of the responses to this law enforcement is demanding a higher level of information risk management and search for more effective tools to be used for identity protection and problem-solving. Two examples of these tools include RAPID and IRMP. However, there is no established system-development model for either of these tools. Further developments to improve the RAPID and IRMP remain as new challenges. In this thesis, a new approach on developing a system security model to be used for information risk management is proposed. To demonstrate this approach, the object-oriented language is used.

A SYSTEMS MODELING DESIGN UTILIZING AN OBJECT-ORIENTED APPROACH CONCERNING INFORMATION RISK MANAGEMENT

By

Noriaki Suzuki

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Master of Science
2005 Fall

Advisory Committee:

Dr. Nelson X. Liu, Assistant Research Scientist, Institute for Systems Research

Professor Eyad Abed, Director of the Institute for Systems Research

Professor Michel Cukier, Assistant Professor, Reliability Engineering

ACKNOWLEDGEMENTS

I would like to express my honest thanks to my advisor, Dr. Nelson X. Liu, for his strong direction and guidance throughout this work. I could not have completed the thesis without his constant advice and help. I would also like to thank my secondary advisor Lee Strickland. He helped me in analyzing current security breaches and investigating the information risk assessment in chapter 3. I would also like to thank Prof. Eyad Abed and Prof. Michel Cukier for agreeing to serve on my committee. Furthermore, I am grateful to my friends Sivakumar Chellathurai, Suchee Nathan, and Brent Anderson for their help and valuable comments in written form of this thesis. Many thanks to Jonathan Eser, Daniela Villar del Saz, Gokul Samy, and Pampa Mondal for their friendship and support throughout my studies in Maryland; without their support I probably would not be where I am now. Finally, I am grateful to the systems engineering program at the University of Maryland, College Park. This study has equipped me with the skills I need in order to make a more significant contribution to the world and offer the tools I will need to overcome obstacles I may face in the future.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Introduction

With the advent of the digital-age, a coherent information policy is required to support the rapid flow of information. Internet technologies have changed the face of both business and personal interaction. Introducing a system to the Internet results in immediate world scale network exposure. Due to this exposure, information trade is easy and fast. However, this exposure also results in security breaches regarding information leak, which occur daily throughout the world. In Japan, the total number of such problems last year amounted to 2297 instances. Just from January to July of 2005, the number of Internet privacy losses already reached 7009 cases[1]. To address this vulnerability, the Information Privacy Law was enacted on April 1, 2005 in Japan[2]. After the law was enacted, an onslaught of system security products were released with many more on the way[3]; however, the products will not be effective unless both system developers and users have an understanding about what kind of information policy that the system requires and how they should deal with the information policy in development security systems[4]. According to the article "The Way to Develop the Secure Information

[1] The present state of privacy information breach problem
http://www.ahnlab.co.jp/virusinfo/security_view.asp?news_gu=03&seq=86&pageNo=4

[2] Ministry of Internal Affair and Communication information privacy law site,
http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm

[3] Systemwalker Desktop keeper, Fujitsu http://systemwalker.fujitsu.com/jp/desktop_keeper/ / IPLOCKS Information Risk Management Platform, IPLOCKS, 2 pages
http://www.iplocks.com/images/newsarticles/3customers_final_052705.pdf

[4] Overreacted t o the information privacy law, Yoshiro Tabuchi, NIKKEI BP in Japan, July. 5 2005,
http://nikkeibp.jp/sj2005/column/c/01/index.html?cd=column_adw

Risk Management System"[5], based on the analysis of 61 cases of privacy information security breach problems published on the Net Security site[6], less than 10% of problems are actually caused by hacker attacks. Nearly all (90%) problems originate at the design stage (41%) and maintenance (52.5%) stage. This demonstrates the lack of regard for information risk management at the design and maintenance stage. The same article concludes that the problems caused at the design stage are due to a lack of understanding on the part of the systems engineer; and security risks compounded as systems near completion. The same poor understanding of security and information risk management on the part of operators is responsible for delayed responses during maintenance. In addition, the report - "Information security: why the future belongs to the quants"[7] indicates that developers should work on quality early in the process, where cost is lower as Table 1 shows. A cost to correct at the design stage is the lowest among the all stages. On the other hand, a cost at the maintenance stage is the highest; it is almost more 100 times than the cost at the design stage. In addition, security defects also tend to occur at certain design stages more than other stages as depicted in Table 2.

[5] The way to develop the secure information risk management system, D add ninth Co., Ltd. Oct 1 2002, http://www.dadd9.com/tech/sec4manager.html

[6] NetSecurity, Livin' on the EDGE Co., Ltd. & Vagabond Co.,Ltd., , https://www.netsecurity.ne.jp/

[7] Information security: why the future belongs to the quants, Security & Privacy Magazine, IEEE, July-Aug. 2003, Volume 1, Issue 4, Page 24 –32

STAGE	RELATIVE COST
Design	1.0
Implementation	6.5
Testing	15.0
Maintenance	100.0

Table 1: Relative Cost to Correct Security Defects by Stage[8]

CATEGORY	ENGAGEMENTS WHERE OBSERVED	DESIGN RELATED	SERIOUS DESIGN FLAWS*
Administrative interfaces	31%	57%	36%
Authentication/access control	**62%**	**89%**	**64%**
Configuration management	42%	41%	16%
Cryptographic algorithms	33%	93%	61%
Information gathering	**47%**	**51%**	**20%**
Input validation	71%	50%	32%
Parameter manipulation	33%	81%	73%
Sensitive data handling	**33%**	**70%**	**41%**
Session management	40%	94%	79%
Total	45%	70%	47%

Table 2: Security Defects by Category[9]

The categories printed in bold in the above table relate to information leak problems. As the above evidences show, it is crucial to be concerned about security issues at the design stage in developing systems. To overcome the abovementioned problems, several information risk management tools such as RAPID[10] and IRSP[11] have been developed.

[8] Information security: why the future belongs to the quants, Security & Privacy Magazine, IEEE, July-Aug. 2003, Volume 1, Issue 4, Page 26

[9] Information security: why the future belongs to the quants, Security & Privacy Magazine, IEEE, July-Aug. 2003, Volume 1, Issue 4, Page 29

[10] Information Security Program Development Using RAPID, http://www.nmi.net/rapid.html

[11] Information Risk Management Program, CSC CyberCare, 5 pages http://www.csc.com/industries/government/knowledgelibrary/uploads/807_1.pdf

RAPID is used for defining necessary business processes and developing guidelines to develop a security system. IRSP provides information risk management programs to support and improve existing client security systems. However, these tools identify only the management steps needed to enforce the existing security system and do not expand on the methodology and models necessary for developing new systems. In developing new systems, which require a significant information policy, the methodology, approach, system modeling, and system model verification must be clearly outlined. This outline significantly helps a systems engineer to work on quality at the early stage in developing systems.

This thesis focuses on an information risk assessment, method of developing information policy, modeling system and system model verification, all of which must be considered in the design stage. Newly developed systems must be forward compatible with new technologies for threats that may occur during the maintenance stage. It is required for the design to have the following:

- Suitable for the addition of various security components
- Re-useable security components for various systems
- Provide common understanding among system developers

Object-oriented design is the most suitable design methodology to overcome the aforementioned requirements, and as the premiere meta-modeling language for analysis and design in the software engineering community, the Unified Modeling Language (UML)[12] will be used. For example, modeling the systems with UML creates a common

[12] OMG (Object Management Group) official site, Unified Modeling Language, http://www.uml.org/

understanding for both developers and user domain experts. A better understanding of how the user systems function facilitates the detection of security problems early in system development.

The following are benefits of using the system developing approach and methodology involving the information risk management model discussed in this thesis.

- ✓ Prioritizes security risk solutions: Information risk assessment helps developers to realize highly required security issue and provide risk solutions.
- ✓ Secures the privacy information: A well-grounded countermeasure and its security solution based on a risk assessment make systems to be secure.
- ✓ Reduces errors: Information risk management, modeling systems, systems model verification at the design stage reduce security defects efficiently and effectively.
- ✓ Facilitates updates for new security threats: A system modeling with UML facilitates developers to update and reuse components in systems, and provides high compatibility to other systems.
- ✓ Provides understandable system design documents: Information risk management with simple concept and design document using UML provides well understanding to any developers and stakeholders.

In this thesis, information risk management is introduced with current security studies and a new model, which is developed herein. Next, following the presentation of this new model for information risk management, 20 current security breach issues will be analyzed and assessed using the risk management assessment method. Then, three worst-case security breach issues will be addressed. Third, information policies will be developed using countermeasures in response to the worst-case security breaches, and then security mechanisms based on these information policies will be shown. Fourth, system modeling will be performed with UML. Fifth, security mechanisms based on dynamic information policies developed in this thesis will be verified. In addition, validation of the system model is shown. A state chart diagram in a case without policy, with static policy, and with dynamic policy is developed. The cases are then validated with UPPALL[13]. UPPALL is an integrated tool environment for modeling, validating and verifying real-time systems modeled as networks of timed automata. Finally, this thesis will conclude by demonstrating how to develop the secured system model discussed in this thesis. This thesis contributes to systems engineering by providing a framework for handling security issues faced by enterprises managing secure information.

[13] UPPAAL homepage, http://www.uppaal.com/

2. Background

2-1. Review of Existing Studies

In this report, outlining a methodology and modeling for developing systems to prevent information leaks are the main themes. Such an effort is significant for systems engineers in developing systems and similar studies are available. In this section, three similar existing studies are reviewed. Their approaches are analyzed and an outstanding methodology with model-based risk assessment is used in developing systems.

1. Information Flow Analysis of Component-Structured Applications, Peter Herrmann, 2001[14]

The diversity and complexity of information flow between components pose the threat of leaking information. Security analysis must be performed in order to provide suitable security solutions. Systems are audited for vulnerabilities, threats, and risks. Based on the audit, effective safeguards are selected, designed, and configured. However, since information flow analysis tends to be expensive and error-prone, object oriented security analysis and modeling is utilized. It employs a UML-based object-oriented modeling techniques and graph rewriting in order to make the analysis understandable and to assure its accuracy even for large systems. Information flow is modeled based on Myers' and

[14] Computer Security Applications Conference, ACSAC 2001 Proceedings 17th Annual 10-14, Dec. 2001, Page 45 – 54

Liskov's[15] decentralized label model combining label-based read access policy models and declassification of information with static analysis.

2. Developing Secure Networked Web-Based Systems Using Model-based Risk Assessment and UMLsec, Siv Hilde Houmb / Jan J¨urjens, 2003[16]

Despite a growing awareness of security issues in networked computing systems, most development processes used today still do not take security aspects into account. This paper shows a process for developing secure networked systems based on CORAS framework[17][18], whose concept is a model based risk assessment using UMLsec. UMLsec is an extension of the Unified Modeling Language (UML) for secures systems development. Enterprise information such as security policies, business goals, policies and processes are supported through activities in a model-based integrated development process. Security requirements at a more technical level can be expressed using UMLsec. Additionally, a support-tool for a mechanical analysis of such requirements is provided.

[15] Decentralized Model for Information Control Flow In Proc. 16th ACM Symposium on Operating Systems Principles, A. C. Myers and B. Liskov. A, Saint-Malo, France, 1997

[16] Software Engineering Conference, Tenth Asia-Pacific 2003, 2003, Page 488 - 497

[17] Towards a UML profile for model-based risk assessment, S.-H. Houmb, F. den Braber, M. S. Lund, and K. Stolen, In J¨urjens et al.

[18] Business Component-Based Software Engineering, chapter Modelbased Risk Assessment in a Component-Based Software Engineering Process, K. Stølen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. Gran, S. Houmb, Y. Stamatiou, and J. Aagedal, The CORAS Approach to Identify Security Risks, Kluwer, 2002, Pages 189–207

3. Model-based Risk Assessment to Improve Enterprise Security, Jan Øyvind Aagedal / Folker den Braber / Theo Dimitrakos§ / Bjørn Axel Gran / Dimitris Raptis‡ / Ketil Stølen, 2002[19]

This paper attempts to define the required models for a model-based approach to risk assessment. CORAS is applied to provide methods and tools for precise, unambiguous, and efficient risk assessment of security critical systems since traditional risk assessment is performed without any formal description of the target of evaluation or results of the risk assessment. CORAS provides a set of models to describe the target of assessment at the right level of abstraction, and medium for communication between different groups of stakeholders involved in a risk assessment. In one step of the risk treatment, a strengthening of the security requirements is suggested to handle identified security problems. In addition, many risk assessment methodologies are presented, such as HazOP[20] and FMEA[21]. HazOP is applied to address security threats involved in a system, and FMEA is applied to identify potential failure in the system's structure. All components in the system's structure are expressed by UML. Many approaches are taken into account in developing systems. The following table is a brief comparison of the approach in this thesis to the three aforementioned approaches.

[19] Model-based Risk Assessment to Improve Enterprise Security, Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International, Sept. 2002, Page 51 – 62

[20] Security Assessments of Safety Critical Systems Using HAZOPs, R. Winther, O. A. Johnsen, and B. A. Gran, 20th International Conference on Computer Safety, Reliability and Security SAFECOMP 2001, Hungary, 2001

[21] FMEA Risk Assessment, http://www.tangram.co.uk/TI-HSE-FMEA-Risk_Assessment.html

Title #	Survey	Risk Analysis	Security Solution	Design	Tool
1	No	Common Criteria[22]	Information Flow	UML	Java Beans-based components
2	No	CORAS framework	UMLsec		MDR[23] UML CASE tool Poseidon[24] (Does not apply)
3	No	CORAS			N/A
		HazOp, FMEA		UML	
This Thesis	Yes	Risk Assessment extending with DOD[25] standard (new)	Information policy and its procedure (new)	UML	UPPAAL[26]

Table 3: Comparison of the Approach of This Thesis to Other Approaches

All approaches are very useful and powerful in developing secure systems; however, the approach in this thesis may be well suited and used widely and easily for recent systems since the concept of this approach is very simple and its security mechanisms are based on countermeasures from current information leak problems.

2-2. Information Risk Management

What is information risk management? According to an article[27] regarding information risk management provided by the Nomura Research Institution[28],

[22] Common Criteria for Information Technology Security Evaluation, I International Standard ISO/IEC, SO/IEC, 1998

[23] Meta-Data Repository, MDR homepage, http://mdr.netbeans.org

[24] UML CASE tool Poseidon, Gentleware homepage, http://www.gentleware.com

[25] Department of Defense home page, http://www.defenselink.mil/

[26] UPPAAL homepage, http://www.uppaal.com/

[27] Understanding Information Risk Management, Nomura Research Institution, 2002, 95 pages http://www.nri.co.jp/opinion/chitekishisan/2002/pdf/cs20020910.pdf

[28] Nomura Research Institution home page, http://www.nri.co.jp/english/index.html

information risk management are those policies which reduce risk inherent in information processing. As enterprises invest in information-oriented systems, databases such as customer information databases have resulted in enterprises maintaining and using greater quantities of information. Poor information management may result in information leaks and hacker attacks, resulting in considerable loss and damage to the enterprises. For example, the information of 900,000 clients of Yahoo! BB in Softbank, which is one of the largest high-speed Internet connection services, was leaked by an ex-employee's misuse of its database system[29]. The leaked information almost spread to the Internet. The company paid $10 to each client as a self-imposed penalty for this lapse in security. Total financial losses reached $9 million. While insider culprits must pay for their crimes, the responsible company must create an environment where such events are defended against. The following figure represents information risk. The upper left graph in the figure shows the probability of risk occurrence in each given process; the bottom left graph shows the magnitude of assets involved in the information for each given process. The information risk level is determined by the combination of the probability and assets. For instance, a combination of high probability of risk exposure and high asset value will be the highest risk level; on the other hand, a combination of low probability of risk exposure and low value of assets will be the lowest risk level. In the case of the aforementioned security breach, the probability of risk exposure is once every 3 years; this probability is low. However, the value of information assets is extremely high. Thus, the risk level will be middle or high. The risk level may be between unacceptable risk and

[29] *The Japan Times;* Softbank leak extortionist won't serve time; July 10, 2004; http://search.japantimes.co.jp/print/news/nn07-2004/nn20040710a4.htm

undesirable risk.

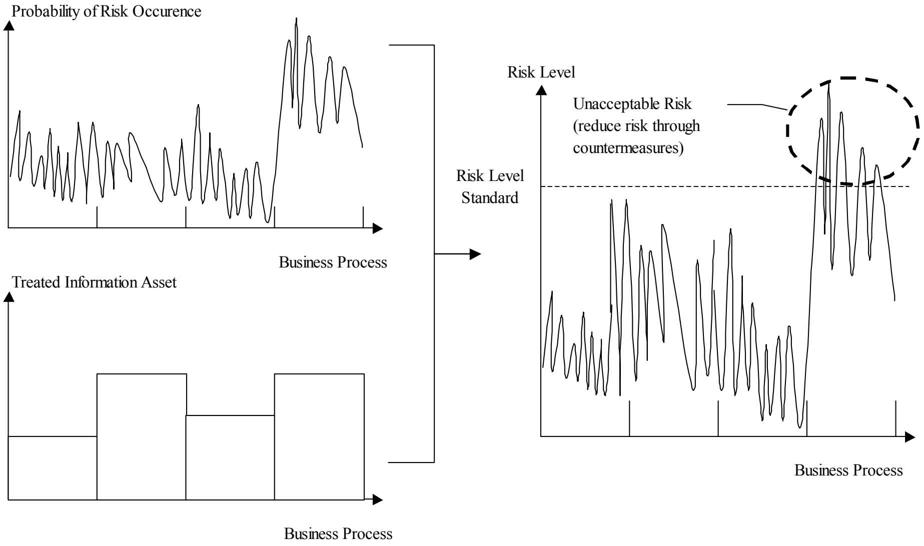


Figure 1: Depicting for Information Risk[30]

In response to emergent security problems, many government agencies in Japan and the United State now require information security management certification. In Japan, ISMS (Information Security Management System) was issued last year[31]. It has become a standard certification for information risk management. In the United State, Congress passed the Federal Information Security Management Act of 2002 (FISMA)[32], which provides the overall information risk management framework for ensuring the effectiveness of information security controls that support federal operations and assets[33].

[30] Understanding Information Risk Management, Nomura Research Institution, 2002, Page 94, http://www.nri.co.jp/opinion/chitekishisan/2002/pdf/cs20020910.pdf

[31] Information Security Management System (ISMS) home page, http://www.isms.jipdec.jp/

[32] Federal Information Security Management Act of 2002 (Title III of E-Gov), Computer Security Resource Center, http://csrc.nist.gov/policies/

[33] Improving Oversight of Access to Federal Systems and Data by Contractors can Reduce Risk, Wanja Eric Naef, GAO, April 2005, 28 pages

Information risk management is required in developing systems. It has become the center of public attention in the last few years. As a result of this demand, many information risk management tools have been introduced. Among these tools, RAPID and IRSP are notable. RAPID is useful for defining necessary business processes and developing guidelines to improve existing security systems. It will fit security systems into existing systems. The processes are 1) risk assessment, 2) security problem identification and awareness review, 3) security program creation and support. IRSP provides an information risk management program to support and improve client security systems. The program defines certain client security policies and provides static and dynamic protection. Protection schemes are as follows:

Static Protection

A rule and definition of security standards, security architecture, security service, recovery interface, and other additional security needs based on countermeasures from personal, physical, administrative, communications, and technology.

Dynamic Protection

Security protection program involving vulnerability alert processes, vulnerability assessment processes, monitoring services, and anti-virus programs plan based on information security best practices.

After analyzing the both types of protection, the program shows certain security compliance standards and specifications based on the static protection. In addition, the program assembles best protection practices and creates the proper program based on the dynamic protection.

However, these tools do not provide any strict methodology or approach to develop new systems with information risk management policies. Certain system models or system development methodologies and approaches must be formally provided to remedy this deficiency. This deficiency in current information risk management tools is the motivation for this thesis. In conjunction with the concepts and ideas from the abovementioned tools and three existing methodologies, a new system development approach and methodology for information risk management will be introduced in this thesis. An overview of the system development model is as follows.

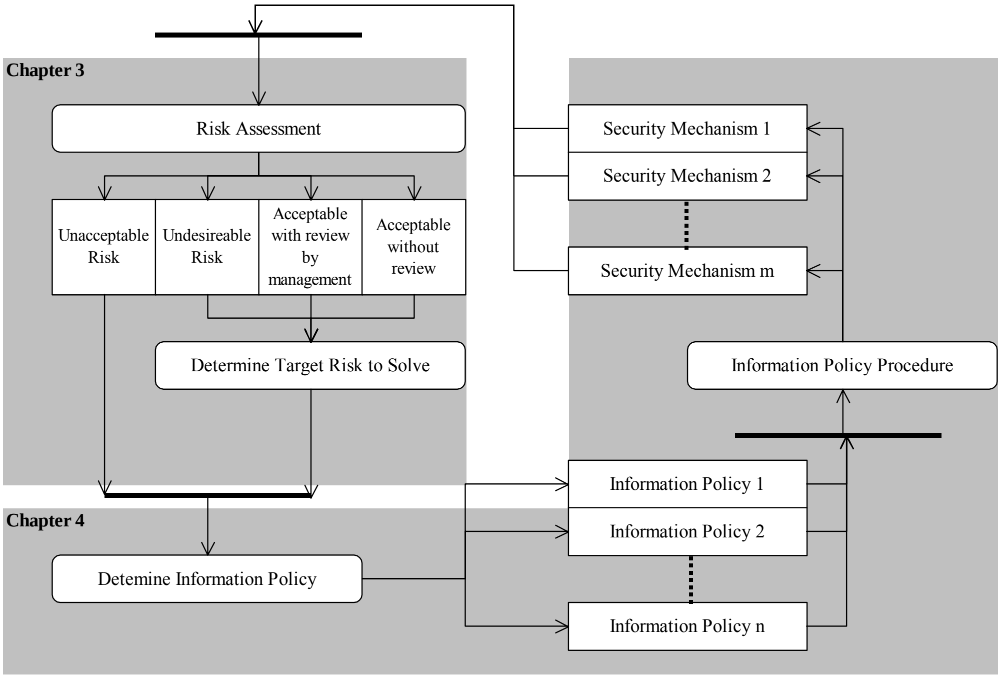


Figure 2: Overview of Information Risk Management Model

Risk management is used to identify risks involved in security breaches and prioritize security solutions for the risks in any field. This will be described in detail in chapter 3. Information policy consists of the rules developed for the target system in order to reduce or prevent the risk. Security mechanism is the procedures used to accomplish the information policy. Security mechanisms will be invoked in the subject system. This process will be shown in chapter 4. In this thesis, some examples following this cycle will be shown in detail.

2-3. Systems Modeling

Modeling is a powerful technique to develop a system effectively and efficiently, and it offers many benefits to any participant of system development such as stakeholders, system developers, and users. According to Mark Austin's lecture notes for the University of Maryland systems engineering program[34], the benefit of using modeling are as follows.

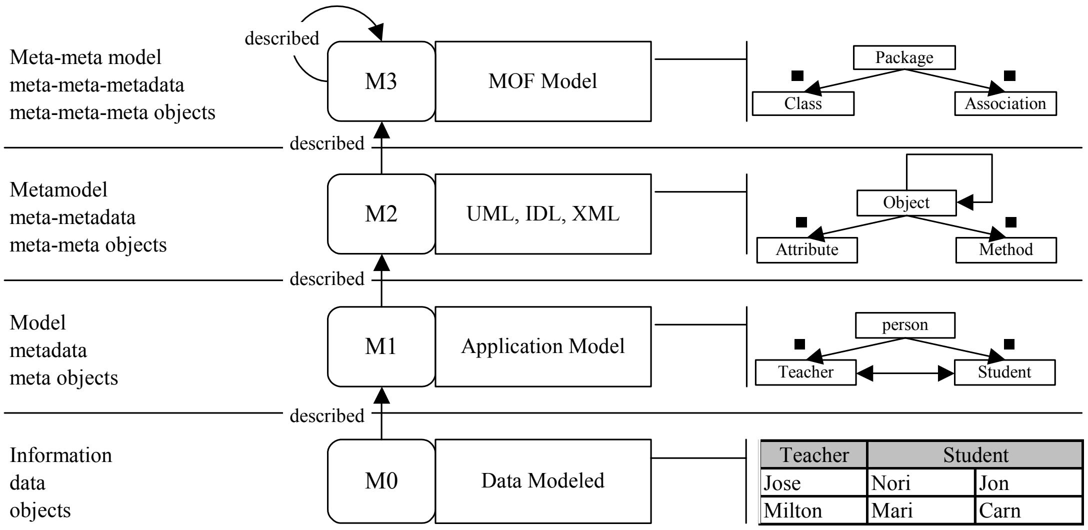
- Assistance in Communication
- Assistance in Coordination of Activities
- Ease of Manipulation
- Efficient Trial-and-Error Experiments
- Reduction of Development Time
- Reduced Cost
- Risk Management

[34] ENSE 622 Lecture notes, Mark Austin, University of Maryland, 2004, Page 78 – 79

The system model provides experiments, rules, and useful information for designing, developing, and implementing the system. By applying the model, cost, time, and risk will be dramatically reduced. For this reason, the modeling process will be the main concern regarding information risk management in systems engineering.

2-3-1. Meta Model

What is the system model? How is it developed? Meta Model Architecture will be introduced in order to answer these questions. Meta modeling is generally described using a four-layer architecture. These layers represent different levels of data and metadata. Figure 1 shows an example of the layers used for modeling a target system.



Teacher	Student	
Jose	Nori	Jon
Milton	Mari	Carn

Figure 3: Meta Model Architecture[35]

[35] Using Metamodels to Promote Data Integration in an e-Government Application Scenario, Adriana Figueiredo, Aqueo Kamada, IEEE, 2003, Page 4

The four layers are:

- Information: The information layer refers to actual instances of information. For example, there are two instances of data representing “Jose” and “Milton” as teachers, and four instances of data representing “Nori”, “Jon”, “Mari”, and “Carn”.
- Model: The model layer (also known as the metadata layer) defines the information layer, describing the format and semantics of the objects, and the relationship among the objects. For example, the metadata specifies the “Person” class, and its instances, which are “Teacher” and “Student”. Relationships between objects are defined such as “Teach (Teacher → Student)” and “Learn (Student → Teacher)”.
- Metamodel: The metamodel layer (also known as the meta-metadata layer) defines the model layer, describing the structure and semantics of the model. For example, the meta-metadata specifies a system design that describes its structure and data-flow. The metamodel can also be thought of as a modeling language used to describe different kinds of systems.
- Meta-metamodel: The meta-metamodel layer defines the metamodel layer, describing the structure and semantics of the meta-metadata. It is the modeling language that is used to define different kinds of metamodels. Typically, the metametamodel is defined by the system that supports the metamodeling environment.

This thesis will focus on developing the M1 layer, which is a model involving meta-data and meta-objects to develop the system model targeting secured systems with information policy to prevent threats of security breach.

2-3-2. UML

UML is the one of standard metadata models and modeling language. A wide variety of object-modeling methodologies were developed during the 1980s, such as OMT, Booch, and OOSE. Although these modeling methodologies were similar, the language and notations used to represent them were different. Moreover, the visual modeling tools that implemented these modeling methodologies were not interoperable, and UML quickly become standard modeling language; it lets the modeling take higher level of abstraction so that the model can be updated easily and re-used for other systems. UML is a standardized modeling language consisting of an integrated set of diagrams, developed to help system and software developers accomplish the following tasks[36]:

- Specification
- Visualization
- Architecture design
- Construction
- Simulation and Testing
- Documentation

UML was originally developed with the idea of promoting communication and productivity among the developers of object-oriented systems. Currently, all of UML is updated for UML2.0[37]. UML2.0 has resolved many of the shortcomings in the previous version UML, such as lack of diagram interchange capability, inadequate semantics

[36] Excerpted UML 2 for Dummies, Michael Jesse Chonoles, James A. Schardt, July 2, 2003, Page 14,15

[37] UML 2.0, The Current Official Version, http://www.uml.org/#Articles

definition and alignment with MOF. UML2.0 has the following features[38]:

- Improved semantics in the class diagrams
- Support for large systems and business modeling
- Diagram interchange capabilities
- Aligned with MOF (Meta Object Facility) and MDA (Model Driven Architecture)

UML2.0 architecture[39] is as follows.

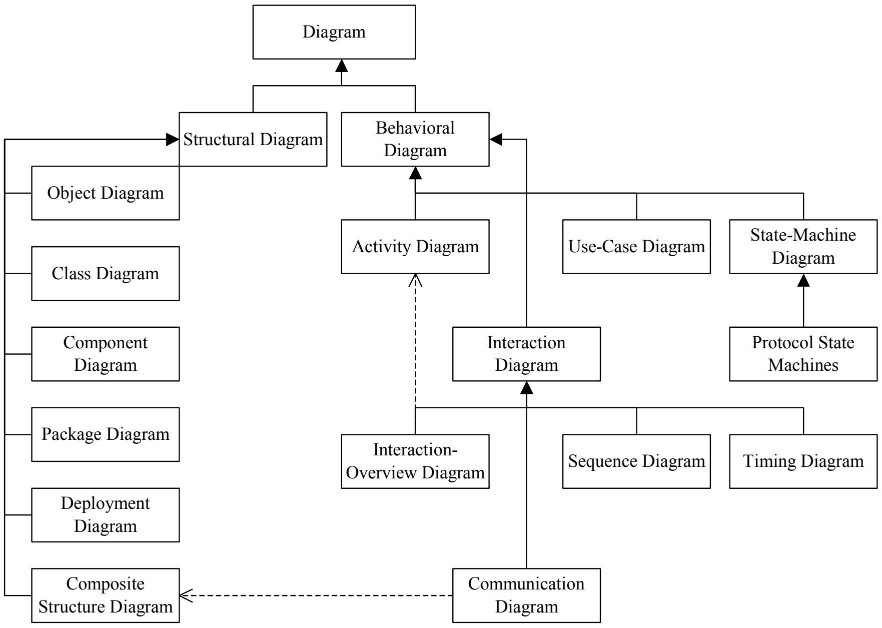


Figure 4: UML 2.0 Architecture

UML 2.0 will be used since this meta-language is the most extensible and compatible with any system.

[38] Excerpted UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 10 – 12

[39] Excerpted UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 19

The system model development process flow using UML is presented as follows.

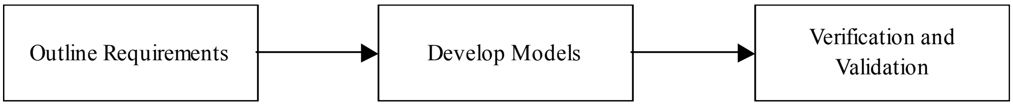


Figure 5: Process Flow to Develop the System Model

First, outline requirements and rules for the system to prevent security breach are described. Second, the system model with usage of UML is developed. UML is the most powerful meta-language to design a system model. The language is understandable, easy to handle, and re-useable for other similar system models. Finally, the system model should be verified. Many verification technologies have been presented recently. UPPALL is one of the powerful verification tools for a system. One scenario from the design will be selected, and it will be verified using UPPALL. Completing verification for the system model will not be performed since the purpose of this thesis is to introduce the system model development process concerning information risk management, not to complete the development of the system. Some sample designs and verifications of the particular scenario shown through this thesis will suffice. The focus here will be on analyzing current security breaches and risk assessment, and developing information policies for preventing unacceptable security breaches. Completing the system development will be taken into account for future work.

3. Risk Assessment using the Current Security Issues

Risk assessment is one of the main components of the information risk management model. In this chapter, common risk assessment concepts will be used for the model, and then improved to be suited for information risk management in this thesis. Finally, the risk level of current security breaches will be determined and security breaches involving unacceptable risk will be addressed; in addition, some suggestions for preventing security breaches will be presented.

3-1. Risk Assessment Methodology

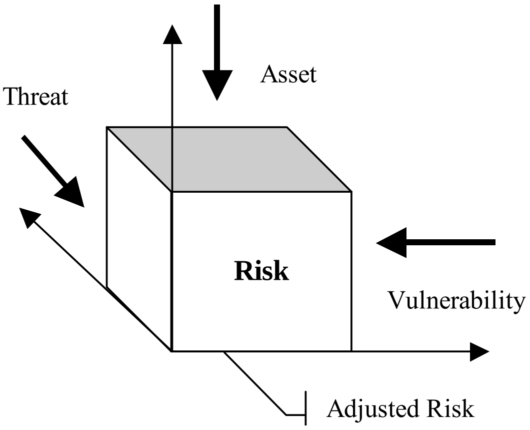


Figure 6: Information Risk Profile[40]

How is information risk levels measured for each security breach? How is the risk assessed? According to the "The Executive Guide to Information Security"[41], the risk

[40] Excerpted from The Executive Guide to Information Security, Mark Egan, Symantec Press, Nov 2004, figure 5-1, Page 109

[41] The Executive Guide to Information Security, Mark Egan, Symantec Press, Nov 2004, Page 104 – 110

level is the set of assets in the organization and system, threat to the asset, and organization or system vulnerability. In this book, the risk level is assessed using the summary matrix involving a brief description of risk assessment measurements, which are the asset, threats, and vulnerability. The assessment is deployed for each set of the three risk assessment measurements. However, it is not a quantitative method; this method results in imprecise assessment. The method should be more quantitative and provide more precise assessment so as to apply the information risk model in systems engineering. As the figure on the previous page shows, each risk assessment measurement may have certain assessment value determined by the system developer and stakeholder; the risk is a function of assets, threats, and vulnerabilities. The threat of the security problem, the vulnerability involved in the system and organization, and the assets in the system and organization should be assessed as opposed to only described. The risk assessment process should be analytical since the information risk management must be a systematic process by which an organization identifies, reduces, and controls its potential risks and losses. At this point, the definition[42] of each risk measurement may be shown in the following table.

Threat	The capacity and intention of an adversary to undertake actions that is detrimental to an organization's interests. It cannot be controlled by the owner or user. The threat may be encouraged by vulnerability in an asset or discouraged by an owner's countermeasures.
Vulnerability	Any weakness in an asset or countermeasure that can be exploited by an adversary or competitor to cause damage to an organization's interests.
Asset	Anything of value (people, information, hardware, software, facilities, reputation, activities, and operations). The more critical the asset is to an organization accomplishing its mission, the greater the effect of its damage or destruction.

Table 4: Terms for Risk Measurement

[42] *National Infrastructure Protection Center*; Risk Management: An Essential Guide to Protecting Critical Assets; November 2002, Page 8 – 9

A new risk assessment process to suit information risk management in systems engineering will be shown in this thesis. Each risk assessment measurement is determined as follows:

- *The asset assessment*: The magnitude and effect of the potential loss in systems and organization
  (What is the likely effect if an identified asset when it is lost or harmed by one of the identified unwanted events?)

- *The threat assessment*: The probability of loss in systems and organization
  (How likely is it that an adversary can and will attack those identified assets?)

- *The vulnerability assessment*: The magnitude of the exploitable situations.
  (What are the most likely vulnerabilities that the adversary will use to target the identified assets?)

Developers, including systems engineers, analysts, and security managers should identify and evaluate the value for each risk assessment measurement. The magnitude is measured by verbal ratings such as high, middle, and low. The risk assessment steps are shown here:

Step 1. Asset Assessment:

Identify and focus confidential information involved in organization and system process. The assets include customer information, business and technology know-how, government secret information, and home security information. For each individual asset, identify undesirable events and the effect that the loss, damage, or destruction of that asset would have on the organization and system process.

Step 2. Threat Assessment:

Focus on the adversaries or events that can affect the identified assets. Common types of adversaries include criminals, business competitors, hackers, and foreign intelligence services. Certain natural disasters and accidents are taken into account even though they are not intentional.

Step 3. Vulnerability Assessment:

Identify and characterize vulnerabilities related to specific assets or undesirable events. Look for exploitable situations created by lack of adequate security, personal behavior, lack of information management, maltreated privilege documents, and insufficient security procedures. Typical vulnerabilities include the absence of guards, poor access controls, lack of stringent process and software, and unscreened visitors in secure areas.

Step 4. Risk Assessment:

Combine and evaluate the former assessments in order to give a complete picture of the risk to an asset of confidential information in organization and system process. The risk is assessed in terms of how each of these ratings (high, middle, low) interacts to arrive at a level of risk for each asset. The terms used in the rating may be imprecise. In situations where more precision is desired, a numerical rating on a 1 to 10 scale can be used. The numerical scale is easier for systems analysts and developers to replicate and combine in an assessment with other scales.

How each risk assessment is evaluated has already been presented. For the next procedure, risk level for an asset will be required. How can the risk level be assessed? For this question, the DOD[43] (Department of Defense) standard definitions[44] for the probability that an undesired event will occur and the severity level are used since the definitions have been adapted for many companies; moreover, the definition is the United State government standard. It may be required for any government information systems. The definition is shown in the following table.

Probability Level	Specific Event
A: Frequent	Likely to occur frequently
B: Probable	Will occur several times
C: Occasional	Likely to occur sometime
D: Remote	Unlikely but possible to occur
E: Improbable	So unlikely it can be assumed occurrence may not be experienced

Table 5: Probability Levels of an Undesired Event

Severity Level	Characteristics
I: Catastrophic	Death, system loss or severe environment damage
II: Critical	Severe injury, severe occupational illness, major system or environment damage
III: Marginal	Minor injury, minor occupational illness, or minor system or environmental damage
IV: Negligible	Less than minor injury, occupational illness, or less than minor system or environmental damage

Table 6: Severity Levels of Undesired Event Consequences

This process results in a matrix that pairs and ranks the most important assets with the threat scenarios most likely to occur. The risk level will be determined by the following matrix on the next page.

[43] Department of Defense home page, http://www.defenselink.mil/

[44] Combating Terrorism Threat and Risk Assessment Can Help Prioritize and Target Program Investments, GAO. April 1998, Page 7

Probability of occurrence	Severity level			
	I. Catastrophic	II. Critical	III. Marginal	IV. Negligible
A. Frequent	I A	II A	III A	IV A
B. Probable	I B	II B	III B	IV B
C. Occasional	I C	II C	III C	IV C
D. Remote	I D	II D	III D	IV D
E. Improbable	I E	II E	III E	IV E

Risk Level 1: Unacceptable (reduce risk through countermeasures)
Risk Level 2: Undesirable (management decision required)
Risk Level 3: Acceptable with review by management
Risk Level 4: Acceptable without review

Table 7: Risk Assessment Matrix[45]

This is the risk assessment definition of DOD widely used for many companies. The definition should be modified to suit the information risk assessment. The probability of occurrence is useful for the information risk assessment as well. However, the definition of severity level should be modified as follows since the information risk assessment deals only with the information risk such as leaking confidential information and privilege documents, and misuse of technical know-how and home security information.

Security Level	Characteristics
I: Catastrophic	Enormous number of secret information, severe potential to misuse and result in severe environment damage
II: Critical	Secret information for particular area and fields, high potential to misuse for only limited area, major system or environment damage
III: Marginal	Confidential information, low potential to misuse, mi minor system or environmental damage
IV: Negligible	Less than minor and unclassified information injury, less than minor system or environmental damage

Table 8: Security Levels of Undesired Event for an Asset in Information Risk Assessment

[45] Combating Terrorism Threat and Risk Assessment Can Help Prioritize and Target Program Investments, GAO. April 1998, Page 8

To asset information risk management, security level will be used instead of severity level. The risk assessment matrix can be used for the information risk assessment since it has been accepted by many companies; moreover, the matrix is still useful for the information risk assessment.

The probability of the unwanted event occurrence clearly increases with increasing threat and increasing vulnerability. In this thesis, the simple formula for the probability over a given time interval is:

Threat * Vulnerability

Each assessment measurement of the threat and vulnerability is shown by a numerical rating (1 to 10). The threat and vulnerability rating will be shown in the section of each assessment. The following matrix is used to determine the probability of the unwanted event occurrence with the numerical rating.

The probability of occurrence	Numerical rating for threat and vulnerability
A. Frequent	81 or more
B. Probable	61 – 80
C. Occasional	41 – 60
D. Remote	21 – 40
E. Improbable	20 or less

Table 9: Rating for the Probability of Occurrence

A security level rating corresponds to an asset raging for the confidential information in organization and system process based on the following matrix.

Security Level	Numerical rating for asset
I: Catastrophic	10
II: Critical	7 – 9
III: Marginal	4 – 6
IV: Negligible	1 – 3

Table 10: Rating for the Security Level

Step 5. Identification of Countermeasure Options:

Provide the risk acceptance authority with countermeasures, or group of countermeasures, which will lower the overall risk to the asset at an acceptable level. By evaluating the effectiveness of possible countermeasures against specific adversaries, the systems engineer can determine the most cost-effective options. In presenting countermeasures to the risk acceptance authority, the systems engineer or security analyst should provide at least two countermeasure packages as options. Each option should also include the expected costs and amount of risk that the decision-maker would accept by selecting a particular option. The graphical representation for the information risk assessment is shown as follows.

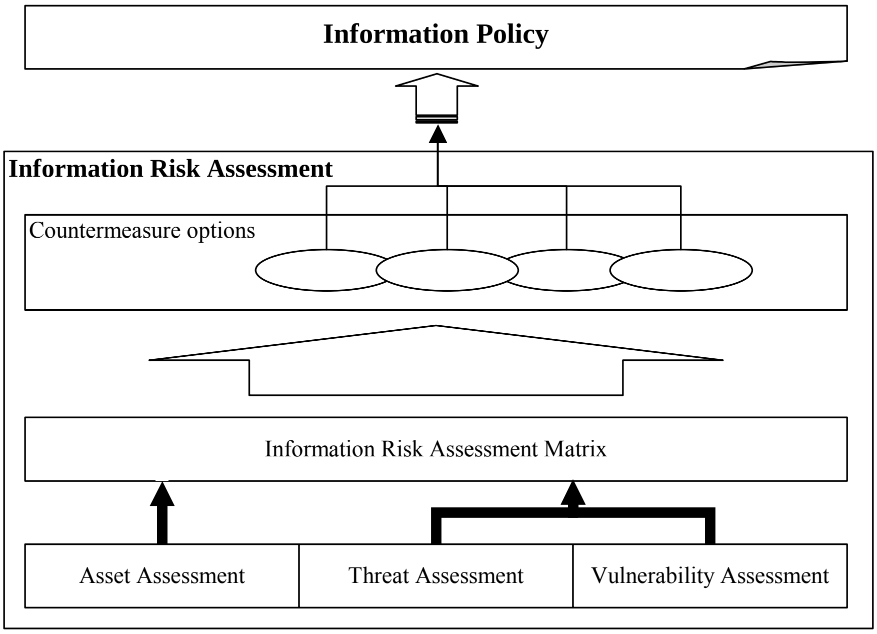


Figure 7: Structure of Workflow for Information Policy Setting

In this report, information policy will be used for the security requirement of the case study. The information policy will be formatted based on assessment of asset, threat, and vulnerability in the organization and system process regarding confidential information. Many information policies can be created. However, only information policies relating to the system development will be focused in this thesis. The information policies relating to the organization will not be the focus of this thesis since the information policy for the system is the main target of this thesis.

3-2. Security Risk Assessment

To acquire crucial security requirements, 20 security breaches involving information risk for the last 3 years are assessed using the aforementioned risk assessment methodology. A summary of the 20 selected recent security breaches is shown in Appendix 1[46]. All the security breaches are related to the leaking and misuse of confidential information issues.

Security breach problems are picked up from the news, information technology security issues, and governmental sites on the Internet. Security breach problems can be categorized by main threats and the magnitude of information asset. The main threats are outsider, insider, and unintentional misuse. The magnitudes are caution level, limited level (leak of less than 5,000 customers' information), medium level (leak of 5,000 – 50,000 customers' information, and large level (leak of more than 50,000 customers' information). Two security breach problems are deployed in the main threat type and magnitude of information asset as follow.

	Possible Caution	Limited or less 5,000	Medium or 5,000 - 50,000	Large or more 50,000
Outsider	[SB-04], [SB-15]	[SB-12], [SB-14]	[SB-02], [SB-03]	[SB-06], [SB-11]*, [SB-16]
Insider	---	[SB-01], [SB-08]	[SB-07], [SB-10]	[SB-11]*, [SB-13], [SB-20]
Unintentional or design fault	[SB-05], [SB-09]	[SB-17], [SB-18]	[SB-19]	---

*[SB-11] caused with both of outsider and insider

Table 11: Category Table for Security Breaches

Caution Level: A precaution for information loss.
Limited Level: Involves only information risk in limited businesses and local areas.
Medium Level: Involves medium scale information risk in higher populated areas or cities.
Large Level: Involves large-scale information risk in nations or worldwide.

[46] Summary of the 20 selected recent security breach, Annex 1 (Summary Security Prob) ver 2.0.doc

There is no caution level of security breach by insiders; furthermore, large-scale information risk does not occur unintentionally. A large-scale information risk occurs by only an intentional insider or outsider attacks.

Each assessment measurement is represented by the numerical value 1 to 10. The rating method may vary among different companies. It is based on discipline, historic data, and security managers' or stakeholders' decisions. In this report, a sample rating method is shown for each assessment section. The higher numbers are more necessary as security requirements.

Low			Medium			High			Severe
1	2	3	4	5	6	7	8	9	10

Table 12: Each Assessment Rating

Asset Assessment

The asset assessment is followed through the steps presented in the previous section. A rating for asset assessment utilizes the aforementioned magnitude of information assets. The asset assessment is shown in the following table. Limited, medium, and large level will be low, medium, and high or severe rating. Caution level rating cannot be identified since its security breach does not occur. The rating may be limited, medium or large.

Case No.	Day	Location	Assets	Undesirable events	Assess.
[SB-1] Boeing Co. privileged documents	Jun, 2004	Boeing Co. USA	- Company credit, reputation	- Loss of confidence with government contracts due to unfair act to the competition. - Occurrence of moral hazard in the company due to neglecting market rule.	Low 3
[SB-2] Hacker penetrates T-mobile systems	Jan, 2005	T-mobile systems, USA	- Customer Data	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	Medium 6
[SB-3] Hacker posts credit card information	Dec, 1999	eUniverse Inc., USA	- Customer Data	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	Medium 6
[SB-4] Identity Thieves can lurk at Wi-Fi spots	Feb, 2005	Hotspot, USA	- Customer itself	- Loss of confidentiality due to unauthorized outsider access - Loss of market confidentiality due to unsecured wireless connection	N/A
[SB-5] Intuit plugs leaks to double click	Mar, 2000	Web sites, USA	- Private information in cookies	- Loss of confidentiality due to poor design of web site.	N/A
[SB-6] More than 145,000 people face identity theft threat	Feb, 2005	Los Angeles, USA	- Personal Information	- Loss of personal asset and private information due to unawareness	High 8
[SB-07] Leaked 24,632 customers' information	Feb, 2005	NTT Docomo, Japan	- Customer Data	- Loss of confidentiality due to unauthorized insider access - Loss of existing customer due to poor control in secured room	Medium 6
[SB-08] Raytheon Company published employment policy	Feb, 1999	Raytheon, USA	- Privileged Information	- Loss of confidentiality due to spread of the company's bad reputation - Deterioration of ability to compete due to leak of company's secret information	Low 2
[SB-9] Security Breach at Buy.com	Oct, 2000	Buy.com, USA	- Customer Data	- Loss of confidentiality due to poor web design	N/A
[SB-10] Medical privacy breach in Univ. Michigan medical system	Feb, 1999	Detroit, USA	- Customer Data	- Loss of confidentiality due to unauthorized insider access - Loss of existing customers due to poor database server control	Medium 6
[SB-11] Leaked over 100,0000 customers' information of the store in Rakuten Internet market.	April, 2005	Mainichi News in Japan	- Customer Data - Virtual store tenant information	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers (buyers). Resulted in loss of virtual store tenants.	Severe 10

[SB-12] Leaked the nuclear plant security information through “Winiy” in the Internet.	February, 2005	Mainichi News in Japan	- Privileged documents (published information)	- Loss of home security information - Information could be utilized by terrorists (However, all documents are published through other media already and are not secret documents)	Low 3
[SB-13] Lost a computer back-up tape holding 200,000 clients’ account data of Bank of America.	March 3, 2005	Enterprise IT Plante.Com	- Customer Account data. - Computer back up data	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of bank clients - Decrease of bank client deposit	Severe 10
[SB-14] Leaked 5,000 personnel student information in an elementary school in Shizuoka, Japan	April 21, 2005	IT Hoken.Com	- Student information	- It could be used to commit crimes involving children - It could be exploited by a vice trader	Low 3
[SB-15] Stolen documents with personnel information from a business car of water works in Kanagawa, Japan	August 16, 2005	IT Hoken.Com	- Waterworks information - Resident information	- Loss of confidentiality due to employee carelessness - It could be exploited by a vice trader - It could be exploited by a thief	N/A
[SB-16] Leaked 61,876 members’ information in sophisticated hacker attack on Adecco web site.	June 27, 2005	IT Hoken.Com	- Member information	- Loss of confidentiality due to poorly designed web server, resulting in decreased number of registered members - It could be exploited for commercial use by a vice trader - Spam mail could be sent to members	High 7
[SB-17] Kitaguni bank accidentally issued other customers’ detailed account statement on ATM	August 4, 2005	IT Hoken.Com	- Bank account information	- Loss of confidentiality due to poor program implementation - It could be exploited by a thief	Low 2
[SB-18] Nagoya Toyota car dealership lost 138 personnel and 67 enterprise customers’ list.	June 6, 2005	IT Hoken.Com	- Customer list	- It could be exploited by a vice trader - It could be exploited by a rival shop	Low 2
[SB-19] Leaked member information by e-mail operation error	July 9, 2004	IT Hoken.Com,	- Member information	- It could be exploited by a vice trader	Medium 4

SB-20] Softbank leak extortionist was caught but not imprisoned	July 10, 2004	The Japan Times	Customer account information	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers due to poor customer information control - It could be exploited by a vice trader	High 9

Table 13: Asset Assessment Worksheet

Threat Assessment

For the next step, the threat assessment is shown as follows. The threat is considered in terms of adversaries. It must be determined if an adversary has the intent and capability to cause an unwanted event, and its history of successful attacks against the assets also must be reviewed in order to assess whether the adversary poses a threat. A higher rating for threat assessment should be delivered to a major adversary, an ultimately tricky attack, or an easier target in a current information security affair. The weight of these factors will be determined based on a survey of information leak problems published on the IT Hoken.com[47]. The followings are rules for weighing factors.

- Weight is determined by a frequency of item in a factor.
- Weight range is 1 to 10. Max weight is delivered if the same item causes all cases.
- "Other" item weight is 1 since this item is not significant.

[47] Hoken.com homepage, http://www.it-hoken.com/cat_aeieoieioeie.html

For instance, adversary weight has three items: insider, outsider, and unintentional misuse. The frequency of insider in a factor is 149. The weight for this item is determined by the following equation.

Adversary Weight (Insider) =
Frequency of insider (149)*9 / Total number of cases (289) + 1 = 5.6

Using the same formula, outsider weight will be 3.5 and unintentional misuse weight will be 2.9. A weight for other factors is also determined with the same fashion. Thus, the weight for all items of three factors is shown in the rating table on the following page. The overall rating for threats is calculated by the weights of the three items. The following equation may be suitable to determine the overall rating. The rating range must be 1 to 10.

Threat Rating =
Adversary Weight * Trick Weight * Target Weight * 10 / Max Total Weight (36.9)

The threat rating of each security breach problem is determined using the rating table.

Adversary

Item	# of Case	Weight
Insider	149	5.6
Outsider	80	3.5
Unintentional	60	2.9
Total	289	

Target

Item	# of Case	Weight
Credit	42	2.3
Bank	38	2.2
Online service	35	2.1
Communication	35	2.1
Government agency	22	1.7
Medical Institution	20	1.6
Lifeline	20	1.6
School	17	1.5
Travel agency	15	1.5
Brokerage firm	13	1.4
Insurance	13	1.4
Car shop	9	1.3
Department Store	4	1.1
Others	6	1.0
Total	289	

Trick

Item	# of Case	Weight
Memory device	59	2.8
Web site	52	2.6
Documents	48	2.5
Wrong Operation	32	2.0
Stolen device	25	1.8
Stolen computer	21	1.7
System Error	19	1.6
Malicious program	15	1.5
System Implementation	14	1.4
Others	4	1.0
Total	289	

Max Total Weight	36.9
Rating (Insider / Memory device / Bank)	9

Total Weight = Adversary weight*Trick weight*Target weight
Rating = Total Weight * 10 / Max Total Weight

*Information Leaking Problems List, IT Hoken.com, http://www.it-hoken.com/cat_aeieoieioeie.html

Table 14: Rating Table for Threat Assessment

Threat rating with an insider (adversary), usage of memory device (trick), and a bank (target) is 9 (5.6*2.8*2.2*10 / 36.9). The threat rating of each security breach is as follows.

Case No.	Undesirable events	Adversary	Intent	Capability	History	Threat
[SB-1]	- Loss of confidence with government contracts due to unfair act to the competition. - Occurrence of moral hazard in the company due to neglecting market rule.	Employee	Yes	Yes	Infrequent	Medium 4
[SB-2]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	Outsider	Yes	Yes	Infrequent	Medium 4

[SB-3]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	Outsider	Yes	Yes	Infrequent	Medium 6
[SB-4]	- Loss of confidentiality due to unauthorized outsider access - Loss of market confidentiality due to unsecured wireless connection	Thief / Outsider	Yes	Yes	No	Medium 4
[SB-5]	- Loss of confidentiality due to poor design of web site.	Poor design web site / Advertise	No	Yes	No	Low 3
[SB-6]	- Loss of personal asset and private information due to unawareness	Fraudulent web site	Yes	No	Intermittent	Medium 6
[SB-7]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customer due to poor control in secured room	Contract Employee	Yes	Yes	Infrequent	High 9
[SB-8]	- Loss of confidentiality due to spread of the company's bad reputation - Deterioration of ability to compete due to leak of company's secret information	Employee	No	No	Intermittent	Low 2
[SB-9]	- Loss of confidentiality due to poor web design	Unchecked database design	No	Yes	Infrequent	Low 3
[SB-10]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customers due to poor database server control	Insider	Yes	Yes	Infrequent	Medium 5
[SB-11]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers (buyers). Resulted in loss of virtual store tenants.	Ex-employee	Yes	Yes	Infrequent	High 8
[SB-12]	- Loss of home security information - Information could be utilized by terrorists (However, all documents are published through other media already and are not secret documents)	Employee	No	Yes	Infrequent	Medium 4
[SB-13]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of bank clients - Decrease of bank client deposit	Outsider or Insider	Yes	Yes	Infrequent	Medium 6
[SB-14]	- It could be used to commit crimes involving children - It could be exploited by a vice trader	Outsider	Yes	No	Infrequent	Low 2
[SB-15]	- Loss of confidentiality due to employee carelessness - It could be exploited by a vice trader - It could be exploited by a thief	Thief	Yes	No	Infrequent	Medium 4
[SB-16]	- Loss of confidentiality due to poorly designed web server, resulting in decreased number of registered members - It could be exploited for commercial use by a vice trader - Spam mail could be sent to members	Outsider	Yes	Yes	Infrequent	Medium 6
[SB-17]	- Loss of confidentiality due to poor program implementation - It could be exploited by a thief	Poor implementati	No	Yes	Infrequent	Low 3

		on				
[SB-18]	- It could be exploited by a vice trader - It could be exploited by a rival shop	Thief	Yes	No	Infrequent	Low 3
[SB-19]	- It could be exploited by a vice trader	Poor operation	No	No	Infrequent	Low 2
[SB-20]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers due to poor customer information control - It could be exploited by a vice trader	Ex-employee	Yes	Yes	Infrequent	High 8

Table 15: Threat Assessment Worksheet

The security problems [SB-07], [SB-11] and [SB-20] involve greater threats than others since it is due to malicious insiders, which have recently become the highest threat. In Japan, 80% of information leak problems are caused by an insider such as ex-employee, outsourcing, and entrusted trader[48].

For the next step, the vulnerability assessment is shown as follows. Vulnerability is a weakness in the system. To determine its rating is difficult since the rating requires detailed information and analysis for a target system, which are not provided in articles and the news. In this report, the rating will be determined as follows. It is defined that a vulnerability rating is dependent on how much existing countermeasures in a security breach problem satisfies the 10 suggestions in section 3.3. The vulnerability rating is increased by 1 for an incomplete suggestion. For example, in the case of [SB-17], 3 suggestions are not considered properly; thus, a vulnerability rating of this case will be 3.0. Other ratings of security breaches before revision are shown in a table on the next page. A maximum and minimum rating is 7.5 and 1.5 before the revision. It is desirable

[48] Inner Guard Master, IGM homepage, http://innerguardmaster.jp/

that the rating is converted into 1 to 10 using the convert table shown as follows. As a result, a 1 to 10 rating will be assigned to the security breach problems.

	1: Correct identification and access control	2: Apply economy mechanism	3: Consider storage device	4: Separation of Information Privilege	5: Least Privilege	6: Accountability	7: Putting the above points to use in design phase	8: Awareness of users, employees, and organizations	9: Create penalties that overweight the hacker's benefits	10: Inspect documents leaving the premises	Rating before revision
[SB-01]		△			△			×	×	×	4.0
[SB-02]	△			×	×	×	△				4.0
[SB-03]	△	△		×		×	△		×		4.5
[SB-04]		△				×		×			2.5
[SB-05]					△		×	△			2.0
[SB-06]	△					×		×	×		3.5
[SB-07]		×	×	×	×	×		×	×	△	7.5
[SB-08]								×	×		2.0
[SB-09]					×		×				2.0
[SB-10]	△	△	×	×		×	×	×	×		7.0
[SB-11]	△	×		×		×	×	×	×	×	7.5
[SB-12]			×					△			1.5
[SB-13]			△					×	×		2.5
[SB-14]			×	×				×	△		3.5
[SB-15]								×		×	2.0
[SB-16]	×	×			×	×	×	×	×		7.0
[SB-17]						×	×	×			3.0
[SB-18]								×		×	2.0
[SB-19]				△				×			1.5
[SB-20]		×	×	×		×	×	×	×		7.0

×: 1 up into vulnerability rating

△: 0.5 up into vulnerability rating

Convert Table for 1 to 10 rating Interval for revision: 0.67 = (7.5 - 1.5) / (10 - 1)

1 to 10 rating	1	2	3	4	5	6	7	8	9	10
Rating before revision	1.5 -	2.17 -	2.83 -	3.5 -	4.17 -	4.83 -	5.5 -	6.17 -	6.83 -	7.50

Table 16: Rating Table for Vulnerability Assessment

Certain existing countermeasures are obtained as available in the following table.

Case No.	Undesirable events	Vulnerabilities	Existing Countermeasures	Vul.
[SB-1]	- Loss of confidence with government contracts due to unfair act to the competition. - Occurrence of moral hazard in the company due to neglecting market rule.	- No penalty regulation against competition rule - High competition - Low employee moral	- None	Medium 4

[SB-2]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	- Absence of security for U.S. secret service e-mail - The e-mail contained too much private information - Low consideration of the importance of customer information	- Standard secured system (sys.)	Medium 4
[SB-3]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	- Absence of security for CDUniverse web server	- Standard secured system (sys.)	Medium 5
[SB-4]	- Loss of confidentiality due to unauthorized outsider access - Loss of market confidentiality due to unsecured wireless connection	- Wireless connection caused lower security - Absence of customer literacy regarding internet security	- Access permitted by user name and password (sys.)	Low 2
[SB-5]	- Loss of confidentiality due to poor design of web site.	- Poor website design - Absence of proper web design technique in terms of security weakness - There are no criteria for developing any website obtained advertisements.	- Some warnings regarding the problems are available on the internet. (org.) - Some web site developers aid in finding the problem. (org.)	Low 1
[SB-6]	- Loss of personal asset and private information due to unawareness	- Absence of internet user literacy regarding internet security - Unclear use of users' information for the internet user	- Some warnings regarding use of user information provided may be available but not emphasized (org. & sys.)	Medium 4
[SB-7]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customer due to poor control in secured room	- Poor access control - Lack of stringent system review - Lack of analysis of access logs	- Screened visitors in secure areas (sys.) - Standard secured system (sys.)	Severe 10
[SB-8]	- Loss of confidentiality due to spread of the company's bad reputation - Deterioration of ability to compete due to leak of company's secret information	- No penalty regulation against the act - Low employee moral - Low royalty for the organization	None	Low 1
[SB-9]	- Loss of confidentiality due to poor web design	- Poor web design - Lack of stringent service contract review	None	Low 1
[SB-10]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customers due to poor database server control	- Unscreened visitors in secure areas - Poor access control - Poor password control - Absence of employee literacy for computer security	- Access permitted by username and password (sys.)	High 9
[SB-11]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers	- Lack of stringent system review - Low employee moral	- Access permitted by username and password (sys.)	Severe 10

	(buyers). Resulted in loss of virtual store tenants.	- Poor employee information access control - Lack of concern for the importance of customer information - Lack of analysis of access logs		
[SB-12]	- Loss of home security information - Information could be utilized by terrorists (However, all documents are published through other media already and are not secret documents)	- Lack of employee awareness - Lack of employee information and computer literacy	- None	Low 1
[SB-13]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of bank clients - Decrease of bank client deposit	- Poor back up data control - Lack of stringent system review - Poor stored data access control in the system	- Encrypted back up data (sys.) - Required access code for the back data (sys.)	Low 2
[SB-14]	- It could be used to commit crimes involving children - It could be exploited by a vice trader	- Poor control of computer disposal - Lack of knowledge about computers	- None	Medium 4
[SB-15]	- Loss of confidentiality due to employee carelessness - It could be exploited by a vice trader - It could be exploited by a thief	- Lack of awareness of employees	- None	Low 1
[SB-16]	- Loss of confidentiality due to poorly designed web server, resulting in decreased number of registered members - It could be exploited for commercial use by a vice trader - Spam mail could be sent to members	- Poor web system design - Poor access control - Lack of stringent system review - Lack of analysis of access logs - Lack of awareness of employees	- Privileged information (sys.) - Access permitted by username and password (sys.)	Severe 10
[SB-17]	- Loss of confidentiality due to poor program implementation - It could be exploited by a thief	- Poor program implementation	- None	Low 3
[SB-18]	- It could be exploited by a vice trader - It could be exploited by a rival shop	- Lack of awareness of employees - Poorly controlled privileged documents	- None	Low 1
[SB-19]	- It could be exploited by a vice trader	- Lack of employee information and computer literacy - Lack of awareness of employees	- None	Low 1
[SB-20]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers due to poor customer information control	- Lack of stringent system review - Low employee moral - Poor employee information access control	- Access permitted by username and password (sys.)	High 9

	- It could be exploited by a vice trader	- Lack of concern for the importance of customer information - Lack of analysis of access logs		

Table 17: Vulnerability Assessment Worksheet

Higher vulnerability is caused by poor access control, poor web service design, low user literacy regarding Internet security, lack of analysis of event log and lack of documents privilege.

For the final step, the previous assessments are assembled so as to determine the risk for each security problem with the use of the abovementioned matrix[49]. The information risk assessment is as follows.

Case No.	Undesirable events	Asset	Threat	Vulnerability	Countermeasure options[50]	Risk
[SB-1]	- Loss of confidence with government contracts due to unfair act to the competition. - Occurrence of moral hazard in the company due to neglecting market rule.	Low 3	Medium 4	Medium 4	- Enforced agreement in order to have fair business competition (org.) - Create a penalty that outweighs the benefit of the documents (org.) - Raised employee business moral (org.)	Risk Level 4
		Negligible	Improbable 16			
[SB-2]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to unsecured server control	Medium 6	Medium 4	Medium 4	- Improve accountability in order to trace any hacker's action (sys.) - Tightly constrain user privileges (sys.) - Inform the customers of any accident (org.)	Risk Level 3
		Marginal	Improbable 16			
[SB-3]	- Loss of confidentiality due to unauthorized outsider access - Loss of existing customers due to	Medium 6	Medium 6	Medium 5	- Improve accountability in order to trace any hacker's action (sys.) - Tightly constrain user privileges (sys.)	Risk Level 3

[49] Table 4: Risk Assessment Matrix, Page 16 in this text.

[50] "(sys.)" means a countermeasure for systems, and "(org.)" means a countermeasure for organization or employees.

	customers due to unsecured server control	Marginal	Remote 30		- Inform the customers of any accident (org.) - Regulate higher penalty than hacking benefit (org.)	
[SB-4]	- Loss of confidentiality due to unauthorized outsider access - Loss of market confidentiality due to unsecured wireless connection	N/A	Medium 4	Low 2	- Warning to input credit card number, its password and any private information through the wireless access (org.) - Encrypt any transaction (sys.) - Do not keep access connection while not in use (org.)	Risk Level 3 or 4
			Improbable 8			
[SB-5]	- Loss of confidentiality due to poor design of web site.	N/A	Low 3	Low 1	- Any web designer must understand how to prevent this problem (org.) - Web browser or web developer aid software should obtain something to fix the problem automatically (sys.)	Risk Level 3 or 4
			Improbable 3			
[SB-6]	- Loss of personal asset and private information due to unawareness	High 8	Medium 6	Medium 4	- Awareness. Users should know how personnel information is used correctly. (org.) - Certain internet security inspection is required in order to censor illegal web sites. (sys.)	Risk Level 2
		Critical	Remote 24			
[SB-07]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customer due to poor control in secured room	Medium 6	High 9	Severe 10	- Censor not only contents but also the amount (sys.) - Check out any media brought out from secured area. (sys. & org.) - Create a penalty that outweighs the benefit of secret information. (org.)	Risk Level 1
		Marginal	Frequent 90			
[SB-08]	- Loss of confidentiality due to spread of the company's bad reputation - Deterioration of ability to compete due to leak of company's secret information	Low 2	Low 2	Low 1	- Awareness of its confidential organization information (org.) - Obligate certain penalty for the act (org.)	Risk Level 4
		Negligible	Improbable 2			
[SB-9]	- Loss of confidentiality due to poor web design	N/A	Low 3	Low 1	- Design customer service strictly and properly (sys.) - Classify confidential and non-confidential user information (sys.)	Risk Level 3 or 4
		N/A	Improbable 3			
[SB-10]	- Loss of confidentiality due to unauthorized insider access - Loss of existing customers due to poor database server control	Medium 6	Medium 5	High 9	- Improve accountability in order to trace any insider hacker's action (sys.) - Censor not only contents but also the amount (sys.) - Create secure room (sys. & org.)	Risk Level 2

		Marginal	Occasional 45		- Create secure room (sys. & org.) - Review any access control to confidential and non-confidential information (sys. & org.) - Create a penalty that outweighs the benefit of obtaining customer information (org.)	
[SB-11]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers (buyers). Resulted in loss of virtual store tenants.	Severe 10	High 8	Severe 10	- Censor not only contents but also the amount (sys.) - Create a penalty that outweighs the benefit of obtaining customer information (org.) - Create certain secure room (sys. & org.) - Improve accountability in order to trace any insider hacker's actions (sys.)	Risk Level 1
		Catastrophic	Probable 80			
[SB-12]	- Loss of home security information - Information could be utilized by terrorists (However, all documents are published through other media already and are not secret documents)	Low 3	Medium 4	Low 1	- Review any access control to confidential and non-confidential information (sys. & org.) - Inspection of any documents which are removed from government office (org.) - Provide exclusive computer to use outside of office (sys. & org.)	Risk Level 4
		Negligible	Improbable 4			
[SB-13]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of bank clients - Decrease of bank client deposit	Severe 10	Medium 6	Low 2	- Review any access control to privileged data including back up data (sys. & org.) - Inspection of any documents which are removed from the company (org.) - Use exclusive computer and authentication with biometric information (sys. & org.)	Risk Level 3
		Catastrophic	Improbable 12			
[SB-14]	- It could be used to commit crimes involving children - It could be exploited by a vice trader	Low 3	Low 2	Medium 4	- Awareness of its confidential organization information (org.) - Review computer disposal process - Provide exclusive computer without store device	Risk Level 4
		Negligible	Improbable 8			
[SB-15]	- Loss of confidentiality due to employee carelessness - It could be exploited by a vice trader - It could be exploited by a thief	N/A	Medium 4	Low 1	- Awareness of its confidential organization information (org.)	Risk Level 3 or 4
			Improbable 4			
[SB-16]	- Loss of confidentiality due to poorly designed web server, resulting in	High 7	Medium 6	Severe 10	- Censor not only contents but also the amount (sys.)	Risk Level

	decreased number of registered members - It could be exploited for commercial use by a vice trader - Spam mail could be sent to members	Critical	Occasional 60		- Create a penalty that outweighs the benefit of obtaining customer information (org.) - Tightly constrain user privileges (sys.) - Improve accountability in order to trace any insider hacker's actions (sys.)	1
[SB-17]	- Loss of confidentiality due to poor program implementation - It could be exploited by a thief	Low 2	Low 3	Low 3	- Provide sufficient implementation effort and time (sys. & org.)	Risk Level 4
		Negligible	Improbable 9			
[SB-18]	- It could be exploited by a vice trader - It could be exploited by a rival shop	Low 2	Low 3	Low 1	- Awareness of its confidential organization information (org.) - Review control of confidential information in a business process (sys. & org.)	Risk Level 4
		Negligible	Improbable 3			
[SB-19]	- It could be exploited by a vice trader	Medium 4	Low 2	Low 1	- Awareness of its confidential organization information (org.)	Risk Level 3
		Marginal	Improbable 2			
[SB-20]	- Loss of confidentiality due to ex-employee insider access and moral hazard - Loss of existing customers due to poor customer information control - It could be exploited by a vice trader	High 9	High 8	High 9	- Improve accountability in order to trace any insider hacker's action (sys.) - Censor not only contents but also the amount (sys.) - Create secure room (sys. & org.) - Review any access control to confidential and non-confidential information (sys. & org.) - Create a penalty that outweighs the benefit of obtaining customer information (org.)	Risk Level 1
		Critical	Probable 72			

Table 18: Risk Assessment and Countermeasure Options Worksheet

[SB-7], [SB-11], [SB-16], and [SB-20] involve unacceptable risks. The targets of the information policy are sophisticated insiders, fraudulent web sites, employees and users. The following are graphical representations of risk assessment for security breaches.

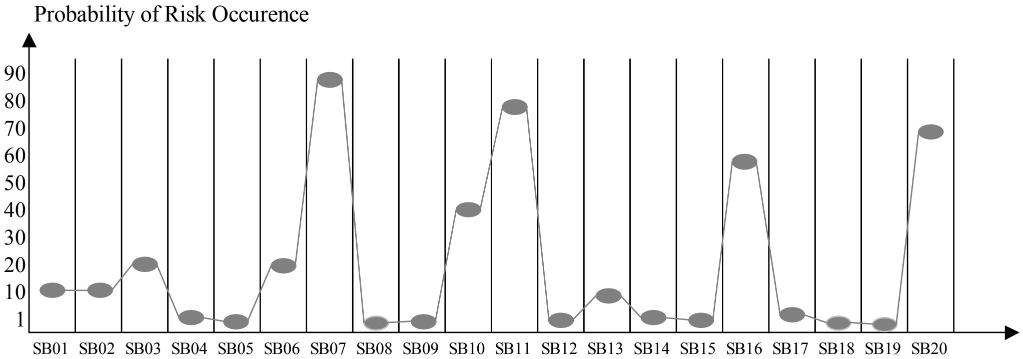


Figure 8: Graphical Representative of Probability of Risk Occurrence

The risk exposure is determined with multiplication of threat and vulnerability. [SB-07] security breach is the highest probability of risk exposure since it involves the highest security threat among security breaches and its vulnerability is too high to prevent security threats. It is required to review the target system of [SB-07].

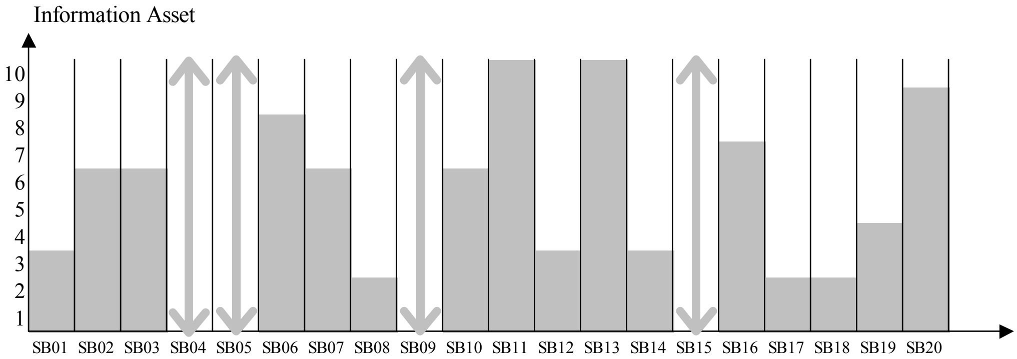


Figure 9: Graphical Representative of Information Asset

Information assets of [SB-04], [SB-05], [SB-09], and [SB-15] are not identified. The information assets have a possible range from 1 to 10 information asset levels.

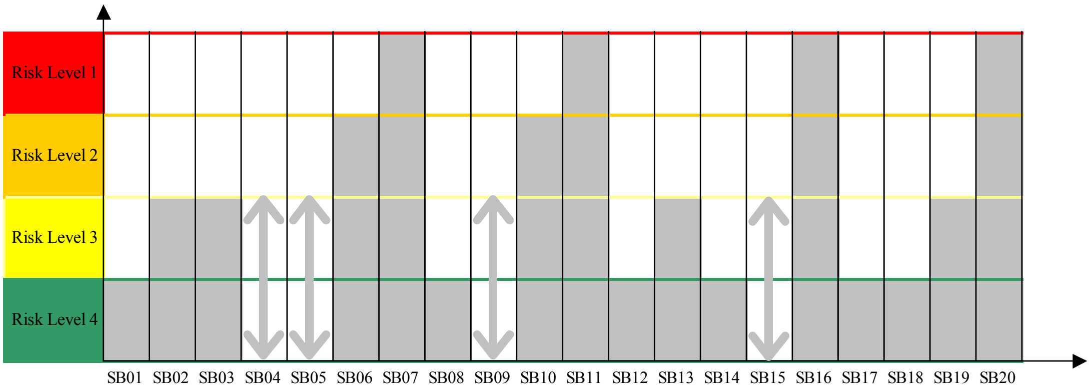


Figure 10: Graphical Representative for Risk Level

The risk level of each security breach problem is presented in the above figure. Some information assets whose assessments are not identified have a possible risk level range 3 to 4. These security breaches will never reach to risk level 1 or 2, so the security breaches are negligible. As the above figure shows, only [SB-07], [SB-11], [SB-16], and [SB-20] are necessary to prevent. Two countermeasures for systems will be focused on since this thesis deals with the methodology in developing systems. Therefore, the following countermeasures will be considered to create information policy to reduce the risk of the problems [SB-7], [SB-11], [SB-16], and [SB-20].

- □ Countermeasure 1: Censor not only content but also its amount
- □ Countermeasure 2: Improve accountability in order to trace any insider hacker's actions

3-3. Suggestions for Preventing Security Breach

Based on the risk assessment presented in the previous section, the following suggestions to prevent security breaches are derived to determine information policy[51] as follows.

1: Correct identification and access control

Execution of Resource access process is essential as explained in the following lines. The process is 1) Identification, 2) Authentication, and 3) Authorization. Definition of each term is as follows[52].

Identification: The process of announcing or revealing identity that is simply who you are.

Authentication: Allowing the people identified to access the resource.

Authorization: Determining whether someone has permission to take the requested course of action.

2: Apply economy mechanism

If the cost to break the system could be more than a benefit attacker supposes to get for that, the system may be secure enough.

3: Consider storage device

In many cases of security breach, an insider utilizes a storage device for stealing

[51] Suggestions 1 to 7 are related to the developing system while suggestions 8 to 10 are related to organizational matters.

[52] Excerpted from Computer Security, Dieter Gollmann, 1999, Page 19 – 24

confidential information. The storage device is not usually used for transferring the data to other machines since LAN (Local Area Network) is available for that. It may not be necessary for a computer to have the storage device except to back up the data[53]. Moreover, if it is desired to keep document integrity, proving a CDR with one write and read only storage device will help to achieve it.

4: Separation of Information Privilege

It is necessary to specify certain access right of each information. The access rights are as follows.

Read: Learn data and its meaning.
Copy: Duplicate data
Modify: Change data
Append: Add data
Delete: Mark data to be removed
Expunge: Destroy data that have been marked for removal

5: Least Privilege

Only least privileges must be provided to a user. Any more privilege than someone needs to accomplish the specific task should be not provided.

6: Accountability

Record all events that happened in a computer. The event will be used for analyzing and recognizing past, present, and even future threat. Then, the implementation of

[53] Countermeasure for leaking information problem, http://www.quality.co.jp/CPN.html

information policy and security mechanism in systems is taken into account.

7: Putting the above points to use in design phase

Use of the aforementioned points for the design model can help us make tremendous steps forward in building systems that resist failure[54].

8: Awareness of users, employees, and organizations

System users and employees in an organization should recognize how much security breaches impact their assets. Moreover, users should know how typed personnel information would be used.

9: Create penalties that overweight the hacker's benefits

Create a penalty that is greater than the suspect's gains from the information assets.

10: Inspect documents leaving the premises

Any confidential documents brought out from an office must be inspected. Secure rooms should be considered to keep the confidential documents secret.

[54] The way to develop the secure information risk management system, D add ninth Co., Ltd., Oct 1 2002, http://www.dadd9.com/tech/sec4manager.html

4. Static and Dynamic Information Policies

In this chapter, how information policy and security mechanism are created is demonstrated. At first, the definition of information policy is presented. Then, examples of information policy are shown corresponding to the two aforementioned countermeasures. Information policy refers to certain rules to prevent security breaches, and security mechanism is a procedure to accomplish the information policy. Information policy can be categorized into “static” and “dynamic”. Static information policy is still useful to reduce a security risk; however it is limited in its prevention of highly sophisticated trick, and it is hard to determine the appropriate value to control a security mechanism in complex systems. Dynamic policy is more suited to preventing sophisticated trick and it changes parameters with its security mechanism.

4-1. Definition

The definition of information policy in terms of systems engineering is presented in this section. Information policy is a rule to prevent security breaches regarding confidential information such as customer information, technical know-how and home security information. Information security policy can be categorized methodically into static information policy and dynamic information policy. Static information policy is an invariable rule to prevent security breach. For static information policy, it does not matter which input occurs. While static information policy does not change parameters in its rule during a specified period, dynamic information policy does; dynamic policy is a variable rule to prevent security problems regarding confidential information. Thus, for dynamic information policy, it matters which input occurs constantly. The following figure shows a methodical categorization of information policy with its property and some available technologies.

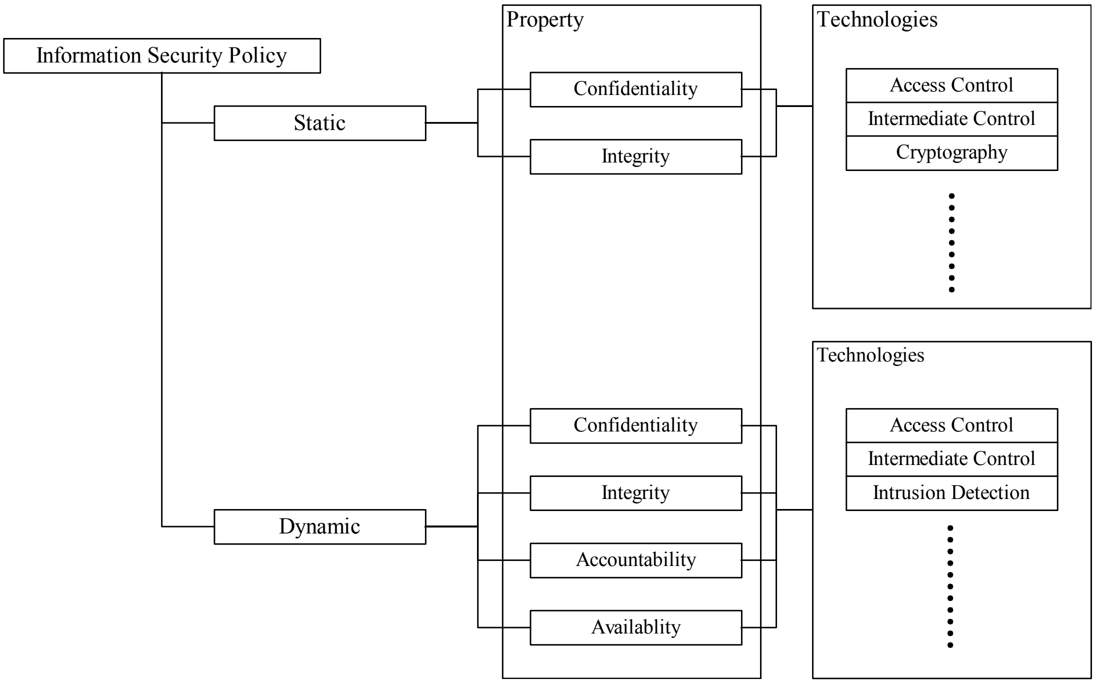


Figure 11: Methodical Categorization of Information Security Policy

Any information policy is categorized with "static" or "dynamic" methodically, and certain property and technology are delivered for it. The property[55] is a security aspect that will be taken into account in systems. The properties are in the following table.

[55] Excerpted from Computer Security, Dieter Gollmann, 1999, Page 5 – 9

Property	Description	Applied for
Confidentiality	Prevention of unauthorized disclosure of information	Static/Dynamic
Integrity	Prevention of unauthorized modification of information	Static/Dynamic
Availability	Prevention of unauthorized withholding of information or resources	Dynamic
Accountability	Audit information must be selectively kept and protected	Dynamic

Table 19: Security Properties

Many technologies are available to prevent the security breach. In this thesis, only technologies used for information policy are presented. An information policy may make use of multiple technologies.

Access Control (Static/Dynamic)[56]

The very nature of "access" suggests that there is an active subject accessing a passive object with some specific access operation, while a reference monitor grants or denies access. Typical subjects are users or processes. Typical objects are files or resources, like memory, printers, or nodes in a computer network.

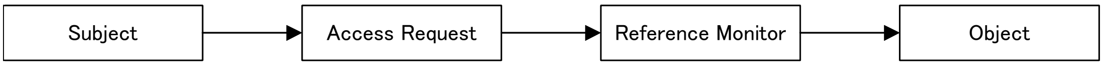


Figure 12: Access Control Model

Access control consists of its access mode and access control matrix defined access right for each user.

Object	Access Control List	
Userinf.Custm.Name	User: Read, Write	Operator: Read
Userinf.Custm.Password	User: Write, Append	

Table 20: Access Control Matrix

[56] Excerpted from Computer Security, Dieter Gollmann, 1999, Chapter 3: Access Control

Intermediate Control (Static/Dynamic)

Control through certain mediation such as group permission, protection ring, and privilege and security level. The followings intermediate controls are presented in Computer Security[57]. This technology supports the access control abovementioned to be enforced. Various intermediate controls are proposed as follows.

- *Groups and negative permissions*: Groups simplify the definition of access control policies. Users with similar access rights are collected in groups and groups are given permission to access objects. All access permissions could not be always mediated through group membership. Certain user access permission may be deployed negatively.

- *Protection Rings*: Protection rings are a particularly simple example for an intermediate layer between subject and objects. Each subject or process and each object is assigned a number, depending on its importance. For example, these numbers could be 0, 1, 2, 3 and processes receive their number according to the rule:

  0: Operating system kernel
  1: Operating System
  2: Utilities
  3: User processes

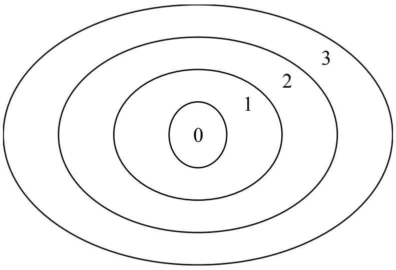


Figure 13: Protection Rings

[57] Excerpted from Computer Security, Dieter Gollmann, 1999, Page 38 – 43

- *Privileges Control:* Typically, privileges are associated with operating system functions and relate to activities like system administration, backup, mail access, or network access. A collection of an application-specific operation (procedures) is called a role. Subjects derive their access rights from the role they are performing. Role-based access control has its focus on the users and on the jobs users performs.

- *Security Level Control*: Security levels are another security attribute, like protection rings, used to label subjects and objects as the basis for expressing security policy. As a simple example, consider the following four linearly ordered security levels, "unclassified", "confidential", "secret" and "top secret".

Cryptography (Static)[58]

Two entities A and B communicate over an unsecured channel. The adversary is a hacker who has full control over this channel, being able to read their information, delete information, and insert malicious information. The entities A and B trust each other. They want protection from the hacker. Cryptography allows them to construct secure logical channel over an insecure physical connection. For the Internet network systems, the traffic between clients and servers is a new point of the attack.

Intrusion Detection (Dynamic)[59]

Once the system has been installed and is operational, its security mechanisms should

[58] Excerpted from Computer Security, Dieter Gollmann, 1999, Chapter 12: Cryptography

[59] Excerpted from Computer Security, Dieter Gollmann, 1999, Page 97

prevent illegal user actions. However, the protection mechanisms may not be adequate or flawed. It is advantageous to have further mechanisms, which allow detecting security violations or other suspicious events when they are happening or after they have happened. It is important to keep the audit log in a secure place. Attackers who are able to change the audit log are in a perfect position to hide their traces. The following is an example of a description of this methodical categorization. An information policy is as follows:

Information Policy: "Document privilege for a user is delivered based on user's security level"

Security level in this information policy will be not changed by the input, which occurs, so the information policy is static. The property of the information policy is kept confidential to prevent the document privilege from lower security level users. For this information policy, access control and intermediate control are the most suitable technology. Thus, this information policy will be classified as follows.

Policy #	Type	Property	Technology
0	Static	Confidentiality	Access Control Intermediate Control

Table 21: Classification for A Sample Information Policy

4-2. Static Information Policy

Static information policy has been widely used for security systems. Operating systems such as UNIX and Windows provides static information policy regarding document privileges. For instance, NTFS (New Technology file system)[60] is designed for multiple users, which is supposed to use different types of document privileges; it supports file-level security, compression and auditing. It also supports large volumes and powerful storage solutions such as RAID. Moreover, it provides the ability to encrypt files and folders to protect sensitive data. This policy can be described as follows.

Policy #	Type	Property	Technology
0	Static	Confidentiality Integrity Accountability	Access Control Intermediate Control Cryptography

Table 22: Classification for NTFS

In chapter 3, two countermeasures are presented to reduce unacceptable risk involving security breaches, [SB-07], [SB-12], and [SB-13]. In this section, static information policy will be developed with the aforementioned countermeasures.

□ *Countermeasure 1: Censor not only contents but also the amount*

Information Policy 1: Operator(i) is allowed to access the contents *n(i)* times per a day. Administrator(j) is allowed to access the contents *m(j)* times per a day. Administrator or security manager determines control value of *n* and *m*.

[60] New Technology File System designed for Windows NT, 2000, XP, http://www.ntfs.com/

Classification:

Policy #	Type	Property	Technology
0	Static	Confidentiality	Access Control Intermediate Control

Table 23: Classification for Information Policy 1 (Static)

Each operator and administrator is able to have a certain maximum number of accesses per day. However, configuration for those numbers is very complicated because of the enormous number of operators and administrators. Furthermore, it is crucial to determine the appropriate number of accesses for each employee. It may be determined by the administrator's experiments or decided by the stakeholder. When the amount of tasks changes, this number will no longer apply and will need to be updated.

□ *Countermeasure 2: Improve accountability in order to trace any insider hacker's action*

Information Policy 2: Deploy certain security level *l* for each object. Screen an event logs involved object with security level *L* or higher.

Classification:

Policy #	Type	Property	Technology
0	Static	Accountability	Intermediate Control

Table 24: Classification for Information Policy 2 (Static)

It is necessary to reduce the size of huge event logs, and distinguish more important event logs from less important event logs. This contributes to improving accountability since the system administrator is able to focus on the more important event logs, resulting in the reduction of his effort and time. Event logs of lower security level will be omitted with this static policy; thus, only event logs with higher security level will remain. However, the size of event logs is still large. It is better if only anomaly event logs with higher security level remain, so user's anomaly access event logs should be detected.

Are the abovementioned static information policies sufficient to prevent any security problems? Recent security breaches were already discussed in the previous chapter. Let's think about security breach problems [SB-07]. In this case, an authorized operator accessed and stole customer information, even though access control functioned properly with the access control matrix. This problem occurred because the system did not concern the object or subject behavior. Moreover, control will become more complicated since some operators might need to access large quantities of customer information depending on their position. In addition, their tasks change every day. It is almost impossible to find the appropriate number of accesses. To prevent current security breaches with static information policy is definitely limited; a more flexible and suitable information policy is required. For this reason, a dynamic information policy is proposed. This method considers object behavior, and then dynamically changes information policy, and performs the defined procedure. It is a more suited information policy for current security breaches caused by misuse and anomalous attacks. It will be presented in the next section.

4-3. Dynamic Information Policy

Dynamic information policy has become more important since hackers have become more sophisticated, and it is also required to detect any misuse and anonymous attacks. The static information policy is able to be default information policy, but it is not enough to prevent current security breaches. How dynamic policy is defined and designed corresponding to two countermeasures for [SB-7], [SB-12] and [SB-13] is shown in this section.

4-3-1. Sample Dynamic Policy 1 (Dynamic/ Confidentiality, Availability/ Access Control, Intrusion Detection/ [SB-7],[SB-12])

To solve the problem, maximum access number will be defined based on an operator tasks and average number of accesses. However, as the size of the operator's task increases, the proper maximum access number should increase. If the maximum access number is unchanged, the system availability will worsen. Contrary to this case, when the task is smaller, an excessive access number will exist, and thus system risk will increase. The maximum access number should be defined by dynamic control to prevent the security breaches of [SB-7] and [SB-12].

A) Statement

Rule engine checks the parameter $\underline{c}$ in recorded access event log to object $\underline{o}$ every $\underline{x}$ minutes. The rule engine generates statistical analysis data $\underline{s}$ for each user $\underline{i^{th}}$ in $\underline{d^{th}}$

date. Then, the rule engine determines the maximum number of accesses $\underline{N}$ corresponding to warning level $\underline{L}$ with $\underline{s}$ during a certain past period $\underline{y}$ according to procedure $\underline{p}$. The system performs defined rules according to the maximum number of accesses $\underline{N}$ and the warning level $\underline{L}$ when the rule engine detects that the warning level $\underline{L}$ is changed.

B) Audited Variables

Parameters: c(i)
c1(i): User Id (Numeric/)
c2(i): User Type (Character/Operator, Admin)
c3(i): Check time (time/)
c4(i): First access time (time/)
c5(i): Last access time (time/)
c6(i): Number of accesses between c4 and c5 (Numeric/)

Statistical analysis data: s(i, d) = f(c1(i),c2(i),c3(i),c4(i),c5(i),c6(i))
s1(i, d): User Id (Numeric/)
s2(i, d): User Type (Character/Operator, Admin)
s3(i, d): Sum of number of accesses per day (Numeric/)

Object: o
o1: Customer Information Object

C) Behavioral Variables

Check interval time x:	A specified number of minutes (1 minute, 2 minutes, 5 minutes and so on)
Estimating period y:	A specified period (1 week, 1 month and so on)
Estimating Date dy:	A specified date, interval of dy^{th}s is y ($dy^{th} – (dy\text{-}1)^{th} = y$)

D) Procedure

N(i, dy) = p1(i, dy) Estimate the base number of accesses for dy^{th}'s week or month.

σ(i, dy) = p2(i, dy) Estimate the unit of extra number of accesses for dy^{th}'s week or month.

This first procedure is to determine the average number of accesses and standard deviation on last y days from dyth.

$$average(s3(i, dy)) = \Sigma(s3(i, dy-k)) [k = 1,2\ldots y] / y$$
$$v(i, dy) = \Sigma(s3(i, dy-k+1) - average(s3(i, dy)))^2 [k = 1,2\ldots y] / y$$
$$\sigma (i, dy)= \sqrt{\ } v(i, d)$$

This second procedure is to determine the average number of accesses and standard deviation on last y days from dyth without excessive access numbers. The excessive access numbers are more than the average access number + 2σ.

$$re\_average(s3(i, dy)) = \Sigma (s3(i, dy-k)) / y, \text{ where } s3(i, dy-k) =< average(s3(i, dy)) + 2*\sigma(i, dy) [k = 1,2\ldots y]$$
$$re\_v(i, dy) = \Sigma(s3(i, dy-k) - re\_average(s3(i, dy)))2 / y, \text{ where } s3(i, d+k) < average(s3(i, d)) + 2*\sigma(i, d)\text{"} [k = 1,2\ldots y]$$
$$re\_ \sigma (i, dy)= \sqrt{\ } re\_v(i, dy)$$
$$N(i, dy) = re\_average(s3(i, dy))$$
$$\sigma(i, dy) = re\_ \sigma (i, dy)$$

Therefore, the base number of accesses and the unit of extra number of accesses are calculated with the parameters audited on the last period. The maximum access number of each warning level consists of these numbers. It is defined as follows.

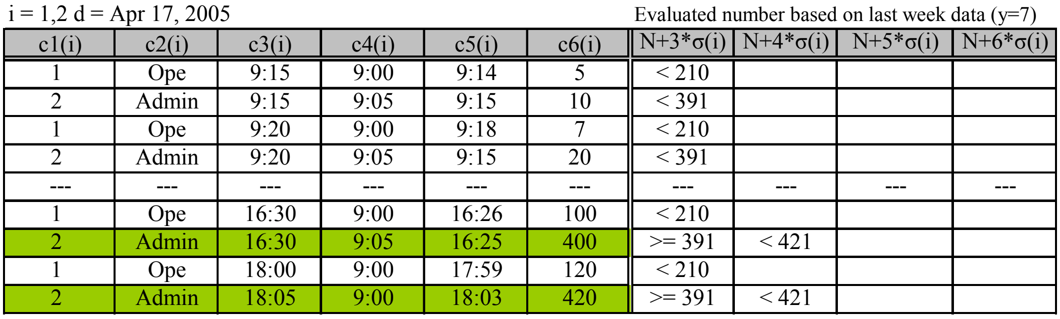
$$\text{Max Access Number } (l) = N(i, dy) + n(l)* \sigma(i, dy),$$
$$[n(l=W1)=3, n(l=W2)=4, n(l=W3)=5, n(l=W4)=6]$$

The following table on the next page shows the defined rule according to the warning levels.

If the number is detected	The defined rule	
*c6(i) < N(i, dy)+3*σ(i, dy)*	Normal level	W0
*N(i, dy)+3*σ(i, dy) =< c6(i) < N(i, dy)+4*σ(i, dy)*	Warning to user (i) and send its status to Manager	W1
*N(i, dy)+4*σ(i, dy) =< c6(i) < N(i, dy)+5*σ(i, dy)*	Warning to user (i) and send its status to Manager. For more access, user (i) needs the manager's authorization.	W2
*N(i, dy)+5*σ(i, dy) =< c6(i) < N(i, dy)+6*σ(i, dy)*	Warning to user (i) and send its status to Manager. For more access, user (i) needs the manager's authorization.	W3
*N(i, dy)+6*σ(i, dy) =< c6(i)*	Canceled user (i) authorization.	W4

Table 25: Rule for each Warning Level for Sample Dynamic Information Policy 1

When the warning level is changed, the system performs the abovementioned functions. The rules may be changed by the system policy or stakeholders. The following example demonstrates this procedure. The maximum number of accesses for the (dy) period is already set using the audited data in the (dy-1) period (Apr 10, 2005 to Apr 16, 2005). The dynamic policy for the (dy) period is shown in the following table.



i = 1,2 d = Apr 17, 2005

Evaluated number based on last week data (y=7)

c1(i)	c2(i)	c3(i)	c4(i)	c5(i)	c6(i)	N+3*σ(i)	N+4*σ(i)	N+5*σ(i)	N+6*σ(i)
1	Ope	9:15	9:00	9:14	5	< 210			
2	Admin	9:15	9:05	9:15	10	< 391			
1	Ope	9:20	9:00	9:18	7	< 210			
2	Admin	9:20	9:05	9:15	20	< 391			
---	---	---	---	---	---	---	---	---	---
1	Ope	16:30	9:00	16:26	100	< 210			
2	Admin	16:30	9:05	16:25	400	>= 391	< 421		
1	Ope	18:00	9:00	17:59	120	< 210			
2	Admin	18:05	9:00	18:03	420	>= 391	< 421		

Figure 14: Audit Data for the Sample Dynamic Information 1, Day 1 in the (dy) Period

Admin (user id=2) is warned as the warning level 1, and then it will be reported to his/her manager at 16:30 since the number of accesses reaches between W1 and W2 level.

i = 1,2 d = Apr 18, 2005

c1(i)	c2(i)	c3(i)	c4(i)	c5(i)	c6(i)	N+3*σ(i)	N+4*σ(i)	N+5*σ(i)	N+6*σ(i)
1	Ope	9:15	9:01	9:14	5	< 210			
2	Admin	9:15			0	< 391			
1	Ope	9:20	9:00	9:18	7	< 210			
2	Admin	9:20	9:18	9:19	20	< 391			
---	---	---	---	---	---	---	---	---	---
1	Ope	18:00	9:01	17:55	120	< 210			
2	Admin	18:00	9:18	17:57	200	< 391			
1	Ope	19:05	9:01	18:45	150	< 210			
2	Admin	19:05	9:18	18:50	240	< 391			

Figure 15: Audit Data for the Sample Dynamic Information 1, Day 2 in the (dy) Period

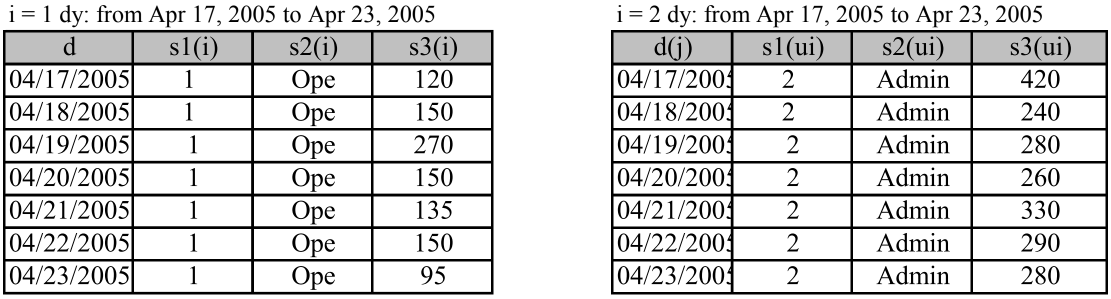
No access number exceeds the max access number on the day.

i = 1,2 d = Apr 19, 2005

c1(i)	c2(i)	c3(i)	c4(i)	c5(i)	c6(i)	N+3*σ(i)	N+4*σ(i)	N+5*σ(i)	N+6*σ(i)
1	Ope	9:00	8:00	8:59	14	< 210			
2	Admin	9:00	8:30	9:00	20	< 391			
1	Ope	9:05	8:00	9:04	18	< 210			
2	Admin	9:05	8:30	9:04	25	< 391			
---	---	---	---	---	---	---	---	---	---
1	Ope	15:05	8:00	15:02	220	>= 210	< 245		
2	Admin	15:05	8:30	15:03	230	< 391			
1	Ope	15:10	8:00	15:08	250	>= 210	>= 245	< 280	
2	Admin	15:10	8:30	15:07	250	< 391			
1	Ope	18:05	8:00	18:03	270	>= 210	>= 245	< 280	
2	Admin	18:05	8:30	18:00	280	< 391			

Figure 16: Audit Data for the Sample Dynamic Information 1, Day 3 in the (dy) Period

The operator (user id=1) is warned and must report to his/her manager at 15:05 since the number of accesses reached between the maximum access number of W1 and W2 level. Operator (user ID=1) is warned and must report to his/her manager. The manager is then required to send the operator permission to access more customer records at 15:10 since the number of accesses reached between the maximum access number of W2 and W3 level. For the other days, it will be controlled according to the defined rule. At the end of the (dy) period, the maximum number of accesses for the next period (dy+1) is determined as follows. The following table is a cross table of the number of accesses in the (dy) period. The number of accesses is formatted with user ID and type and is ordered by the day of the (dy) period.



i = 1 dy: from Apr 17, 2005 to Apr 23, 2005

d	s1(i)	s2(i)	s3(i)
04/17/2005	1	Ope	120
04/18/2005	1	Ope	150
04/19/2005	1	Ope	270
04/20/2005	1	Ope	150
04/21/2005	1	Ope	135
04/22/2005	1	Ope	150
04/23/2005	1	Ope	95

i = 2 dy: from Apr 17, 2005 to Apr 23, 2005

d(j)	s1(ui)	s2(ui)	s3(ui)
04/17/2005	2	Admin	420
04/18/2005	2	Admin	240
04/19/2005	2	Admin	280
04/20/2005	2	Admin	260
04/21/2005	2	Admin	330
04/22/2005	2	Admin	290
04/23/2005	2	Admin	280

Figure 17: Cross Table of The Number of Accesses in the (dy) period

Some statistical data are determined with usage of the data in the above table through the first procedure as follows.

i = 1 dy: from Apr 17, 2005 to Apr 23, 2005

Ave:	153
Variance	2642
Standard Deviation	52
Average+2 σ	257

i = 2 dy: from Apr 17, 2005 to Apr 23, 2005

Ave:	300
Variance	3058
Standard Deviation	56
Average+2 σ	412

Table 26: Statistical Analyzed Max Number of Accesses I

As the second procedure, the statistical data are recalculated without excessive access numbers, which is more than the average + 2* σ .

i = 1 dy: from Apr 17, 2005 to Apr 23, 2005

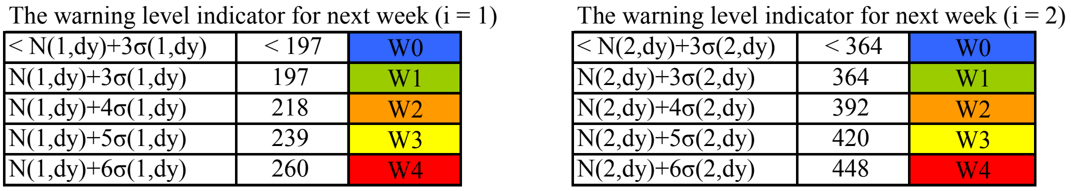
R_Ave	134
R_Variance	414
R_Standard Deviation	21

i = 2 dy: from Apr 17, 2005 to Apr 23, 2005

R_Ave	280
R_Variance	767
R_Standard Deviation	28

Table 27: Statistical Analyzed Max Number of Accesses II

For example, the user ID 1 has one excessive access number 270 (>258) on Apr 19, 2005. The statistical data for the user ID 1 will be recalculated without the excessive access number on this day. Recalculated statistical data are in the above table. For the user ID 2, the same method will be applied. Finally, the maximum number of accesses for each warning level will be determined by the abovementioned rules. The result is shown in the following table.



The warning level indicator for next week (i = 1)

$< N(1,dy)+3\sigma(1,dy)$	< 197	W0
$N(1,dy)+3\sigma(1,dy)$	197	W1
$N(1,dy)+4\sigma(1,dy)$	218	W2
$N(1,dy)+5\sigma(1,dy)$	239	W3
$N(1,dy)+6\sigma(1,dy)$	260	W4

The warning level indicator for next week (i = 2)

$< N(2,dy)+3\sigma(2,dy)$	< 364	W0
$N(2,dy)+3\sigma(2,dy)$	364	W1
$N(2,dy)+4\sigma(2,dy)$	392	W2
$N(2,dy)+5\sigma(2,dy)$	420	W3
$N(2,dy)+6\sigma(2,dy)$	448	W4

Table 28: The Final Estimated Statistical Analyzed Max Number of Accesses

The dynamic policy changes according to the historical access number of each user. Statistically, the possibility of an access number going beyond the warning level 1 (W1: $> N(i,dy) + 3\sigma(i,dy)$) is less than 0.135%. The possibility of going beyond warning level 4 will be less than $1*10^{-9}$ %: statistically, it is almost impossible that this will occur even if the user accesses the object (user customer information) intensively. Unusual activity must occur intentionally if the access number exceeds the maximum number of accesses. The defined rule provides the system reaction at every change of the warning level. This enables the system security manager to detect misuse and anomalous attacks before serious problems happen. Moreover, sending a warning message incites fear in the hackers, and discourages them from invading the system.

4-3-2. Sample Dynamic Policy 2 (Dynamic/ Availability, Accountability/ Intermediate Control, Intrusion Detection/ [SB-12], [SB-13])

As shown in the previous dynamic information policy, historical event logs play a very important role in the system in order to achieve a suitable dynamic information policy. However, the historical event log of the entire system can be an enormous amount of data. It is extremely hard to find an event log containing only the necessary information among the huge enormous amount of event log data. This results in not detecting crucial misuse and anomalous activities recorded in the logs. Many unnecessary logs become camouflaged to hide the traces of the hacker’s activities. For example, in the case of [SB-12] and [SB-13], it took a very long time to trace the hacker’s activities among the huge amount of event logs in their system. The hackers were not sophisticated and their access tracks were recorded in the event log, so it was possible to detect their activities before the problem occurred. However, the organization did not realize the importance of detecting the event log since this activity requires much time and effort. Moreover, the event log was traced a few weeks after the secret information was stolen. The event log was too huge to trace properly. In addition, some important traces of questionable activities were missed. It is crucial to detect misuse and anomalous activities effectively and efficiently. To solve this problem, a static information policy may be proposed in order to detect only important event logs. For instance, only highly confidential object access logs and unauthorized user access logs are separated from other event logs since these event logs may be very important in detecting the misuse activities. The highly confidential object access logs are too large; misuse and anomaly activities can be detected more easily but it still takes a considerable amount of time. Moreover, authorized users can be malicious hackers. In fact, authorized hackers, called insiders, have recently become more of a threat. The static information may contribute to a decreased effort to censor the event log, but it may work only for a few cases; moreover, the organization may miss an important event log. The information policy to separate the significant event logs from other event logs should be determined dynamically based on some current conditions such as access frequency of a subject, frequency of access to the object, and occupational rate of the subject per certain time interval. The second dynamic information policy with the abovementioned ideas is as follows.

A) Statement

A rule engine checks audited logs involved in a system every *x* minute. The rule engine generates statistical data, access frequency and occupation rate *si* for user *i*, and confidential rate *so* for object *o*. Audit level *L* for user *i* (subject) and *o* (Object) is determined by procedure *p* corresponding to the access frequency, occupation rate *si* of a subject, and frequency of access to the object *so*. The system performs defined rules according to the audit level *L* for the user *i* and target *o* every *y* time interval.

B) Audited Variables

Parameters: a(i), b(o)
a1(i): User Id (Numeric/)
a2(i): User Type (Character/Operator, Admin)
a3(i): Last access time (time/)
a4(i): Check time (time/)
a5(i): Number of accesses between a3 and a4 (Numeric/)

b1(o): Object Type (Numeric/)

b2(o): Object Confidential (Numeric/)
b3(o): Last access time (time/)
b4(o): Check time (time/)
b5(o): Number of accesses to the object between b3 and b4 (Numeric/)

Statistical analysis data: si(i) = f(a1(i),a2(i),a3(i),a4(i),a5(i))
si1(i, d): User Id (Numeric/)
si2(i, d): User Type (Character/Operator, Admin)
si3(i, d): Sum of Number of accesses in a day (Numeric/)
si4(i, d): Max of occupation rate in a day (Numeric/)
(si4(i, d) = max((c5(i)*100) / Σ c5(i) [i: all users] of x time interval in a day))

Statistical analysis data: so(i) = f(b1(o),b2(o),b3(o),b4(o),b5(o))
so1(o): Object Type (Numeric/)
so2(o): Object Confidential (Numeric/1, 2 and 3)
(The confidential object should be determined depending on certain organization policy. For convenience purposes, it is determined by 1, 2, and 3 on this report)
so3(o): Sum of Number of accesses to the object in a day (Numeric/)

C) Behavioral Variables

Check interval time x: A specified number of minutes (30 minutes, 1 hour, 2 hours and so on)

Estimating period y: A specified period (1 day, 2 days, 1 week and so on)

D) Procedure

The event log generally involves subject and object. The subject is an entity to access the object like user. On the other hand, the object is an entity to be accessed by the subject like customer information. The audit level of each event log will be determined by the following equation.

L(i, o, dy) = k1*p1(i, dy)*p3(o, dy) + k2*p2(i, dy)*p3(o, dy)
Estimate the audit level from Feb 10, 2003 to Feb 18, 2003.
(k1 and k2 are adjusted coefficients determined by security managers, stakeholders, or organization policy.)

This procedure is to determine the audit level of each event with the abovementioned statistical data, the access frequency of a subject, occupation rate of a subject and frequency of access to the object in a period of certain dyth. As the first procedure, the maximum number of accesses *p1* of each user in a period y is determined as follows.

$$p1(i, dy) = \max(si3(i, dy) \text{ in a y period}) = \max(si3(i, dy-k+1)) \; [k = 1,2\ldots y]$$

As the second procedure, the average of the maximum occupation rate *p2* of each user in a period y is determined as follows.

$$p2(i, dy) = \text{average}(si4(i, dy) \text{ in a y period}) = \Sigma(si4(i, dy-k+1)) \; [k = 1,2\ldots y] / y$$

As the third procedure, the maximum frequency of access to the object in a period y is determined as follows.

$$p3(o, dy) = \max(so2(o, dy)*so3(o, dy) \text{ in a y period}) = \max(so2(o, dy-k+1)*so3(o, dy-k+1)) \; [k = 1,2\ldots y]$$

Finally, the audit level is determined by the abovementioned equation using p1, p2 and p3. The value of k1 and k2 are adjusted coefficients. These values should be determined by experiment in the organization and its policy. The sample value for the adjusted coefficients will be determined using demo data from this report. Using the abovementioned equation, the audit level will be various numeric values. When applying the defined rule, it should be simplified as level 1, level 2, and level 3. The simplified audit level and defined rule corresponding to the audit level is presented on the following table.

The audit level	The defined rule	
$L(i, o, dy) = 0\text{-}2$	Less important event log. It may be neglected	A1
$L(i, o, dy) = 2\text{-}8$	Ordinary important even log. It may be checked if it is able to be made effort by the administror	A2
$L(i, o, dy) = 8$ -	Crucial event log, it must be checked every y period.	A3

Table 29: Rule each Audit Level for Sample Dynamic Information Policy 2

An example of the aforementioned dynamic policy 2 is presented as follows. The table on the next page is a sample of 100 historical event logs. The sample data is generated randomly following an interface of the dynamic policy 2[61]. This imaginary data is used to show an example of a procedure in the dynamic policy 2.

[61] See page 42, “B) Audited Variables”.

Sample Event Log (i = 1,2…5, o = 1,2…4) / Apr 18, 2005 / x = 60 r

a1(i)	a2(i)	a3(i)/b3(o)	a4(i)/b4(o)	b1(o)	b2(o)
2	Ope	9:00	10:00	1	1
3	Ope	9:09	10:00	2	2
3	Ope	9:18	10:00	4	3
1	Admin	9:27	10:00	1	1
3	Ope	9:34	10:00	3	2
4	Custm	9:37	10:00	2	2
2	Ope	9:46	10:00	2	2
5	Custm	9:52	10:00	2	2
3	Ope	9:52	10:00	1	1
4	Custm	10:00	11:00	2	2
3	Ope	10:02	11:00	4	3
2	Ope	10:12	11:00	2	2
5	Custm	10:17	11:00	2	2
4	Custm	10:25	11:00	2	2
3	Ope	10:27	11:00	3	2
5	Custm	10:29	11:00	2	2
2	Ope	10:29	11:00	2	2
2	Ope	10:32	11:00	3	2
3	Ope	10:41	11:00	2	2
5	Custm	10:46	11:00	1	1
4	Custm	10:56	11:00	1	1
3	Ope	11:04	12:00	3	2
2	Ope	11:11	12:00	1	1
5	Custm	11:14	12:00	2	2
3	Ope	11:20	12:00	4	3
2	Ope	11:20	12:00	1	1
4	Custm	11:30	12:00	2	2
5	Custm	11:37	12:00	1	1
4	Custm	11:45	12:00	2	2
4	Custm	11:48	12:00	2	2
5	Custm	11:53	12:00	1	1
2	Ope	11:59	12:00	1	1
4	Custm	12:00	13:00	2	2
1	Admin	12:08	13:00	1	1
3	Ope	12:13	13:00	4	3
2	Ope	12:16	13:00	3	2
5	Custm	12:26	13:00	2	2
3	Ope	12:26	13:00	2	2
4	Custm	12:28	13:00	1	1
3	Ope	12:33	13:00	2	2
4	Custm	12:34	13:00	1	1
2	Ope	12:38	13:00	3	2
4	Custm	12:46	13:00	2	2
2	Ope	12:49	13:00	4	3
3	Ope	12:59	13:00	2	2
3	Ope	13:04	14:00	2	2
2	Ope	13:07	14:00	3	2
4	Custm	13:12	14:00	1	1
2	Ope	13:13	14:00	2	2
3	Ope	13:22	14:00	2	2
3	Ope	13:31	14:00	1	1
3	Ope	13:41	14:00	4	3
1	Admin	13:48	14:00	1	1
2	Ope	13:51	14:00	1	1
3	Ope	13:57	14:00	3	2
2	Ope	14:00	15:00	1	1
2	Ope	14:10	15:00	2	2
2	Ope	14:18	15:00	2	2
2	Ope	14:19	15:00	2	2
2	Ope	14:24	15:00	3	2
4	Custm	14:33	15:00	2	2
2	Ope	14:37	15:00	2	2
5	Custm	14:47	15:00	2	2
4	Custm	14:50	15:00	2	2
3	Ope	14:54	15:00	2	2
2	Ope	14:58	15:00	2	2

Sample Event Log (i = 1,2…5, o = 1,2…4) / Apr 19, 2005 / x = 60 r

a1(i)	a2(i)	a3(i)/b3(o)	a4(i)/b4(o)	b1(o)	b2(o)
3	Ope	9:05	10:00	4	3
4	Custm	9:11	10:00	1	1
2	Ope	9:17	10:00	2	2
2	Ope	9:25	10:00	3	2
5	Custm	9:32	10:00	2	2
2	Ope	9:42	10:00	3	2
4	Custm	9:48	10:00	2	2
2	Ope	9:56	10:00	1	1
4	Custm	9:58	10:00	2	2
5	Custm	9:59	10:00	2	2
4	Custm	10:09	11:00	2	2
2	Ope	10:10	11:00	4	3
4	Custm	10:18	11:00	2	2
3	Ope	10:21	11:00	3	2
3	Ope	10:24	11:00	2	2
2	Ope	10:30	11:00	3	2
3	Ope	10:39	11:00	4	3
5	Custm	10:48	11:00	1	1
2	Ope	10:52	11:00	3	2
4	Custm	10:55	11:00	2	2
3	Ope	11:05	12:00	2	2
2	Ope	11:11	12:00	4	3
2	Ope	11:19	12:00	3	2
4	Custm	11:23	12:00	1	1
3	Ope	11:26	12:00	2	2
5	Custm	11:31	12:00	2	2
1	Admin	11:38	12:00	2	2
5	Custm	11:45	12:00	1	1
2	Ope	11:51	12:00	4	3
3	Ope	11:53	12:00	3	2
2	Ope	12:02	13:00	2	2
2	Ope	12:02	13:00	2	2
2	Ope	12:11	13:00	2	2
2	Ope	12:19	13:00	1	1
2	Ope	12:21	13:00	1	1
2	Ope	12:23	13:00	3	2
2	Ope	12:31	13:00	2	2
2	Ope	12:40	13:00	2	2
4	Custm	12:47	13:00	2	2
2	Ope	12:51	13:00	2	2
2	Ope	12:58	13:00	2	2
3	Ope	13:07	14:00	3	2
5	Custm	13:11	14:00	2	2
3	Ope	13:18	14:00	2	2
5	Custm	13:26	14:00	1	1
3	Ope	13:33	14:00	2	2
4	Custm	13:41	14:00	1	1
4	Custm	13:45	14:00	1	1
5	Custm	13:54	14:00	2	2
3	Ope	13:55	14:00	3	2
3	Ope	14:04	15:00	1	1
3	Ope	14:09	15:00	3	2
3	Ope	14:10	15:00	1	1
4	Custm	14:12	15:00	1	1
2	Ope	14:17	15:00	3	2
1	Admin	14:19	15:00	4	3
4	Custm	14:29	15:00	2	2
3	Ope	14:35	15:00	2	2
2	Ope	14:35	15:00	2	2
2	Ope	14:37	15:00	3	2
2	Ope	14:37	15:00	4	3
4	Custm	14:44	15:00	2	2
4	Custm	14:51	15:00	2	2
2	Ope	14:54	15:00	2	2
3	Ope	14:58	15:00	1	1
2	Ope	15:03	16:00	4	3

Figure 18: Sample Event Log from Apr 18 to Apr 19 in 2005

Every log has the subject, object and time stamp. For the purpose to simplify the dynamic policy, only auditing variables are shown on the table, and every one-hour (x = 60 minutes) the logs are checked by the rule engine to generate statistical variables. The audit level is determined with the statistical variables in two days (y = 2, dy = Apr 18, 2005 to Apr 19, 2005). The following is the audited variables grouped by user *i* and the statistical data 1 *si(i)* corresponding to the audited variables in the period, Apr 18 2005 and April 19 2005.

i = 1,2…5, d = Apr 18, 2005, x = 60 minutes

a1(i)	a2(i)	a3(i)	a4(i)	a5(i)	a1(i)	a2(i)	a3(i)	a4(i)	a5(i)
1	Admin	9:27	10:00	1	1	Admin	13:48	15:00	0
2	Ope	9:46	10:00	2	2	Ope	14:58	15:00	7
3	Ope	9:52	10:00	4	3	Ope	14:54	15:00	1
4	Custm	9:37	10:00	1	4	Custm	14:50	15:00	2
5	Custm	9:52	10:00	1	5	Custm	14:47	15:00	1
1	Admin	9:27	11:00	0	1	Admin	15:38	16:00	3
2	Ope	10:32	11:00	3	2	Ope	15:38	16:00	4
3	Ope	10:41	11:00	3	3	Ope	14:54	16:00	0
4	Custm	10:56	11:00	3	4	Custm	15:46	16:00	2
5	Custm	10:46	11:00	3	5	Custm	15:56	16:00	1
1	Admin	9:27	12:00	0	1	Admin	16:27	17:00	2
2	Ope	11:59	12:00	3	2	Ope	16:51	17:00	5
3	Ope	11:20	12:00	2	3	Ope	16:56	17:00	3
4	Custm	11:48	12:00	3	4	Custm	16:42	17:00	2
5	Custm	11:53	12:00	3	5	Custm	16:03	17:00	1
1	Admin	12:08	13:00	1	1	Admin	17:30	18:00	1
2	Ope	12:49	13:00	3	2	Ope	17:51	18:00	4
3	Ope	12:59	13:00	4	3	Ope	17:28	18:00	2
4	Custm	12:46	13:00	4	4	Custm	17:10	18:00	2
5	Custm	12:26	13:00	1	5	Custm	17:38	18:00	2
1	Admin	13:48	14:00	1					
2	Ope	13:51	14:00	3					
3	Ope	13:57	14:00	5					
4	Custm	13:12	14:00	1					
5	Custm	12:26	14:00	0					

Table 30: Audit Data 1 for the Sample Dynamic Information 2, Day 1 in the (dy) Period

si1(i)	si2(i)	si3(i)	si4(i)
1	Admin	9	30%
2	Ope	34	64%
3	Ope	24	50%
4	Custm	20	31%
5	Custm	13	27%

	si4(1, time)	si4(2, time)	si4(3, time)	si4(4, time)	si4(5, time)
10:00	11%	22%	44%	11%	11%
11:00	0%	25%	25%	25%	25%
12:00	0%	27%	18%	27%	27%
13:00	8%	23%	31%	31%	8%
14:00	10%	30%	50%	10%	0%
15:00	0%	64%	9%	18%	9%
16:00	30%	40%	0%	20%	10%
17:00	15%	38%	23%	15%	8%
18:00	9%	36%	18%	18%	18%

Table 31: Statistical Data 1 for the Sample Dynamic Information 2, Day 1 in the (dy) Period

i = 1,2…5, d = Apr 19, 2005, x = 60 minutes

a1(i)	a2(i)	a3(i)	a4(i)	a5(i)	a1(i)	a2(i)	a3(i)	a4(i)	a5(i)
1	Admin	---	10:00	0	1	Admin	14:19	15:00	1
2	Ope	9:56	10:00	4	2	Ope	14:54	15:00	5
3	Ope	9:05	10:00	1	3	Ope	14:58	15:00	5
4	Custm	9:58	10:00	3	4	Custm	14:51	15:00	4
5	Custm	9:59	10:00	2	5	Custm	13:54	15:00	0
1	Admin	---	11:00	0	1	Admin	15:14	16:00	1
2	Ope	10:52	11:00	3	2	Ope	15:39	16:00	5
3	Ope	10:39	11:00	3	3	Ope	15:58	16:00	3
4	Custm	10:55	11:00	3	4	Custm	15:47	16:00	6
5	Custm	10:48	11:00	1	5	Custm	15:57	16:00	1
1	Admin	11:38	12:00	1	1	Admin	16:45	17:00	1
2	Ope	11:51	12:00	3	2	Ope	16:54	17:00	3
3	Ope	11:53	12:00	3	3	Ope	16:42	17:00	2
4	Custm	11:23	12:00	1	4	Custm	16:36	17:00	4
5	Custm	11:45	12:00	2	5	Custm	16:59	17:00	2
1	Admin	11:38	13:00	0	1	Admin	17:14	18:00	1
2	Ope	12:58	13:00	10	2	Ope	17:45	18:00	2
3	Ope	11:53	13:00	0	3	Ope	17:40	18:00	2
4	Custm	12:47	13:00	2	4	Custm	17:33	18:00	2
5	Custm	11:45	13:00	0	5	Custm	16:59	18:00	0
1	Admin	11:38	14:00	0					
2	Ope	12:58	14:00	0					
3	Ope	13:55	14:00	4					
4	Custm	13:45	14:00	2					
5	Custm	13:54	14:00	3					

Table 32: Audit Data 1 for the Sample Dynamic Information 2, Day 2 in the (dy) Period

si1(i)	si2(i)	si3(i)	si4(i)
1	Admin	5	14%
2	Ope	35	83%
3	Ope	23	44%
4	Custm	26	38%
5	Custm	11	33%

	si4(1, time	si4(2, time	si4(3, time	si4(4, time)	si4(5, time)
10:00	0%	40%	10%	30%	20%
11:00	0%	30%	30%	30%	10%
12:00	10%	30%	30%	10%	20%
13:00	0%	83%	0%	17%	0%
14:00	0%	0%	44%	22%	33%
15:00	7%	33%	33%	27%	0%
16:00	6%	31%	19%	38%	6%
17:00	8%	25%	17%	33%	17%
18:00	14%	29%	29%	29%	0%

Table 33: Statistical Data 1 for the Sample Dynamic Information 2, Day 2 in the (dy) Period

The following are the audited variables grouped by user *o* and the statistical data 2 *so(o)* corresponding to the audited variables in the period, Apr. 18, 2005 and Apr. 19, 2005. The access frequency to the object so2(o) is determined by a numeric value corresponding to the object's role. For the purpose to be simplified, the following objects and their confidential levels are shown in the below table.

Object Type	Object Role	Confidential Level
1	Customer unclassified Information	1
2	Customer confidential Information	2
3	Operator Information	2
4	Administrator Information	3

Table 34: Object Confidential Level

o = 1,2…4, d = Apr 18, 2005, x = 60 minutes

b1(o)	b2(o)	b3(o)	b4(o)	b5(o)	b1(o)	b2(o)	b3(o)	b4(o)	b5(o)
1	1	9:27	10:00	3	1	1	14:00	15:00	1
2	2	9:52	10:00	4	2	2	14:58	15:00	9
3	2	9:34	10:00	1	3	2	14:24	15:00	1
4	3	9:18	10:00	1	4	3	13:41	15:00	0
1	1	10:56	11:00	2	1	1	15:56	16:00	5
2	2	10:41	11:00	7	2	2	15:38	16:00	5
3	2	10:32	11:00	2	3	2	14:24	16:00	0
4	3	10:02	11:00	1	4	3	13:41	16:00	0
1	1	11:59	12:00	5	1	1	16:13	17:00	2
2	2	11:48	12:00	4	2	2	16:42	17:00	10
3	2	11:04	12:00	1	3	2	16:56	17:00	1
4	3	11:20	12:00	1	4	3	16:27	17:00	0
1	1	12:34	13:00	3	1	1	17:51	18:00	2
2	2	12:59	13:00	6	2	2	17:38	18:00	4
3	2	12:38	13:00	2	3	2	17:30	18:00	4
4	3	12:49	13:00	2	4	3	17:41	18:00	1
1	1	13:51	14:00	4					
2	2	13:22	14:00	3					
3	2	13:57	14:00	2					
4	3	13:41	14:00	1					

Table 35: Audit Data 2 for the Sample Dynamic Information 2, Day 1 in the (dy) Period

so1(i)	so2(i)	so3(i)	so2*so3(i)	
1	1	26	26	Customer Information 1 (Unclassified)
2	2	47	94	Customer Information 2 (Confidential)
3	2	18	36	Operator Information
4	3	9	27	Admistrator Information

Table 36: Statistical Data 2 for the Sample Dynamic Information 2, Day 1 in the (dy) Period

o = 1,2…4, d = Apr 19, 2005, x = 60 minutes

b1(o)	b2(o)	b3(o)	b4(o)	b5(o)
1	1	9:56	10:00	2
2	2	9:59	10:00	5
3	2	9:42	10:00	2
4	3	9:05	10:00	1
1	1	10:48	11:00	1
2	2	10:55	11:00	4
3	2	10:52	11:00	3
4	3	10:39	11:00	2
1	1	11:45	12:00	2
2	2	11:38	12:00	4
3	2	11:53	12:00	2
4	3	11:51	12:00	2
1	1	12:21	13:00	2
2	2	12:58	13:00	8
3	2	12:23	13:00	1
4	3	11:51	13:00	0
1	1	13:45	14:00	3
2	2	13:54	14:00	4
3	2	13:55	14:00	2
4	3	11:51	14:00	0
1	1	14:58	15:00	4
2	2	14:54	15:00	6
3	2	14:37	15:00	3
4	3	14:37	15:00	2
1	1	15:57	16:00	2
2	2	15:58	16:00	12
3	2	15:39	16:00	1
4	3	15:03	16:00	1
1	1	16:54	17:00	4
2	2	16:59	17:00	6
3	2	16:21	17:00	2
4	3	15:03	17:00	0
1	1	17:14	18:00	1
2	2	17:40	18:00	5
3	2	16:21	18:00	0
4	3	17:45	18:00	1

Table 37: Audit Data 2 for the Sample Dynamic Information 2, Day 2 in the (dy) Period

so1(i)	so2(i)	so3(i)	so2*so3(i)	
1	1	21	21	Customer Information 1 (Unclassified)
2	2	54	108	Customer Information 2 (Confidential)
3	2	16	32	Operator Information
4	3	9	27	Admistrator Information

Table 38: Statistical Data 2 for the Sample Dynamic Information 2, Day 2 in the (dy) Period

i = 1 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d	si3(1)	si4(1)
04/18/2005	9	30%
04/19/2005	5	14%

i = 2 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d(j)	si3(2)	si4(2)
04/18/2005	34	64%
04/19/2005	35	83%

i = 3 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d	si3(3)	si4(3)
04/18/2005	24	50%
04/19/2005	23	44%

i = 4 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d(j)	si3(4)	si4(4)
04/18/2005	20	31%
04/19/2005	26	38%

i = 5 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d	si3(5)	si4(5)
04/18/2005	13	27%
04/19/2005	11	33%

o = 1 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d	so3*so4
04/18/2005	26
04/19/2005	21

o = 2 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d(j)	so3*so4
04/18/2005	94
04/19/2005	108

o = 3 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d	so3*so4
04/18/2005	36
04/19/2005	32

o = 4 dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

d(j)	so3*so4
04/18/2005	27
04/19/2005	27

Table 39: Summary of the Statistical Variables in the Period

dy: from Apr 18, 2005 to Apr 19, 2005 , y = 2

	p1(i)	**p2(i)**
1	**9**	**22%**
2	**35**	**73%**
3	**24**	**47%**
4	**26**	**34%**
5	**13**	**30%**

	p3(o)
1	**26**
2	**108**
3	**36**
4	**27**

Table 40: Procedure Output Statistical Variable in the Period

The audit level is determined by the variables p1(i), p2(i) and p3(i) in the above table and the following equation.

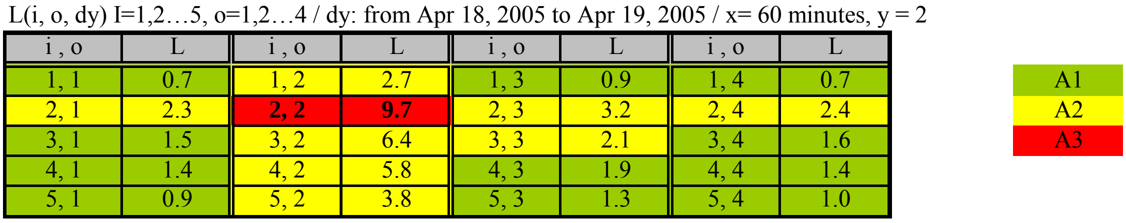
$$L(i, o, dy) = k1*p1(i, dy)*p3(o, dy) + k2*p2(i, dy)*p3(o, dy)$$

The coefficient k1 and k2 may be adjusted depending on certain experiments in a target system, and security manager’s, or stakeholder opinion to reach a suitable audit level for the target system. The audit level range is from 0 to 10. In this report, the following values are estimated as k1 and k2 coefficient values.

$k1 = 0.0012$

k2 = 0.065

According to the equation, audit level will be deployed for each combination of the subject *i* and object *o* in the period. The audit levels are shown in the following table.



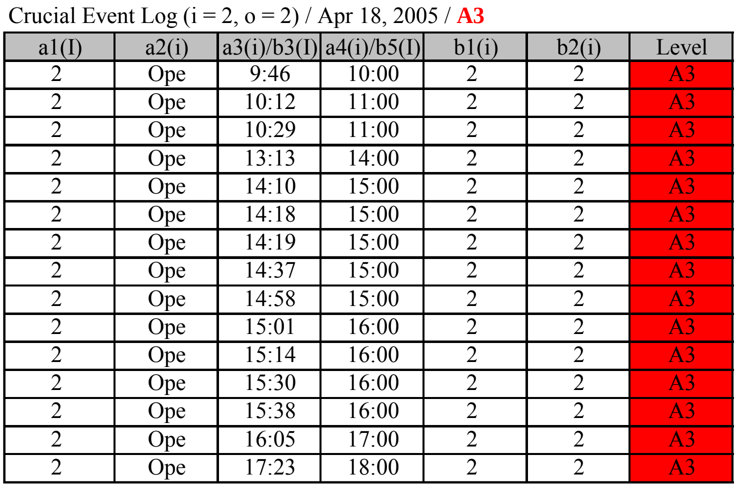
L(i, o, dy) I=1,2…5, o=1,2…4 / dy: from Apr 18, 2005 to Apr 19, 2005 / x= 60 minutes, y = 2

i , o	L	i , o	L	i , o	L	i , o	L
1, 1	0.7	1, 2	2.7	1, 3	0.9	1, 4	0.7
2, 1	2.3	**2, 2**	**9.7**	2, 3	3.2	2, 4	2.4
3, 1	1.5	3, 2	6.4	3, 3	2.1	3, 4	1.6
4, 1	1.4	4, 2	5.8	4, 3	1.9	4, 4	1.4
5, 1	0.9	5, 2	3.8	5, 3	1.3	5, 4	1.0

A1
A2
A3

Table 41: The Final Estimated Statistical Analyzed Audit Level

According the table, the event log, which involve User ID = 2 and Object Type = 2, is the most crucial event log. It is assessed as the crucial audit log level "A3". The crucial event log will be grouped by A3 audit level, thus the event logs are screened as follows.



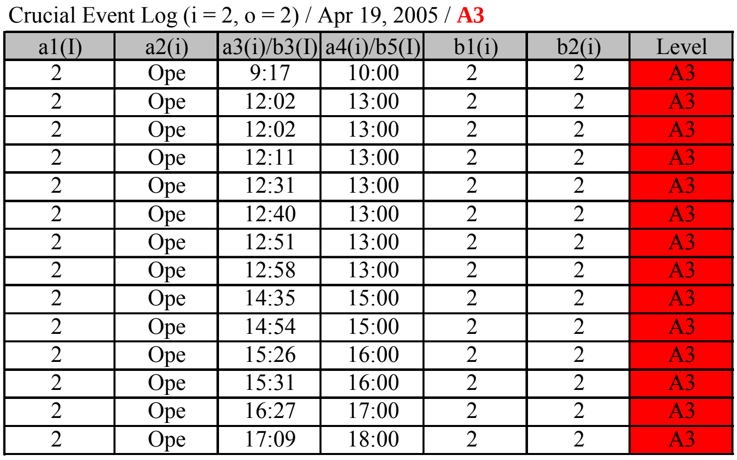
Crucial Event Log (i = 2, o = 2) / Apr 18, 2005 / **A3**

a1(I)	a2(i)	a3(i)/b3(I)	a4(i)/b5(I)	b1(i)	b2(i)	Level
2	Ope	9:46	10:00	2	2	A3
2	Ope	10:12	11:00	2	2	A3
2	Ope	10:29	11:00	2	2	A3
2	Ope	13:13	14:00	2	2	A3
2	Ope	14:10	15:00	2	2	A3
2	Ope	14:18	15:00	2	2	A3
2	Ope	14:19	15:00	2	2	A3
2	Ope	14:37	15:00	2	2	A3
2	Ope	14:58	15:00	2	2	A3
2	Ope	15:01	16:00	2	2	A3
2	Ope	15:14	16:00	2	2	A3
2	Ope	15:30	16:00	2	2	A3
2	Ope	15:38	16:00	2	2	A3
2	Ope	16:05	17:00	2	2	A3
2	Ope	17:23	18:00	2	2	A3

Figure 19: The Crucial Event Log on Apr 18, 2005

The crucial event logs will be moved to read only media to protect them from being modified or erased by hackers. The amount of event log is decreased from 100 to

15 for Apr 18, 2005; the dynamic policy contributes to decrease the even log by 85%.



Crucial Event Log (i = 2, o = 2) / Apr 19, 2005 / **A3**

a1(I)	a2(i)	a3(i)/b3(I)	a4(i)/b5(I)	b1(i)	b2(i)	Level
2	Ope	9:17	10:00	2	2	A3
2	Ope	12:02	13:00	2	2	A3
2	Ope	12:02	13:00	2	2	A3
2	Ope	12:11	13:00	2	2	A3
2	Ope	12:31	13:00	2	2	A3
2	Ope	12:40	13:00	2	2	A3
2	Ope	12:51	13:00	2	2	A3
2	Ope	12:58	13:00	2	2	A3
2	Ope	14:35	15:00	2	2	A3
2	Ope	14:54	15:00	2	2	A3
2	Ope	15:26	16:00	2	2	A3
2	Ope	15:31	16:00	2	2	A3
2	Ope	16:27	17:00	2	2	A3
2	Ope	17:09	18:00	2	2	A3

Figure 20: The Crucial Event Log on Apr 19, 2005

On Apr. 19, 2005, the event log size will decrease from 100 to 14; it is 86% decrease. If the same information policy is applied for similar event logs, the event log size will decrease. It will be possible to check and analyze the important event logs and will help the engineers to reduce their amount of work.

As shown in this section, this dynamic policy contributes to discriminate between more important log information and less important log information with the dynamic usage of statistical techniques depending on users' behavior and object confidentiality, and show more crucial event log information. This results in reducing engineers' tasks and ensuring that they will give their attention to checking the crucial event log.

In this chapter, both static and dynamic information policies were presented. With regard to current security breaches, the static information policy by itself does not have the capability to solve the problems. Dynamic policy is able to play a main role in solving current security breaches. The two dynamic policies shown in this section are very useful and easy to understand. Following the approach shown in this section, other dynamic policies will be created easily. The two dynamic policies in this chapter will be taken into account regarding the system model in the next chapter.

5. Developing the Security Model with UML

The security model preventing three cases of security breach [SB-07], [SB-12] and [SB-13] presented in the chapter 3 will be developed through the sample credit card online system. Some components, objects and classes, are re-used for other system models. At the beginning, the sample system boundary, use case and scenario are presented in order to show the sample system overview. For next section, system structure models are presented. The system models show structural model design for the security model such as class and object diagrams with usage of UML 2.0. The model is capable for the static and dynamic information policy preventing the security breach [SB-07], [SB-12] and [SB-13]. For the final section of this chapter, some system behavior models are presented such as activity diagrams, and state chart diagrams. Through the behavioral system models, the security model will be readily usable as some ideas are re-useable for other systems requiring benefited security. The behavioral system models are also capable for the static and dynamic policy.

5-1 Sample System Overview

5-1-1. System Boundary

Personal credit card information is the most targeted privacy information for outsider and insider hackers since many people utilize online credit card shopping and the Internet is used for many of the transactions. As shown in chapter 3 of this thesis, the higher risk security breach occurs through insider and outsider hacking. For security model demonstration purposes, the credit card online system is the suitable. The sample system will be shown on the next page. The following are the boundaries for the system:

Outline Requirement

- Customer is able to access his credit card account via the Internet to refer his credit card statement
- Customer may change the credit card account password
- Operator is able to access the customer's information from LAN in headquarters office and the web site in a branch office
- Operator may send a letter concerning customer's credit statement
- Operator may consult user's credit statement
- Operator may modify, add, and delete customer's information
- Administrator is able to access the customer's information from LAN in headquarters office and the web site in a branch office
- Administrator may access to the customer information for maintenance
- The system sample involves security breach threats, customers could be malicious outsider hackers, operators and administrators could be malicious insiders
- A Dynamic Policy Engine Server will be included so as to provide the two dynamic policies presented in the previous chapter.

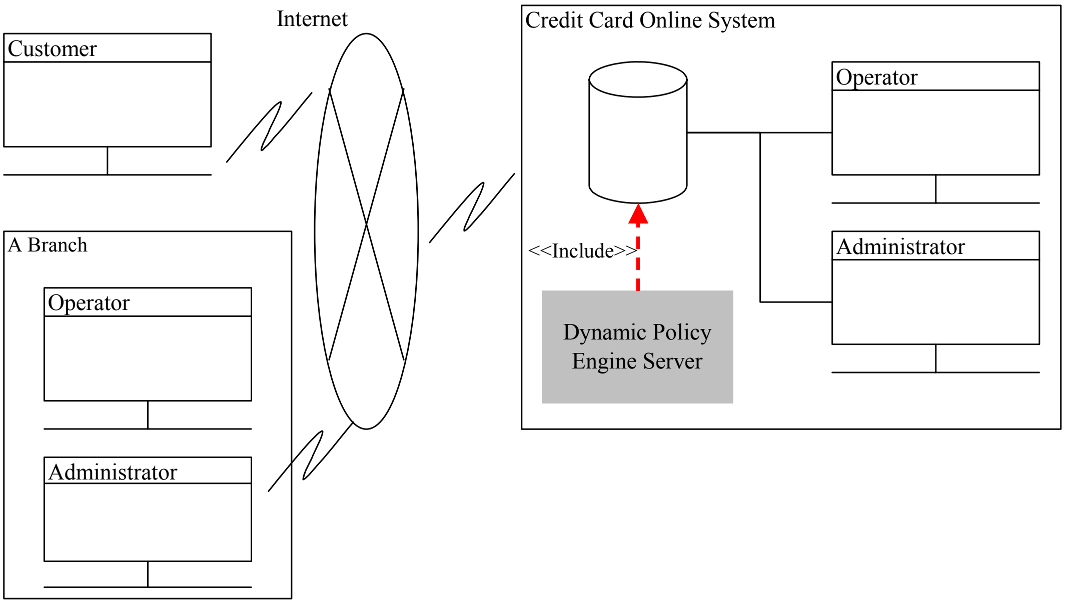


Figure 21: Sample Credit Card Online System

5-1-2. Use Case

Use cases are useful in order to examine all actors, and the relationships between the actors and the system. The use case diagram for the system concerned the security model is presented below:

- Customer: A Credit Account Owner
- Operator: Credit Card Online System Operator
- Administrator: Credit Card Online System Administrator

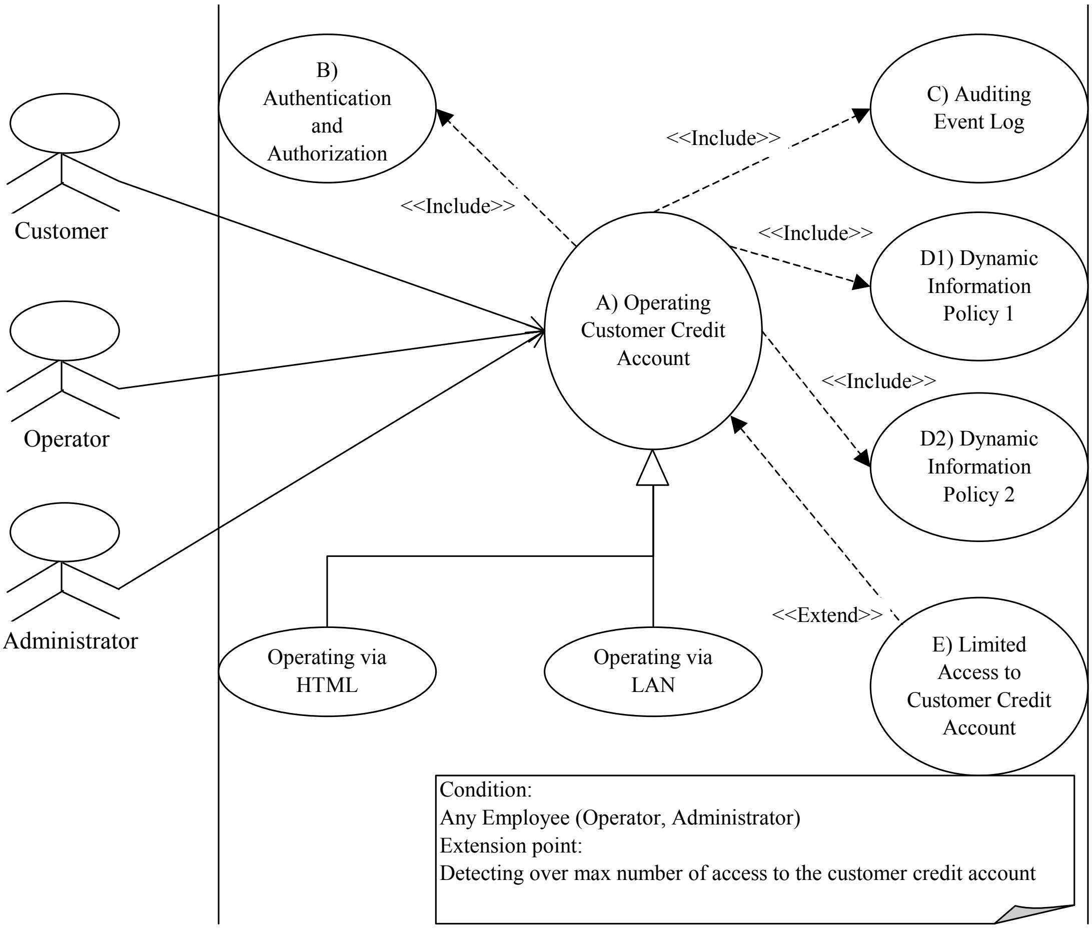

B) Authentication and Authorization
C) Auditing Event Log
<<Include>>
<<Include>>
<<Include>>
<<Include>>
Customer
D1) Dynamic Information Policy 1
A) Operating Customer Credit Account
Operator
D2) Dynamic Information Policy 2
Administrator
<<Extend>>
Operating via HTML
Operating via LAN
E) Limited Access to Customer Credit Account
Condition:
Any Employee (Operator, Administrator)
Extension point:
Detecting over max number of access to the customer credit account

Figure 22: Use Case for the Secured System Model

5-1-3. Scenarios

A scenario is a particular activity path for the system. The scenario demonstrates the system flow and system purposes. Scenarios for each use case component are presented below:

A-1. Normal Transaction with Customer

A.1-1. Customer accesses the credit card online system via web site.

A.1-2. Credit card online system shows the authentication window.

A.1-3. The customer enters his/her "account No.", "account password" and "web access password" and submits to the system. This event will be recorded.

A.1-4. The customer is approved to access the online system. This event will be recorded.

A.1-5. Store the following information into the working memory in the system, "account No.", "access IP address", "access thread ID", "login time", and "expiration time", and add this information into the returning data to the customer.

A.1-6. The online system shows the customer account statement via the web site.

A.1-7. Customer checks his/her own credit card account statement. The access is allowed only for his or her own account and followed with the access control matrix provided by the customer information object.

A.1-8. The customer disconnects from the connection to the online system. This event will be recorded.

A.1-9. The online system disconnects the customer service and shows the service ending windows.

A-2. Normal Transaction with Operator and Administrator

A.2-1. Operator or administrator accesses the credit card online system via web site or LAN.

A.2-2. Credit card online system shows the authentication window.

A.2-3. The operator or administrator use his/her "user ID" and "biometric data" to access the system. This event will be recorded. (The access is allowed from only exclusive computers for this system.)

A.2-4. The operator or administrator is approved to access the online system. This event will be recorded.

A.2-5. Store the following information into the working memory in the system, "user ID", "access IP address", "access thread ID", "login time", and "expiration time", and add this information into the returning data to the operator or administrator.

A.2-6. The online system shows the online system main menu to handle the customer information via web site or LAN.

A.2-7. The operator or administrator consults customer information with its "account No.". This event will be recorded.

A.2-8. The system shows the customer information corresponding to the "account No.".

A.2-9. A.2-7 and A.2-8 may be repeated.

A.2-10. The operator or administrator disconnects from the connection to the online system. This event will be recorded.

A.2-11. The online system disconnects the service and shows the service ending windows. This event will be recorded.

A-3. Invalid Authentication with Customer

A.3-1. Customer accesses the credit card online system via web site.

A.3-2. Credit card online system shows the Authentication window.

A.3-3. The customer enters his/her “account No.”, “account password” and “web access password” into the system. This event will be recorded.

A.3-4. The input data is invalid to access the online system. This event will be recorded.

A.3-5. A.3-3 and A.3-4 transactions are repeated 2 times.

A.3-6. The customer account status will move to "Prohibited" state.

A.3-7. The customer needs to call the customer center to verify the customer authentication information and recover his/her account status normally.

A-4. Invalid Authentication with Operator and Administrator

A.4-1. Operator or administrator accesses the credit card online system via web site or LAN.

A.4-2. Credit card online system shows the Authentication window.

A.4-3. The operator or administrator uses “user ID” and “biometric data” to access the system. This event will be recorded. (The access is allowed from only exclusive computers for this system.)

A.4-4. The biometric information is invalid to access the online system. This event will be recorded.

A.4-5. A.4-3 and A.4-4 transactions are repeated 2 times.

A.4-6. The operator or administrator account status will move to "Prohibited" state.

A.4-7. The operator or administrator needs to call the security manager to check if there is any malicious usage, fix the problem and recover his/her account status normally.

B-1. Authentication and Authorization with Customer

B.1-1. Retrieve “account No.”, “account password” and “web access password” from the Authentication window.

B.1-2. Match the input authentication data, “account password” and “web access password” with the authentication data in customer information database corresponding to the customer “account No.”.

B.1-3. If both of the authentication data match, the system approves the customer to access the system.

B.1-4. If both of the authentication data do not match, the system sends an invalid authentication message to the customer.

B-2. Authentication and Authorization with Operator and Administrator

B.2-1. Retrieve “user ID” and “biometric data” from the authentication window.

B.2-2. Match the authentication data, “biometric data”, and the authentication in employee information database corresponding to the employee “user ID”.

B.2-3. If both of the authentication data match, the system approves the operator or administrator to access the system.

B.2-4. If both of the authentication data do not match, the system sends an invalid authentication message to the operator or administrator.

C-1. Auditing Event Log for Customer

C.1-1. Retrieve “user ID”, “access IP address” and "login time/logoff time".

C.1-2. Store the retrieved event log into the ROM media so as not to modify the event log.

C-2. Auditing Event Log for Operator and Administrator

C.2-1. Retrieve “user ID”, “user type” and “access IP address”.

C.2-2. If the login or logoff action occurs, "Login/logoff Time" is retrieved.

C.2-3. If a customer information access action occurs, the action type "Create/Read/Write/Delete", the customer’s “account No.”, “object type” and "Access Time" are retrieved.

C.2-4. If an employee information access action occurs, the action type "Create/Read/Write/Delete", the employee’s “user ID”, “object type” and "Access Time" are retrieved.

C.2-5. Store the retrieved event log into the ROM media so as not to modify the event log.

D1-1. Dynamic Information Policy 1 (Normal Procedure)

D1.1-1. The online system notifies the dynamic policy engine that the system has been activated.

D1.1-2. The dynamic policy engine server checks the event logs in the online system.

D1.1-3. The dynamic policy engine server retrieves the following data: “user ID”, “user type”, “check time”, “first access time”, “last access time”, and “number of accesses (up to the last access time)” for each user (employee).

D1.1-4. Repeat D1.1-2 and D1.1.3 every certain specified minute.

D1.1-5. At the end of day, the dynamic policy engine server processes the retrieved data from the event logs statistically according to the procedure for dynamic policy 1, and stores the statistical data.

D1.1-6. On every certain specified day, the dynamic policy engine server determines the average number of accesses and standard deviation. The max number of accesses is determined for each warning level.

D1-2. Dynamic Information Policy 1 (Detected illegal number of accesses)

D1.1-1. The online system notifies the dynamic policy engine that the system has been activated.

D1.2-2. The dynamic policy engine server checks the event logs in the online system.

D1.2-3. The dynamic policy engine server retrieves the following data: “user ID”, “user type”, “check time”, “first access time”, “last access time”, and "number of accesses (up to the last access time)” for each user (employee).

D1.2-4. Repeat D1.2-2 and D1.2.3 every certain specified minute.

D1.2-5. If more than or equal to the average number of accesses plus 3 times of the standard deviation determined in the last period is detected in a number of accesses for an operator or administrator, the engine notifies the system that the “user ID” is at the warning level 1.

D1.2-6. Repeat D1.2-2 and D1.2.3 every certain minute.

D1.2-7. If more than or equal to the average number of accesses plus 4 times of the standard deviation determined in the last period is detected in a number of accesses for an operator or administrator, the engine notifies the system that the “user ID” is at the warning level 2.

D1.2-8. Repeat D1.2-2 and D1.2.3 every certain minute.

D1.2-9. If more than or equal to the average number of accesses plus 5 times of the standard deviation determined in the last period is detected in a number of accesses for an operator or administrator, the engine notifies the system that the “user ID” is at the warning level 3.

D1.2-10. Repeat D1.2-2 and D1.2.3 every certain minute.

D1.2-11. If more than or equal to the average number of accesses plus 6 times of the standard deviation determined in the last period is detected in a number of accesses for an operator or administrator, the engine notifies the system that the “user ID” is at the warning level 4.

D2-1. Dynamic Information Policy 2 (Normal Procedure)

D2.1-1. The online system notifies the dynamic policy engine that the system has been activated.

D2.1-2. The dynamic policy engine server checks the event logs in the online system.

D2.1-3. The dynamic policy engine server retrieves the following data: "user ID", "user type", "last access time", "check time", and "number of accesses (from the Last Check Time)" for each user (employee).

D2.1-4. The dynamic policy engine server retrieves the following data: "object type", "object confidential", "last access time", "check time", and "number of accesses (from the last check time)" to each object type (customer and employee information).

D2.1-5. Repeat D2.1-2 to D2.1.4 every certain specified minute.

D2.1-6. At the end of a day, the dynamic policy engine server processes the retrieved data from the event logs statistically according to the procedure for dynamic policy 2, and stores the statistical data.

D2.1-7. On every certain specified day, the dynamic policy engine server determines the numeric audit level for every access combination of the subject and object. The numeric audit level may be simplified such as level A1, A2 and A3.

D2-2. Dynamic Information Policy 2 (Filtering Event Logs)

D2.2-1. The online system notifies the dynamic policy engine that the system has been activated.

D2.2-2. The dynamic policy engine server checks the event logs in the online system.

D2.2-3. The system requires the dynamic policy engine server to filter the event logs with A3 audit level.

D2.2-4. The dynamic policy engine server filters the event logs using the required audit level for the system.

E-1. Limited Access to Customer Credit Account

E.1-1. The online system shows the main menu to handle the customer information via web site or LAN.

E.1-2. The operator or administrator consults customer information with its "account No.". This event will be recorded.

E.1-3. The system detects that the operator or administrator reaches warning level 1 of the dynamic policy 1.

E.1-4. The system notices the operator or administrator that its number of accesses has reached the warning level 1.

E.1-5. The system notices the manager.

E.1-6. Repeat E.1-2.

E.1-7. The system detects that the operator or administrator reaches warning level 2 of the dynamic policy 1.

E.1-8. The system notices the operator or administrator that its number of accesses has reached the warning level 2.

E.1-9. The system notices the manager if access can be permitted. If access is allowed, the customer information corresponding to the “account No.” is shown to the operator or administrator. If not, the warning window is shown and the operator is advised to contact the manager.

E.1-10. Repeat E.1-2.

E.1-11. The system detects that the operator or administrator reaches warning level 3 of the dynamic policy 1.

E.1-12. The system notices the operator or administrator that its number of accesses has reached the warning level 3.

E.1-13. Repeat E.1-9.

E.1-14. Repeat E.1-2.

E.1-15. The system detects that the operator or administrator reaches warning level 4 of the dynamic policy 1.

E.1-16. The system notices the operator or administrator that its number of accesses has reached the warning level 4.

E.1-17. The system notices the manager and forces the operator or administrator to be disconnected from the system. If the operator or administrator needs to access the system, contact with a manager or other person in charge will be required.

5-2. Structural System Model corresponding to the information policies

5-2-1. Class Description

A class in the sample system is created based on the abovementioned use case and scenario. As the first step, objects are identified from the scenarios in a use case, and then, the objects will be grouped into a class. The following table shows identified objects and the class of each use case.

Use Case	Identified Objects	Class	Explication
A) Operating Customer Credit Account	- Customer - Operator - Administrator	User instance	Enter customer, operator, and administrator information and request into the computers
	- Customer information - Employee information	User information instance	Store customer and employee information
	- Access control matrix	Access control matrix instance	Provide right of access for customer, operator and administrator
	- Authentication window - Authentication data prompt	Authentication instance	Allow customer, operator, and administrator to access stored customer and employee information
B) Authentication and Authorization	- Customer - Operator - Administrator	User instance	Enter customer, operator, and administrator authentication information on their computers.
	- Customer information - Employee information	User information instance	Store customer and employee authentication information
	- Authentication window - Authentication data prompt	Authentication instance	Authenticate access customer, operator, and administrator with stored customer and employee information
C) Auditing Event Log	- Event log	Event log instance	Audit any event log regarding operating customer account
D1) Dynamic Information Policy 1	- Retrieved data from event logs	Dynamic policy variable instance	Retrieve data for dynamic policy 1 from event logs
	- Statistical data	Dynamic policy statistical process instance	Statistical process with the retrieved data for dynamic policy 1
	- Procedure	Dynamic policy procedure instance	Procedure to determine a warning level of each user

	- Control variables - Warning level	Dynamic policy instance	Control dynamic policy 1 and store a warning level of each user
D2) Dynamic Information Policy 2	- Retrieved data from the event log	Dynamic policy variable instance	Retrieve data for dynamic policy 2 from event logs
	- Statistical data	Dynamic policy statistical process instance	Statistical process with the retrieved data for dynamic policy 2
	- Procedure	Dynamic policy procedure instance	Procedure to determine audit level of each combination of user and object
	- Control variables - Audit level	Dynamic policy instance	Control dynamic policy 2 and store a audit level of each combination of user and object
E) Limited Access to Customer Credit Account	- Warning level - Number of accesses	Limit access control instance	Control and notify warning to customer, operator, and administrator
	- Customer - Operator - Administrator - Manager	User instance	Customer, operator, and administrator are notified by a warning on their computers

Table 42: Identified Objects and Class Table

With the above table, the identified objects are grouped into 10 classes in the online credit card system. The classes' descriptions are shown in the following table. The classes are re-useable for similar systems.

Class	Description
UserPC	User (Customer, Operator, Administrator) entity class
Userinf	User's (Customer, Operator, Administrator)'s information class
DynP	Dynamic Information Policy class
DVariable	Retrieving variables class for the dynamic information policy
DStat	Statistical value class for the dynamic information policy
DProc	Procedure class for the dynamic information policy
ACM	Access control matrix class
EvLog	Event log class
Authent	Authenticating class
LimitAcc	Limited access control class

Table 43: Class Description for the Security System Model

5-2-2. Class Diagram

The following diagram is a class diagram of the sample system. Please consult references[62] for basic rules regarding the class diagram. Activity control matrix (ACM) class controls the access between "UserPC" and "UserInf." The static information policy is applied for this control. Every access and log on/off action will be recorded. According to dynamic policy, every certain specified minute, the rule engine server checks the event logs. If anomalous activity is detected, "LimitAcc" class will be activated.

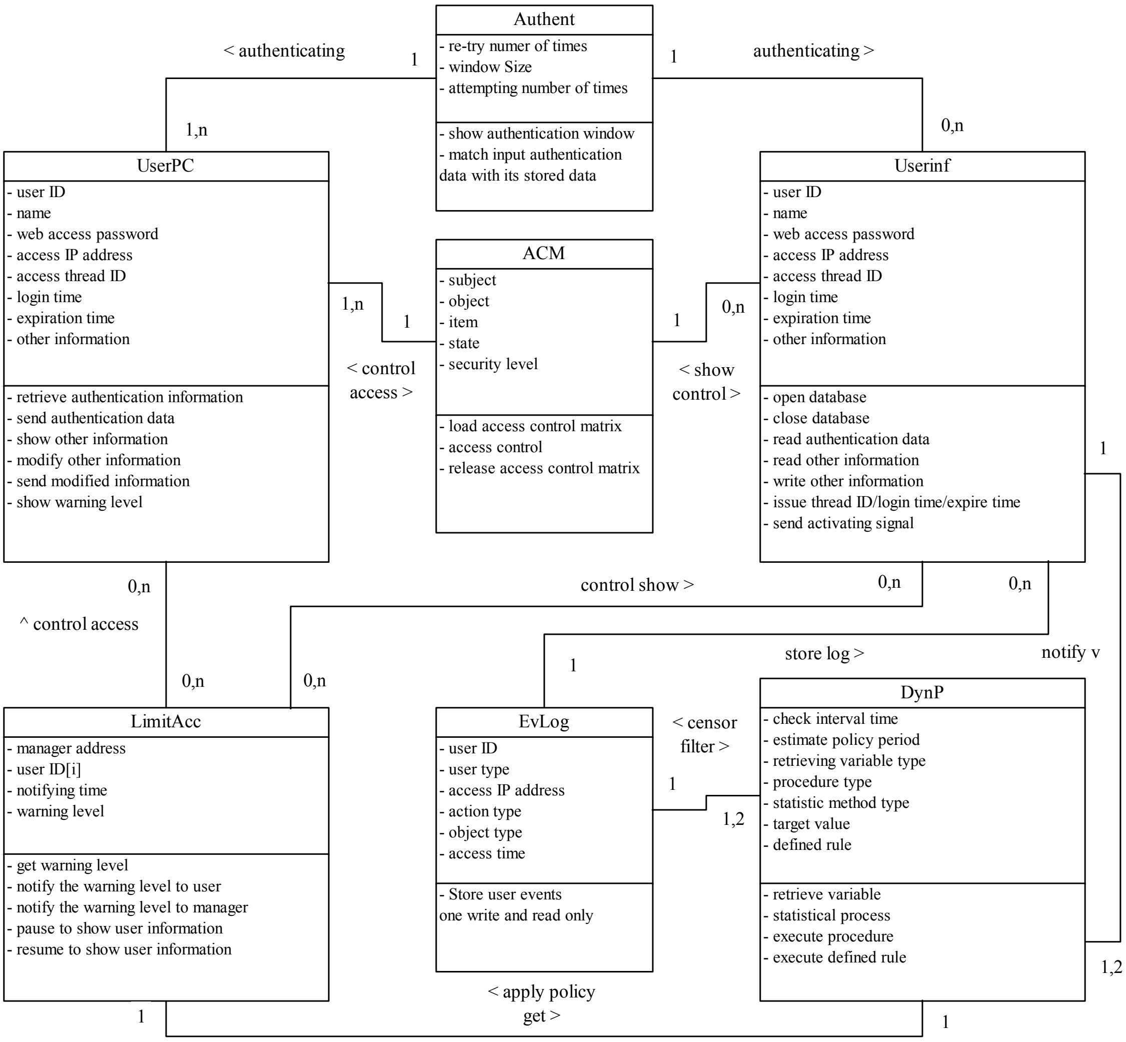


Figure 23: Class Diagram for the Security System Model (Part I)

[62] UML 2 for Dummies, Michael Jesse Chonoles, Page 20 –32 / UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 32 –38

The following additional class diagram is for the dynamic policy class. The dynamic policy consists of the “Dvariable” class (retrieve and store variables), “Dstat” class (day statistical process), and “Dproc” class (determine target value for controlling the dynamic policy).

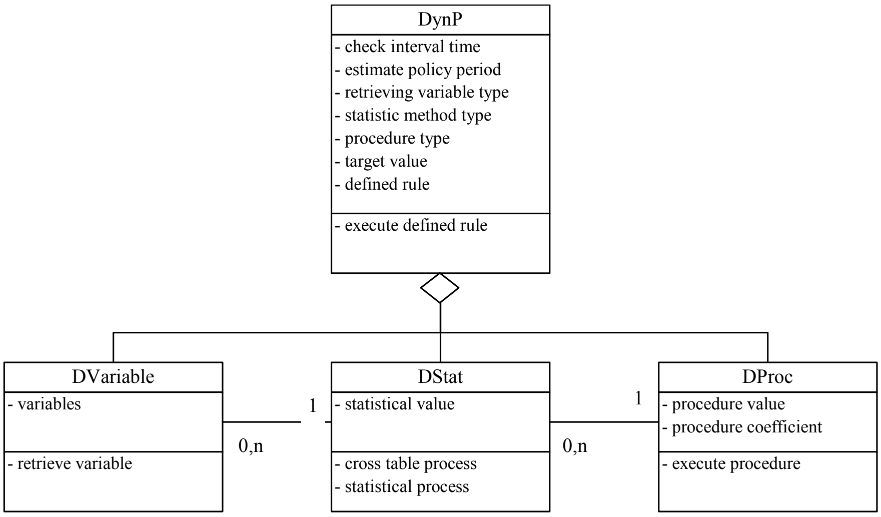


Figure 24: Class Diagram for the Security System Model (Part II)

5-2-3. Object Description

Class	Object	Description
UserPC	Admin	System administrator object for the credit card online system
UserPC	Opertr	Oprator object for the credit card online system
UserPC	Custm	Customer object for the credit card online system
Userinf	Employ	Employee information
Userinf	Custm	Customer information and credit card statement
DynP	Policy1	Dynamic information policy 1 object
DynP	Policy2	Dynamic information policy 2 object
Dvariable	Policy1	Retrieving variable from event log in the system object for dynamic information policy 1
Dvariable	Policy2	Retrieving variable from event log in the system object for dynamic information policy 2
Dproc	Policy1	Procedure for dynamic information policy 1 object to determine max number of access
Dproc	Policy2	Procedure for dynamic information policy 2 object to determine audit level
Dstat	Policy1	Statistical value to use for procedure of dynamic information policy 1
Dstat	Policy2	Statistical value to use for procedure of dynamic information policy 2
EvLog	EvLog	Event log object for the system
Authent	Authent	Authenticating user (customer, Operator, Adminstrator) object
LimitAcc	LimitAcc	Limited access control object corresponding to dynamic information policy 1

Table 44: Object Description for the Security System Model

The previous table shows objects in the sample system. The below objects are identified through the aforementioned scenarios. See the “table 42: Identified Objects and Class Table”. Some objects have the same name as their respective classes. For example, object “EvLog” has the same name as class “EvLog”. This means that “EvLog” class has only one “EvLog” object.

5-2-4. Object Diagram

UserPC class object

“Administrator”, “Operator”, and “Customer” objects inherit their attributes and methods from “UserPC” class. On the “Customer” object window, only own account is shown. On the “Operator” object window, all customer account information is shown. On the “Administrator” object window, any user involved, customer, operator, and administrator information are shown.

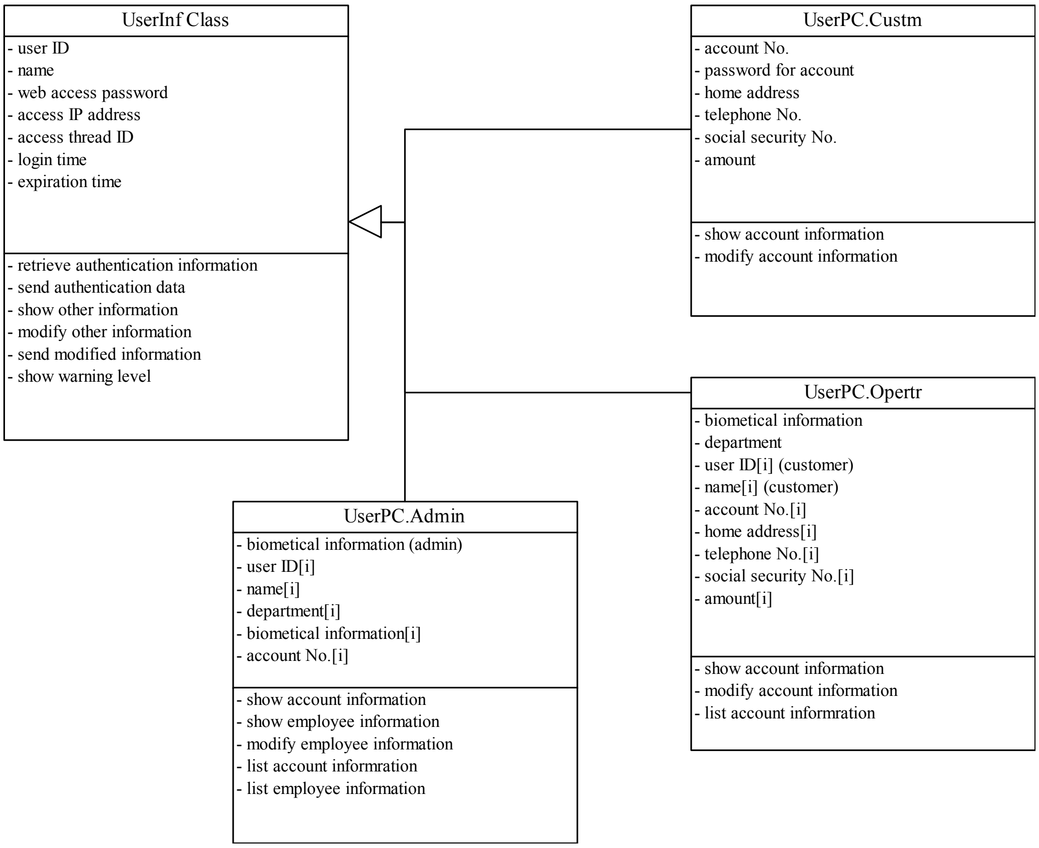


Figure 25: Object Diagram :: UserPC Class

UserInf class object

“Customer Information” Object and “Employee Information” object inherit from “UserInf” class. Customer authenticates his/her “account No.”, “password for the account” and “web access password” while employee authenticates his/her “user ID”, “web access password” and “biometric information”

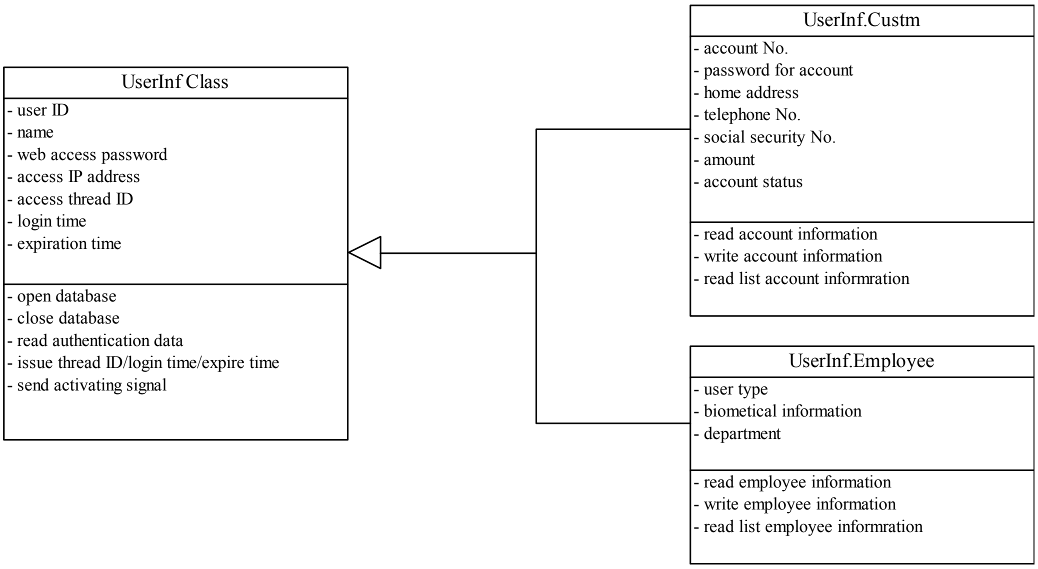


Figure 26: Object Diagram :: UserInf Class

ACM (Access Control Matrix) object

ACM class object has the following access control matrix. This matrix will be loaded into the system working memory when the system initiates. This access control matrix has updated from the access control matrix presented in the previous chapter. "Print" and "Delete" access right is added for this access control matrix.

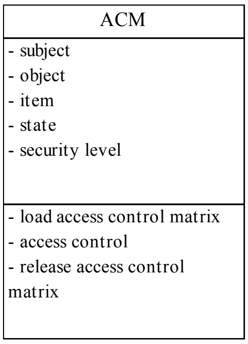


Figure 27: Object Diagram :: ACM Class

Subject	Object	Item	Level	State		
				unregistered	registered	prohibited
Customer	Customer Information	user ID	unclassified	--	--	--
		name	unclassified	--	write	--
		account No.	unclassified	--	read	--
		web access password	protected	apend	delete/apend	--
		password (account)	protected	apend	delete/apend	--
		home address	confidential	--	write	--
		telephone No.	confidential	--	write	--
		social security No.	confidential	--	write	--
		amount	confidential	--	read	--
		account status	confidential	--	--	--
Operator		user ID	unclassified	write	read/print	read/print
		name	unclassified	write	read/print	read/print
		account No.	unclassified	write	read/print	read/print
		web access password	protected	--	delete	--
		password (account)	protected	--	delete	--
		home address	confidential	write	read/print	read/print
		telephone No.	confidential	write	read/print	read/print
		social security No.	confidential	write	read	read
		amount	confidential	--	read	read
		account status	confidential	write	write/print	write/print
Administrator		user ID	unclassified	--	read/print	read/print
		name	unclassified	--	read/print	read/print
		account No.	unclassified	--	read/print	read/print
		web access password	protected	--	--	--
		password (account)	protected	--	--	--
		home address	confidential	--	--	--
		telephone No.	confidential	--	--	--
		social security No.	confidential	--	--	--
		amount	confidential	--	--	--
		account status	confidential	--	write/print	write/print
Customer	Employee Information	user ID	confidential	--		
		user type	confidential			
		name	confidential	--		
		web access password	protected			
		department	confidential	--		
		biometric information	protected	--		
Operator		user ID	confidential	--		
		user type	confidential	--		
		name	confidential	--		
		web access password	protected	delete/apend		
		department	confidential	--		
		biometric information	protected	write		
Administrator		user ID	confidential	write/print		
		user type	confidential	write/print		
		name	confidential	write/print		
		web access password	protected	delete/apend		
		department	confidential	write/print		
		biometric information	protected	write		

Table 45: Load Access Control Matrix for the Security System Model

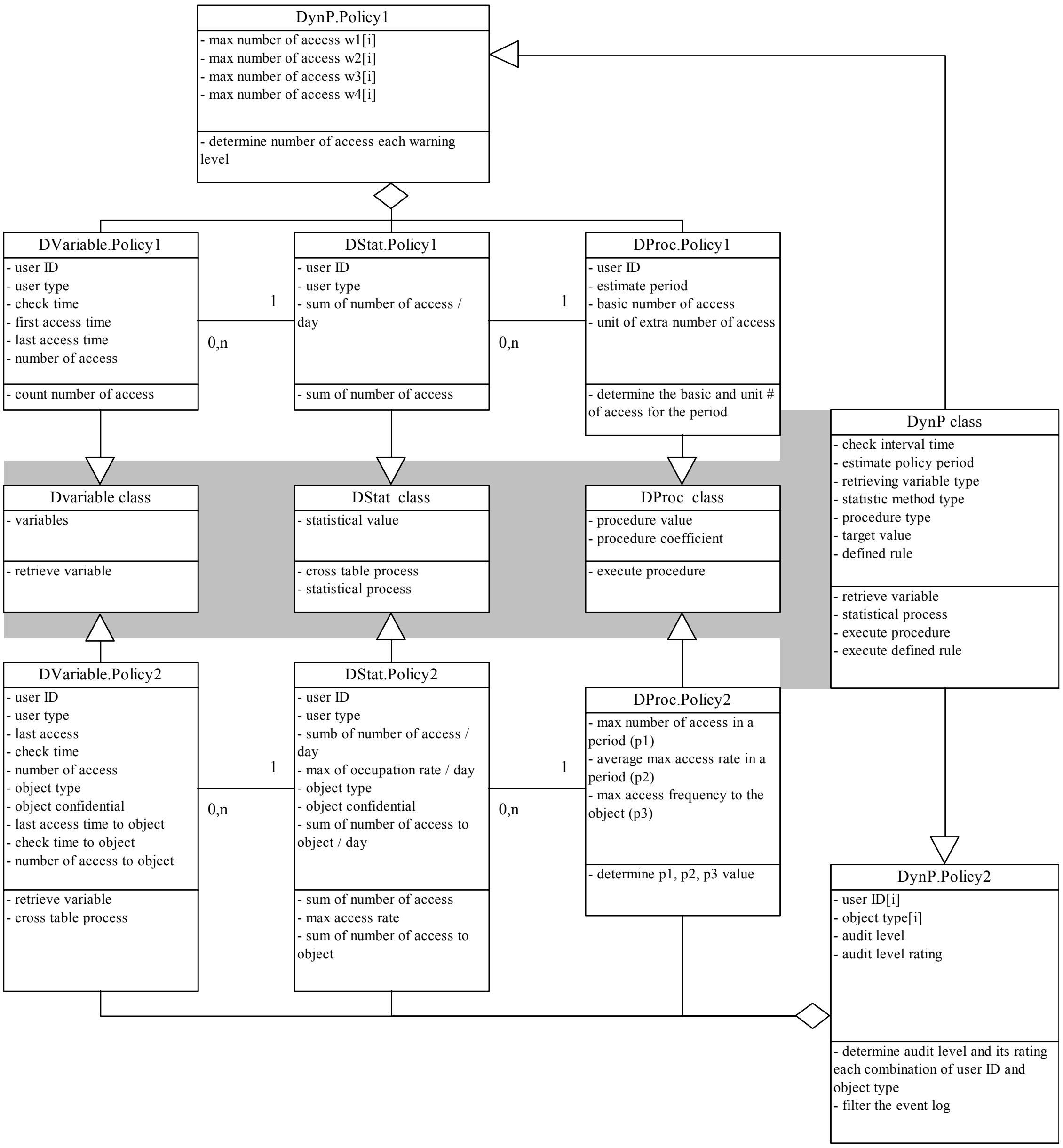


Figure 28: Object Diagram :: Dynamic Policy Class

Dynamic policy class object

The objects relating to dynamic policy are shown in the above figure. Two dynamic information policies are accounted for in the system model. Any dynamic policy consists of variable object, statistical process object, and procedure object. The variable object retrieves and stores necessary items from the event log. The statistical process object processes the retrieved variables to generate statistical values everyday. The procedure object defines some target values for controlling the dynamic policy. For example, in the previous chapter, the number of accesses for each user is retrieved and stored. The retrieved value will be the number of accesses per day through the statistical process object. Afterward, the average and standard deviation of the number of accesses during certain periods are calculated through the procedure, and then the max number of accesses for each user for next period will be estimated. Similarly, the dynamic information policy 2 is also exerted through the dynamic policy 2 objects on the previous page.

Entire Object Diagram

The whole object diagram is shown on next page. Because of limited page size, attributes and methods of each object are omitted. It is clear how the objects relate each other. For example, the dynamic policy 1 checks the event log every certain minute, and the certain value determine with three objects, "DVariable.Policy1", "DStat.Policy1" and "DProc.Policy1". If the anomaly activity is detected, the dynamic policy 1 will be applied, and "LimitAcc" is activated. For the dynamic policy 2, the certain value will be determined with the same fashion as the dynamic policy 1. Afterward, applying the dynamic policy 2, the event log will be filtered and show only higher important event log. Access between "UserPC" and "UserInf" is controlled by the ACM (access control matrix) object.

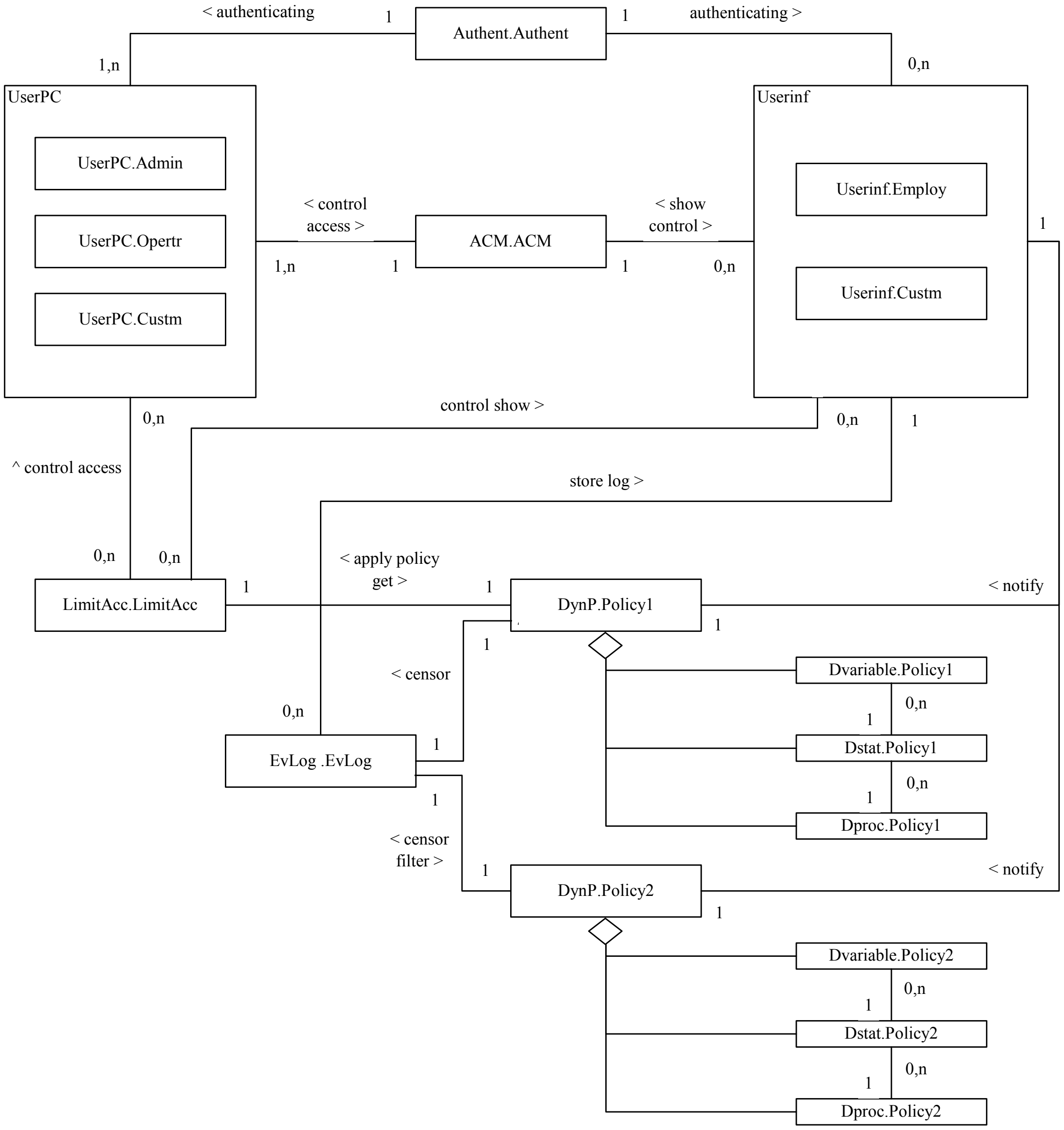


Figure 29: Object Diagram for the Security System Model

5-3. Behavioral System Model corresponding to the information policies

Behavioral system model shows how objects act in the system and communicate the other objects. Each behavioral system diagram has particular purpose. “Activity Diagram” will be presented from the behavioral diagrams provided in UML.

5-3-1. Activity Diagram

User Login

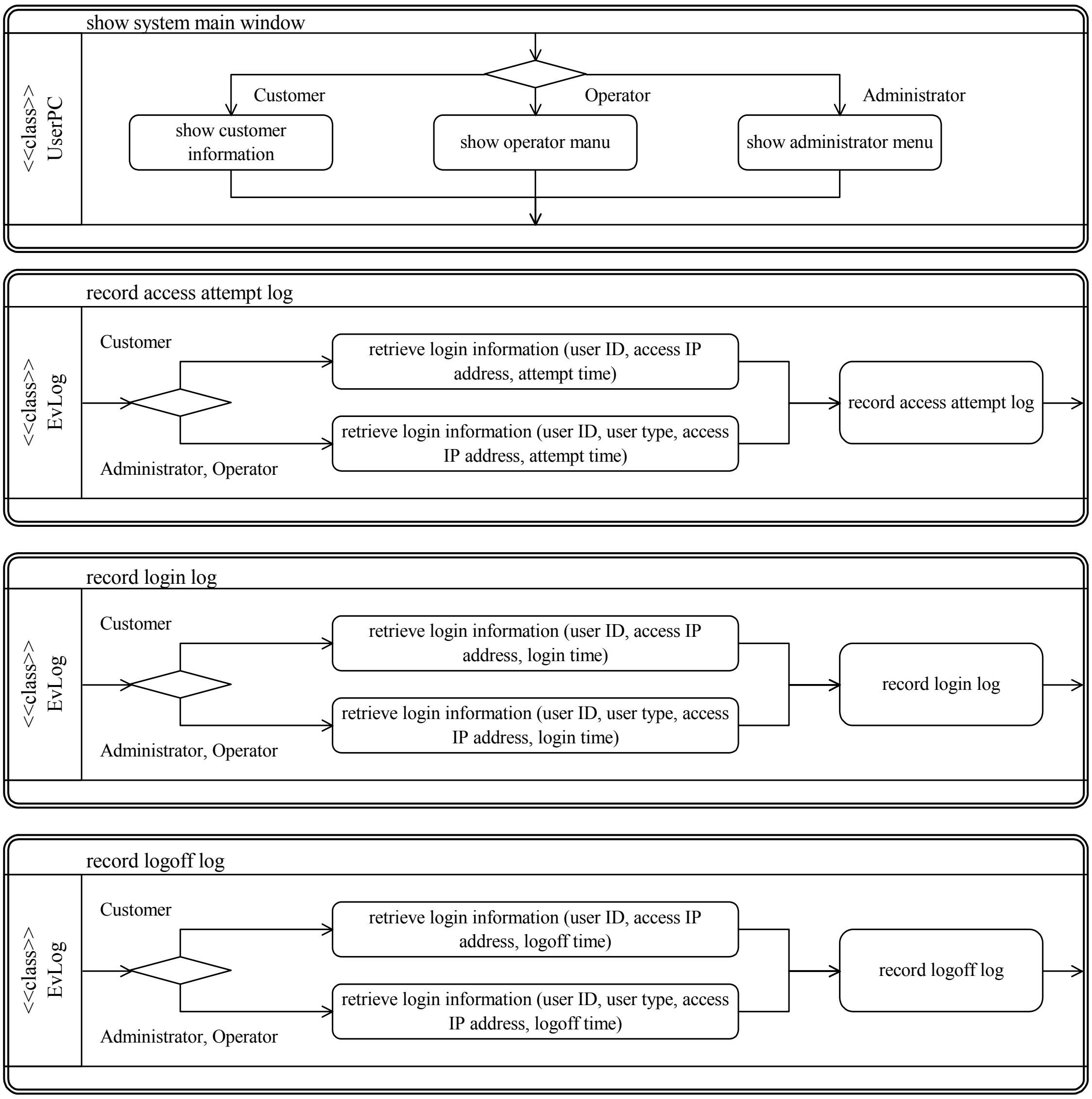

show system main window
<<class>>
UserPC
Customer
Operator
Administrator
show customer information
show operator manu
show administrator menu
record access attempt log
<<class>>
EvLog
Customer
Administrator, Operator
retrieve login information (user ID, access IP address, attempt time)
retrieve login information (user ID, user type, access IP address, attempt time)
record access attempt log
record login log
<<class>>
EvLog
Customer
Administrator, Operator
retrieve login information (user ID, access IP address, login time)
retrieve login information (user ID, user type, access IP address, login time)
record login log
record logoff log
<<class>>
EvLog
Customer
Administrator, Operator
retrieve login information (user ID, access IP address, logoff time)
retrieve login information (user ID, user type, access IP address, logoff time)
record logoff log

Figure 30: Activity Diagram for User Login (Part I)

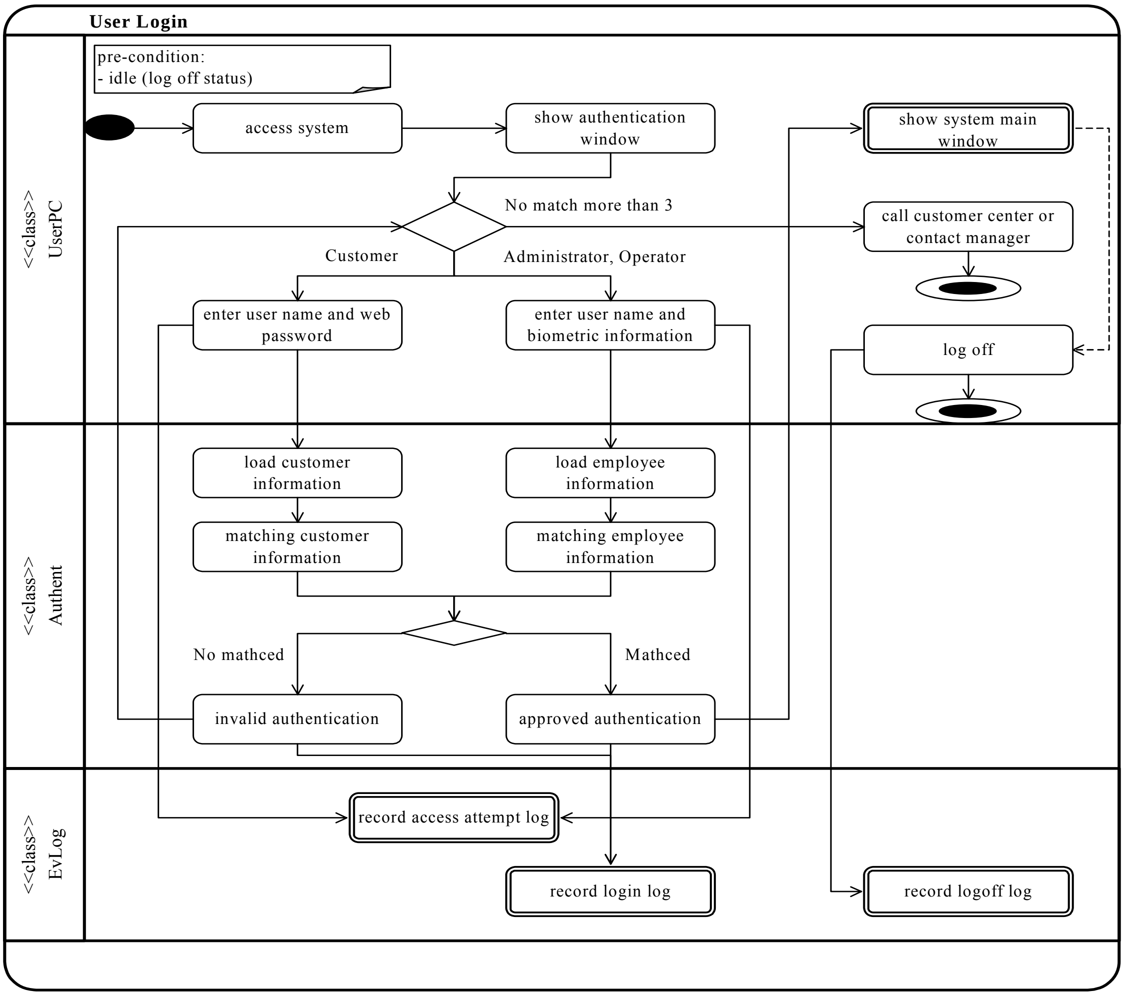


Figure 31: Activity Diagram for User Login (Part II)

Activity diagrams show how the object acts for certain function. The first activity diagram is for user login function. “UserPC” class, “Authent” class and “EvLog” classes are related to this function. The activity diagram is divided with three classes. The process belongs to its class. Its attribute and method also belong to its class. This design is introduced in UML from its version 2.0. The activity diagram shows the scenario in case of occurring valid login, invalid login. The scenario auditing event log is also included.

User Access

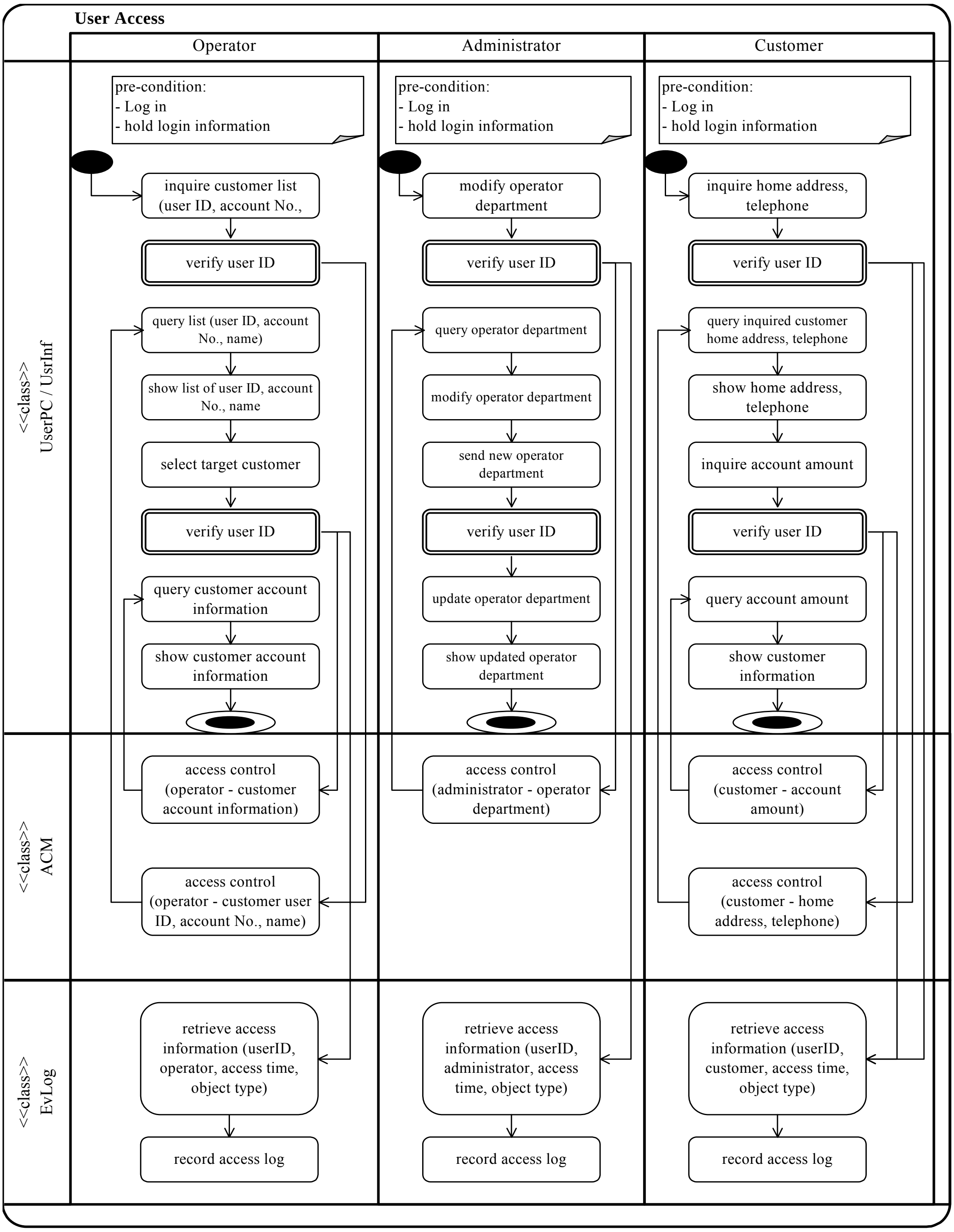

User Access
Operator
Administrator
Customer
<<class>> UserPC / UsrInf
<<class>> ACM
<<class>> EvLog
pre-condition:
- Log in
- hold login information
pre-condition:
- Log in
- hold login information
pre-condition:
- Log in
- hold login information
inquire customer list (user ID, account No.,
verify user ID
query list (user ID, account No., name)
show list of user ID, account No., name
select target customer
verify user ID
query customer account information
show customer account information
modify operator department
verify user ID
query operator department
modify operator department
send new operator department
verify user ID
update operator department
show updated operator department
inquire home address, telephone
verify user ID
query inquired customer home address, telephone
show home address, telephone
inquire account amount
verify user ID
query account amount
show customer information
access control (operator - customer account information)
access control (operator - customer user ID, account No., name)
access control (administrator - operator department)
access control (customer - account amount)
access control (customer - home address, telephone)
retrieve access information (userID, operator, access time, object type)
record access log
retrieve access information (userID, administrator, access time, object type)
record access log
retrieve access information (userID, customer, access time, object type)
record access log

Figure 32: Activity Diagram for User Access (Part I)

The second activity diagram is for user access. “UserPC” class, “ACM” class and “EvLog” class are related to this function. The activity diagram is divided by three columns, which are “Operator”, “Administrator”, and “Customer” besides of the related classes. It is very useful to compare a role with other roles and it helps the developer to understand the interface among the objects. At every access to the customer or employee information, “ACM” class is called, and then according to the access control matrix, the system allows the user to access the information. Every access event is recorded.

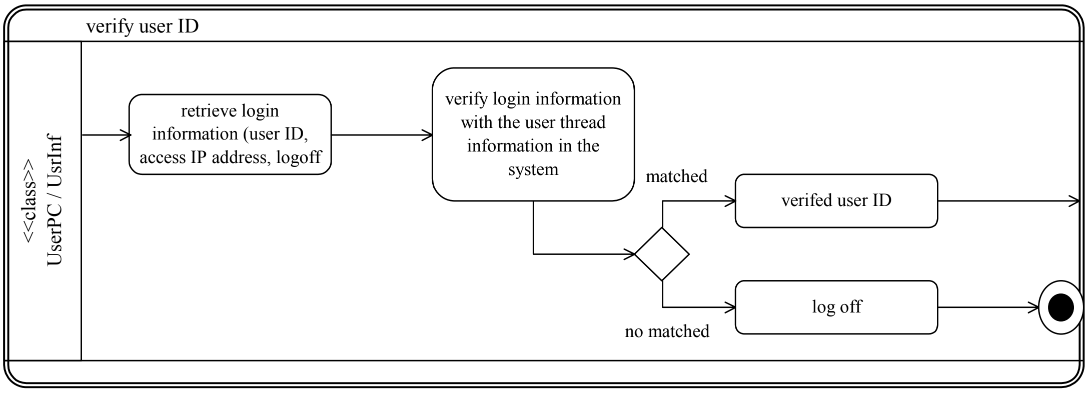

verify user ID
<<class>>
UserPC / UsrInf
retrieve login information (user ID, access IP address, logoff
verify login information with the user thread information in the system
matched
verifed user ID
no matched
log off

Figure 33: Activity Diagram for User Access (Part II)

The below sub-activity diagram shows how the system verify that the user hold the same login information such as “user ID”, “access IP address”, “access thread ID”, and “login time” as the system for the user.

Dynamic Policy 1

The next activity diagram is for dynamic policy 1. Many classes are related to the function. “DynP.Policy1” object checks the event log every certain minute. Its descendent object retrieves some necessary variables and generates statistical value. After certain period, the max number of accesses each warning level will be determined based on the procedure defined in the previous chapter. When the anomaly number of accesses is detected, the defined rule will be applied correspond to the warning level. This detection is provided by “LimitAcc” object. The following activity diagram shows this process flow clearly.

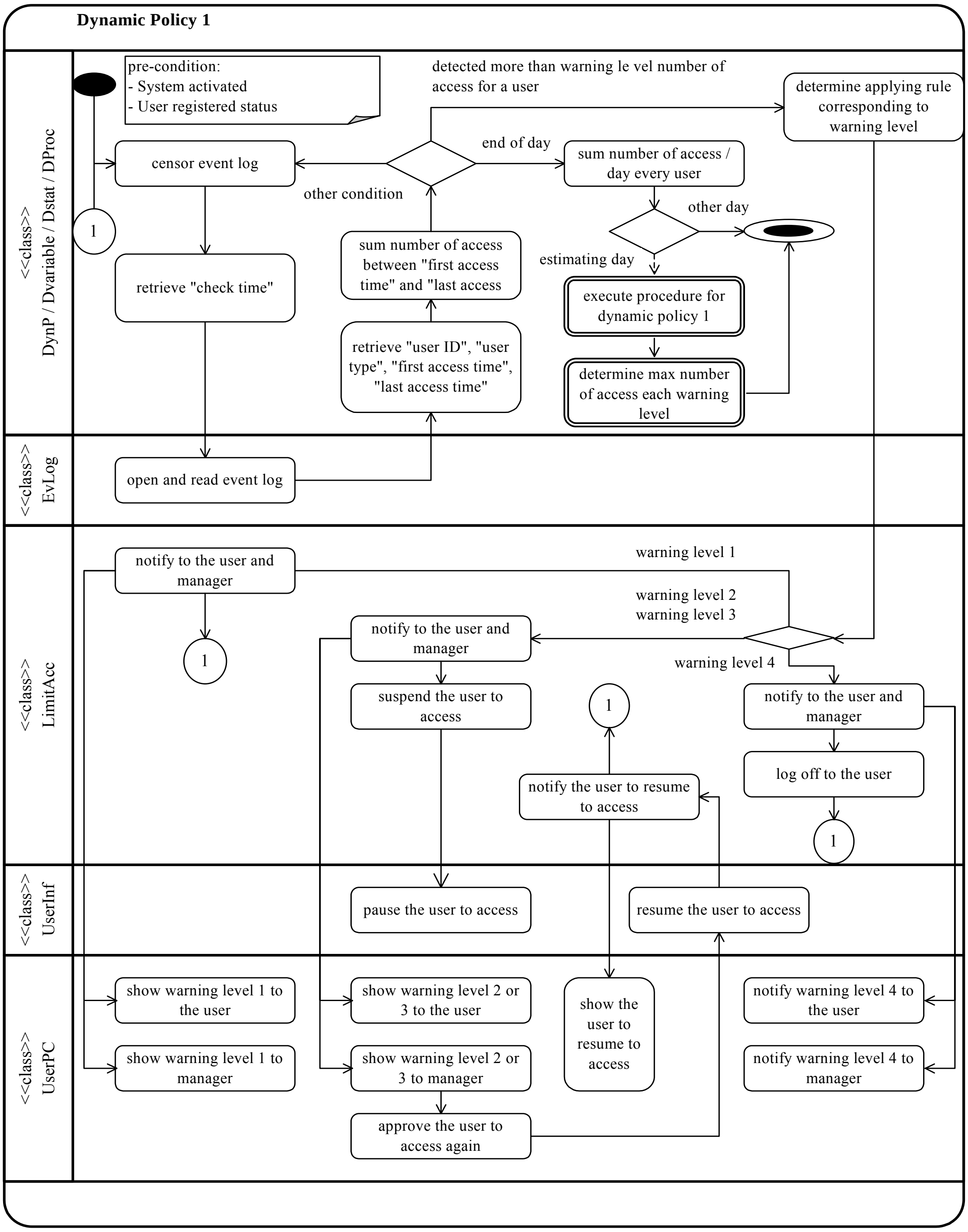

Dynamic Policy 1
<<class>> DynP / Dvariable / Dstat / DProc
<<class>> EvLog
<<class>> LimitAcc
<<class>> UserInf
<<class>> UserPC
pre-condition:
- System activated
- User registered status
detected more than warning le vel number of access for a user
determine applying rule corresponding to warning level
censor event log
end of day
sum number of access / day every user
other condition
other day
1
sum number of access between "first access time" and "last access
estimating day
retrieve "check time"
execute procedure for dynamic policy 1
retrieve "user ID", "user type", "first access time", "last access time"
determine max number of access each warning level
open and read event log
notify to the user and manager
warning level 1
warning level 2
warning level 3
notify to the user and manager
1
warning level 4
suspend the user to access
1
notify to the user and manager
log off to the user
notify the user to resume to access
1
pause the user to access
resume the user to access
show warning level 1 to the user
show warning level 2 or 3 to the user
show the user to resume to access
notify warning level 4 to the user
show warning level 1 to manager
show warning level 2 or 3 to manager
notify warning level 4 to manager
approve the user to access again

Figure 34: Activity Diagram for Dynamic Policy 1 (Part I)

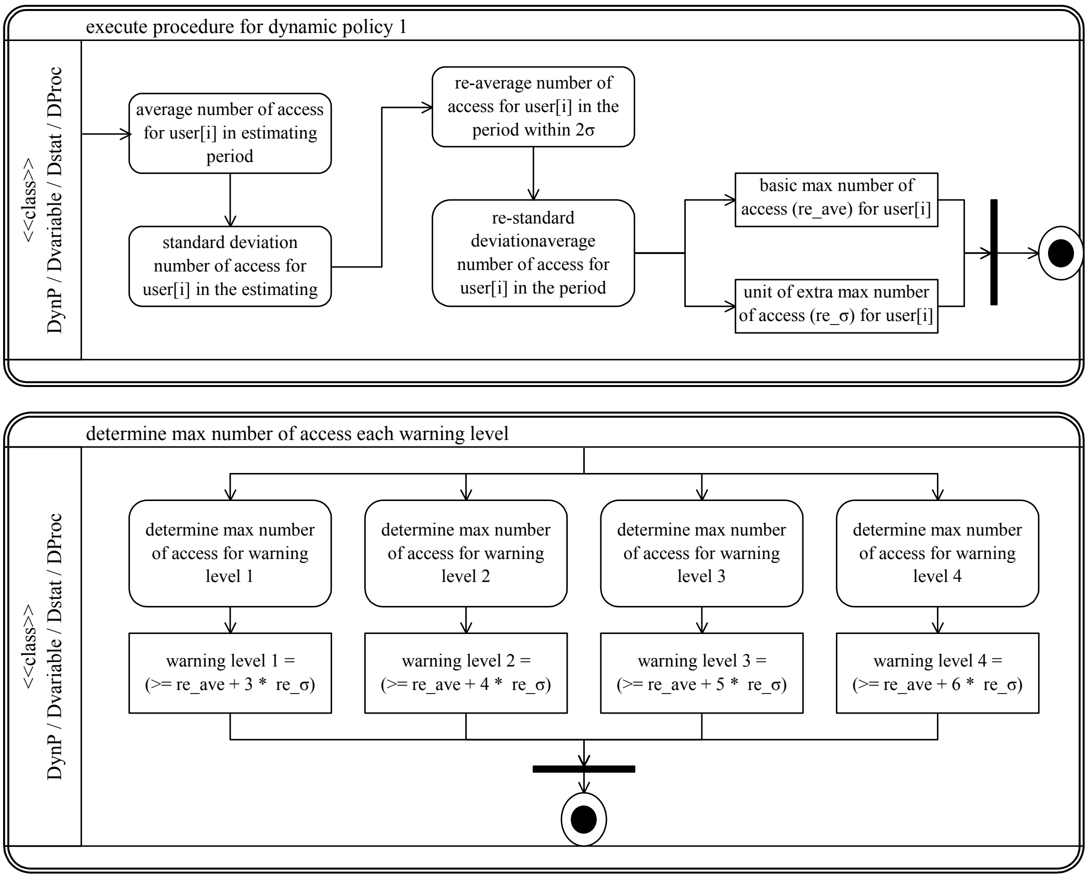

execute procedure for dynamic policy 1
<<class>>
DynP / Dvariable / Dstat / DProc
average number of access for user[i] in estimating period
standard deviation number of access for user[i] in the estimating
re-average number of access for user[i] in the period within 2σ
re-standard deviationaverage number of access for user[i] in the period
basic max number of access (re_ave) for user[i]
unit of extra max number of access (re_σ) for user[i]
determine max number of access each warning level
<<class>>
DynP / Dvariable / Dstat / DProc
determine max number of access for warning level 1
determine max number of access for warning level 2
determine max number of access for warning level 3
determine max number of access for warning level 4
warning level 1 = (>= re_ave + 3 * re_σ)
warning level 2 = (>= re_ave + 4 * re_σ)
warning level 3 = (>= re_ave + 5 * re_σ)
warning level 4 = (>= re_ave + 6 * re_σ)

Figure 35: Activity Diagram for Dynamic Policy 1 (Part II)

Dynamic Policy 2

The next activity diagram is for dynamic policy 2. “DynP.Policy2” object and “EvLog” object are related to the function. At every certain minute, the “DynP.Policy” object checks the event log, and its descendent objects retrieve the variable for the dynamic policy. Through the “DVariable.policy2” object, every user will have two values, determining the frequency of access and occupation rate among other users, to assess the unusual use level. For the same fashion for the object, the frequency of access to the object is delivered for each object.

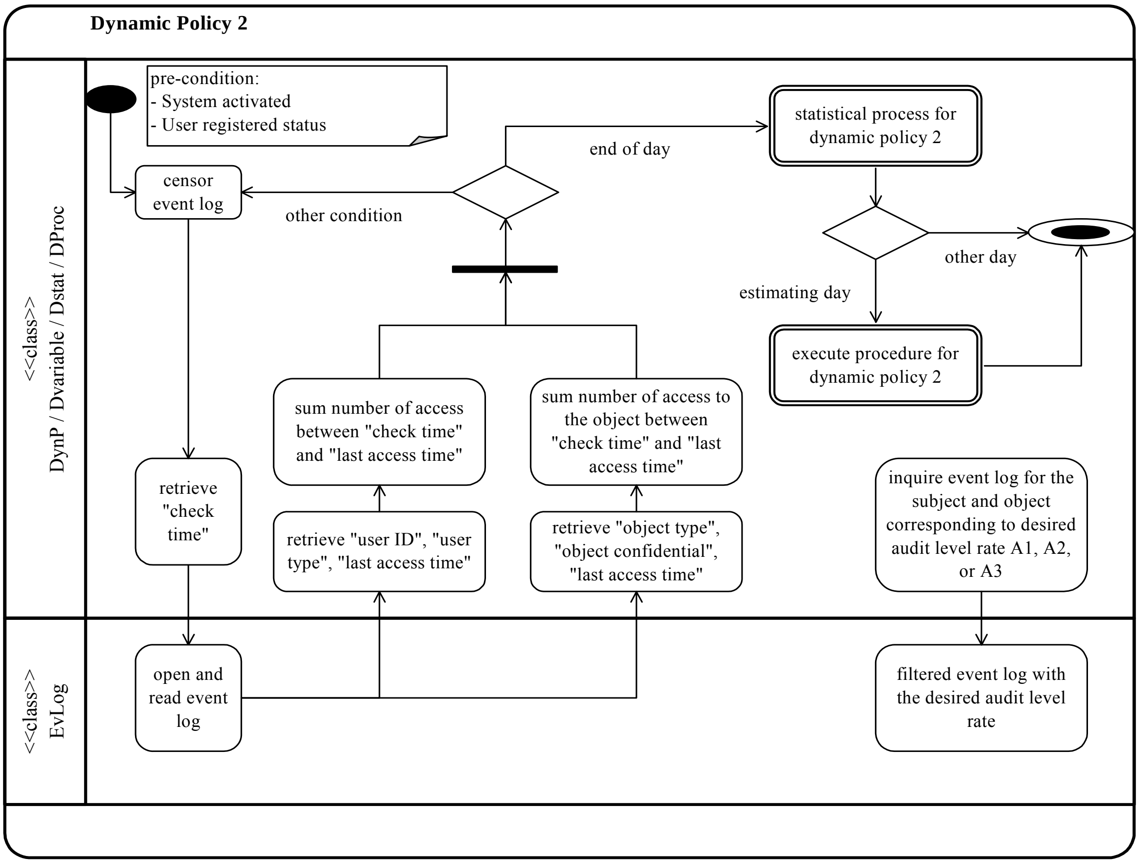

Dynamic Policy 2
<<class>>
DynP / Dvariable / Dstat / DProc
<<class>>
EvLog
pre-condition:
- System activated
- User registered status
censor event log
other condition
end of day
statistical process for dynamic policy 2
other day
estimating day
execute procedure for dynamic policy 2
sum number of access between "check time" and "last access time"
sum number of access to the object between "check time" and "last access time"
retrieve "check time"
retrieve "user ID", "user type", "last access time"
retrieve "object type", "object confidential", "last access time"
inquire event log for the subject and object corresponding to desired audit level rate A1, A2, or A3
open and read event log
filtered event log with the desired audit level rate

Figure 36: Activity Diagram for Dynamic Policy 2 (Part I)

As the same fashion as the dynamic policy 1, the statistical value generated everyday, and the audit level is determined through the “DProc.Policy2” object. The audit level will be determined every combination of user[i] and object[o]. Any event log always includes subject (who access) and object (whom accessed), so audit level value should be a linear value with the frequency of access, occupation rate among other users, and the frequency of access to the object. Audit level can be expressed as:

$$L(i, o): \text{ Event log} = \text{certain } i \text{ access certain } o$$

As a result, each event log will be deployed with the audit level. Using current audit level, only higher important event log will be shown.

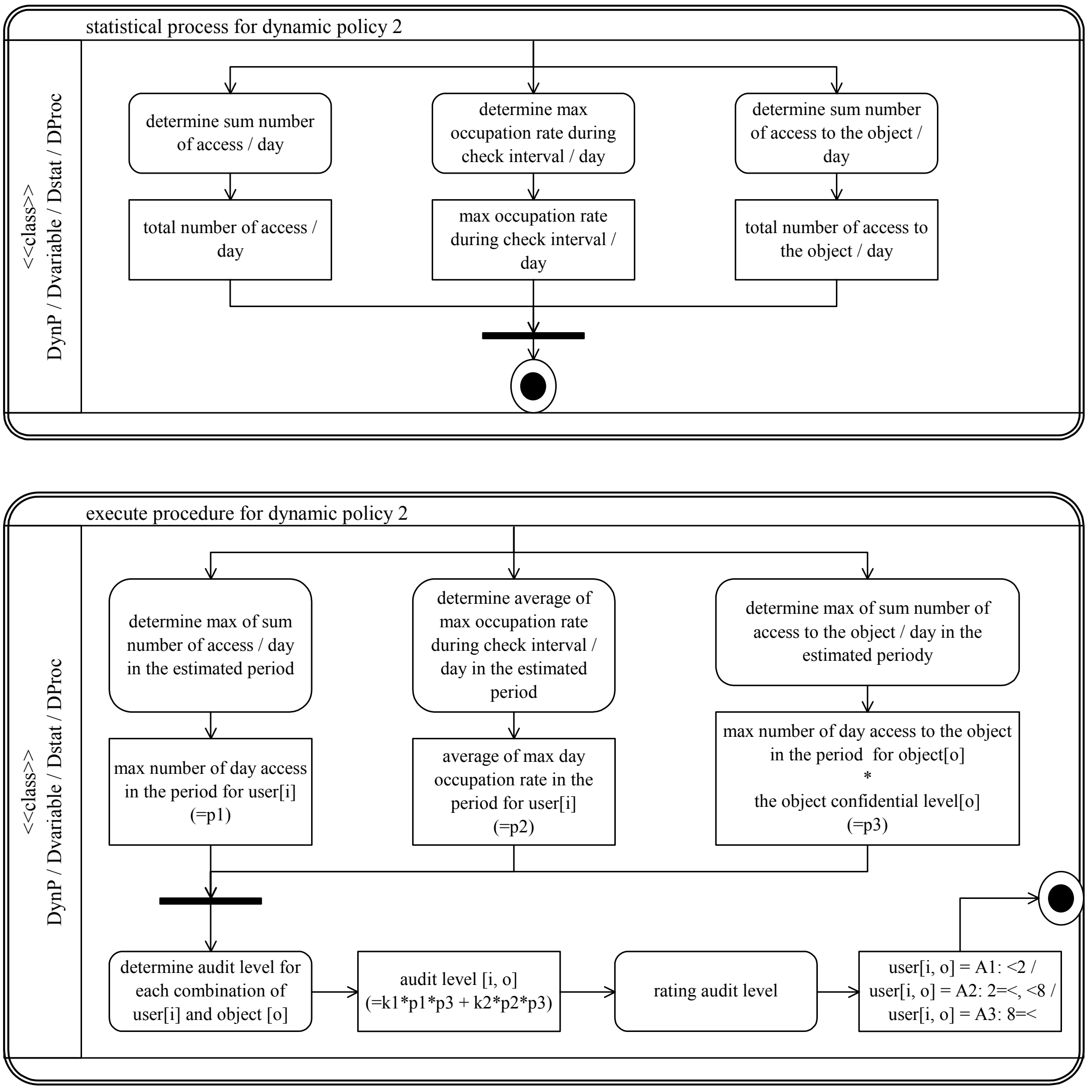

statistical process for dynamic policy 2
<<class>>
DynP / Dvariable / Dstat / DProc
determine sum number of access / day
determine max occupation rate during check interval / day
determine sum number of access to the object / day
total number of access / day
max occupation rate during check interval / day
total number of access to the object / day
execute procedure for dynamic policy 2
<<class>>
DynP / Dvariable / Dstat / DProc
determine max of sum number of access / day in the estimated period
determine average of max occupation rate during check interval / day in the estimated period
determine max of sum number of access to the object / day in the estimated periody
max number of day access in the period for user[i] (=p1)
average of max day occupation rate in the period for user[i] (=p2)
max number of day access to the object in the period for object[o] * the object confidential level[o] (=p3)
determine audit level for each combination of user[i] and object [o]
audit level [i, o] (=k1*p1*p3 + k2*p2*p3)
rating audit level
user[i, o] = A1: <2 /
user[i, o] = A2: 2=<, <8 /
user[i, o] = A3: 8=<

Figure 37: Activity Diagram for Dynamic Policy 2 (Part II)

The equation to calculate the audit level is already presented in the previous chapter. The audit level is determined with k1, k2, p1, p2, and p3. The coefficient k1 and k2 may be different from each system since the system goal, or system engineer and stakeholder policy are different at every system. For this thesis, delivered value for k1 is 0.0012, and the value for k2 is 0.065. The coefficient value is determined with 200 sample event logs. Finally, audit level should be rated with A1, A2, or A3 to be simplified the audit level assessment.

5-4. Systems Verification

The verification process is one of the most important processes for systems engineers. During the progress of the thesis, it was revealed usage of dynamic information policy reduces information risks. Through an analysis of recent security breaches, two countermeasures are recognized, and based on the analysis dynamic information policies and security mechanisms are developed. This section aims to verify whether the information policies and security mechanisms reduce the threat of information risk.

5-4-1. Test Data

It is desirable to use realistic test data containing customer access event logs to verify the security mechanism. Test data are provided in commercialized publications in Japan. For instance, J-sys software[63] released a test data generator, ER/DataGen[64]. This tool generates test data based on ER (entity relationship) diagrams[65], database specification such as table name and field name, defined items such as customer name and account number, and malicious activity scenarios. Another company, Aglaia Co.[66] provides customized test data through a consultation and briefing. Aglais Co. has kindly

[63] J-sys software co., ltd. homepage, http://www.jsys.co.jp

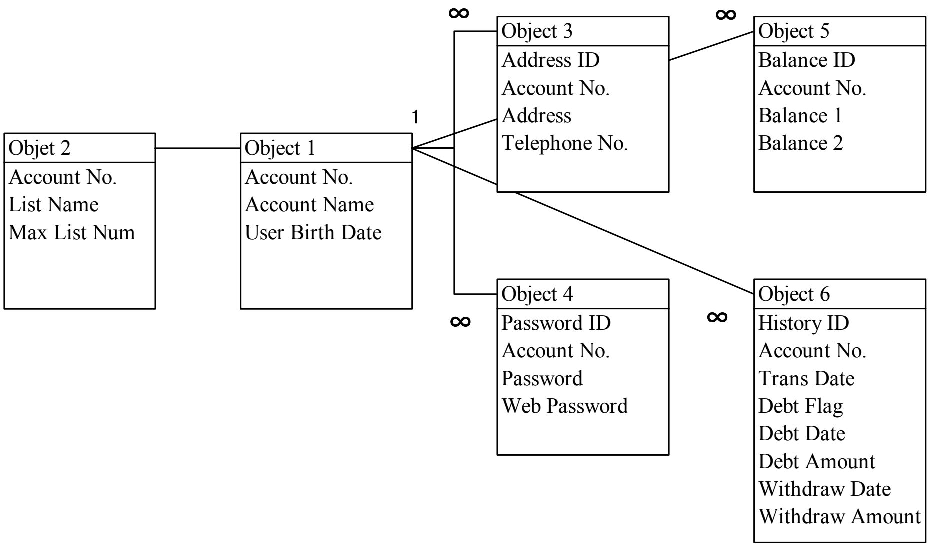
[64] ER/DataGen Catalog http://www.jsys-products.com/download/catalog/ERDataGen_200502.pdf

[65] Entity-Relationship Diagrams (ERD), http://www.umsl.edu/~sauter/analysis/er/er_intro.html

[66] Aglaia Co. Homepage, http://aglaia.cc/profile.html

provided simple test data used for information leak tests for the research purpose. The following specification is used to generate the test data.

□ Entity-Relationship Diagram and Table Structure



□ Items

Subject	
1	Yukiko Tanaka
2	Tsutomu Maebashi
3	Shinichi Sekine

** Assumed Users

Object (Item)	
1	Accoun No., Name, Birth
2	Account List (low level)
3	Address, Telephone No.
4	Password (unvisible)
5	Balance
6	Account History

□ Malicious Scenario

- On Feb. 17, 2003, “User3” stole 30 customers’ account balance information during a lunch break (12:00PM – 13:00PM).
- On Feb. 18, 2003, “User3” stole 35 customers’ credit history during a lunch break (12:00PM – 13:00PM).

Figure 38: Required Material to Generate Test Data

Two malicious activities by user3 must be detected by static and dynamic policies. It results in reducing information risk.

5-4-2. Data Analysis

The test data are analyzed with the aforementioned security mechanism based on a dynamic information policy in chapter 4. The following steps are shown in the security mechanism.

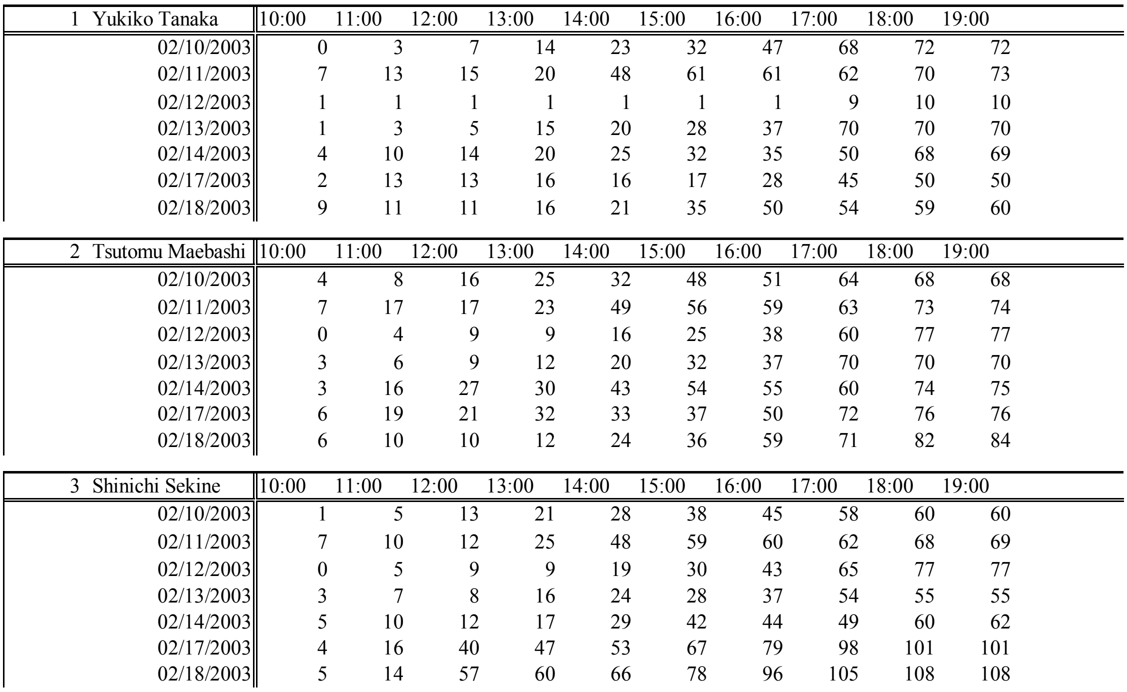
- Step 1. Identify necessary variables
- Step 2. Statistical process
- Step 3. Performing procedure

Data analysis for each dynamic policy is shown as follows.

Dynamic Information Policy 1: (*Censor not only contents but also the amount*)

Step 1: Identify necessary variables

Access date, access time, user ID, and number of accesses every 10 minutes are tracked. The following table shows the number of accesses accumulated every hour. It would be most desirable to show the accumulated number every 10 minutes. However, this has been reduced for lack of space.



1 Yukiko Tanaka	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00
02/10/2003	0	3	7	14	23	32	47	68	72	72
02/11/2003	7	13	15	20	48	61	61	62	70	73
02/12/2003	1	1	1	1	1	1	1	9	10	10
02/13/2003	1	3	5	15	20	28	37	70	70	70
02/14/2003	4	10	14	20	25	32	35	50	68	69
02/17/2003	2	13	13	16	16	17	28	45	50	50
02/18/2003	9	11	11	16	21	35	50	54	59	60

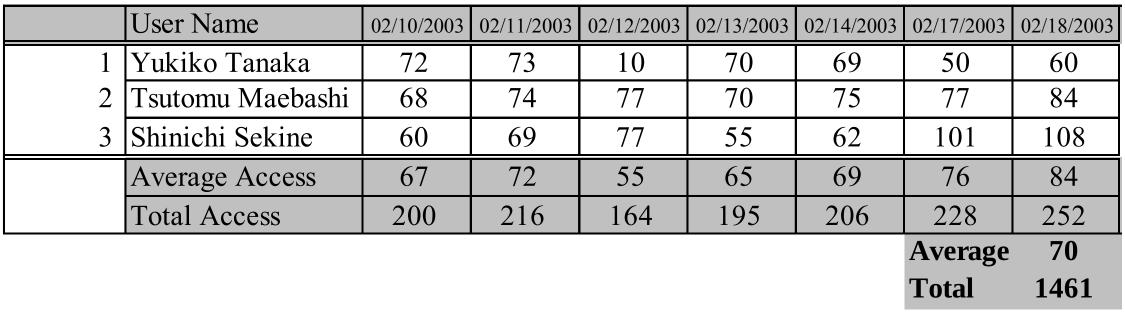
2 Tsutomu Maebashi	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00
02/10/2003	4	8	16	25	32	48	51	64	68	68
02/11/2003	7	17	17	23	49	56	59	63	73	74
02/12/2003	0	4	9	9	16	25	38	60	77	77
02/13/2003	3	6	9	12	20	32	37	70	70	70
02/14/2003	3	16	27	30	43	54	55	60	74	75
02/17/2003	6	19	21	32	33	37	50	72	76	76
02/18/2003	6	10	10	12	24	36	59	71	82	84

3 Shinichi Sekine	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00
02/10/2003	1	5	13	21	28	38	45	58	60	60
02/11/2003	7	10	12	25	48	59	60	62	68	69
02/12/2003	0	5	9	9	19	30	43	65	77	77
02/13/2003	3	7	8	16	24	28	37	54	55	55
02/14/2003	5	10	12	17	29	42	44	49	60	62
02/17/2003	4	16	40	47	53	67	79	98	101	101
02/18/2003	5	14	57	60	66	78	96	105	108	108

Figure 39: Datasheet of Number of Accesses by User 1, 2, and 3

Step 2: Statistical Process

Amounts of number of accesses for users from Feb. 10, 2003 to Feb. 18, 2003 are totaled every day. The following table is the totaled number of accesses.



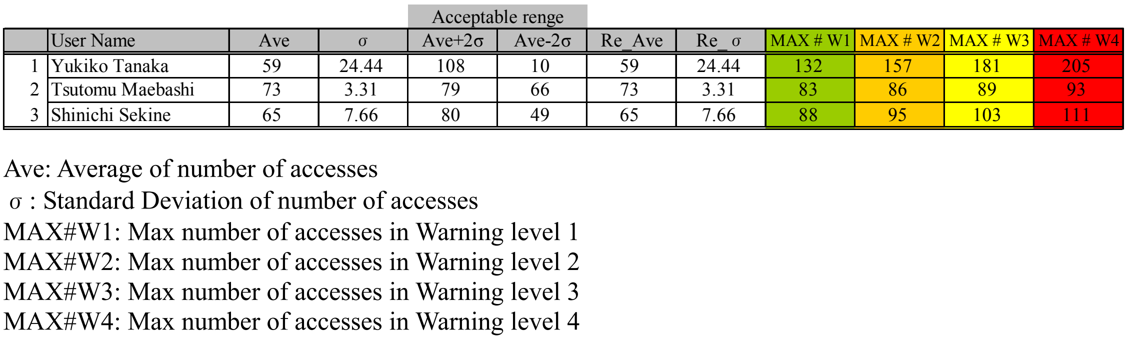
	User Name	02/10/2003	02/11/2003	02/12/2003	02/13/2003	02/14/2003	02/17/2003	02/18/2003
1	Yukiko Tanaka	72	73	10	70	69	50	60
2	Tsutomu Maebashi	68	74	77	70	75	77	84
3	Shinichi Sekine	60	69	77	55	62	101	108
	Average Access	67	72	55	65	69	76	84
	Total Access	200	216	164	195	206	228	252
							Average	**70**
							Total	**1461**

Figure 40: Datasheet of Totaled Number of Accesses each Day

Malicious activities occurring on Feb. 17, 2003 and Feb. 18, 2003 will be detected based on number of accesses in the dy (Feb. 10, 2003 to Feb. 14, 2003: 5days) period.

Step 3: Performing Procedure

The procedure developed in chapter 4 is performed. Please see the detailed explanation for this procedure on page 60 to 62[67]. The results of this procedure are shown as follows.



				Acceptable renge							
	User Name	Ave	σ	Ave+2σ	Ave-2σ	Re_Ave	Re_σ	MAX # W1	MAX # W2	MAX # W3	MAX # W4
1	Yukiko Tanaka	59	24.44	108	10	59	24.44	132	157	181	205
2	Tsutomu Maebashi	73	3.31	79	66	73	3.31	83	86	89	93
3	Shinichi Sekine	65	7.66	80	49	65	7.66	88	95	103	111

Ave: Average of number of accesses
σ : Standard Deviation of number of accesses
MAX#W1: Max number of accesses in Warning level 1
MAX#W2: Max number of accesses in Warning level 2
MAX#W3: Max number of accesses in Warning level 3
MAX#W4: Max number of accesses in Warning level 4

Figure 41: Datasheet of Procedure Process for Dynamic Information Policy 1

Finally, the following activities are detected with the above procedure and defined rule in the procedure.

- Feb. 17, 2003 17:10:00, user3 access is detected, and a warning message is sent to user3
- Feb. 17, 2003 17:20:00, user3 access is detected, and manager approval is required.
- Feb. 18, 2003 16:40:00, user3 access is detected, and warning message is sent to user3.
- Feb. 18, 2003 16:50:00, user3 access is detected, and manager approval is required.
- Feb. 18, 2003 18:00:00, user3 access is detected, and manager approval is required.
- Feb. 18, 2003 19:00:00, user2 access is detected, and warning message is sent to user2.

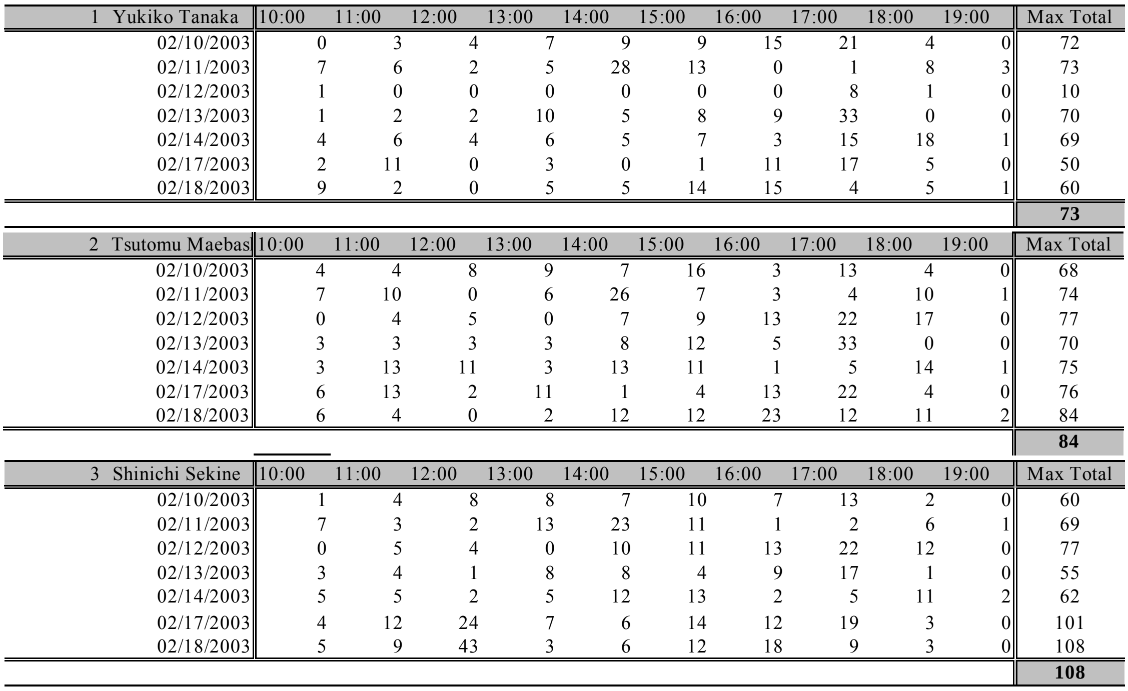
[67] Please see 4-3-1: Dynamic Information Policy 1 about definition of each

The dynamic policy provides a chance to alert a manager or security manager of user3's malicious activity. When the malicious activities are recognized, it will be easy to identify a suspect. Moreover, a warning message and the requirement of manager approval threaten user3. User3 might not attempt to steal confidential customer data.

Dynamic Information Policy 2: (*Improve accountability to trace any insider hacker's action*)

Step 1: Identify necessary variables

Access date, access time, user ID, access frequency of a subject, access occupation rate, and access frequency to an object are identified every hour. The data table containing the above-identified data is as follows.



1 Yukiko Tanaka	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
02/10/2003	0	3	4	7	9	9	15	21	4	0	72
02/11/2003	7	6	2	5	28	13	0	1	8	3	73
02/12/2003	1	0	0	0	0	0	0	8	1	0	10
02/13/2003	1	2	2	10	5	8	9	33	0	0	70
02/14/2003	4	6	4	6	5	7	3	15	18	1	69
02/17/2003	2	11	0	3	0	1	11	17	5	0	50
02/18/2003	9	2	0	5	5	14	15	4	5	1	60
											73

2 Tsutomu Maebas	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
02/10/2003	4	4	8	9	7	16	3	13	4	0	68
02/11/2003	7	10	0	6	26	7	3	4	10	1	74
02/12/2003	0	4	5	0	7	9	13	22	17	0	77
02/13/2003	3	3	3	3	8	12	5	33	0	0	70
02/14/2003	3	13	11	3	13	11	1	5	14	1	75
02/17/2003	6	13	2	11	1	4	13	22	4	0	76
02/18/2003	6	4	0	2	12	12	23	12	11	2	84
											84

3 Shinichi Sekine	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
02/10/2003	1	4	8	8	7	10	7	13	2	0	60
02/11/2003	7	3	2	13	23	11	1	2	6	1	69
02/12/2003	0	5	4	0	10	11	13	22	12	0	77
02/13/2003	3	4	1	8	8	4	9	17	1	0	55
02/14/2003	5	5	2	5	12	13	2	5	11	2	62
02/17/2003	4	12	24	7	6	14	12	19	3	0	101
02/18/2003	5	9	43	3	6	12	18	9	3	0	108
											108

Figure 42: Datasheet of Frequency of Access of User

1 Yukiko Tanaka	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Ave Max
02/10/2003	0%	27%	20%	29%	39%	26%	60%	45%	40%	0%	60%
02/11/2003	33%	32%	50%	21%	36%	42%	0%	14%	33%	60%	60%
02/12/2003	100%	0%	0%	0%	0%	0%	0%	15%	3%	0%	100%
02/13/2003	14%	22%	33%	48%	24%	33%	39%	40%	0%	0%	48%
02/14/2003	33%	25%	24%	43%	17%	23%	50%	60%	42%	25%	60%
02/17/2003	17%	31%	0%	14%	0%	5%	31%	29%	42%	0%	42%
02/18/2003	45%	13%	0%	50%	22%	37%	27%	16%	26%	33%	50%
											60%

2 Tsutomu Maebas	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Ave Max
02/10/2003	80%	36%	40%	38%	30%	46%	12%	28%	40%	0%	80%
02/11/2003	33%	53%	0%	25%	34%	23%	75%	57%	42%	20%	75%
02/12/2003	0%	44%	56%	0%	41%	45%	50%	42%	57%	0%	57%
02/13/2003	43%	33%	50%	14%	38%	50%	22%	40%	0%	0%	50%
02/14/2003	25%	54%	65%	21%	43%	35%	17%	20%	33%	25%	65%
02/17/2003	50%	36%	8%	52%	14%	21%	36%	38%	33%	0%	52%
02/18/2003	30%	27%	0%	20%	52%	32%	41%	48%	58%	67%	67%
											64%

3 Shinichi Sekine	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Ave Max
02/10/2003	20%	36%	40%	33%	30%	29%	28%	28%	20%	0%	40%
02/11/2003	33%	16%	50%	54%	30%	35%	25%	29%	25%	20%	54%
02/12/2003	0%	56%	44%	0%	59%	55%	50%	42%	40%	0%	59%
02/13/2003	43%	44%	17%	38%	38%	17%	39%	20%	100%	0%	100%
02/14/2003	42%	21%	12%	36%	40%	42%	33%	20%	26%	50%	50%
02/17/2003	33%	33%	92%	33%	86%	74%	33%	33%	25%	0%	92%
02/18/2003	25%	60%	100%	30%	26%	32%	32%	36%	16%	0%	100%
											71%

Figure 43: Datasheet of Occupancy Rate of User

	1 Accoun No., Nan	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 1)	02/10/2003	2	0	2	6	5	8	9	9	2	0	43
	02/11/2003	6	5	0	6	21	5	0	1	4	0	48
	02/12/2003	0	3	5	0	6	5	8	11	8	0	46
	02/13/2003	2	2	0	5	3	7	6	20	0	0	45
	02/14/2003	4	5	5	7	4	9	2	4	14	1	55
	02/17/2003	4	7	2	5	1	5	12	18	3	1	58
	02/18/2003	3	4	0	3	3	15	17	6	1	0	52
												58

	2 Account List (lov	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 1)	02/10/2003	0	0	4	5	4	7	4	13	2	0	39
	02/11/2003	1	3	0	7	17	6	3	0	3	0	40
	02/12/2003	0	2	0	0	1	7	5	11	6	0	32
	02/13/2003	4	4	0	7	4	5	4	19	1	0	48
	02/14/2003	2	4	2	2	10	8	1	9	9	1	48
	02/17/2003	1	7	0	5	3	3	4	11	2	0	36
	02/18/2003	5	4	0	1	4	9	10	8	7	0	48
												48

	3 Address, Telepho	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 1)	02/10/2003	1	2	4	3	7	11	4	10	3	0	45
	02/11/2003	3	5	0	4	9	10	0	1	7	4	43
	02/12/2003	1	0	0	0	4	3	3	11	7	0	29
	02/13/2003	0	1	1	1	3	5	6	9	0	0	26
	02/14/2003	1	5	3	2	5	5	0	4	6	0	31
	02/17/2003	3	4	0	1	1	5	9	8	3	0	34
	02/18/2003	4	1	0	1	7	5	14	4	3	0	39
												45

4 Password (unvisil		10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 2)	02/10/2003	0	1	0	0	0	0	0	2	0	0	3
	02/11/2003	1	0	1	1	0	0	0	0	0	0	3
	02/12/2003	0	0	1	0	0	0	0	0	0	0	1
	02/13/2003	0	0	0	0	1	0	0	2	0	0	3
	02/14/2003	0	0	0	0	1	0	0	0	0	0	1
	02/17/2003	0	0	0	0	0	1	0	1	0	0	2
	02/18/2003	0	0	2	0	1	0	0	0	1	0	4
												4

5 Balance		10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 2)	02/10/2003	1	3	5	5	3	5	3	9	2	0	36
	02/11/2003	6	5	2	2	11	5	1	2	4	0	38
	02/12/2003	0	1	2	0	2	2	6	7	7	0	27
	02/13/2003	1	1	2	3	5	4	4	13	0	0	33
	02/14/2003	1	5	4	2	7	4	2	2	7	1	35
	02/17/2003	2	9	0	2	1	4	8	7	3	0	36
	02/18/2003	5	5	41	2	3	6	9	4	5	1	81
												81

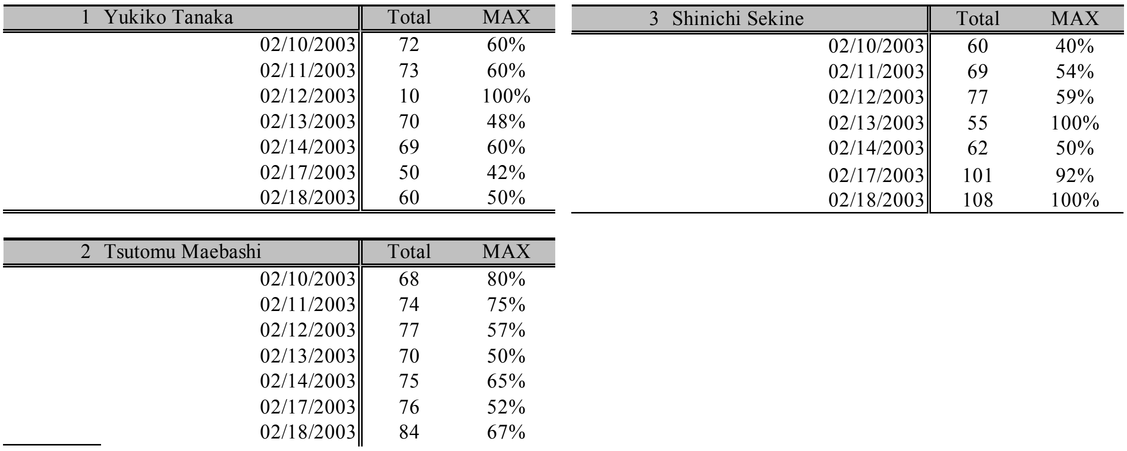
6 Account History		10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	Max Total
(level 2)	02/10/2003	1	5	5	5	4	4	5	4	1	0	34
	02/11/2003	4	1	1	4	19	5	0	3	6	1	44
	02/12/2003	0	3	1	0	4	3	4	12	2	0	29
	02/13/2003	0	1	3	5	5	3	3	20	0	0	40
	02/14/2003	4	5	3	1	3	5	1	6	7	1	36
	02/17/2003	2	9	24	8	1	1	3	13	1	0	62
	02/18/2003	3	1	0	3	5	3	6	3	2	2	28
												62

Figure 44: Datasheet of Frequency of Access to an Object

Step 2: Statistical Process

Access frequency of user1 to 3 and max of occupation rate (% / h)[68] of the users from Feb. 10, 2003 to Feb. 18, 2003 are totaled every day. The following table is a cross table of the above data.

[68] Please see 4-3-2: Dynamic Information Policy 2 about statistical variables



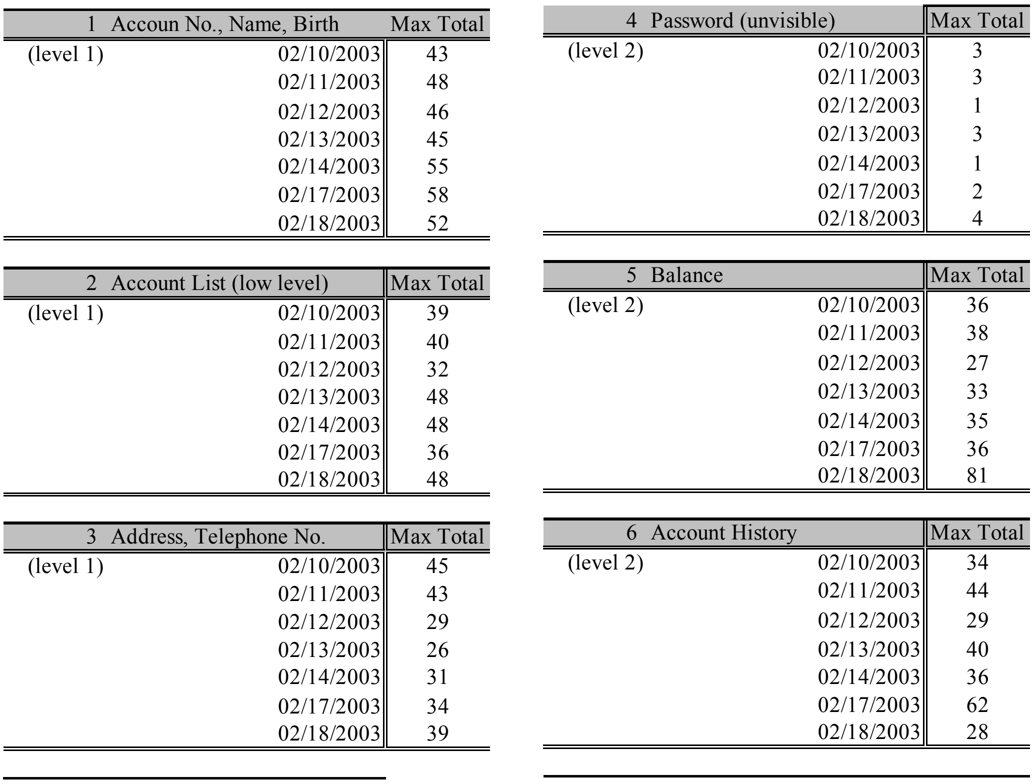
1 Yukiko Tanaka	Total	MAX
02/10/2003	72	60%
02/11/2003	73	60%
02/12/2003	10	100%
02/13/2003	70	48%
02/14/2003	69	60%
02/17/2003	50	42%
02/18/2003	60	50%

3 Shinichi Sekine	Total	MAX
02/10/2003	60	40%
02/11/2003	69	54%
02/12/2003	77	59%
02/13/2003	55	100%
02/14/2003	62	50%
02/17/2003	101	92%
02/18/2003	108	100%

2 Tsutomu Maebashi	Total	MAX
02/10/2003	68	80%
02/11/2003	74	75%
02/12/2003	77	57%
02/13/2003	70	50%
02/14/2003	75	65%
02/17/2003	76	52%
02/18/2003	84	67%

Figure 45: Datasheet of Totaled Number of Accesses and Maximum Occupancy each Day

In addition, access frequency to object 1 to 6 in the same period as the other statistical variables are totaled every day. The following table is shown the variables.



1 Accoun No., Name, Birth		Max Total
(level 1)	02/10/2003	43
	02/11/2003	48
	02/12/2003	46
	02/13/2003	45
	02/14/2003	55
	02/17/2003	58
	02/18/2003	52

4 Password (unvisible)		Max Total
(level 2)	02/10/2003	3
	02/11/2003	3
	02/12/2003	1
	02/13/2003	3
	02/14/2003	1
	02/17/2003	2
	02/18/2003	4

2 Account List (low level)		Max Total
(level 1)	02/10/2003	39
	02/11/2003	40
	02/12/2003	32
	02/13/2003	48
	02/14/2003	48
	02/17/2003	36
	02/18/2003	48

5 Balance		Max Total
(level 2)	02/10/2003	36
	02/11/2003	38
	02/12/2003	27
	02/13/2003	33
	02/14/2003	35
	02/17/2003	36
	02/18/2003	81

3 Address, Telephone No.		Max Total
(level 1)	02/10/2003	45
	02/11/2003	43
	02/12/2003	29
	02/13/2003	26
	02/14/2003	31
	02/17/2003	34
	02/18/2003	39

6 Account History		Max Total
(level 2)	02/10/2003	34
	02/11/2003	44
	02/12/2003	29
	02/13/2003	40
	02/14/2003	36
	02/17/2003	62
	02/18/2003	28

Figure 46: Datasheet of Totaled Frequency of Access to an Object

Step 3: Performing Procedure

The procedure developed in chapter 4 is performed. Please see a detail explanation for this procedure on page 67 to 71. The results of this procedure are shown as follows.

	p1(i)	p2(i)
i = 1	**73**	**60%**
i = 2	**84**	**64%**
i = 3	**108**	**71%**

	Max Total	Level	p3(o)
o = 1	58	1	**58**
o = 2	48	1	**48**
o = 3	45	1	**45**
o = 4	4	2	**8**
o = 5	81	2	**162**
o = 6	62	2	**124**

Figure 47: Datasheet of Procedure Process for Dynamic Information Policy 2

Using the above equation, an audit level for each combination of a subject and object are determined. At this moment, a delivered value (k1 = 0.0012, k2 = 0.065) in chapter 4 is used as coefficients k1 and k2. An audit level matrix is shown as follows.

i , o	L	i , o	L	i , o	L
1, 1	7.3	1, 2	6.1	1, 3	5.7
2, 1	**8.2**	2, 2	6.8	2, 3	6.4
3, 1	**10.2**	**3, 2**	**8.4**	3, 3	7.9

i , o	L	i , o	L	i , o	L
1, 4	1.0	**1, 5**	**20.5**	**1, 6**	**15.7**
2, 4	1.1	**2, 5**	**23.0**	**2, 6**	**17.6**
3, 4	1.4	**3, 5**	**28.4**	**3, 6**	**21.8**

$L(i, o, dy) = k1*p1(i, dy)*p3(o, dy) + k2*p2(i, dy)*p3(o, dy)$

Estimate the audit level from Feb 10, 2003 to Feb 18, 2003.

k1 and k2 are adjusted coefficients determined by security managers, stakeholders, or organization policy.

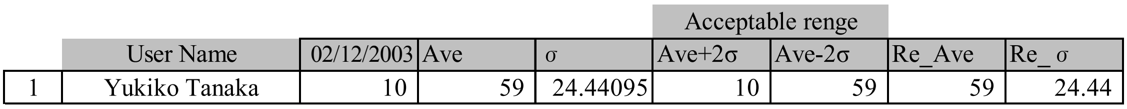
Figure 48: Audit Level Matrix in Test Data

With the dynamic policy 2, a log size will be 903 records. The total test log size is 1461, so it is decreased by 38%. It is only a small contribution to reduce log size. Improvisation or revision is required in this case. Improvement will be shown in section 5-3-3: Improvement.

5-4-3. Improvements

<u>Dynamic Policy 1:</u>

Some improvements may be required. For example, in the dynamic policy 1, it is required to revise the average number of accesses and standard deviation, which are factors to determine a warning level (1 to 4). Warning level for user 1 is determined based on the number of accesses from Feb. 10, 2003 to Feb. 14, 2003. On Feb. 12, 2004, the number of accesses is only 10. The number is taken into account in revising the average number of accesses and the standard deviation, even though it is not desirable since the number is quite small.

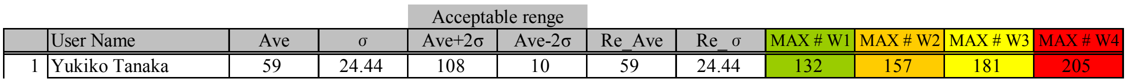


					Acceptable renge			
	User Name	02/12/2003	Ave	σ	Ave+2σ	Ave-2σ	Re_Ave	Re_ σ
1	Yukiko Tanaka	10	59	24.44095	10	59	59	24.44

*Number of accesses on Feb, 12, 2003 (10) is still ranges between 10 and 59.

Figure 49: Datasheet of Number of Accesses on Feb. 12, 2003

Moreover, if such a small number is taken into account in determining the number of accesses for each warning level, the number of each warning level will be too high to accept.



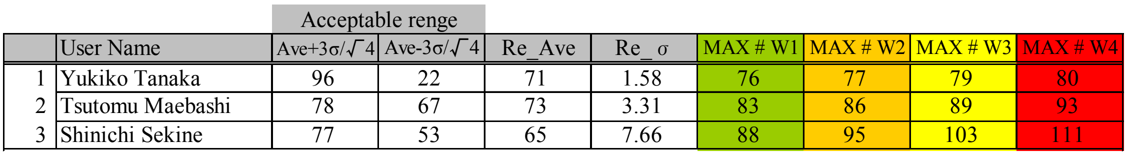
	User Name	Ave	σ	Acceptable renge Ave+2σ	 Ave-2σ	Re_Ave	Re_σ	MAX # W1	MAX # W2	MAX # W3	MAX # W4
1	Yukiko Tanaka	59	24.44	108	10	59	24.44	132	157	181	205

Figure 50: Datasheet of Procedure Process for User 1

Another algorithm is required to determine an acceptable range. Quality management in systems[69] presents a suitable idea to determine the acceptable range. In this book, the following equation is provided in order to determine a control limit.

$$\mathbf{UCL = Average + 3^{*}}\ \sigma\ /\sqrt{\ \mathbf{number\ of\ sample}}$$
$$\mathbf{LCL = Average - 3^{*}}\ \sigma\ /\sqrt{\ \mathbf{number\ of\ sample}}$$

The above equation will be applied to determine the acceptable range. The result is as follows.



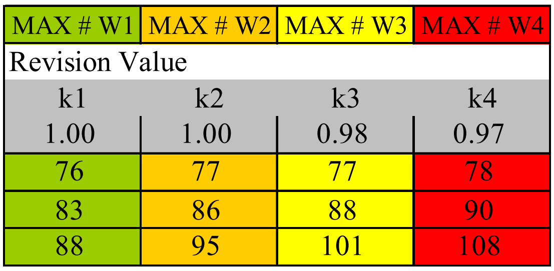
	User Name	Acceptable renge Ave+3σ/√4	 Ave-3σ/√4	Re_Ave	Re_σ	MAX # W1	MAX # W2	MAX # W3	MAX # W4
1	Yukiko Tanaka	96	22	71	1.58	76	77	79	80
2	Tsutomu Maebashi	78	67	73	3.31	83	86	89	93
3	Shinichi Sekine	77	53	65	7.66	88	95	103	111

Figure 51: Datasheet of Procedure Process after Improvement

Using the aforementioned equation, the number of accesses on Feb. 12, 2003 will be out of the acceptable range, and average and standard deviation after revision will be the most suitable valuea to determine the number of accesses for each warning level.

Another possible improvement is that the number of accesses for each warning level can have revision value k1 to k4. This allows systems to have a more suitable number of accesses each warning level. The following table is an example.

[69] Quality Management in Systems, Guangming Zhang, University of Maryland, 1998, Page 24 – 26



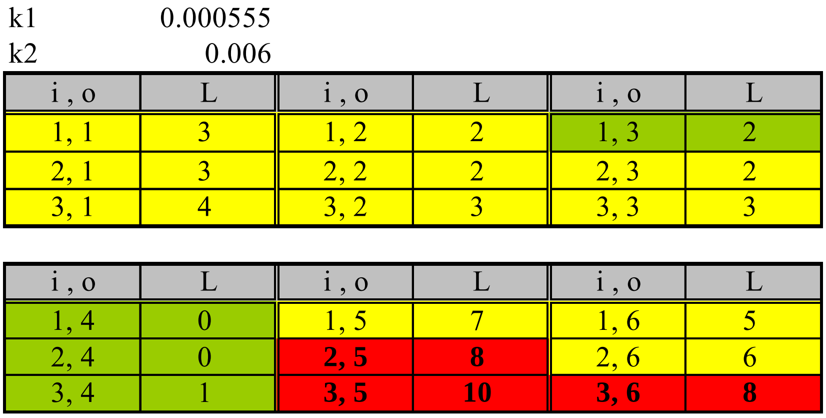
MAX # W1	MAX # W2	MAX # W3	MAX # W4
Revision Value			
k1	k2	k3	k4
1.00	1.00	0.98	0.97
76	77	77	78
83	86	88	90
88	95	101	108

Figure 52: Example of Revision for Maximum Number of Accesses for each Warning Level

The maximum number of accesses with revision is determined by k1*MAX#W1, k2*MAX#W2, k3*MAX#W3, and k4*MAX#W4. The dynamic information policy is very flexible to determine the number of accesses each warning level, and depends on developers' experiments and systems environments.

Dynamic Policy 2:

Using delivered coefficients (k1 = 0.0012, k2 = 0.065) in chapter 4, the dynamic policy 2 contributes to reduce a log size by only 38%, since the coefficient values are not appropriate for the test data. The coefficients must be adjusted depending on certain experiments in a target system and security manager's or stakeholder opinions so as to reach a suitable audit level for the target system. An audit level is basically 0 to 10. The coefficients values (k1 and k2) will be adjusted so that a combination of user 3 and object 5, and a combination of user 3 and object 6 are an audit level 3 (> 8). An audit level matrix after this revision is as follows.



k1	0.000555
k2	0.006

i , o	L	i , o	L	i , o	L
1, 1	3	1, 2	2	1, 3	2
2, 1	3	2, 2	2	2, 3	2
3, 1	4	3, 2	3	3, 3	3

i , o	L	i , o	L	i , o	L
1, 4	0	1, 5	7	1, 6	5
2, 4	0	**2, 5**	**8**	2, 6	6
3, 4	1	**3, 5**	**10**	**3, 6**	**8**

Figure 53: Audit Level Matrix in Test Data after Revision

With these coefficients, log size will be 322, so it is decreased by 78%. The log size is considerably reduced, helping systems administrators and security managers to reduce the effort needed to analyze the event logs. However, it is desirable to have a certain mathematical model in order to determine the proper coefficient, yielding an audit level with a range between 0 and 10.

5-4-4. Results

Is the dynamic policy more powerful than static policy? This section shows a validation of this question through a demonstration using UPPAAL. State chart diagrams are developed with UPPAAL under the following conditions: 1) there is no policy, 2) static information policy is applied, and 3) dynamic information policy is applied for countermeasures 1 and 2[70]. These diagrams are meta-layer 0. They are developed based on meta-systems model (meta-layer 1) shown in the previous sections, and involve

[70] See the recognized countermeasure on page 37 in this thesis.

objects such as user1 and user2, and data such as the number of accesses for user1 on Feb. 18, 2003 and maximum number of accesses for a warning level 3 (101). These objects and data come from the aforementioned test data. All necessary objects and data are defined in the diagram in UPPAAL. Results of the information policies are discussed regarding the aforementioned countermeasures as follows.

Countermeasure 1: Censor not only content but also amount

No Information Policy

The following figure is a state chart diagram without information policy. Defined objects and data in the state chart diagram are also shown.

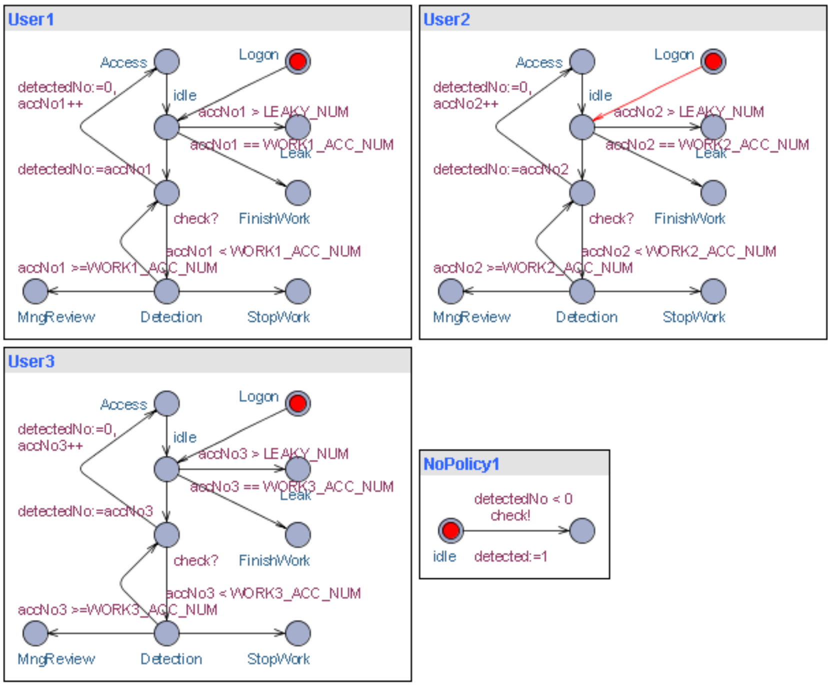


Figure 54: SCD of Security Mechanism without Policy for Countermeasure 1

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
UserPC	User1	User Name	User1 (Yukiko Tanaka)
		Number of Accesses	60
	User2	User Name	User2 (Tsutomu Maebashi)
		Number of Accesses	84
	User3	User Name	User3 (Shinichi Sekine)
		Number of Accesses	108 (65)*

* “65” is necessary number of accesses; otherwise, “43” is unnecessary number of accesses.

Table 46: Objects and Data for Security Mechanism without Policy for Countermeasure 1

“User3” is an insider and stole 35 customers’ information on Feb. 18, 2003. It is desirable to detect this malicious activity. However, without an information policy, inspection of event occurring in the systems is never done. As a result, customer confidential information is stolen. It is demonstrated in the below figure.

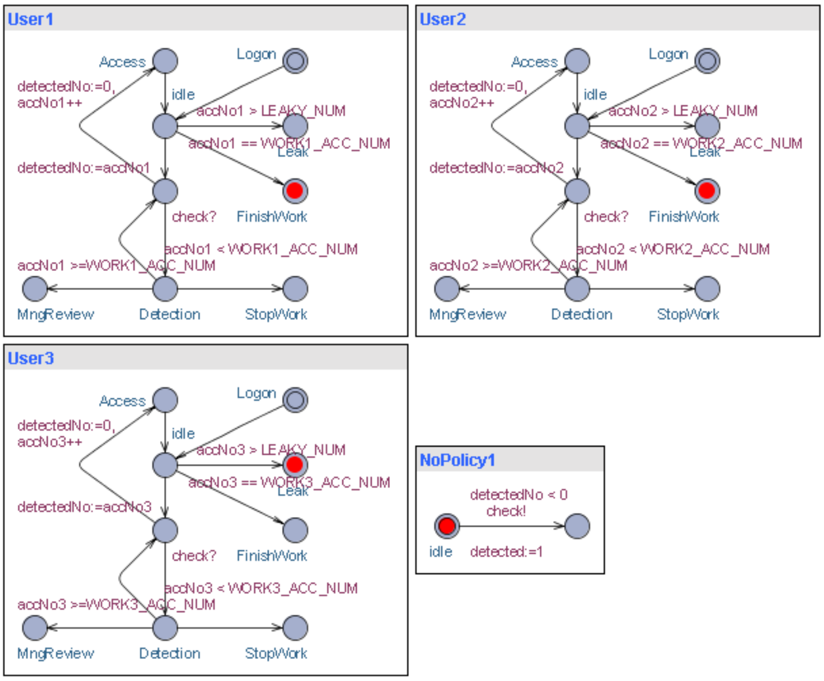


Figure 55: SCD of Result without Policy for Countermeasure 1

“User3” is in a state of “Leak”, which means that the information is leaked. For the next, a system with static information policy is shown.

Static Information Policy 1

A static information policy does not change its policy even though a property and behavior change in a system. Each user may have own maximum and average number of accesses. However, the static policy cannot deliver the own limited number of accesses each user appropriately since the static policy does not provide updating limited number of access to the user if the user changes the frequency of his/her transactions. Thus, the limited number of accesses will be the same value for every user[71]. The state chart diagram is shown on the next page with its defined objects and data.

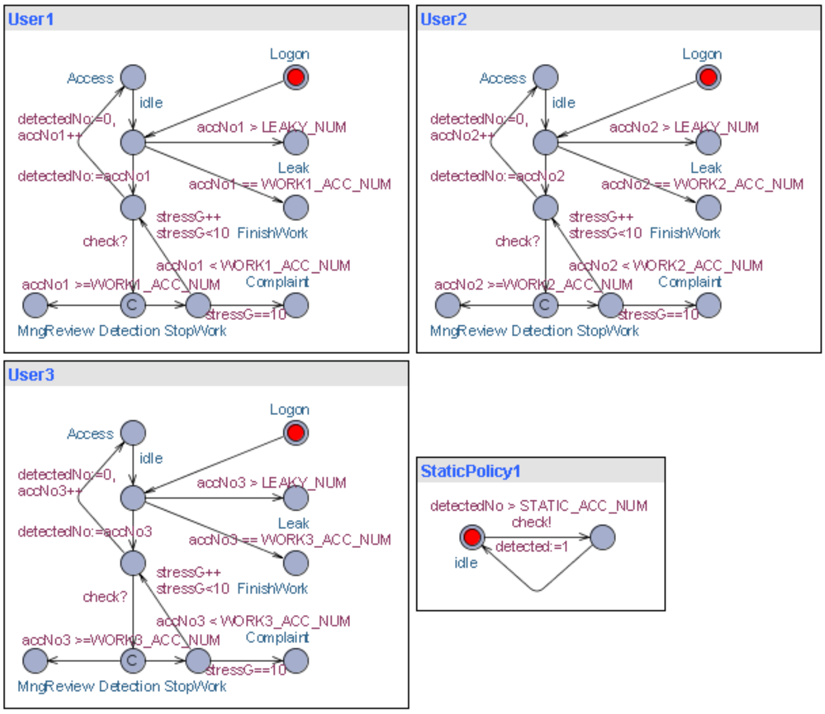


Figure 56: SCD of Security Mechanism with Static Policy 1

[71] The limited number of access may be delivered depend on user's role or position; however, in this thesis, it is supposed that all users have the same role and position.

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
UserPC	User1	User Name	User1 (Yukiko Tanaka)
		Number of Accesses	60
	User2	User Name	User2 (Tsutomu Maebashi)
		Number of Accesses	84
	User3	User Name	User3 (Shinichi Sekine)
		Number of Accesses	108 (65)*
N/A	N/A	Limited Number of Accesses	70**

* “65” is necessary number of access; otherwise, “43” is unnecessary number of access.
**”70” is calculated with the average number of accesses (65) + 5.

Table 47: Objects and Data for Security Mechanism Static Policy for Countermeasure 1

It is also desirable to detect malicious activities by “User3”. A system involving the static information is demonstrated on the next page. The demonstration shows the state when the malicious activity is detected. The static policy is also available to detect the information leak; however, the policy force “User2” to stop working. Even though “User2” does not finish working, the static policy detects a normal activity in “User2”. The demonstration shows that “User2” is in “Complaint” state, which means that “User2” is complaining to the system. As a result, the static policy is able to detect the malicious activity; however, the policy is not flexible, and weakens system availability. In addition, the defined limited number of accesses is not well-grounded value, and may be inaccurate

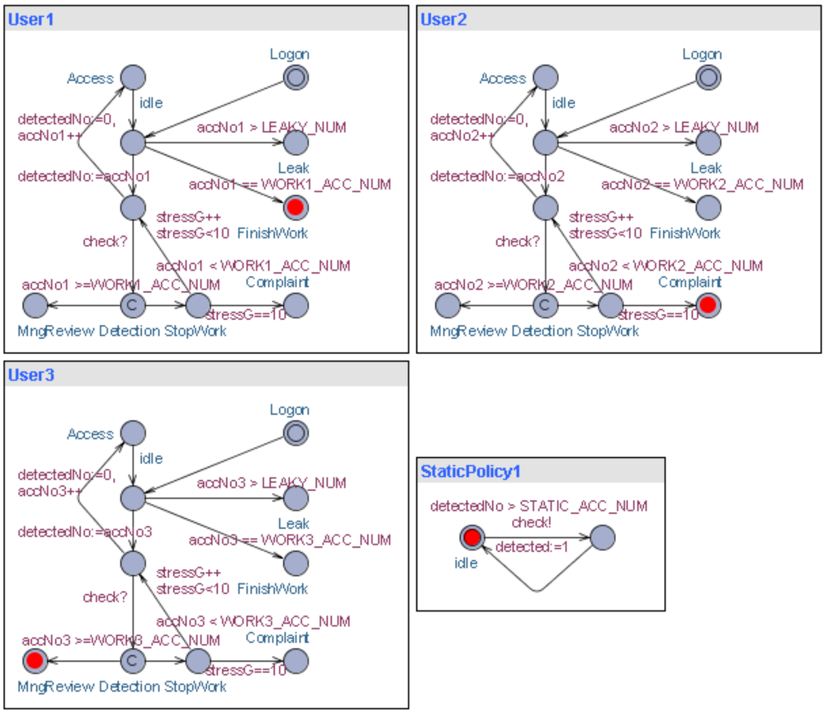


Figure 57: SCD of Result with Static Policy 1

Dynamic Information Policy 1

A dynamic information policy changes its policy when a property or behavior changes in a system. Each user will have own appropriate limited number of accesses based on history of number of accesses in the system. The dynamic information policy may deliver a default of limited number of accesses for a new user. Then, the policy deliver an updated number of accesses for the new user depend on a frequency of the new user's transactions. In addition, the dynamic policy provides an available inspection to a user. Depend on a current number of accesses, the policy determines maximum number of accesses each warning level. The detail security mechanism is shown in the section 4-3-1: Sample Dynamic Policy 1. The state chart diagram with the dynamic information is shown on the next page. Defined objects and data are also presented additionally.

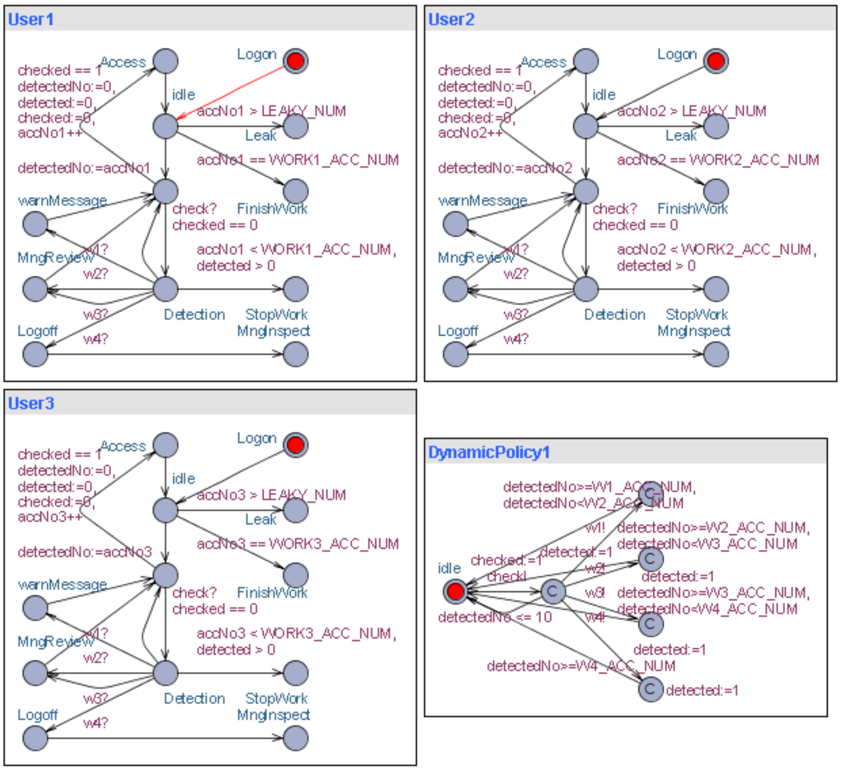


Figure 58: SCD of Security Mechanism with Dynamic Policy 1

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
UserPC	User1	User Name	User1 (Yukiko Tanaka)
		Number of Accesses	60
	User2	User Name	User2 (Tsutomu Maebashi)
		Number of Accesses	84
	User3	User Name	User3 (Shinichi Sekine)
		Number of Accesses	108 (65)
DynP.Policy1	DynamicPolicy1	Max number of accesses w1[i]	User1: 76
			User2: 83
			User3: 88
		Max number of accesses w2[i]	User1: 77
			User2: 86
			User3: 95
		Max number of accesses w3[i]	User1: 77
			User2: 88
			User3: 101
		Max number of accesses w4[i]	User1: 78
			User2: 90
			User3: 108

Table 48: Objects and Data for Security Mechanism Dynamic Policy 1

A system involving the dynamic information is demonstrated in the below figures. The figures show a state when an anomalous number of accesses are detected, and then a defined rule[72] is executed corresponding to a warning level.

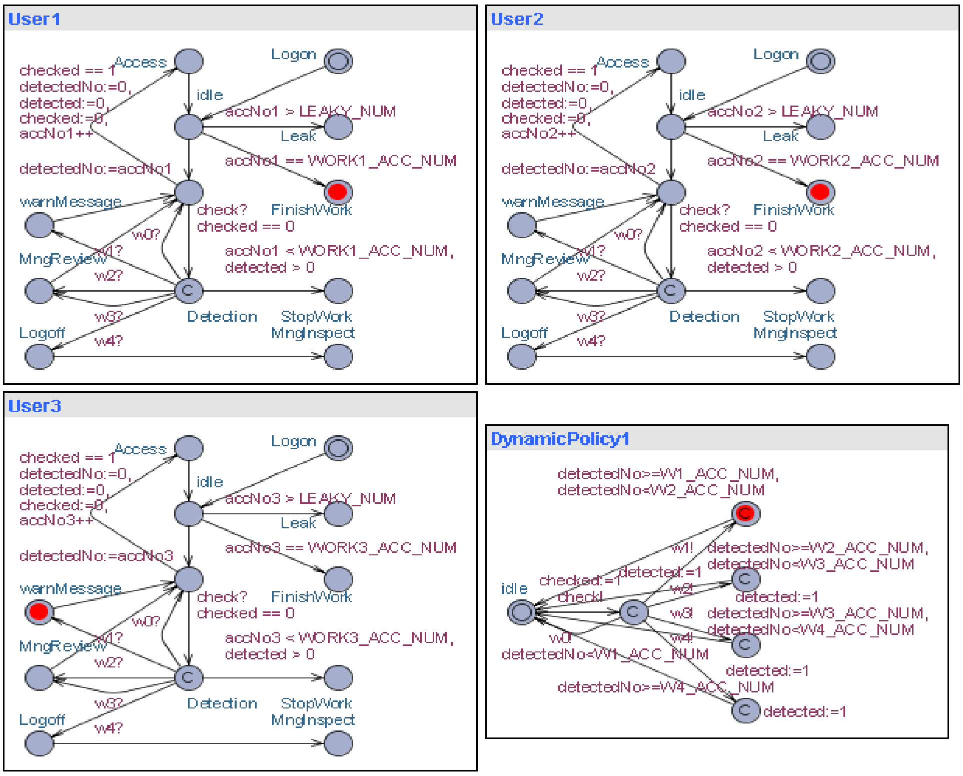


Figure 59-1: The State Detected with Warning Level 1

[72] See Table 25: Rule for each Warning Level for Sample Dynamic Information Policy 1.

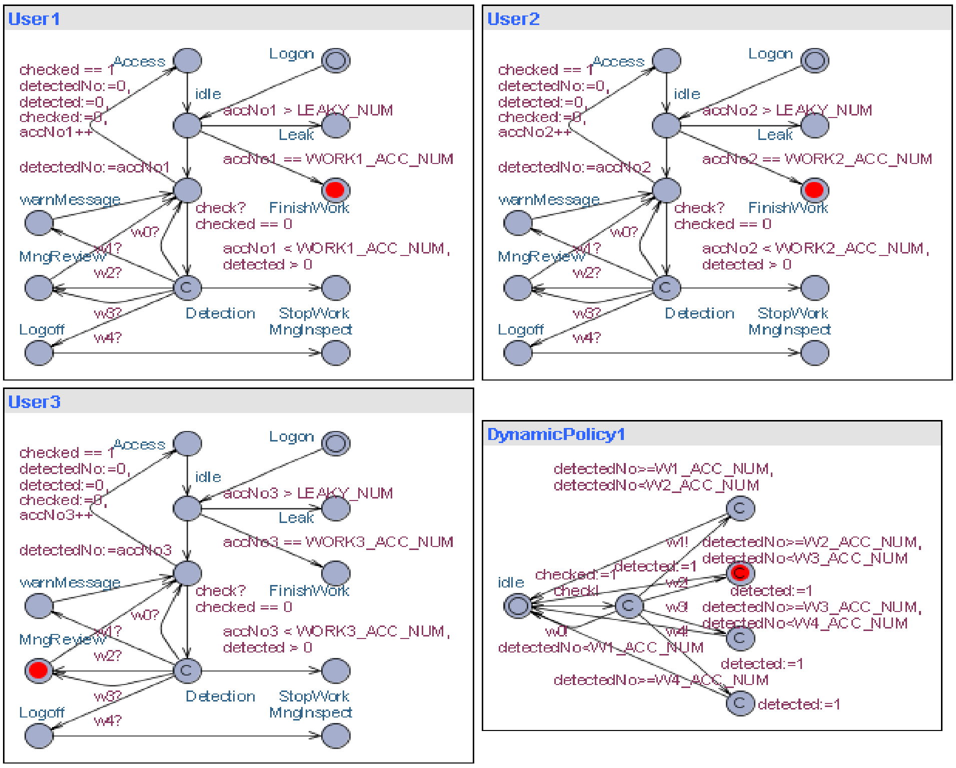


Figure 59-2: The State Detected with Warning Level 2

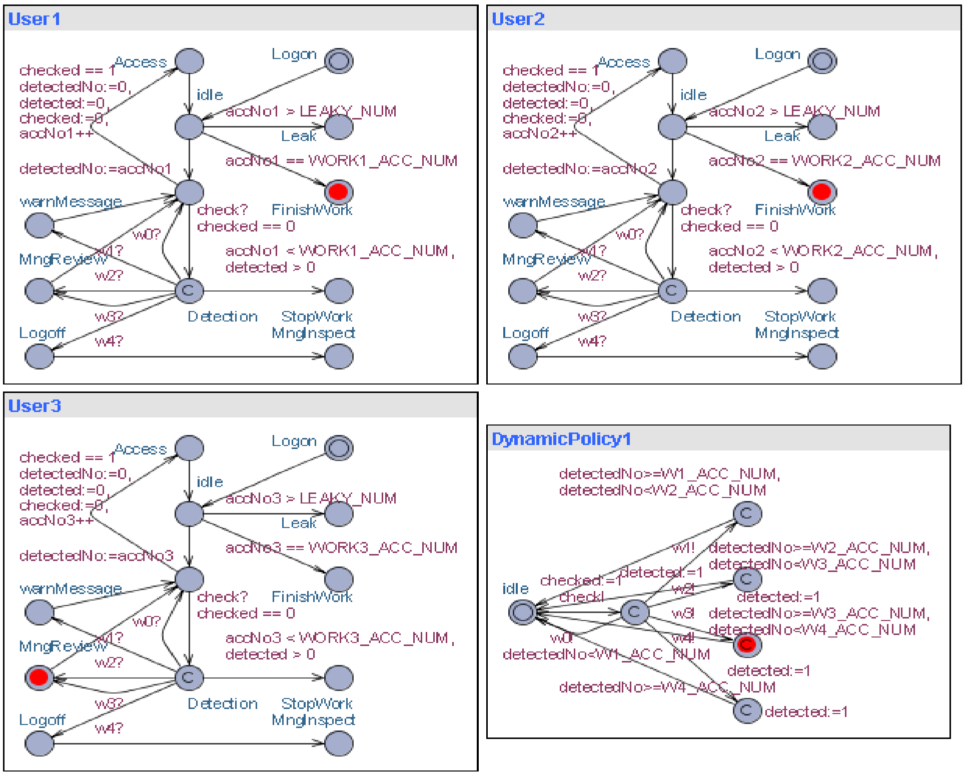


Figure 59-3: The State Detected with Warning Level 3

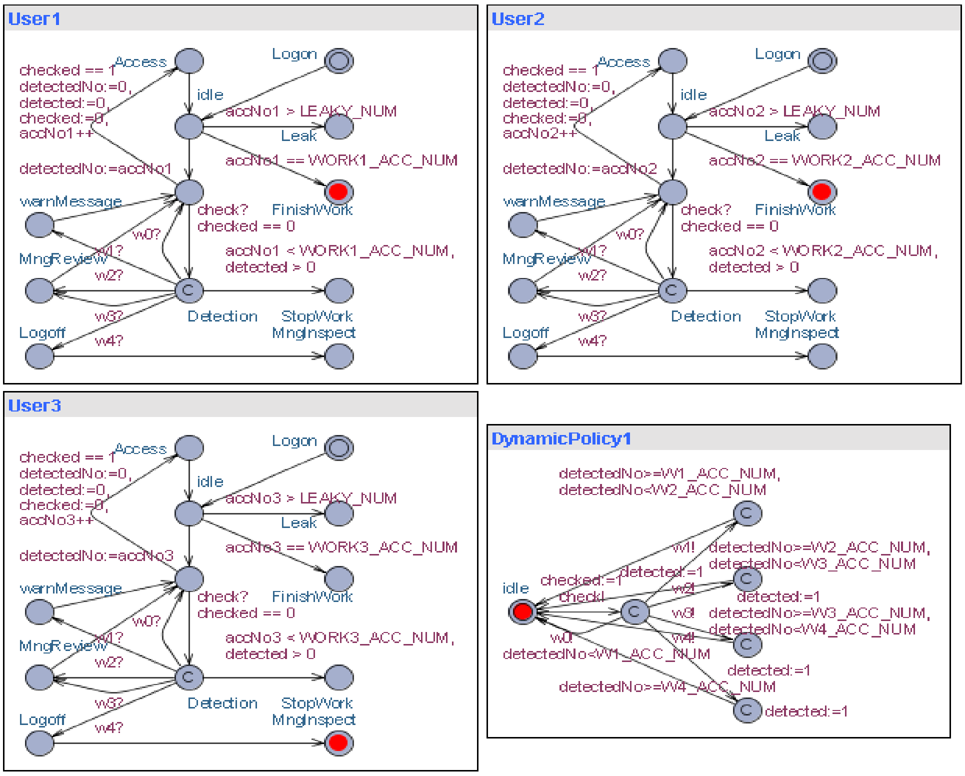


Figure 59-4: The State Detected with Warning Level 4

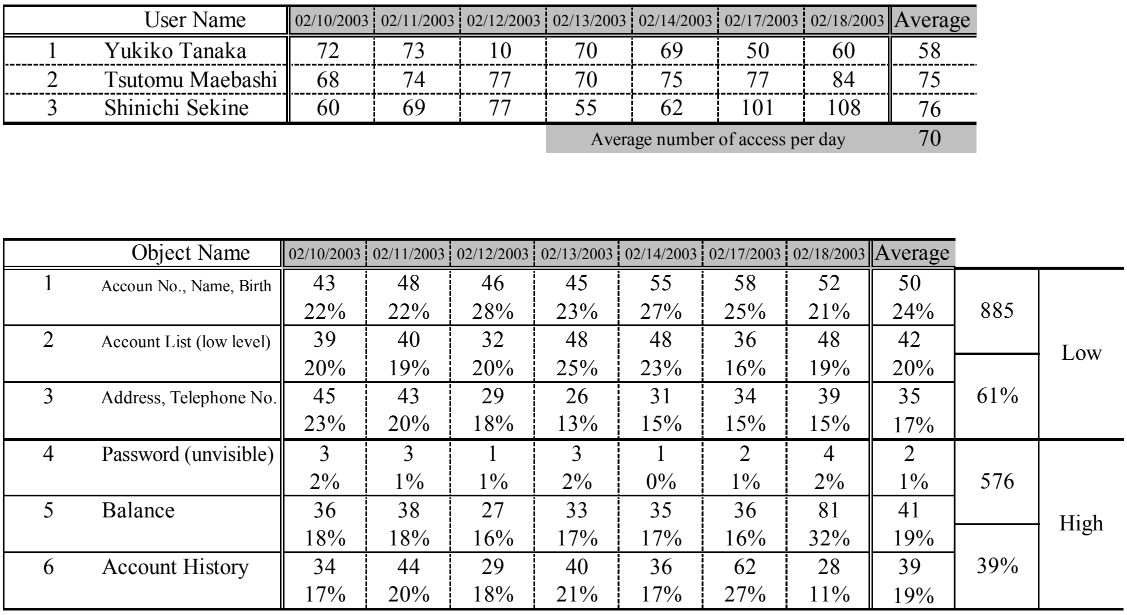
Figure 59: SCD of Result with Dynamic Policy 1

The left upper figure shows when “User3” activity is detected with a warning level 1. The right upper and left bottom figures show when “User3” activity is detected with a warning level 2 and 3. Finally, the right bottom figure shows when “User3” activity is detected with a warning level 4. “User3” is disconnected from the system. Manager inspection will be required for “User3”, and an information leak will be discovered. “User1” and “User2” are able to finish their work without interruption of the dynamic policy.

As the above demonstration shows, the dynamic information policy 1 provides more accurate and available control than others. This mechanism should be taken into account in developing system at the design stage in order to make the systems secure.

Countermeasure 2: Improve accountability in order to trace any insider hacker's actions

The state chart diagram in UPPAAL requires defining objects and data. Necessary objects and data are shown in the following table. All objects and data are from the test data.



	User Name	02/10/2003	02/11/2003	02/12/2003	02/13/2003	02/14/2003	02/17/2003	02/18/2003	Average
1	Yukiko Tanaka	72	73	10	70	69	50	60	58
2	Tsutomu Maebashi	68	74	77	70	75	77	84	75
3	Shinichi Sekine	60	69	77	55	62	101	108	76
					Average number of access per day				70

	Object Name	02/10/2003	02/11/2003	02/12/2003	02/13/2003	02/14/2003	02/17/2003	02/18/2003	Average		
1	Accoun No., Name, Birth	43 22%	48 22%	46 28%	45 23%	55 27%	58 25%	52 21%	50 24%	885	Low
2	Account List (low level)	39 20%	40 19%	32 20%	48 25%	48 23%	36 16%	48 19%	42 20%	61%	
3	Address, Telephone No.	45 23%	43 20%	29 18%	26 13%	31 15%	34 15%	39 15%	35 17%		
4	Password (unvisible)	3 2%	3 1%	1 1%	3 2%	1 0%	2 1%	4 2%	2 1%	576	High
5	Balance	36 18%	38 18%	27 16%	33 17%	35 17%	36 16%	81 32%	41 19%	39%	
6	Account History	34 17%	44 20%	29 18%	40 21%	36 17%	62 27%	28 11%	39 19%		

Figure 60: Datasheet of Objects and Data from Test Data

The upper table has "UserPC" objects and a log size per day from Feb. 10 2003 to Feb. 18 2003, and the bottom table has "UserInf" objects and total frequency of access to an object from Feb. 10 2003 to Feb. 18 2003. The data in the above table will be defined in the state chart diagrams.

No Information Policy

The below figure is a state chart diagram without information policy. Defined objects and data in the state chart diagram are also shown.

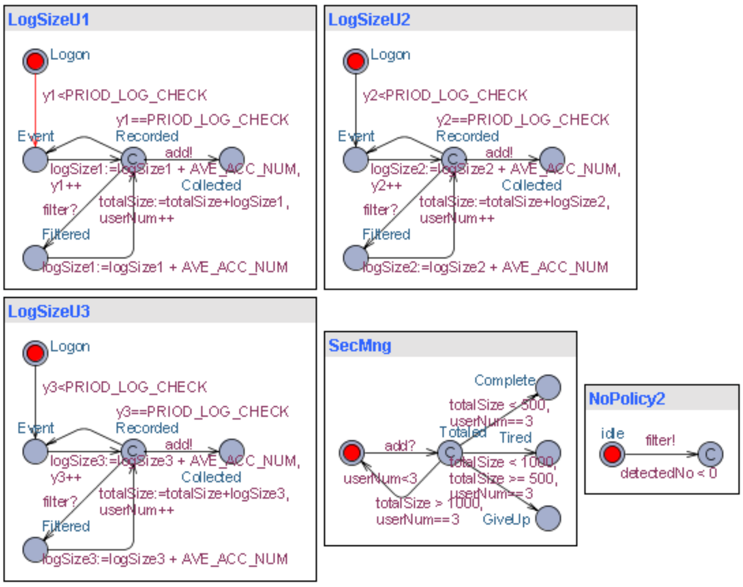


Figure 61: SCD of Security Mechanism without Policy for Countermeasure 2

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
EvLog	User1	User ID	1 (Yukiko Tanaka)
	User2	User ID	2 (Tsutomu Maebashi)
	User3	User ID	3 (Shinichi Sekine)
EvLog	Object 1	Frequency of access	N/A
		Security level	N/A
	Object 2	Frequency of access	N/A
		Security level	N/A
	Object 3	Frequency of access	N/A
		Security level	N/A
	Object 4	Frequency of access	N/A
		Security level	N/A
	Object 5	Frequency of access	N/A
		Security level	N/A
	Object 6	Frequency of access	N/A
		Security level	N/A
N/A	N/A	Average log size per day	70
N/A	SecMng	Condition	GiveUp

Table 49: Objects and Data for Security Mechanism without Policy for Countermeasure 2

Event logs are not filtered without policy. It is required for a security manager or other systems administrator to analyze entire event logs. Total log size is 1470 (70*7*3) for a week. The log size can be much larger depending on the number of operators. As a result, the security manager may give up or leave to check the event logs because of the large amount of work. See the below figure.

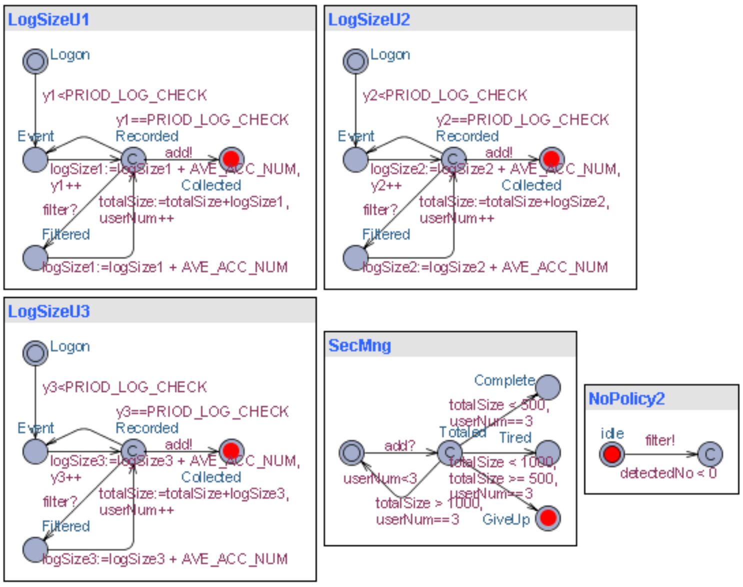


Figure 62: SCD of Result without Policy for Countermeasure 2

<u>Static Information Policy 2</u>

It is desirable to show only important logs regarding information leak. The following conditions can be used to recognize the important log:

✓ The log involving a user who has an anomalous number of accesses

(Whenever an information leak occurs, there are numerous accesses by a certain user)

✓ The log involving a user who has high occupancy in a certain interval

(Insider may try to steal information in the absence of other personnel in the company, at this time; user occupancy will be much higher)

✓ The log involving an object which has a high frequency of access

(Whenever an information leak occurs, there are numerous accesses to a certain object)

✓ The log involving a highly confidential object

(A highly confidential object involves high information asset)

However, the static information policy cannot recognize a user and object behavior. Therefore, the static information policy recognizes only a level of confidential information since the confidential level is static. The state chart diagram in the static information policy is shown as follows with its defined objects and data.

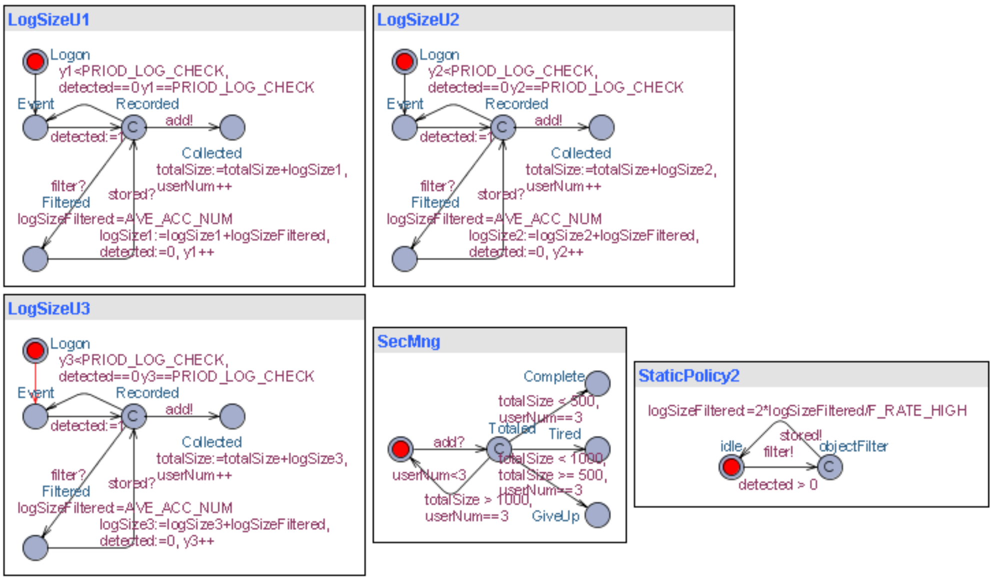


Figure 63: SCD of Security Mechanism with Static Policy 2

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
EvLog	User1	User ID	1 (Yukiko Tanaka)
	User2	User ID	2 (Tsutomu Maebashi)
	User3	User ID	3 (Shinichi Sekine)
EvLog	Object 1	Frequency of access	N/A
		Security level	1: Low
	Object 2	Frequency of access	N/A
		Security level	1: Low
	Object 3	Frequency of access	N/A
		Security level	1: Low
	Object 4	Frequency of access	N/A
		Security level	2: High
	Object 5	Frequency of access	N/A
		Security level	2: High
	Object 6	Frequency of access	N/A

		Security level	2: High
N/A	N/A	Average log size per day	70
N/A	SecMng	Condition	Tired

Table 50: Objects and Data for Security Mechanism Static Policy for Countermeasure 2

The static information policy filters event logs with an object's security level. The policy will remove unclassified information (security level is "Low"). According to the test data analysis in the previous section, log size is decreased by 61%. Accountability in the systems has been improved. However, the filtered event logs still involve unimportant logs. The following figure shows a result of filtering with the static information policy.

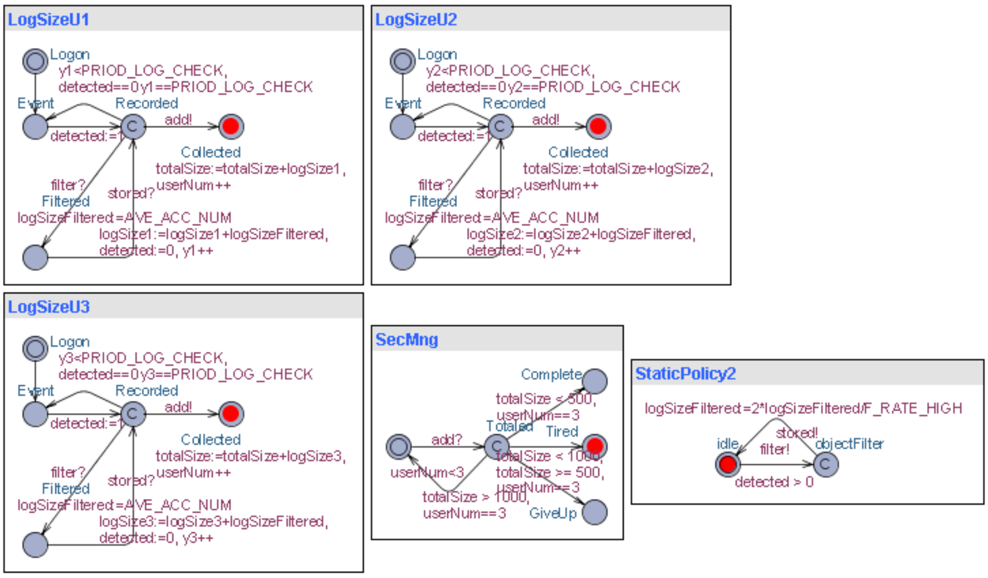


Figure 64: SCD of Result with Static Policy 2

As a result of simulation, a security manager object still feels tired. It may still be desirable to improve the filtering of event logs.

Dynamic Information Policy 2

The following figure is a state chart diagram with dynamic information policy. The dynamic information policy is able to recognize a user and object behavior.

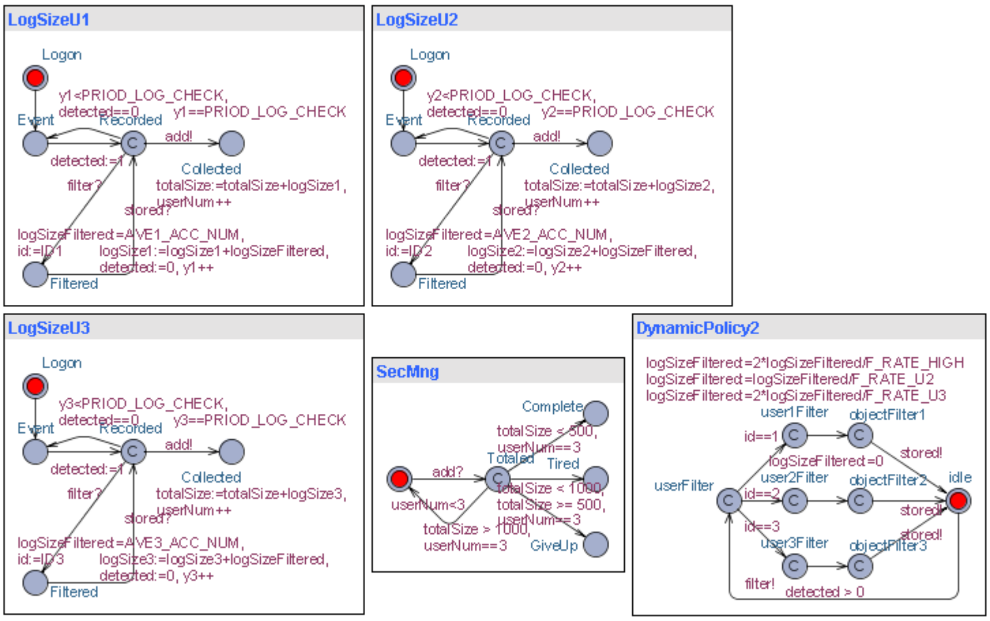


Figure 65: SCD of Security Mechanism with Dynamic Policy 2

Meta-Object	Object	Meta-Data	Data (Feb. 18, 2003)
EvLog	User1	User ID	1 (Yukiko Tanaka)
		Frequency of access	58 (maximum: 73)
		Occupancy rate	60%
	User2	User ID	2 (Tsutomu Maebashi)
		Frequency of access	75 (maximum: 84)
		Occupancy rate	64%
	User3	User ID	3 (Shinichi Sekine)
		Frequency of access	76 (maximum: 108)
		Occupancy rate	71%
EvLog	Object 1	Frequency of access	50 (24%)
		Security level	1: Low
	Object 2	Frequency of access	42 (20%)
		Security level	1: Low
	Object 3	Frequency of access	35 (17%)
		Security level	1: Low
	Object 4	Frequency of access	2 (1%)
		Security level	2: High
	Object 5	Frequency of access	41 (19%)
		Security level	2: High
	Object 6	Frequency of access	41 (19%)
		Security level	2: High
N/A	SecMng	Condition	Complete

Table 51: Objects and Data for Security Mechanism Dynamic Policy 2

The event logs are filtered with a user's frequency of accesses, occupancy rate of accesses, and an object's frequency of accesses besides security level of an object. All event logs regarding "User1" are filtered since the importance is less than that of other users. Low security level logs are also removed, as well as the static information policy. In addition, the frequency of access to the object 4 is so low that object 4's log is eliminated. As a result, the log size is decreased by 78% with the dynamic information policy. The next figure shows the result of filtering with the dynamic information in the systems. A security manager or systems administrator is therefore able to complete his/her work.

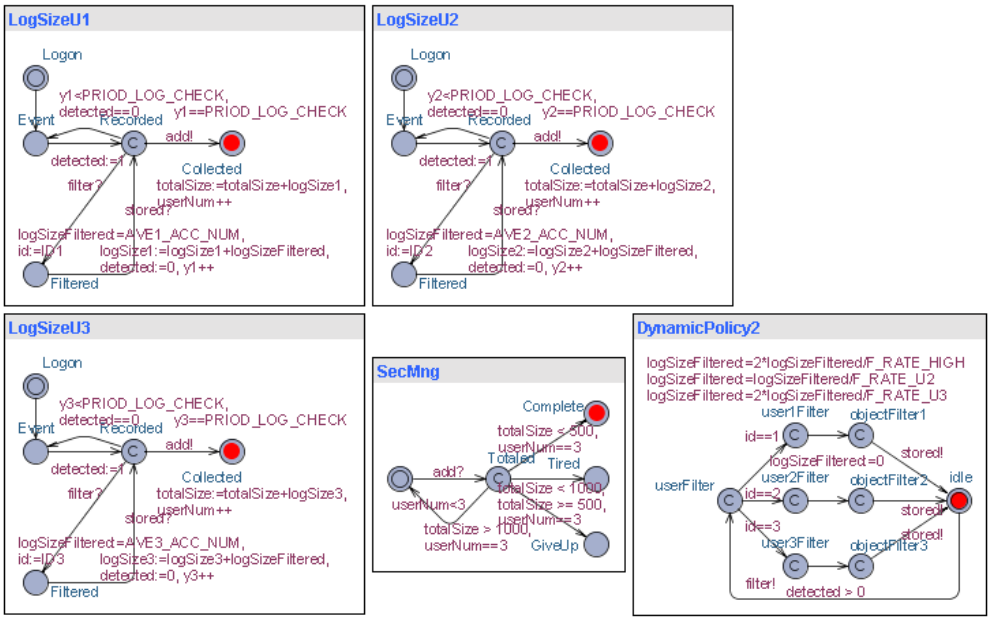


Figure 66: SCD of Result with Dynamic Policy for Countermeasure 2

As the above demonstration shows, the dynamic information policy 2 is the most suitable policy to improve accountability. This mechanism should be taken into account in developing a system at the design stage in order to make the system secure as well as the information dynamic policy 1.

All diagrams are developed with UPPAAL, which simulates the abovementioned security mechanisms. A UPPAAL data file whose file type is XML involves the diagram. The data file name and its diagram name are as follows.

- leakNoPolicy1.xml: Security Mechanism for countermeasure 1 without policy
- leakStpolicy1.xml: Security Mechanism for countermeasure 1 with a static information policy
- leakDypolicy1.xml: Security Mechanism for countermeasure 1 with a dynamic information policy
- leakNoPolicy2.xml: Security Mechanism for countermeasure 2 without policy
- leakStpolicy2.xml: Security Mechanism for countermeasure 2 with a static information policy
- leakDypolicy2.xml: Security Mechanism for countermeasure 2 with a dynamic information policy

The following table shows an overview of the aforementioned policies. It makes difference between the policies clearly.

Countermeasure 1:

	Without Policy	Static Information Policy	Dynamic Information Policy
Methodology	No detection	Define static value of detection	Deliver appropriate value of detection
Estimation	Involves High Risk	Reduces risk, but system availability worsen	Reduces risk with high availability

Countermeasure 2:

	Without Policy	Static Information Policy	Dynamic Information Policy
Methodology	No filtering	Filter by security level	Filter by user and object behavior
Estimation	0%	61 % reduction of effort	78 % reduction of effort
	Results in high Risk	Results in less risk	Results in less risk than static

Table 52: Validation of Information Policies

In this section, security mechanisms in the meta-system model developed in the previous section are verified thorough the demonstration of UPPAAL. In addition, the addressed question at the beginning of this section is also answered. It is validated that a dynamic information policy provides more accuracy and available control in systems, and contributes to reducing the risk of information leak more effectively than other methods.

6. Conclusions

Many aspects and processes of security system modeling are shown in this thesis. The first step was to analyze 20 current security breaches, and assess the risk level for each security breach utilizing the risk management assessment technique. Three severe security breaches were then chosen to be cases for further analysis. The second step included developing the information policies. It was apparent that the static information policy utilized currently for computer network security is not a strong enough policy for overcoming current security threats. A more comprehensive policy is required for such systems. In this thesis, the dynamic information policy was also introduced as the more powerful policy to prevent the greater security breaches. Two dynamic information policy samples were presented. One of these is for handling the number of accesses to the object for each user depending on the frequency with which the user accesses the object. The other is for differentiating the audit importance level among large numbers of events logged in the system. The policy contributes to reducing network or security administrators' role in analyzing the event logs. Then, the system model and its security mechanisms were developed using UML. The system design with UML is described by graphical language. It is very understandable for anyone from programmers to users and stakeholders. Use of UML also revealed that some components might be re-useable for other systems. Finally, security mechanisms based on defined dynamic information policies are verified with realistic test data containing customer information access events. This proves the security mechanism will work in real systems. In addition, the system model design developed in this thesis is validated with UPPALL. Through a demonstration using UPPAAL, the power of the dynamic information policies and their suitability are presented.

The processes presented in this thesis should be invoked at the beginning of the system design. It is desirable to apply the aspects and processes to any system required to be secure either by the system engineer or other users and stakeholders. Moreover, the system model is developed by UML. It is suitable to update for new security threats. The work in this thesis contributes to systems engineering by developing the security aspects of systems working with confidential information such as personnel credit/bank account information, governmental information, and national defense information.

7. Future Effort

It is desirable to develop a more dynamic policy to ensure that systems will be secure and prevent new security threats. Moreover, completing system design and verification are also desirable. Providing a complete system design package with verification for all scenarios of the system design is beyond the scope of this thesis and separate studies may be undertaken on this topic. In further studies, the JAVA language may help to develop commercial security enforcement components for networked systems.

APPENDIX A: Summary of Security Breach

[SB-01] Boeing Co privileged documents

Business Week , June 28, 2004

Boeing Co. took out full-page ads in several newspapers Monday to acknowledge that some of its employees used privileged documents from rival aerospace company Lockheed Martin to win a $1.88 billion federal rocket contract.

[SB-02] Hacker penetrates T-Mobile systems

Security Focus Jan 11 2005

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor U.S. Secret Service e-mail, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities, Security Focus has learned.

[SB-03] Hacker Posts Credit Card Info in December 2002

Wired News Report Page, Jan. 10, 2003

In December 2002, an attacker identifying himself as a 19-years-old Russian named “Maxim” broke into the CDUniverse web store operated by eUniverse Inc. and copied more than 300,000 credit card numbers. Maxim then sent a fax to eUniverse threatening to post the stolen credit card on the Internet if the store didn’t pay him $100,000. On December, when the company refused to bow to the blackmail attack, the hacker distributed up to 25,000 of the stolen numbers on the hacker web site “Maxus Credit Card

Pipeline” during the last two weeks.

[SB-04] Identity Thieves Can Lurk at Wi-Fi Spots

USA TODAY, Feb 2005

Thieves are using wireless devices to impersonate legitimate Internet access points to steal credit card numbers and other personal information, security experts warn. So-called evil-twin attacks don't require technical expertise. Anyone armed with a wireless laptop and software widely available on the Internet can broadcast a radio signal that overpowers the hot spot. Then, masquerading as the real thing, they view the activities of wireless users within several hundred feet of the hot spot.

[SB-05] Intuit plugs leaks to Double Click

CNET News.com, March 2, 2002

The leakage was discovered by Richard Smith, an increasingly famous Internet security consultant, who said the problem is not limited to Intuit but appears at sites across the Web. So far, he has noticed similar problems at nearly 15 sites, including Travelocity.com and Buy.com. In October, Smith alerted AltaVista that it was sending people's home addresses to DoubleClick, an Internet advertising firm. Intuit was at first unaware of the problem and didn't quite understand it, said Smith. Once the company had more information, it began to address the problem.

[SB-06] More Than 145,000 People Face Identity Theft Threat

LOS ANGELES, Feb. 17, 2005

About 145,000 people nationwide are being notified that their personal information may have been stolen by thieves who fraudulently signed up with a company that collects consumer data. ChoicePoint Inc. announced Wednesday that it was sending warning letters to 110,000 possible victims beyond the 35,000 in California, where a unique state law requires such disclosure.

[SB-07] Leaked 24,632 customers' information NTT Docomo, Japan

MSN News, Feb 14, 2005

Recognized suspect stole 24,632 customers' information from terminals in secured room in NTT Docomo. Only 254 people are authorized to access to the computer in the room. The room authenticates with iris identification system. 227 people have been authenticated after the stolen data generated.

[SB-08] Raytheon Company published employment policy

Massachusetts, February 1, 2002

On February 1, 2002, Raytheon filed suit against 21 employees it alleges posted or discussed confidential corporate information on a Yahoo! Message board, in violation of their employment contracts and Raytheon's published employment policy, and claiming, in addition, that this conduct constituted a misappropriation of Raytheon's trade secrets. To identify the "John Does" Raytheon obtained a court order allowing its counsel to take out-of-state discovery from Yahoo, AOL, Earthlink and various other ISPs, seeking documents and information identifying the 21.

[SB-09] Security Breach at Buy.com

Wired News, Oct. 12, 2002

A security hole on buy.com's website exposed the personal information of customers who returned products to the company. For several hours on Thursday, the buy.com website allowed determined visitors to peruse the names, addresses, and phone numbers of customers. Wired News verified that the problem affected at least hundreds, and perhaps thousands, of buy.com customers who have sent products to the company's North Wales, Pennsylvania, warehouse. The security breach works like this: buy.com's Microsoft NT server provides customers who want to make a return with a unique URL -- including a customer number -- so they can easily print a mailing label. The label includes return addresses and phone numbers.

[SB-10] Medical Privacy Breach in University of Michigan Medical System

The Detroit News, February 2002

In many places, legal protections are granted for medical records. Many such regulations have various loopholes that patients might be surprised to discover. Of course, there is also the risk of exposure of the information accidentally, as happened in 2002 with the University of Michigan health system. A student trying to find information about a doctor followed a link and found files with thousands of private patient records, including names, addresses, phone numbers, Social Security numbers, job status, and treatments. All of these data were available on the public web.

[SB-11] Leaked over 100,0000 customer information of the store in Rakuten Internet market.

Mainichi News, April 2005

On April 21 2005, 2,500 customers information included the customer home address, home telephone number, credit card account number, purchased products information and other the customer private information. Rakuten provides many virtual stores on the Internet; the company is the biggest virtual market in Japan. Ex-employee stole and sold the information with 30 US$ per a customer to a suspect. Rakuten has over 10,000 virtual stores. It is thought that over 100,000-customer‘s information may have been compromised according to the suspect’s testimony.

[SB-12] Leaked the nuclear plant security information through “Winiy” in the Internet.

Mainichi News, February 2005

The economic ministry the nuclear safety committee reported that some documents of the nuclear plant security in the local inspection agency of the committee were leaked onto the Internet through the file transfer application “Winiy”. The leaked documents are not included technical and confidential information, and personnel information. The local agency employees brought the documents to their home to work. Then, the documents were leaked through their personal computer into the Internet with “Winiy”. The ministry warned its employees not to work with the documents on the computer that installed any file transfer application, and told them not to keep any work documents in their hard disk. Moreover, any document must be inspected before they bring it out from the local agency.

[SB-13] Lost a computer back-up tape holding 200,000 client account data of Bank of America.

Enterprise IT Plante.Com, March 3, 2005

A computer back-up tape holding 200,000 client accounts in Bank of America was lost. Hackers stole 1.4 million customer credit card numbers from shoe retailer DSW. The bank said in February that it lost tapes containing the account information of more than a million federal government employees -- including members of the Senate now considering legislation to curb the problem. “The bank decided to notify all customers whose data was on the tapes. Letters were also sent to some customers who were not on the tapes, so they could either protect themselves or stop worrying” said Bank of America spokeswoman Shirley Norton. Since the tapes were lost in December 2004, no cases of fraud due to the lost data have emerged, she said.

[SB-14] Leaked 5,000 personnel student information in an elemental school in Shizuoka, Japan.

IT Hoken.Com, April 21, 2005

It is reported that 5,000 personnel student information including student name, home address, telephone number, and grade was leaked. It is suspected that the information was leaked from disposed computers in the elemental school. The school entrusts the disposal to a disposal trader in its prefecture.

[SB-15] Stolen documents with personnel information from a business car of water works in Kanagawa, Japan.

IT Hoken.Com, August 16, 2005

Waterworks in Kanagawa reported that documents with 60 persons were stolen from its business car on the street in Sagamihara-shi. The documents involve a leaked water pipe location, resident's name, and telephone number. It also has a rough sketch of the houses. It is assumed that a deviate trader who pretended to be an employee of the company tricked residents by pretending to have the ability to repair a water leak. The company has given sincere apologies to these individuals and plans to take a more aggressive role in combating such security breaches in the future.

[SB-16] Leaked 61,876 members' information by sophisticated hacker attack from Adecco web site.

Adecco web site, June 27, 2005

An attacker broke into Adecco web sites, and stolen 61,876 members' information from the site. Adecco provides a temporary personnel service through the web site. The member inscribes his/her name, home address, birth date, telephone number, e-mail address, and job history. The information did not obtain the member's job history. The mainframe database system was not accessed, and 720,000 member's information remains safe. An individual has been arrested for suspected illegal access to the web site. This attack came to light with checking access event logs from January 18, 2005 to June 2, 2005.

[SB-17] Kitaguni bank issued accidentally other customers' detailed account statement on ATM.

IT Hoken.Com, August 4, 2005

Kitaguni bank announced that documents with personnel information was lost on July 2005. At the same time a customer's detailed account statement was accidentally issued, copy of another customer's account statement was also printed out on ATM from July 17 PM 12:07 to July 19 AM 8:45 in Kamiyanai branch. Information printed out on the account statement involves customer name, account number, branch number and transaction record. It caused wrong implementation of detailed account statement process. The bank identified the customer who received the other customer's detailed statement and collected them.

[SB-18] Nagoya Toyota car dealer shop lost 138 personnel and 67 enterprise customers' list.

IT Hoken.Com, June 6, 2005

Nagoya Toyota car dealer shop announced that 138 personnel information and 67 corporations information list was lost. The list contains, customer address, name, telephone number, and car owner information. It is suspected that a car seller lost the list during working time. The shop enforces protection to personnel information and makes effort to prevent a recurrence.

[SB-19] Leaked member information by e-mail operation error

IT Hoken.Com, July 9, 2004

Anesb Sunrise Co. announced that member information was sent accidentally by e-mail handle error when an operator was sending goods guidance to customers. The e-mail involved 10,000 customers' name, e-mail address, and Anesb card member account number. No confidential information was released at end.

[SB-20] Softbank leak extortionist won't serve time

The Japan Times;; July 10, 2004

On July 7, 2004, the information of 900,000 clients of Yahoo! BB in Softbank, which is one of the largest high-speed Internet connection services, was leaked by an ex-employee's misuse of its database system. The leaked information almost spread to the Internet. The information involves customer name, home address, telephone number, member account number, credit card account number, and expiration data. The company paid $10 to each client as a self-imposed penalty for this lapse in security. Total financial losses reached $9 million.

References

[1] The present state of privacy information breach problem, http://www.ahnlab.co.jp/virusinfo/security_view.asp?news_gu=03&seq=86&pageNo=4

[2] Ministry of Internal Affair and Communication information privacy law site, http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm

[3] Systemwalker Desktop keeper, Fujitsu, http://systemwalker.fujitsu.com/jp/desktop_keeper/ / IPLOCKS Information Risk Management Platform, IPLOCKS, 2 pages, http://www.iplocks.com/images/newsarticles/3customers_final_052705.pdf

[4] Overreacted t o the information privacy law, Yoshiro Tabuchi, NIKKEI BP in Japan, July 5 2005, http://nikkeibp.jp/sj2005/column/c/01/index.html?cd=column_adw

[5] The way to develop the secure information risk management system, D add ninth Co., Ltd., Oct 1 2002, http://www.dadd9.com/tech/sec4manager.html

[6] NetSecurity, Livin' on the EDGE Co., Ltd. & Vagabond Co.,LTD., https://www.netsecurity.ne.jp/

[7] Information security: why the future belongs to the quants, Security & Privacy Magazine, IEEE, July-Aug. 2003, Volume 1, Issue 4, Page 24 –32

[8] Information Security Program Development Using RAPID, http://www.nmi.net/rapid.html

[9] Information Risk Management Program, CSC CyberCare, 5 pages, http://www.csc.com/industries/government/knowledgelibrary/uploads/807_1.pdf

[10] OMG (Object Management Group) official site,; Unified Modeling Language, http://www.uml.org/

[11] UPPAAL homepage, http://www.uppaal.com/

[12] Computer Security Applications Conference, ACSAC 2001 Proceedings 17th Annual 10-14, Dec. 2001, Page 45 – 54

[13] Decentralized Model for Information Control Flow In Proc. 16th ACM Symposium on Operating Systems Principles, A. C. Myers and B. Liskov. A, Saint-Malo, France, 1997

[14] Software Engineering Conference, Tenth Asia-Pacific 2003, 2003, Page 488 - 497

[15] Towards a UML profile for model-based risk assessment, S.-H. Houmb, F. den Braber, M. S. Lund, and K. Stolen, In J¨urjens et al.

[16] Business Component-Based Software Engineering, chapter Modelbased Risk Assessment in a Component-Based Software Engineering Process, K. Stølen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. Gran, S. Houmb, Y. Stamatiou, and J. Aagedal, The CORAS Approach to Identify Security Risks, Kluwer, 2002, Pages 189–207

[17] Model-based Risk Assessment to Improve Enterprise Security, Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International, Sept. 2002, Page 51 – 62

[18] Security Assessments of Safety Critical Systems Using HAZOPs, R. Winther, O.-A. Johnsen, and B. A. Gran, 20th International Conference on Computer Safety, Reliability and Security SAFECOMP 2001, Hungary, 2001

[19] FMEA Risk Assessment, http://www.tangram.co.uk/TI-HSE-FMEA-Risk_Assessment.html

[20] Common Criteria for Information Technology Security Evaluation, I International Standard ISO/IEC, SO/IEC, 1998

[21] Meta-Data Repository, MDR homepage, http://mdr.netbeans.org

[22] UML CASE tool Poseidon, Gentleware homepage, http://www.gentleware.com

[23] Department of Defense home page, http://www.defenselink.mil/

[24] Understanding Information Risk Management, Nomura Research Institution, 2002, 95 pages, http://www.nri.co.jp/opinion/chitekishisan/2002/pdf/cs20020910.pdf

[25] Nomura Research Institution home page, http://www.nri.co.jp/english/index.html

[26] The Japan Times; Softbank leak extortionist won't serve time; July 10, 2004, http://search.japantimes.co.jp/print/news/nn07-2004/nn20040710a4.htm

[27] Understanding Information Risk Management, Nomura Research Institution, 2002, Page 94, http://www.nri.co.jp/opinion/chitekishisan/2002/pdf/cs20020910.pdf

[28] Information Security Management System (ISMS) home page, http://www.isms.jipdec.jp/

[29] Federal Information Security Management Act of 2002 (Title III of E-Gov), http://csrc.nist.gov/policies/

[30] Improving Oversight of Access to Federal Systems and Data by Contractors can Reduce Risk, Wanja Eric Naef, GAO, April 2005, 28 pages

[31] ENSE 622 Lecture notes, Mark Austin, University of Maryland, 2004, Page 78 – 79

[32] Using Metamodels to Promote Data Integration in an e-Government Application Scenario, Adriana Figueiredo, Aqueo Kamada, IEEE, 2003, Page 4

[33] UML 2 for Dummies, Michael Jesse Chonoles, James A. Schardt, July 2, 2003, Page 14,15

[34] UML 2.0, The Current Official Version, http://www.uml.org/#Articles

[35] UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 10 – 12

[36] UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 19

[37] The Executive Guide to Information Security, Mark Egan, Nov 2004, Page 104 – 110

[38] The Executive Guide to Information Security, Mark Egan, Nov 2004, figure 5-1, Page 109

[39] National Infrastructure Protection Center; Risk Management: An Essential Guide to Protecting Critical Assets; November 2002, Page 8 – 9

[40] Combating Terrorism Threat and Risk Assessment Can Help Prioritize and Target Program Investments, GAO. April 1998, Page 7

[41] Combating Terrorism Threat and Risk Assessment Can Help Prioritize and Target Program Investments, GAO. April 1998, Page 8

[42] Inner Guard Master, IGM homepage, http://innerguardmaster.jp/

[43] Computer Security, Dieter Gollmann, 1999, Page 19 – 24

[44] Countermeasure for leaking information problem, http://www.quality.co.jp/CPN.html

[45] Computer Security, Dieter Gollmann, 1999, Page 5 – 9

[46] Computer Security, Dieter Gollmann, 1999, Chapter 3: Access Control

[47] Computer Security, Dieter Gollmann, 1999, Page 38 – 43

[48] Computer Security, Dieter Gollmann, 1999, Chapter 12: Cryptography

[49] Computer Security, Dieter Gollmann, 1999, Page 97

[50] New Technology File System designed for Windows NT, 2000, XP, http://www.ntfs.com/

[51] UML 2 for Dummies, Michael Jesse Chonoles, Page 20 –32 / UML 2.0 in a Nutshell, Dan Pilone, Neil Pitman, Page 32 –38

[52] J-sys software co., ltd. homepage, http://www.jsys.co.jp

[53] ER/DataGen Catalog, http://www.jsys-products.com/download/catalog/ERDataGen_200502.pdf

[54] Entity-Relationship Diagrams (ERD), http://www.umsl.edu/~sauter/analysis/er/er_intro.html

[55] Aglaia Co. Homepage, http://aglaia.cc/profile.html

[56] Quality Management in Systems, Guangming Zhang, University of Maryland, 1998, Page 24 – 26

[57] Legal Issues in Managing Information Text Book, Chapter 8: Developments in Privacy Law

[58] A Risk Management Approach Can Guide Preparedness Efforts, GAO, Oct. 31, 2001

[59] Awareness: The Key to Information Security power point document, Sep. 26, 2002

[60] A case study in repository selection for a distributed software engineering environment, IEEE, 2001

[61] An extended object-oriented security model for high secure office environments, IEEE, 2001

[62] e-Government Interoperability Framework Technical Standards Catalogue, e-GIF, Nov. 11, 2004

[63] Domain-Specific Metamodels for Heterogeneous Information Systems, IEEE, 2002

[64] SoftDock: A Distributed Collaborative Platform for Model-based Software Development, IEEE, 2003

[65] Constraint Diagrams Visualizing Invariants in Object-Oriented Models, IEEE, 1999

[66] Documenting Software Architecture, IEEE, June 2002

[67] Paving the Way for Transparent Application and Data Interchange A Javaä API for Metadata, By Wayne W. Eckerson and Anne Thomas Manes; November 1999

[68] Platform Based Physical Response Modeling, IEEE, 2001

[69] A Workbench for Synthesizing Behavior Models from Scenarios, IEEE, 2002

[70] A Conceptual Model for Computer Security Risk Analysis, IEEE, 1999

[71] Security architecture for agent-based mobile systems, IEEE, 2003

[72] Agent-based Dynamic Information Security Model, IEEE, 2003

[73] An approach to designing security model for mobile agent based systems, IEEE, 1998

[74] An Efficient Information Flow Analysis of Recursive Programs based on a Lattice Model of Security Classes, IEEE, 2002

[75] Design and development of a practical security model for a mobile agent system, IEEE, July 2002

[76] Security analysis and the DSM model, IEEE, Sept 2002

[77] Security model consistency in secure object-oriented systems, IEEE, 1990

[78] Security models and information flow, IEEE, 1990

[79] Next-generation Intrusion Detection Expert System (NIDES) A Summary1, IEEE, 1995

[80] Probabilistic multilateral security model for ubiquitous multimedia services, IEEE, 2003

[81] The IT security model, IEEE, Oct.- Nov 2003

[82] Chinese Wall security model and conflict analysis, IEEE, 2000