Viewpoint of Probabilistic Risk Assessment in Information Security Audit

Naoki Satoh, Hiromitsu Kumamoto

***Abstract*—** After the information security audit, the auditor commonly points out the importance of information assets, the vulnerability of the audited information system, and the need of countermeasures. On such an occasion, the audited often ask the auditor for the quantitative assessment of the risk so that they can take specific measures. Nevertheless, in reality, the auditor can hardly meet this requirement because they do not have any appropriate methods to assess the risk quantitatively and systematically.

Therefore, this paper proposes the approach that makes it possible to identify the scenarios of information security accidents systematically, to assess the risk of the occurrence of the scenario quantitatively, and to point out the importance of taking countermeasures by incorporating Probabilistic Risk Assessment in information security audit. For the concrete description and explanation of this approach, this paper takes the case of the audit of password management as an example.

By enumerating the possible scenarios that indicate how initiating events, the vulnerability of mitigation systems, and the failures of operations can allow illegal accesses to the information assets, this paper shows that it is possible to assess the security risks by the pair of defenseless time span and its occurrence frequency of each scenario.

Finally, since the parameters necessary for risk quantification such as the occurrence frequency of password theft, the probability of theft detection, and the probability of taking countermeasure after the theft have uncertainty, the uncertainty of the occurrence of the scenario itself is assessed by propagating the incompleteness of the knowledge of these parameters with random digits.

Keywords— information Security Audit, Probabilistic Risk Assessment, Scenario, Defenseless Time Span, Occurrence Frequency

I. Introduction

Recently security management has become the important issue that the management should seriously deal with because accidents relating to information security exert great influence on the corporate confidence and thereby on corporate economy [1].

As the prior condition of information security, it is necessary for an organization to equip information security management system based on PDCA (plan-do-check-act), and the information security audit plays the role of "Check" in PDCA [2]. In the information security audit, it is designated that the independent and expert auditor should detect and assess whether or not the risk control of the information assets of the organization is appropriately equipped and implemented as well as the auditor gives advice and assurance [2-4,11,13].

On the other hand, the auditor is quite often asked by the audited for the quantitative assessment of the risk so that they can take specific countermeasures. However, in reality, the auditor can hardly meet this requirement because there are no appropriate methods to assess the risk quantitatively and systematically.

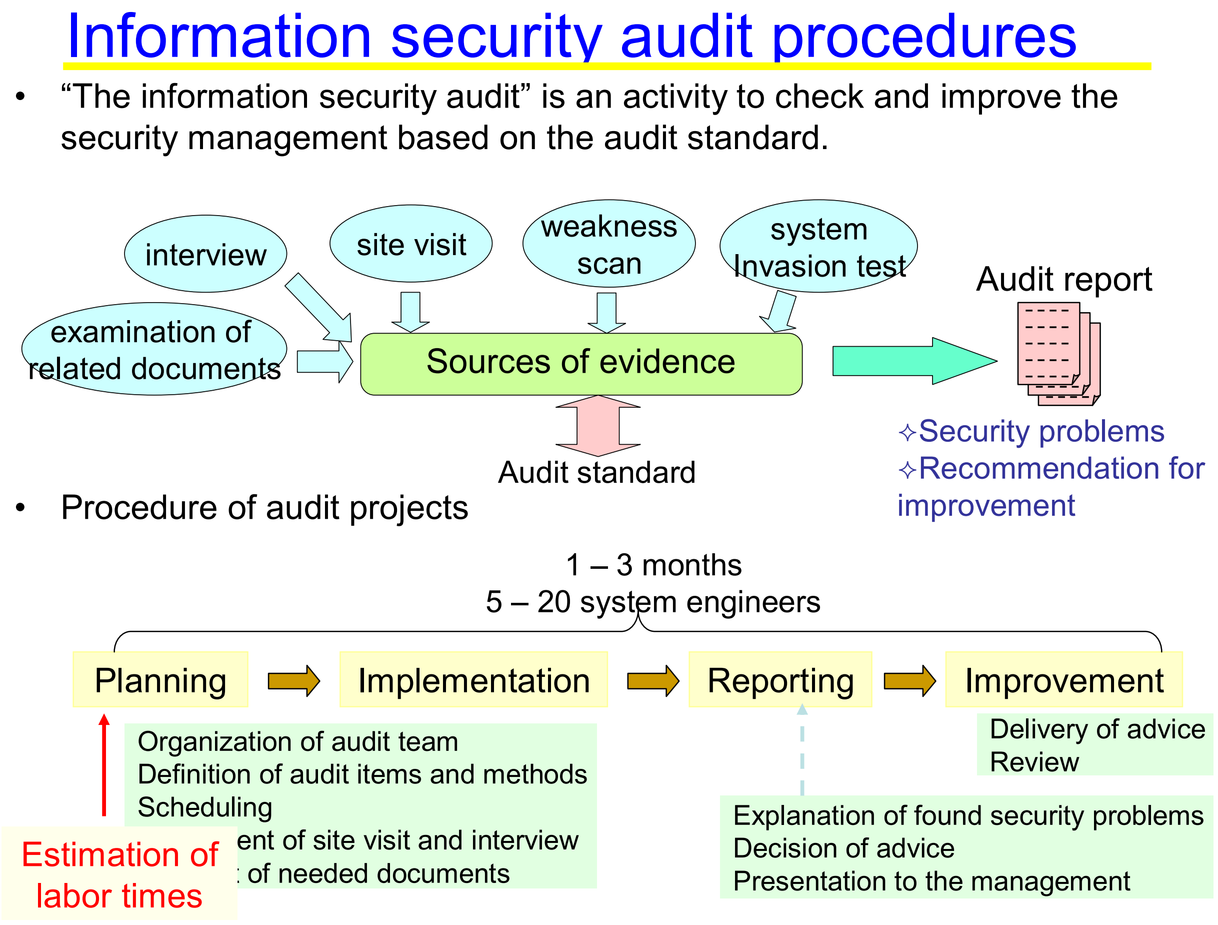
The traditional method of assessing the risk of information asset is GMITS (Guidelines for the Management of IT Security) in ISO, in which the risk value of the information asset to be protected is calculated by multiplying the assessment values of "information asset", "threat", and "vulnerability" [9].

Risk Value = Information Asset Value× Threat Value × Vulnerability Value

In the equation above, "Information Asset Value" is gained by multiplying the scores of the confidentiality, accuracy, and feasibility of the information asset. "Threat Value" means the attack on the information asset, and the higher the occurrence frequency and influence, the higher the value. "Vulnerability Value" means the weakness of security control, and the stronger the weakness, the higher the value.

In this way, GMITS has the easiness to assess risks with three values. However, it should be noted that these three values are generated individually and qualitatively; that is, these values are not based on scenarios of concrete information security accidents.

Naoki Satoh is with Graduate School of Informatics, Kyoto University (e-mail: Sato@sys.i.kyoto-u.ac.jp).
Hiromitsu Kumamoto is with Graduate School of Informatics, Kyoto University (e-mail: kumamoto@i.kyoto-u.ac.jp).



Information security audit procedures

- "The information security audit" is an activity to check and improve the security management based on the audit standard.

✧Security problems
✧Recommendation for improvement

- Procedure of audit projects

Organization of audit team
Definition of audit items and methods
Scheduling
ent of site visit and interview
: of needed documents

Estimation of labor times

Delivery of advice
Review

Explanation of found security problems
Decision of advice
Presentation to the management

Fig1:Information Security Audit Procedures

Table 1. Baseline and the parameters (using a card system): Effects of PRA

Initiating Event	Leak Frequency	Detection Probability	Response Probability	Effect
1) Memorandum	Exist (Zero)	Failure	Zero	Exist
2) Unlocked	Exist (Exist)	Almost Failure	Almost Zero	Doubtful (hole)
3) Trial & Error	Exist (Zero)	Failure	Zero	Exist
4) Borrow	Exist (Exist)	Failure		Doubtful
5) Loss	Exist (Exist)	Finite Value		Doubtful
6) Transfer	Certain (Exist) *card uncollected	Finite Value	Finite Value	Doubtful
7) Terminal Memory	Certain (Certain)	Finite Value	Finite Value	Doubtful
8) Card Forgery	(Exist)			
9) Supervisor	Different Problem			

In the meantime, as a tool to categorize the causes of an information security accident, the notion of Attack Trees has been proposed [10], which is similar to that of Fault Trees (FT),. However, it only schematically enumerates the contributing factors to an accident; therefore, it does not describe various scenarios including partial success of security measures. The notion of Attack Trees has the intrinsic limitation of FT that it contains only AND-OR trees and thus does not contain NOT trees.

In the physical systems of nuclear reactors and chemical plants, Probabilistic Risk Assessment (PRA) has been employed in order to enumerate the accident scenarios. In this paper, the author attempts to show that PRA can be applied to virtual audit of information security and that it is possible by PRA to quantify the security risk that the audited quite often require to the auditor.

For risk quantification, it is necessary to quantify the occurrence frequency of an accident and the damage it could cause, but PRA focuses, first of all, on identifying the scenarios that describe the process of accident occurrence. In order to identify all the numerous possible scenarios, PRA systematically clarifies the relationship between the event that triggers the accident, the response of the mitigation system, and the occurrence of the accident. To be concrete, the scenario clearly describes what event can initiate the accident, how the mitigation systems and mitigation operations can respond, and what damage can occur with the success or failure of the responses.

In order to explain concretely, in this paper, the audit on login information management such as the management of the password for inventory system is taken as an example. The relationship between the events that can initiate the accident (so-called Initiating Event) and the mitigation system/operation is described in the scenario by means of Event Trees. The risk of the scenario is quantified with the pair of defenseless time span and its occurrence frequency by setting the probability of the occurrence frequency of the initiating event and the probabilities of success and failures of mitigation systems/operations. Since the basic parameters necessary for risk quantification have uncertainty, they are evaluated with uncertainty taking into consideration that such uncertainty may exert influence on the scenario risk.

Focusing on the management of login information and Section 2 of this paper describes the real situation of information security audit and gives the examples of what the auditor pointed out and what countermeasures the auditor proposed.

In Section 3, possible Initiating Events of the virtual problem of login information management are enumerated. Concrete examples of mitigation system/operation against each Initiating Event are also given. Moreover, each scenario that starts with each Initiating Event is described by means of Event Trees. Finally, this section will prove that security risk can be illustrated as the pair of defenseless time span and its occurrence frequency, depending on the parameters such as regular inspection intervals.

In Section 4 is the conclusion part of this paper.

II. SECURITY AUDIR ON LOGIN INFORMATION SYSTEM

In this section, a sample case is discussed; therefore, in regard to the details of PRA, please refer to the literature and our previous study[12,14].

A. *Procedure*

Fig1 indicates information security audit procedures. The process of information security audit consists of 4 phases: planning, implementation, reporting, and follow-up (improvement based on the audit) [5].

At the planning phase, which includes the audit on the information protected by login system, the procedure of the audit is planned. The procedure includes the examination of the documented control code of login information and the audit of how such information is input [6]. Concretely, the jobs to be done are to figure out the business content, to confirm the whereabouts of the data to be audited, to determine the range of audit, etc., and the quantity of work varies according to the configuration of the audit, the scale of the system to be audited, and the approach of the business to information security [7].

At the implementation phase, the audit is done one audit item after another along the audit plan, and the work is composed of the interview on the audit items and field survey.

At the report phase, the auditor submits the documented report to the audited. This report includes evaluation results, noncompliant items, suggestions, correction requirements, and so on.

At the follow-up phase, the auditor makes a plan how to improve the noncompliant items and other suggested items.

Finally, in this paper, the occurrence probability of the risk of the suggested items that is reported at the report phase is evaluated.

B. *A CASE EXAMPLE OF THE AUDIT REPORT*

At the report phase, the auditor makes suggestions to the audited, who usually want to know the quantity of the risk. However, in reality, the auditor can hardly answer. Thus, if the risk occurrence can be quantified by a method of some sort, it can be an original way of audit report.

Let us take the example of the audit on the information protected by login system. Suppose that the management of the information is insufficient, and that the password has ample possibility to be stolen. In this case, the auditor points out the followings:

1) General user function is not protected
2) Auto-login function is used partially
3) ID/Password management codes are not clear.

Then the auditor suggests the followings:

1) To abolish auto-login function
2) To establish ID/Password management codes and to make them acquainted.

It is quite often the case that, being suggested as above, the audited ask the auditor for the quantitative evaluation of the risk. However, as I have already pointed out, it is almost impossible for the auditor to quantify the risk. However, if the auditor can quantify the occurrence frequency of the initiating events and the probabilities of the failure of mitigation system and show them to the audited, the audited can take specific countermeasures..

III. APPLICATION OF PROBABILISTIC RISK ASSESSMENT TO INFORMATION SECURITY AUDIT

Let us take the audit on password control situation as an example. The initiating event is the intention to access to the system by login with the stolen password. The attacker tries to access to the confidential information of the company by illegal login. The mitigation system is the resetting of the password. With this mitigation system, those who can access to the confidential information are identified. In this paper, the scenario is a typical one, but in the real audit, the scenario can be a more complicated one including other factors.

For the concrete description, let us suppose a closed intranet inventory control system in a factory. In order to login to this system, it is necessary to input the user ID and the password through the keyboard. There are dozens of users, and most of them (general users) use this system to manage the entering and dispatching of the inventory from warehouse, while several privileged users can access to the confidential information such as the prices and the names of the confidential parts. Thus these few are given special passwords to access such information. If the login information (password and user ID) of the privileged users is leaked and a general user has obtained it, he or she can access to the confidential information through his or her own terminal computer.

As the initiating events in **Table1** indicate, various situations of password leak can be supposed, but here the explanation is based on the case in **Table1**. In each case, the leak frequency and its probability are different. With the countermeasure, the leak frequency can be ZERO from EXIST. Here, uncertainty study of main points is shown:

An example of uncertainty study

By employing a card system, one can access to the confidential information only from the specific terminal computer in a specific room. Suppose that the card and the password can be stolen due to the unlocked room. With this countermeasure (a card system), the probabilities of detection and responses can increase. Most of the defenseless time span is when no one but the attacker is in the room. **Table1** indicates the risk situation before (no card, common terminal computer) and after (using the card and specific terminal computer) the introduction of the card system. The failure of the response after the success of detection would be the case of fraud or robbery.

1) It is possible that the privileged user pastes login information on the display, thus the user ID and the password are leaked to the general user who has seen them. (In this case, it is difficult to detect the leak. Thus only one ET (event tree) is not sufficient including its probability. It is necessary to divide the initiating event more specifically.)
2) The privileged user may keep the memorandum of his or her user ID in the unlocked desk, and the ID leaks to a general user. (In this case, only the frequency of the leak decreases, but it is difficult to detect the leak.)
3) The attacker obtains the login information by guessing with trial and error, and may login as a privileged user.
4) While the privileged user is absent due to the assignment or is absent in front of the terminal, the general user may use the login information which he or she temporally borrowed from the privileged user so as to meet the request from the customer. (Difficult to detect)
5) The privileged user lost the notebook in which the login information is written, and the general user who found it in the factory may know the ID and password. (Theft frequency probability is not 1, but cannot be neglected. Rather easy to detect)
6) The privileged user who was transferred to another worksite and became the general user may access to the confidential information using the previous ID and password. (The theft frequency probability is 1. The problem is whether or not the transfer is detected.)
7) The privileged user may let his or her terminal computer memorize the login information. (The password is stolen and leaked to unauthorized users.) Since the access is done through this terminal computer, detection and response depend on the person who is near the terminal.
8) The attacker may counterfeit the card.
9) The supervisor may make his or her subordinate (the privileged user) access to the confidential information and get it. (This case is different from other cases in that the attacker makes another person access.),

Countermeasures

1) Baseline (the lowest level): without any countermeasures (login information is left to others or is memorized in the terminal computer, or the password is not used or is a simple one.)
2) Access history to the confidential information must be seen online by the privileged users. Or the access history of the previous day is sent to the privileged users the next morning. This can make the items that are difficult to detect detectable.
3) To change the login information into the sequence of complicated letters and numbers.
4) When the privileged user lost the login information, he or she must report it, and the user ID and the password must be changed.
5) To respond personnel management like transfer.
6) To keep login information in the locked situation.
7) To forbid lending of the login information.
8) To use a card instead of user ID. Pasting of the memorandum and trial & errors of login must be detected. When the privileged user is transferred, his or her card must be collected.

9) To use biometric identification instead of login information. However, it is impossible to use it in case that the privileged user is hospitalized or dead.
10) To make sure that one can access only from the specific terminal in the specific room.
11) To implement regular check on the terminal computers.
12) To implement the education for supervisors and the privileged users. To establish the request system that uses E-mail and/or documents.

Table 2 indicates the audit items and the supposed scenario of the login access with the password.

Fig 3 indicates the responses of the mitigation system with two-branch trees after the initiating event of illegal access during LOGON occurred. To begin with, the initiating event occurs with the annual occurrence frequency F1. When APPLID is not determined against the initiating event, illegal access can be prevented as scenario 5 shows.

Next, when APPLID is determined, the probability of the occurrence of the initiating event is noted as P2, and the probability of the success of password obtaining is as P3. When the password and the ID are identified, login can be successful or failure within 3 times, and the success probability is noted as P4. Also login can be successful or failure within the limited time span. In this case, the probability is noted as P5. After all, only if the password is identified, login is successful within 3 trials, and login is successful within the limited time span, then the illegal access cannot be prevented. In all the other cases, prevention is successful.

In PRA, this two-branch tree is called Event Tree.
Fig2 indicates Event Tree and Fault Tree and Probabilistic Risk Assessment .Branching probability to the success (P2 to P5) are conditional probabilities that are conditioned by the events on the left side.

Table2: Audit items and the supposed scenario

Audit Item	Objective	Supposed scenario
Logon Procedure	You should use safe log on process to access to the information service.	It is desirable that access to the information service is achieved through the safe logon process. It is also desirable that the procedure to login the computer system is designed to minimize the unauthorized access. Therefore, in the logon procedure, it is desirable that information disclosure of the computer system is minimized so as not to give unnecessary help to the unauthorized users. a) The identifier of the system or the business software must not be displayed until the logon procedure is safely completed. (To hold the login display: To decrease the intention of the attacker) b) The warning that the access to the computer is limited only to the authorized users must be displayed. (To decrease the probability of theft: To decrease the illegal access, if the user has this intention) c) Nothing that can help the unauthorized user must be displayed in the logon procedure. (To reduce the illegal use when the user has the password) d) The verification of the validity of the logon information must be done only when all the data have been input. If input error happens, the system must not point out what part of the input data is wrong or right. (To prevent the illegal access by trial & error) e) The number of the logon trial must be limited (3 is recommended), and the followings measures should be taken. (To prevent the illegal access by trial & error) 1) To record the failed theft. 2) To set certain time span intentionally before the next logon trial is done, or reject the next logon trial without special permission. 3) To disconnect the data-link connection. f) The maximum and minimum time span for log on procedure must be limited, and if the logon trial is out of these time spans, the system must quit logon procedure. (To detect the illegal holding of the password: To limit the password input) g) When logon is safely completed, the following must be displayed. (To detect illegal holdings of password and ID: To detect illegal access) 1) The date and time of the previous successful logon. (To detect illegal holdings of password and ID 2) If there is a failure logon trial after the previous successful logon, the details of the trial. The user may use the borrowed password. (To detect illegal access)

Probabilistic Risk Assessment (PRA)

The PRA methodology consists of two steps:

Event Tree Analysis (ETA)

for describing accident sequences,

Fault Tree Analysis (FTA)

for analyzing the reason of abnormal situation.

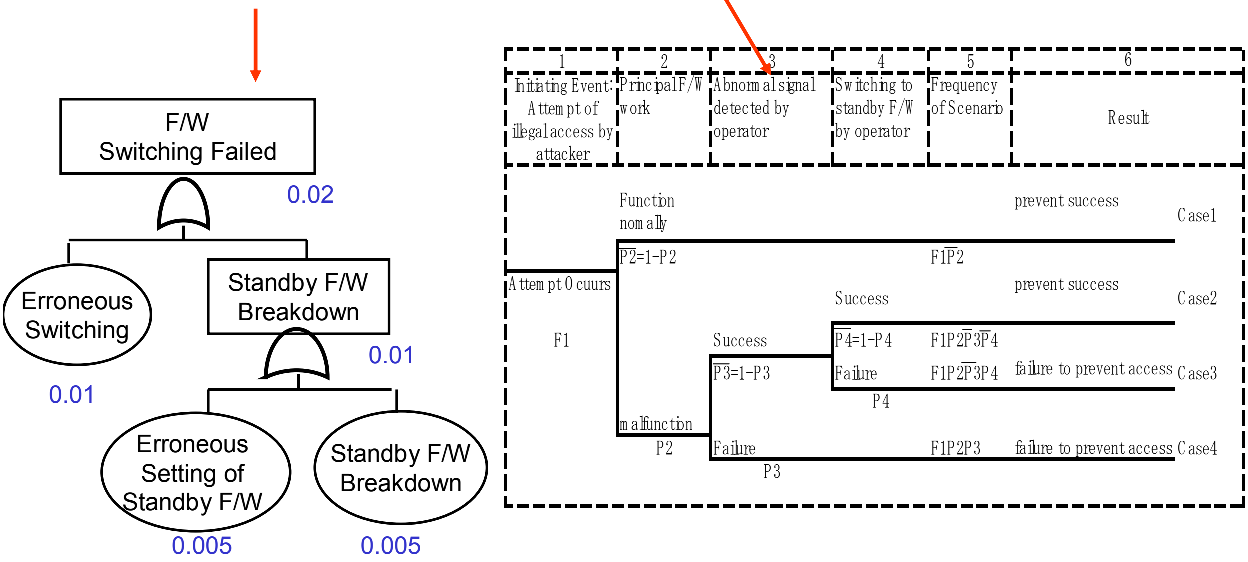


Fig2: The PRA methodology consisted of ET and FT

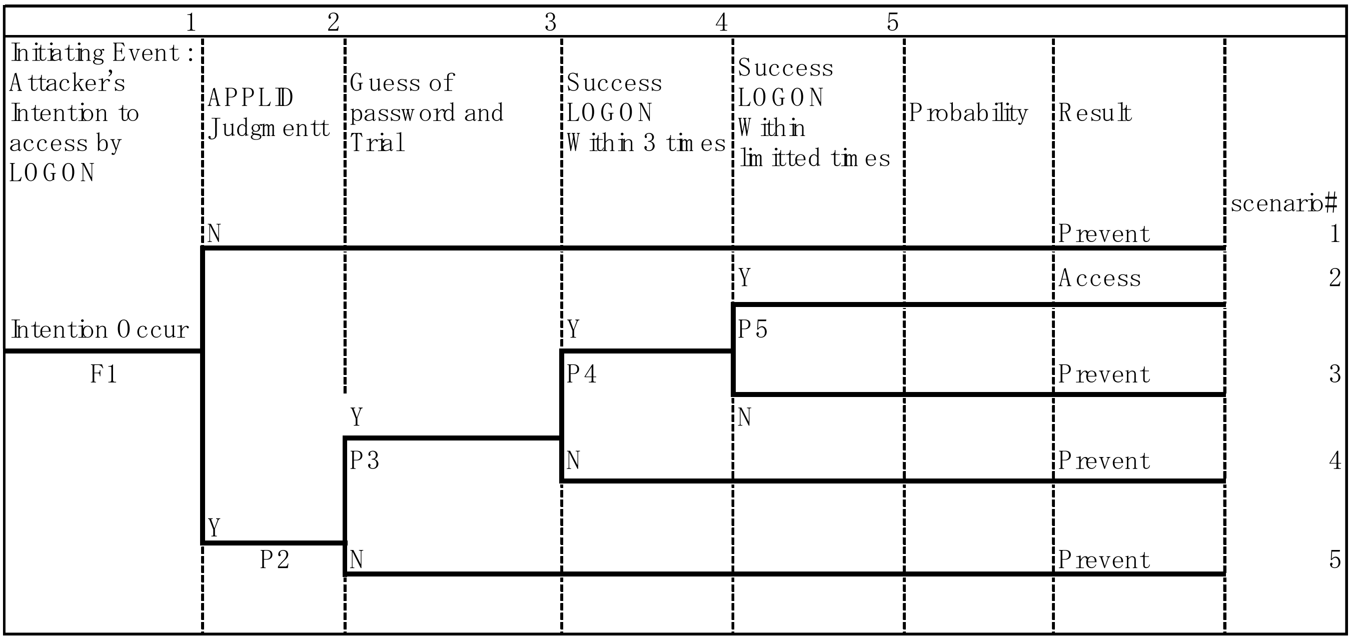

1
2
3
4
5
Initiating Event : Attacker's Intention to access by LOGON
APPLID Judgmentt
Guess of password and Trial
Success LOGON Within 3 times
Success LOGON Within limitted times
Probability
Result
scenario#
N
Prevent
1
Y
Access
2
Intention Occur
F1
Y
P5
P4
Prevent
3
Y
N
P3
N
Prevent
4
Y
P2
N
Prevent
5

Fig. 3 Event Tree with the initiating event of illegal access during LOGON **(The attacker sits in front of TP)**

IV. Conclusion

5. Conclusion

In the information security audit, the auditor points out the initiating events that could lead to the accident and the vulnerability of the mitigation systems. On such an occasion, the audited often ask the auditor for the quantitative assessment of the risk; however, in reality, the auditor can hardly meet this requirement because they do not have any appropriate methods to assess the risk quantitatively and systematically.

In this paper, the author attempted to apply PRA (Probabilistic Risk Assessment), which has been employed in the risk assessment of physical system such as nuclear reactors and chemical plants, to virtual information security, and quantified the risk occurrence probabilities of the items that are pointed out at the report phase of the audit by means of PRA.

Specifically, taking the audit on password control system as an example, this paper showed that, by encompassing the scenarios that indicate how the vulnerability of the control could lead to the illegal access to the information assets, the risks of each scenario can be assessed by the pair of defenseless time span and its occurrence frequency. The risks were quantified by means of the scenarios with the combination of Event Tree and Fault Tree, which are based on the responses of the mitigation systems.

Furthermore, in order to overcome the uncertainty of the probabilities of password theft, theft detection, and response against the theft, the author statistically analyzed them by employing the random digits generated in 20,000 to 50,000 time trials. As a result, these probabilities were estimated, which made it possible to take specific countermeasures against these risks. This can contribute to promote the effect of information security audit by means of PRA.

Finally, this paper clarified the usefulness of the application of PRA to information security audit.

Acknowledgement

This paper could not have been completed without various useful advices from my project members and party involved. I would like to express my sincere gratitude to these people.

References

1. Ministry of Internal Affairs and Communications. White Paper on Telecommunications 2004, Gyosei (2004)
2. Ministry of Economy, Trade and Industry. Standards of System Audit (2004)
3. Japan Information Processing Development Corporation. ISMS Users Guide on Compliance: ISMS Certification Criteria Version2.0 (2005)
4. Shinya Tsumori & Masaaki Oishi. Total Risk Management, Chuokeizaisha (2005)
5. Ministry of Economy, Trade and Industry.5. Information Security Audit Criteria Version1.0 (2003)
6.Haruki Tabuchi. Information Security and Risk Management for ISMS, Ohm, Inc (2003)
7. Japan Information Processing Development Corporation. Audit Guideline on Privacy Mark System, 1st Ed (2000)
8. ASME: Standard for probabilistic risk assessment for nuclear power plant applications, ASME RA-S-2002 (2002)
9. ISO: The Guidelines for the management of IT security, TR13335(2002)
10. E.J. Byres, M. Franz, D. Miller : The use of attack trees in assessing vulnerabilities in SCADA systems , International Infrastructure Survivability Workshop, Lisbon, IEEE(2004)
11 Naoki Satoh and Norihisa Komoda; An Analysis of Influential Factors fo r the Information Security Audit Labor Time and Regressive Estimation of th e Labor Times, WSEAS Trans. on Information Science and Applications, Issu e 1, Vol.3, pp.154-161 (2006)
12 N. Satoh & H. Kumamoto,Viewpoint of ISO GMITS and Probabilistic Risk Assessment in information Security, WSEAS Trans on information science and Application, issue 4 , Vol.2, pp237-244(2008)
13 N. Satoh & H. Kumamoto, Estimation Model of labor Time at the Information Security Audit and Standardization of Audit Work by Probabilistic Risk Assessment, International Journal of Computers, Vol.3, No.3, pp.311-320 (2009)
14 N. Satoh & H. Kumamoto, Analysis of Information Security Problem by Probabilistic Risk Assessment, International Journal of Computers, Vol.3, No.3, pp.337-347 (2009)