Comparison of ISO GMITS and Probabilistic Risk Assessment in Information Security*

Naoki Satoh[1] Hiromitsu Kumamoto[2]
1 IBM Japan, Ltd., 2 Kyoto University, Graduate School of Informatics
(E-mail: e16869@jp.ibm.com; kumamoto@i.kyoto-u.ac.jp)

Abstract Among the previous studies on the quantification of information security risks, one of the most popular tools is ISO GMITS, which quantifies the risk of information asset on the whole based on the scores of information asset, threat, and vulnerability. However, in our previous study, we maintained that "probabilistic risk assessment" (hereafter abbreviated as PRA), which has been traditionally employed in assessing the risk of physical systems such as a nuclear reactor and a chemical plant, is superior to GMITS in the ability of generating the scenario of hazard occurrence, and so on. In this paper, by taking Firewall (F/W) as an example, we will clarify the advantages of PRA over GMITS in generating more detailed scenario, in the ability of risk quantification, and so on.
Key words initiating event, event tree, fault tree, information security

1 Introduction

The importance of information security requires many words of explanation. If risk assessment can quantify what parts of safety measures play a crucial role, it is possible to take effective measures. A typical quasi-quantification method of information security risk would be GMITS in ISO, which wholly quantifies the risk of information asset based on the value of information asset, threat, and vulnerability [1]. The impact is evaluated from the importance of asset, while the likelihood from threats and vulnerabilities.

On the other hand, in the fields of nuclear reactors and chemical plants, PRA[2,3] has been used for the qualification of accident risk since the 1970s and is now a standard method. The first landmark application of the PRA occurred more than 30 years ago. This is known as the WASH-1400 reactor Safety Study[4]. Sophisticated models and attitudes developed for nuclear PRAs have found their way into other industries including chemical, railroad, aerospace systems[5]. The PRA methodology has advanced and matured to a point where standards become available to guide and evaluate each PRA performed for a particular nuclear plant. The ASME standard, for example, consists of high level requirements and supporting requirements for each major step of PRA. The risk is defined as a pair of impact and likelihoods. Both qualitative and quantitative risk assessments can be performed by generating scenarios called accident sequences. Initiating events, mitigation systems and event trees are used to enumerate these scenarios[6,7].

In our previous study, we maintained the overall advantage of PRA over GMITS in that in identifying detailed scenario of information leak[8]. In this paper, we will attempt to clarify the concrete difference between PRA and GMITS by taking Firewall (F/W) as an example.

2 The Method of ISO GMITS

GMITS calculates the risk value of the information asset that is to be protected by multiplying each value of the information asset, threat, and vulnerability:

Risk value = (information asset value) × (threat value) × (vulnerability value)

It is true that GMITS has the simplicity in that risk is evaluated with the scores of these three factors, but GMITS cannot describe the scenario of individual information accident.

3 Comparison of GMITS and PRA in the Case of Firewall

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[8,9].

3.1 A Sample Case: Firewall

* 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.

As indicated in Figure 1, Firewall(F/W) is set in order to protect information asset from illegal access. This is a dual system composed of the main F/W, which usually runs, and the standby F/W, which runs when the main F/W is out of order. The break down of the main F/W triggers an alarm, and the operator, who has caught the alarm, switches to the standby F/W.

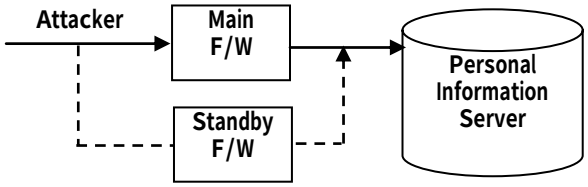

Figure 1 Illegal Access and F/W as a Mitigation System

3.2 Generation of an Accident Scenario with Event Trees

As illustrated in Figure 2, in PRA, the scenario of accident occurrence is described with a binary tree called Event Tree, and the point where the two branches diverge each other is called Node. The initiating event is written on the left of the scenario. In this case, the initiating event is "the attempt of an illegal access by the attacker," and the F/W responses to this initiating event as a mitigation system. In other words, an initiating event can be defined as the event that requires the response of the mitigation system.

To begin with, while the main F/W is working normally, the illegal access can be prevented, which means the mitigation system is working effectively. This is the Scenario 1 in Fig 2.

Next, let us suppose that the main F/W does not work, i.e., it has broken down. In this case, as has been stated in Section 3.1, an alarm is usually triggered, and the operator detects the abnormality of the main F/W. If the operator is successful in detecting the abnormality, he/she switches to the standby system. The case that the operator succeeded both in detecting the abnormality and in switching to the standby system is Scenario 2 that corresponds to Node 2.

Scenario 2 further diverges into another two branches. In the physical system like a nuclear reactor and a chemical plant, the operator has enough time-allowance for switching to the standby system. Therefore, if the operator has successfully detected the breakdown of the main system and switched to the standby system, the accident can be prevented.

However, in the case of information security, it is possible for the attacker to access during the time slot between the break down of the main system and the time when the standby system begins to work. Thus, Scenario 2 further diverges. In Scenario 2.1, illegal access is prevented because both the detection of the abnormality of the main system and the switching to the standby system are successful. In Scenario 2.2, illegal access is not prevented during the time slot between the breakdown and switching, even though both the detection of the abnormality and switching were successful.

As for the length of the blank time slot in the numerical example that will be stated later in Section 3.4, for the sake of simplicity, it is assumed that it takes 5 minutes to detect the abnormality of the main system and 5 minutes to switch to the standby system; that is, the total length of the blank time slot is 10 minutes. In this example, this time slot length is long enough for the attacker to illegally access because our aim is to explain PRA. Therefore, it goes without saying that depending on the way of access, it can be impossible for the attacker to access.

Now let us suppose for the sake of simplicity that the inspection cycle of the dual F/W is one month, that the two F/Ws come back to the mint condition after the inspection, and that the initiating event of "the attempt of illegal access by the attacker presents during the half of the one-month inspection cycle.

If the initiating event exists during the blank time slot, illegal access is possible. For example, the occurrence frequency of illegal access per month is 1 % in Scenario 2, the possible access frequency per month in Scenario 2.2 is 0.5 %. Needless to say, in Scenario 2.1, because the standby F/W is normally working, illegal access is prevented despite the presence of the initiating event.

In Scenario 3, the detection of the breakdown of the main system was successful but switching to the standby system failed. In this case, the standby F/W does not work and, as a result, illegal access cannot be prevented. From the viewpoint of maintenance, the situation that illegal access cannot be prevented continues until the next routine inspection. Likewise, in Scenario 4, since the detection of the abnormality of the main F/W has failed, illegal access cannot be prevented until the next routine

inspection. In Section 3.4, we will discuss the occurrence frequencies of these scenarios.

3.3 Analysis of the Cause of Branching with Fault Tree

The diagram in the lower part of Fig 2 is called Fault Tree that is used for the analysis of the reasons why each Event Tree diverges downwards.

As an example of Fault Tree of the dysfunction of the main F/W, the breakdown of the main F/W itself is a Fault tree on the one hand, which stems from the breakdown of either the hardware or the soft ware, and on the other hand, the mistake in setting the main F/W is also a Fault Tree.

Likewise, as for the cause of the failure of the detection of the breakdown of the main system, the dysfunction of the alarm and the misleading by the operator are the Fault Trees. In addition, as for the cause of the failure of switching to the standby system, erroneous operation and the breakdown of the standby system F/W are the Fault Trees. The latter can be divided into the breakdown of the main F/W itself and the error in setting the main F/W.

The events that are located at the bottom of the Fault Tree are called Basic Events, and in PRA, it is assumed that occurrence frequency and/or occurrence probability can be assigned.

Here, if we assign the numerical values to Basic Events in Fig 2, and if we assume that these events are independent each other, we can approximate the Top Event. For example, let us suppose that the occurrence frequency of the breakdown of the main F/W is 0.0005 times, and that the occurrence frequency of the breakdown of the main F/W that is caused by other reasons than erroneous setting is 0.005 times. Then, it can be approximated that the occurrence frequency of the breakdown of the main F/W is 0.01.Likewise, if it is assumed that the probability of the dysfunction of the alarm under the condition that the main F/W is broken down is 0.01, and that the probability of the erroneous recognition of the alarm by the operator is 0.01, then, it can be approximated that the probability of detection error (so-called Demand Breakdown Probability) is 0.02.Moreover, if it is assumed that the probability of switching failure under the condition that the detection is successful is 0.01, that the probability of the breakdown of the standby F/W caused by the erroneous setting is 0.005, and that the probability of the breakdown of the standby F/W caused by other reasons is 0.005, then it can be approximated that the probability of switching failure after the success of detection is 0.02.

In addition, when the same person set both the main system and the standby system by copying, the dysfunction of the main system means the dysfunction of the standby system, and thereby illegal access cannot be prevented. In this case, the independence of the Basic Events cannot be assumed; therefore, it is necessary to quantify based on the Minimal Cut Set, a failure mode. For example, the pair of the two Basic Events, i.e., the erroneous setting of the main F/W and the dysfunction of the alarm, is a Minimal Cut Set, and is also one of the failure modes of the dual F/W. Therefore, its occurrence frequency can be attained by multiplying the probability or the frequency of the Basic Events. In general, since there exist several Minimal Cut Sets, the scenario is quantified as the total of the occurrence frequency of each Cut Set.

Finally, the probability varies according to the different cases such as when the same person set the main F/W and the standby F/W individually without copying or when different persons set the main system and the standby system; therefore, it is possible to quantify the safety measures even though it is a relative estimation. Likewise, in the case of alarm detection, the scenario can be assumed that either the operator or the automatic switching worked or not.

3.4 Analysis with Concrete Numerical Numbers

As is indicated in Fig 2, if it is supposed that the breakdown frequency of the main F/W is 0.01 times per month, the probability of the detection failure is 0.02, and the probability of the switching failure after the successful detection is 0.02, the occurrence frequency under the presence of the initiating event is 0.0096, because $0.01\times0.98\times0.98=0.0096$.If this scenario occurs, since it is assumed that it takes 10 minutes to finish switching, the expected value of the time slot is 0.096 minutes, because$0.0096\times10=0.0096$.

Here, in order to exemplify, let us suppose that the real initiating event of the illegal access by the attacker occurs during half of the time slot, then by multiplying 0.096 (the expected value) by 0.5 (the probability of the presence of the initiating event), we can gain 0.048 minutes, which is the time length of illegal access per month in scenario 2.2.In other words, it can be estimated that during 0.048 minutes in a given month, illegal access of scenario 2.2 occurs. In order to reduce this time length, reduction of the time necessary for detection and switching can be considered.

Likewise, in scenario 3, the occurrence frequency is 0.000196, because$0.01\times0.98\times0.02=0.000196$.Here, for the sake of simplicity, it is assumed that this scenario occurs at the middle point of the inspection period. Then, because during the 15 days or 21600 minutes,

which is the time after the inspection, the dual F/W system is open to illegal access, the expected value is 4.23 minutes, because0.000196×21600=4.23.This is around 44 times longer than that of scenario 2.2.If the real illegal access is done during half of the times when the dual F/W is open to illegal access, the time length of the illegal access can be estimated as 2.11 minutes per month. In order to reduce this time length, the contraction of the routine inspection cycle and the reduction of the probability of switching failure can be considered.

Likewise, n scenario 4, the occurrence frequency is 0.0002, because0.01×0.02=0.0002.Here, for the sake of simplicity, it is assumed that this scenario occurs at the middle point of the inspection period. Then, because during the 15 days or 21600 minutes, which is the time after the inspection, the dual F/W system is open to illegal access, the expected value is 4.32 minutes, because0.0002×21600=4.32.This is around 45times longer than that of scenario 2.2.If the real illegal access is done during half of the times when the dual F/W is open to illegal access, the time length of the illegal access can be estimated as 2.16 minutes per month. In order to reduce this time length, the contraction of the routine inspection cycle and the reduction of the probability of detection failure can be considered.

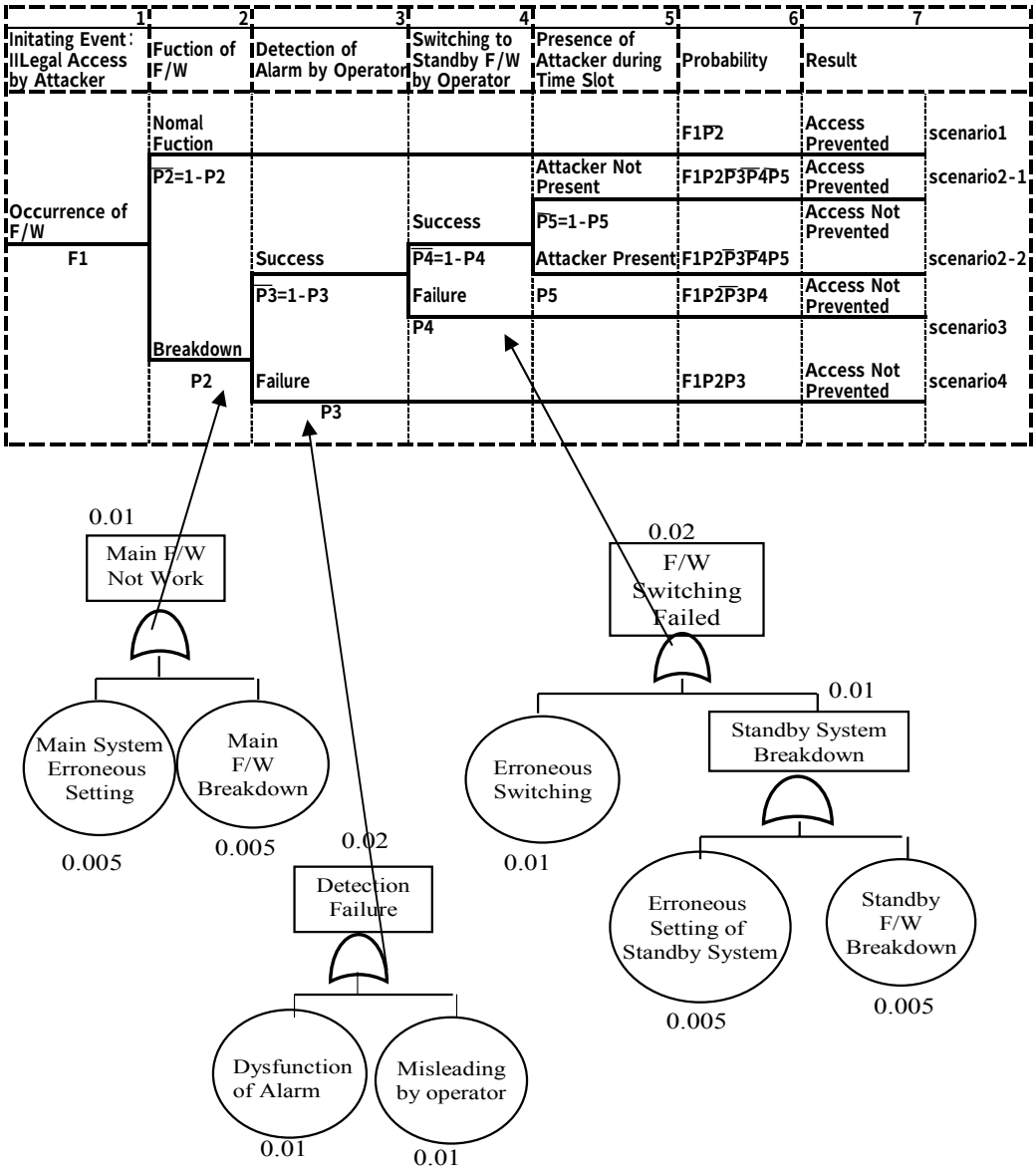

Figure 2 Event Tree and Fault Tree of Illegal Access as Initiating Event

4 Conclusion

In this paper, we have attempted to apply probabilistic risk assessment (PRA), which has been traditionally employed in assessing the risk of physical systems such as a nuclear reactor and a chemical plant, to the area of virtual information security. This is because we believe that ISO GMITS, the existing technique to quantify a risk of information asset based on the scores of information asset, threat, and vulnerability, lays emphasis on the easiness and is not based on the scenario of individual information accident.

Therefore, in this paper, following the method of PRA, we have attempted to quantify the risk of information asset by describing a scenario based on the responses of the mitigation systems to the initiating event of each Event Tree and Fault Tree. To be concrete, we supposed a case that an illegal access to the dual F/W, described its scenarios, calculated the occurrence probability of each scenario, and calculated the expected value of the time length of the illegal access.

As a result, it has been quantitatively revealed that to what extent the reduction of the time lengths of switching to the standby system, of the inspection, and of the probability of the failure in detecting dysfunctions and switching exerts influence on the expected value. It is impossible for GMITS to make such analyses.

References

[1] ISO: The guidelines for the management of IT security, TR13335 (2002)

[2] ASME: Standard for probabilistic risk assessment for nuclear power plant applications, ASMEA-S-2002 (2002)

[3] H. Kumamoto: Modern Reliability Engineering, Corona Inc. (2005)

[4] USNRC: Reactor safety study: An assessment of accident risk in U.S. commercial nuclear powerplants. USNRC, WASH1400, NUREG-75/014(1975)

[5] G.E. Apostolakis, J.H. Bickel, S. Kaplan: Probabilistic risk assessment in the nuclear power utility industry, Reliability Engineering and System Safety, vol. 24 no. 2,91-94(1989)

[6] H. Kumamoto, E.J. Henley: Probabilistic risk assessment and management for engineering andscientists, IEEE Press(1996)

[7] H. Kumamoto: Satisfying safety goals by probabilistic risk assessment, Spinger(2007)

[8] N. Satoh & H. Kumamoto, Enumeration of initiating events of information security accidents,2007 International Conference Innovation & Management, pp. 119-124(2007)

[9] H. Kumamoto, E. J. Henley: Probabilistic risk assessment and management for engineers and scientists, IEEE Press (1996)