An Advantage Factor of Probabilistic Risk Assessment in Information Security

Naoki Satoh, Hiromitsu Kumamoto
Kyoto University, Graduate School of Informatics
36-1, Yoshida-honmachi, Sakyoku, Kyoto, 606-8501 JAPAN
Sato@sys.i.kyoto-u.ac.jp, kumamoto@i.kyoto-u.ac.jp

Abstract: In our previous study, we maintained that “probabilistic risk assessment”, which has been traditionally employed in assessing the risk of physical systems such as a nuclear reactor and a chemical plant, is superior to other method in the ability of generating the scenario of hazard occurrence, and so on. In this paper, by taking Firewall System as an example, we will clarify the advantages of PRA over other method in generating more detailed scenario, in the ability of risk quantification, and so on.

Key Words: Initiating event, Probabilistic risk assessment, Event tree, Fault tree, Safety measures, Information security

1. Introduction
The probabilistic risk assessment (PRA) is the most powerful approach to quantifying risks of physical systems such as nuclear power plant, chemical plant, and railroad facility. The PRA began with the US reactor safety study in 1975 with a code name of WASH-1400 [1]. Since then the methodology has advanced to a point where international standards in US, Europe, and Japan are available for quality assurance of the PRA [2].

A full-scale PRA is divided into three levels. Level 1 PRA deals with the occurrence of accident, level 2 with the progression of accident and release of toxic material into the environment, and level 3 with the material transport and damage to people, facility and environment [3, 4]. This paper is concerned with the level 1 PRA typically used to examine satisfaction of a performance goal such as core damage frequency, rather than a more remote safety goal such as fatality rate [5].

Even if an accident type such as explosion is fixed, various paths or scenarios or sequences yield the accident. Obviously, these scenarios have to be first enumerated to quantify the risk. A most remarkable characteristic of PRA is that the scenarios are enumerated for each event in a list of “initiating events”. Event trees (ET) are used to visualize the enumeration. A fault tree (FT), on the other hand, is used to search for basic causes of a specific branch on the ET. A complete list of initiating events is available for traditional systems such as a nuclear power plant.

The initiating event is a crucial concept specific to the PRA. This can be defined as the event with the following characteristics.
1) During a design-base situation, mitigation systems are activated to cope with the initiating event, and the accident is prevented.
2) During a beyond-design-base situation, failed mitigation systems can not cope with the initiating event, and the accident occurs. Completely different approaches from PRA have been used for the information security risk assessment. Key concepts such as assets, threats, vulnerabilities, impacts, l
likelihoods, and safeguard emerged during the 1990's, yielding a qualitative approach called GMITS (Guidelines for the Management of safeguards of IT Security) [6]. The information security accident is defined as a breach of confidentiality, integrity, or availability [7, 8]:

1) Confidentiality: The information is protected from unauthorized or accidental disclosure.
2) Integrity: The information is as intended without inappropriate modification or corruption.
3) Availability: Authorized users can access applications and systems when required to perform their jobs.

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:

\[
\text{Risk value} = (\text{information asset value}) \times (\text{threat value}) \times (\text{vulnerability value})
\]

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.

A scenario enumeration from the initiating event to the accident has not been performed.

The cyber security article [9] is a good survey of information security risk assessment. There is a superficial resemblance between a threat and an initiating event. However, the former can not replace the latter. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) uses event trees to classify the threats [10]. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, although interesting, are quite different from the ones used for ordinary PRA event trees which model responses of mitigation systems. OCTAVE neither enumerates initiating events nor accident scenarios in a way of traditional PRAs.

Fault trees are used in "attack tree" articles [11,12]. An attack tree represents how an attacker succeeds in achieving the intention. Only a limited number of scenarios can be enumerated due to the use of fault trees. The traditional PRA uses event trees to enumerate scenarios; the fault trees are used to search a superficial resemblance between a threat and an initiating event. However, the former can not replace the latter. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) uses event trees to classify the threats [10]. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, although interesting, are quite different from the ones used for ordinary PRA event trees which model responses of mitigation systems. OCTAVE neither enumerates initiating events nor accident scenarios in a way of traditional PRAs.

Fault trees are used in "attack tree" articles [11,12]. An attack tree represents how an attacker succeeds in achieving the intention. Only a limited number of scenarios can be enumerated due to the use of fault trees. The traditional PRA uses event trees to enumerate scenarios; the fault trees are used to search a superficial resemblance between a threat and an initiating event. However, the former can not replace the latter. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) uses event trees to classify the threats [10]. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, although interesting, are quite different from the ones used for ordinary PRA event trees which model responses of mitigation systems. OCTAVE neither enumerates initiating events nor accident scenarios in a way of traditional PRAs.

Fault trees are used in "attack tree" articles [11,12]. An attack tree represents how an attacker succeeds in achieving the intention. Only a limited number of scenarios can be enumerated due to the use of fault trees. The traditional PRA uses event trees to enumerate scenarios; the fault trees are used to search a superficial resemblance between a threat and an initiating event. However, the former can not replace the latter. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) uses event trees to classify the threats [10]. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, although interesting, are quite different from the ones used for ordinary PRA event trees which model responses of mitigation systems. OCTAVE neither enumerates initiating events nor accident scenarios in a way of traditional PRAs.

Fault trees are used in "attack tree" articles [11,12]. An attack tree represents how an attacker succeeds in achieving the intention. Only a limited number of scenarios can be enumerated due to the use of fault trees. The traditional PRA uses event trees to enumerate scenarios; the fault trees are used to search a superficial resemblance between a threat and an initiating event. However, the former can not replace the latter. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) uses event trees to classify the threats [10]. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, although interesting, are quite different from the ones used for ordinary PRA event trees which model responses of mitigation systems. OCTAVE neither enumerates initiating events nor accident scenarios in a way of traditional PRAs.
ble the PRA application to the information security risk assessment.

2. SECURITY ACCIDENT PHASES

The steps toward an information security accident are below phase.
1) Phase 1: An attacker enters the facility boundary.
2) Phase 2: The attacker approaches to a target information asset.
3) Phase 3: The attacker breaches confidentiality, integrity, or availability of the information asset.

Phase 1 is a physical intrusion through the facility boundary. Another type of intrusion through network gate is not dealt with here, although both seem similar to each other because a password, for instance, corresponds to a virtual password like password.

The target information asset can not always be approached to even if the attacker succeeds in entering the facility boundary. The asset may be hidden. The attacker may have to pass additional gate to find the asset.

Suppose that the information asset is a USB memory on a desk. Then the attacker in phase 3 can simply take the memory out of the facility. Suppose on the other hand, that the information asset is stored in a PC hard disk protected by a log-in password. Then, the infringement of information would be harder than the USB case.

This paper deals with the first phase, the intrusion through the facility boundary because this is a first stage to examine the feasibility of PRA application to information security problem.

3. 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 PRA sample case: Firewall

As indicated in Fig 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.

![Diagram of Illegal Access and F/W as a Mitigation System](image)

3.2 Generation of an accident scenario with event trees

As illustrated in Fig 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 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 ano
her 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 breakdown 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 software, 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 0.01×0.98×0.98=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 0.0096×10=0.096.

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 0.01×0.98×0.02=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, because 0.000196×21600=4.23. This is around 44 times longer t
han 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, in scenario 4, the occurrence frequency is 0.0002, because $0.01 \times 0.02 = 0.0002$. Here, for the sake of simplicity, it is assumed that this scenario occurs at the middle point of the inspection period. This is around 45 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 2.16 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.

4. Physical Access Attacker

Consider an entrance control by electronic cards. A duplicated entrance controller permits entrance for personnel with an authorized card. A principal controller, an operator, and a standby controller constitute a mitigation system. Note that this tree has the same structure as Figure 2, considering this event tree, In spite of the fact that the latter deals with physical access, while the former with network access. This indicates that, once an event tree is constructed, a similar version can be applied to other problems of information security.

5. 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 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.

Acknowledgement

This paper could not have been completed without various useful advices from my project members and party involved. We would like to express our sincere gratitude to these people.
The image contains a flowchart and a table describing a process involving illegal access by an attacker, followed by the detection of that access by an operator. The flowchart illustrates the sequence of events leading to the initiation of a Standby F/W by the operator, which results in the prevention of access in some scenarios.

**Table:**

<table>
<thead>
<tr>
<th>Event</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Function</td>
<td>P=1-P1</td>
</tr>
<tr>
<td>Failure</td>
<td>P1=1-P1</td>
</tr>
<tr>
<td>Occurrence of F/W</td>
<td></td>
</tr>
<tr>
<td>Success</td>
<td>P1=1-P1</td>
</tr>
<tr>
<td>Failure</td>
<td>P1=1-P1</td>
</tr>
<tr>
<td>Breakdown</td>
<td>P1=F</td>
</tr>
</tbody>
</table>

**Event Tree and Fault Tree of Illegal Access as Initiating Event, F/W example**

The flowchart shows the various paths and probabilities associated with the different events and outcomes.

**REFERENCES**

11. B. Schneider: Attack trees, Dr. Dobb’s Journal, December(1999)