A Method of Selecting Optimal Measures for Security and Usability with Fault Tree Analysis and State Transition Diagram

Koichi Kato[*] and Yoshimi Teshigawara[**]
Faculty of Engineering, Soka University, Japan
[*]kokatou@soka.ac.jp, [**]teshiga@t.soka.ac.jp

Abstract—A high level of security must be maintained on a network to protect information assets, but usability is required to achieve the network's designed purpose. Security and usability, however, have a trade-off relation. Selecting appropriate security measures is difficult because (i) chain relations exist for risks and services use and (ii) the relations among risks, usability and security measures are complex. This paper proposes a method of analyzing risk/usability and selecting measures by using Fault Tree Analysis (FTA) and State Transition Diagrams (STDs). This method is used to analyze risk and usability visually and quantitatively in consideration of chain relations. The method also allows the causes of incidents to be inferred by converting the STD to a Bayesian network. Accordingly, we can estimate the interdependence among risks and usability, and thereby find a critical point for risks and usability. As a result, we can select optimal measures to control and monitor network security and usability.

Keywords: Risk Management, Usability, Fault Tree Analysis, State Transition Diagram, Bayesian Network.

1 INTRODUCTION

Recently, a variety of network environments have been constructed, such as home networks, enterprise and university networks, and high-speed public wireless networks. These networks are established for various purposes such as accessing to the Internet, sharing resources and conducting business efficiently.

However, information systems on a network are exposed to many risks including information leakage and unauthorized access (e.g., hacking). The occurrence of a security incident can cause not only direct damages such as lost business or system recovery costs, but also loss of organizational credibility. Therefore, a variety of security measures are now implemented on networks to reduce risk.

For a network to fulfill its designed purpose, a suitable balance must be struck between the security of information assets and usability of services. However, security and usability are generally in a trade-off relation. For example, security measures can disturb comfortable use of information systems by increasing the number of steps in a process or slowing the execution speed of the system; excessive security measures decrease the level of usability. In contrast, excessive usability decreases the level of security. Accordingly, balancing security with usability is a difficult but critical task.

In addition, risks and usability must be managed and monitored to determine whether security incidents occur and whether services are properly provided [1]. However, deciding appropriate monitoring points is difficult for a network consisting of many devices.

In related studies on the prioritization of risk, Zuccato [2] described the decision matrix and Guan et al. [3] evaluated security with the Analytic Hierarchy Process and the risk level matrix. They analyzed risks only from the viewpoint of expert users and did not consider the existence of multiple stakeholders. Yajima et al. [4] proposed the multiplex risk communicator to decide measures based on agreement among stakeholders. However, they did not analyze usability in detail. Kotenko and Stepashikin [5] as well as Wang [6] described security evaluation methods using the attack graph, which allows the events of an incident to be analyzed visually and measures to be implemented in consideration of the network configuration. However, the effects on usability of the selected measures cannot be expressed.

In our research, we have approached this matter in two ways, devising (i) a method of selecting optimal measures when the implemented measures are changed [7] and (ii) an expression model of risks, usability and security measures [8]. Combining the above-mentioned method and model, we propose a method of selecting optimal measures to construct a network that has high usability to conduct business efficiently and sufficient security to protect information assets. With this method, phases of risks and services use can be analyzed by using Fault Tree Analysis (FTA) and State Transition Diagrams (STDs). In this way, we can estimate the interdependence among risks and usability, and thereby find their critical point for risk and usability. As a result, we can select optimal measures intuitively by quantifying and visualizing risks, usability and the effects of security measures.

2 RESEARCH ISSUE

2.1 Analysis of Risk and Usability Having Chain Relations

There exist risk chains where the occurrence of a single risk event leads to multiple other risks. In addition, in risk chains, a fundamental part of a risk event can diverge to other risks. Similarly, there exist usability chains where the deterioration of usability in one area adversely affects the usability in other areas. Therefore, analyzing the relations among risks and usability with chain relations is necessary to maintain usability and to reduce risk.

2.2 Relations among Risk, Usability and Measures

The relations among security measures, risks and usability are complex. Several security measures can be taken against a single risk, but a measure can also be effective

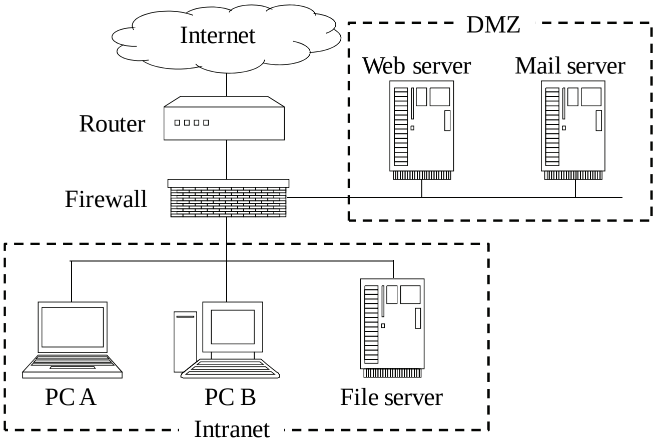

Figure 1: Example of network configuration.

against multiple risks. Moreover, measures to address risks can affect usability. In order to control risks and usability appropriately, a critical point must be found for risks and usability that is more sensitive to the effects of a security measure. The implementation of a measure at the critical point can cause a considerable increase or decrease in security and usability. Therefore, analyzing these relations properly and effectively is crucial.

2.3 Relations among Risk, Usability and Measures

The relations among security measures, risks and usability are complex. Several security measures can be taken against a single risk, but a measure can also be effective against multiple risks. Moreover, measures to address risks can affect usability. In order to control risks and usability appropriately, a critical point must be found for risks and usability that is more sensitive to the effects of a security measure. The implementation of a measure at the critical point can cause a considerable increase or decrease in security and usability. Therefore, analyzing these relations properly and effectively is crucial.

2.4 Selection of Optimal Measures

We define “optimal measures” as the combination of measures that system administrators and users accept with satisfaction from the viewpoints of security and usability. In this research, we target the phases of both implementing and modifying security measures. The requirements for security and usability can vary depending on the situation; for example, the security and usability requirements of users and system administrators differ.

Objective evaluation of the security and usability levels that would results from implementation of candidate measures is needed to select appropriate measures. Our method quantifies the probability and value of risks, which are general metrics, and usability. The value of usability in our method is the rate of comfortable service use relative to the completely unrestricted use of the service without implementation of security measures.

Administrators and users may select excessive or insufficient measures that cause undesirable decreases in security and usability if we only calculate the theoretical optimal measures. Therefore, a scheme for selecting appropriate measures intuitively is needed.

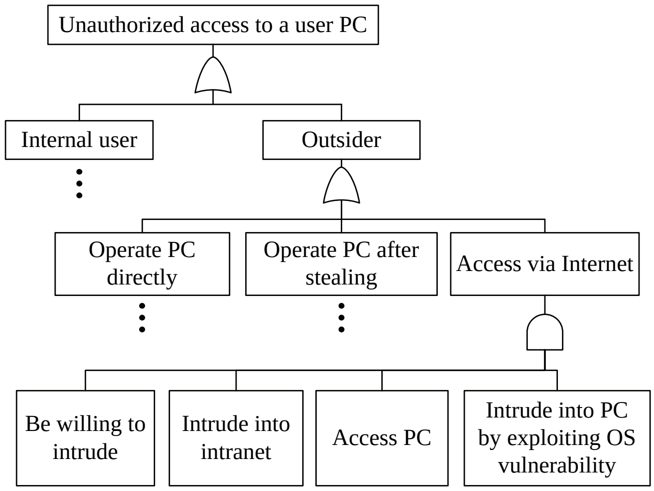

Figure 2: Fault tree for unauthorized access to a user PC.

In addition, the validity of monitoring points for security and usability cannot be evaluated because the points are often decided by experimental rules. Moreover, there exist no objective metrics to infer causes of incidents when a risk event occurs, and as such the scope of the analysis to determine the cause can become unnecessarily broad. Therefore, a scheme for selecting monitoring points and determining the causes of incidents is needed.

3 RISK AND USABILITY ANALYSIS WITH FTA

Our method adopts FTA as a quantification method. FTA has following features: (i) it can analyze factors that prevent the achievement of a specific goal, (ii) it can organize measures to control each factor and (iii) it can decide appropriate measures for specific issues. FTA is used to construct Fault Tree (FT) where the top represents an event as the result of other causal events; these events are joined by logical AND/OR gates [9].

3.1 Example Network

To describe the proposed method, we next present tangible examples. We assume a simple network as shown in Figure 1. The network is separated into a DMZ and the Intranet. A web server and a mail server are located in the DMZ. General users work on user PCs. The users can use files on a file server, browse web sites, and send and receive e-mails.

3.2 Risk Analysis

Generally, a risk event consists of several phases. A risk can be reduced by implementing security measures to prevent the occurrence of each phase based on the concept of defense in depth [10].

In order to quantify risk probabilities, the proposed method makes FTs of risks. First, an unexpected risk event is placed at the top of the FT. Second, attack phases are incorporated at the bottom as shown in Figure 2. Third, measures related to each basic event are clarified. Finally, the probability of a basic event, the decrease in the risk of the targeted

Table 1: Analysis of risks and security measures.

Basic event	Probability	Measure	Risk decrease	State
Be willing to intrude	0.7	-	-	-
Intrude into intranet	0.7	Authentication for network access	0.9	0
		FW access control	0.7	1
Access PC	0.7	At PC: PFW access control	0.5	1
Intrude into PC by exploiting OS vulnerability	0.4	At PC: OS update	0.7	1

basic event caused by a security measure, and the implementation state of a measure, which has yes or no selectively, are assigned as shown in Table 1. Note that the acronyms FW and PFW stand for firewall and personal firewall, and the value of the implementation state (described as "state" in Table 1) is 0 for "not implemented" or 1 for "implemented".

The risk probability is formulated as follows. The probability of the top event is calculated from the minimal cut sets, which are the minimum collections of basic events defined such that if they all occur, the top event also occurs.

The probability of the top event, P_{top}, is given by the following equation:

$$P_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} P_e \prod_i \left(1 - X_i \Delta P_{e,i} \right) \right\}, \qquad (1)$$

where c is a minimal cut set, C is a set of c, e is a basic event in a cut set, E_c is a set of e in c, P_e is the probability of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the decrease in the risk of event e by implementation of measure i.

3.3 Usability Analysis

The process of service use consists of several phases. The usability of a service can become insufficient because security measures prevent the realization of some phases.

To quantify the usability of services, we use the proposed method to construct FTs of services use. First, an object service is placed at the top of the FT. Second, phases of use are placed at the bottom, as shown in Figure 3. Third, measures related to each basic event are clarified. Finally, the usability of a basic event, the decrease in the usability of the targeted basic event because of the implemented measure and the implementation state of a measure are assigned as shown in Table 2. Note that the value of usability for each basic event is taken as 1 as a standard according to the definition in Section 2.3.

Through this analysis based on the concept of phases, the proposed method can be used to calculate the effective measures preferentially because a measure related to the violated phase recovers the usability better than one related to another phase. Therefore, our method can select appropriate measures considering actual service use.

The usability of the top event, U_{top}, is given by the following equation:

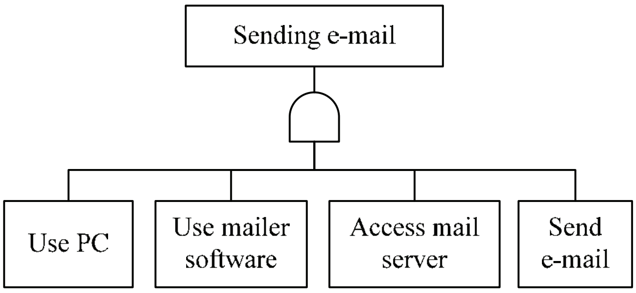

Figure 3: Fault tree for usability of sending e-mail.

Table 2: Analysis of services use and security measures.

Basic event	Usability	Measure	Usability decrease	State
Use PC	1	-	-	-
Use mailer software	1	At PC: password for mailer software	0.3	1
Access mail server	1	At PC: PFW access control	0.1	1
Send e-mail	1	At mail server: Authentication for sending e-mail	0.1	1

$$U_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} U_e \prod_i \left(1 - X_i \Delta U_{e,i} \right) \right\}, \qquad (2)$$

where U_e is the usability of the basic event e and $\Delta U_{e,i}$ is the decrease in the usability of event e by implementation of measure i.

4 RELATIONAL ANALYSIS WITH STATE TRANSITION DIAGRAM

We analyze risks, usability and their chain relations with STDs. FTA can also be used to analyze the relations by combining FTs. However, combining FTs complicates the analysis greatly because FTs can become extremely large. In this case, identifying where each event in the FTs occurs on the target network is difficult. In contrast, the method of making STDs and incorporating them with a network model can be used to analyze risk, usability and these relations visually and intuitively.

4.1 Creating and Combining the STDs of Risk and Usability

The STD of a risk shown in Figure 4 is created by taking the basic event in the FT in Figure 2 as the event in the STD; then, we take the result of the event in the FT as the state in the STD. Similarly, the STD of usability shown in Figure 5 is created from Figure 3.

Each arrow from one state to another represents the probability of the state transition, which is equal to the probability/usability of a basic event as shown in Table 1 and Table 2, owing to the correspondence between the FT and STD. In addition, measures to prevent the realization of a phase are placed on the arrow. Multiple measures can be placed on a single arrow.

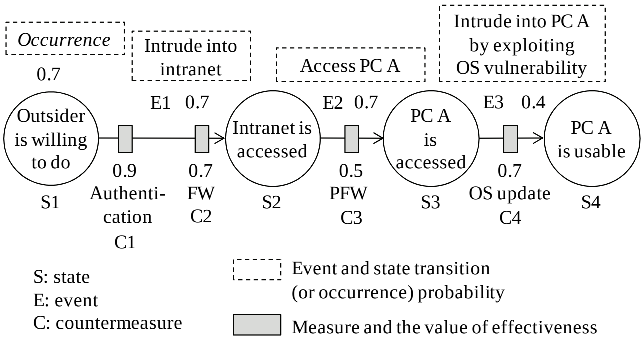

Figure 4: STD of unauthorized access to a user PC.

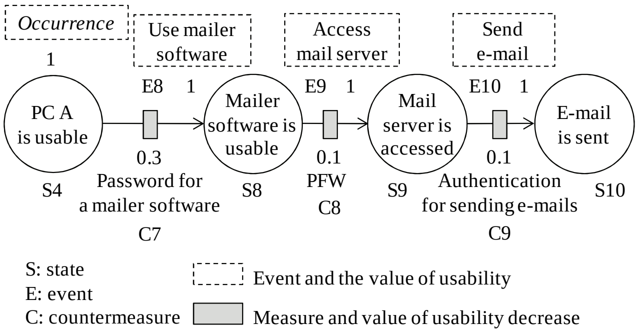

Figure 5: STD of sending e-mail.

In Figure 4 and Figure 5, the decreases in risk/usability caused by a measure are equal to those shown in Table 1 and Table 2. The value is treated as the rate of blocking the state transition. Additionally, a state occurring independently, such as motivation (i.e., "be willing to do something"), has a probability of occurring.

The STDs can be combined by merging identical states, as shown in Figure 6. In order to combine the STDs, idempotent and distributive laws are applied because the STDs correlate with the FTs, and the states and events in the STD can be treated as constituent factors of risks and usability [9]. Note that commutative law cannot be applied because state transition has direction.

The STDs of both risks and usability are also combined by merging identical states such as "PC A is usable" in both Figure 4 and Figure 5. For example, in the case of data leakage from PC A by e-mail, the value 1, which is the standard of usability, can be directly converted into the probability of a successful attack. Therefore, the STD of usability changes to that of risk.

The STDs are deployed on a network model. The organization has some network segments such as a DMZ and an intranet, which can be further divided into additional areas, for example, business departments. Based on the existing defense in depth model [11], our method creates a network model that has network segments and machines in each segment. The machines are also treated as several layers.

For example, the simple network configuration shown in Figure 1 is converted into the model shown in Figure 7 by dividing the network into the DMZ and intranet and developing each machine into the layers of host, application and data. The STDs are deployed on this network model as shown in Figure 8. Each state occurs on a specific layer.

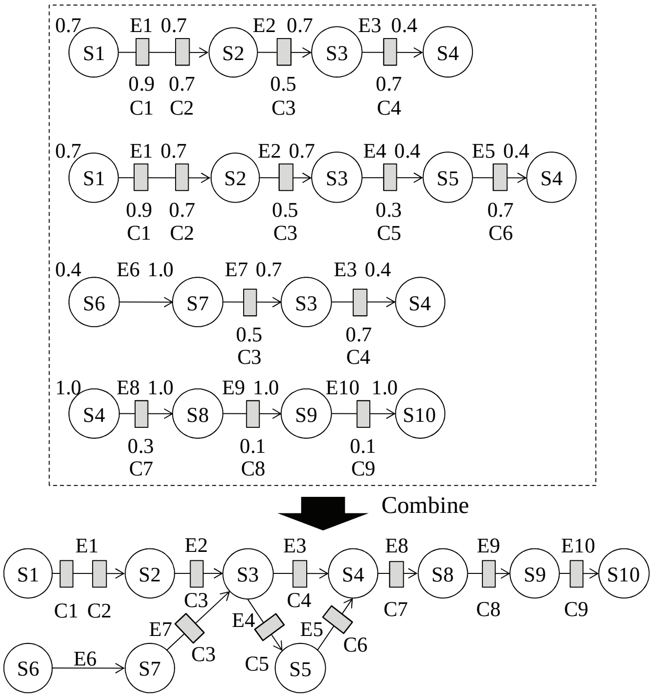
0.7 S1 E1 0.7 S2 E2 0.7 S3 E3 0.4 S4
0.9 C1 0.7 C2 0.5 C3 0.7 C4
0.7 S1 E1 0.7 S2 E2 0.7 S3 E4 0.4 S5 E5 0.4 S4
0.9 C1 0.7 C2 0.5 C3 0.3 C5 0.7 C6
0.4 S6 E6 1.0 S7 E7 0.7 S3 E3 0.4 S4
0.5 C3 0.7 C4
1.0 S4 E8 1.0 S8 E9 1.0 S9 E10 1.0 S10
0.3 C7 0.1 C8 0.1 C9
Combine
S1 E1 C1 C2 S2 E2 C3 S3 E3 C4 S4 E8 C7 S8 E9 C8 S9 E10 C9 S10
E7 C3 E4 C5 S5 E5 C6
S6 E6 S7

Figure 6: Combining STDs.

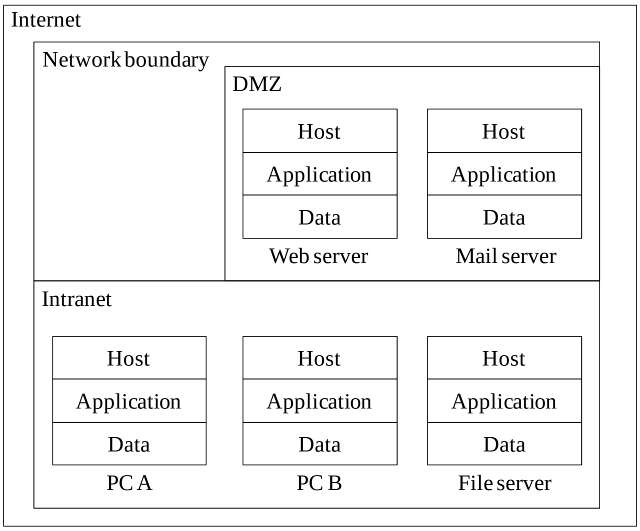

Figure 7: Model of network (cf. Figure 1).

Each arrow passes to a related layer. Each security measure is implemented on a layer.

In addition, STDs can be copied from one machine to another that has identical risks. Differences between machines such as the implementation states of security measures can also be customized as needed.

Details of the model should be set depending on the objectives and accuracy of risk analysis that the organization requires. In the case of Figure 7, the firewall is excluded because we regard it as a security measure. The router is also omitted because we do not consider it to face threats. The network model can treat several segments as a single area and add layers related to hardware such as data storage devices (e.g., hard disks) and I/O devices (e.g., LAN cards).

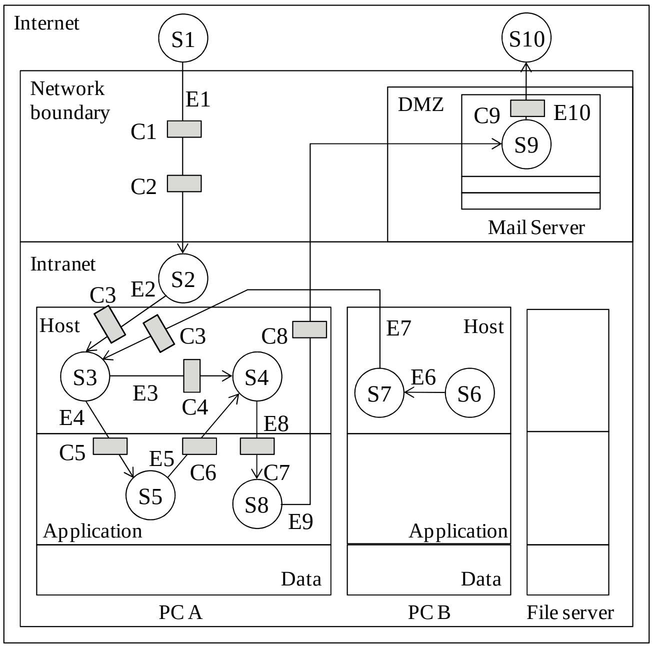

Figure 8: Deployment of risks, usability and security measures on the network model.

4.2 Quantification of Risks and Usability

With Formula (1) and (2) obtained by FTA, we quantify each risk and usability. The STD expressing chain relations can also be used to quantify them.

The risk probability, the value of a risk and the value of usability can be quantified using a model such as the one shown in Figure 8. First, we select the starting and ending states of a target risk. At this time, several starting states can be selected. Next, we extract paths going from each starting state to the ending state. Then, the risk probability P_n for path n is given as follows:

$$P_n = \prod_{e \in E_n} P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right), \qquad (3)$$

where e is an event included in path n (e can be the occurrence of a starting state), E_n is a set of e, P_e is the probability of a state transition or the probability of the occurrence of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the decrease in the probability of event e caused by measure i.

Finally, the total probability P_{total}, that is, the probability of at least one of the paths being realized, is given by

$$P_{total} = 1 - \prod_{n \in N} \left(1 - P_n\right), \qquad (4)$$

where N is a set of all paths.

In addition, Formulas (3) and (4) are related to Formula (1) because STDs have a correspondence relation to FTs. Therefore, we must not exponentiate the same state transition probability and the decrease in risk/usability by the same measure in the case that several paths include a common event. We must replace the exponent as follow [9]:

$$\left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}^2 \rightarrow \left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}$$

Table 3: Transforming state transition probability to conditional probability.

P(S1)
P_{S1}

P(S6)
P_{S6}

S1	P(S2)
T	P_{E1}
F	0

S6	P(S7)
T	P_{E6}
F	0

S2	S7	P(S3)
T	T	1-(1-P_{E2}) (1-P_{E7})
T	F	P_{E2}
F	T	P_{E7}
F	F	0

S3	P(S5)
T	P_{E4}
F	0

S3	S5	P(S4)
T	T	1-(1-P_{E3}) (1-P_{E5})
T	F	P_{E3}
F	T	P_{E5}
F	F	0

* P(S2), P(S3), P(S4), P(S5) and P(S7) are the conditional probability.
T: transition to the state is done.
F: transition is not done.

Furthermore, we can calculate the value of risks in consideration of the value of assets. This paper defines the value of risk as

Value of risk = *Value of assets* × *Risk probability*.

For example, when a selected ending state is on the data layer, the risk relates to data. The value of the risk is calculated using the value of the data and the risk probability using Formulas (3) and (4).

Similarly, usability is calculated using Formulas (3) and (4) based on paths for use of a service. Note that $\Delta P_{e,i}$ is the decrease in usability of event e caused by measure i.

4.3 Causal Inference of Incidents

We can regard STDs (e.g., Figure 8) as a probabilistic model of cause-and-effect relations. Therefore, we can treat STDs as a Bayesian network by changing the state transition probability into conditional probability. Note that each state transition probability must be independent of the previous and following phases. As a result, we can infer the probability of causes of an incident.

For example, in Figure 8, we suppose that the state S4 occurs and all measures were not implemented. Table 3 shows the conditional probability of states in the path to S4. The probability that S1 occurred is given as follows

$$P(S1|S4) = P(S1 \cap S4) / P(S4).$$

When no state in the selected paths has an occurrence probability such as {S2, S3, S4, S5}, we calculate the arrival probability of S2 as the occurrence probability with Formula (3) and (4).

5 EXPERIMENT

We apply our method at the stages of implementing and modifying security measures in an example of a simple network. We then confirm that our method can be used to analyze phases of risks and usability and to select optimal measures in consideration of where they are implemented.

5.1 Assumptions

In order to avoid complex analysis, we assume a simple network as shown in Figure 1. As discussed in Section 3.1, general network users browse websites, send and receive e-mails and use files on a file server.

We analyze risks selectively because real results of risk analysis in actual organization networks are unavailable due to the confidentiality of security information. The targeted risks are (i) unauthorized access to a PC via networks, (ii) data leakage of a confidential file via networks and (iii) virus infection on a PC. The target services related to usability are (i) browsing websites, (ii) sending e-mails, (iii) reading e-mails and (iv)using files on the file server.

In this experiment, each value is quantified at a certain level. Regarding risks, the state transition probability of a phase has four levels (0.1, 0.4, 0.7, 1.0). The decrease in risk caused by a security measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). Regarding usability, the state transition probability of a phase has a standard value 1. The decrease in usability caused by a security measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). The implementation state of a measure has two levels (0, 1).

5.2 Visual and Quantitative Risk Analysis and Measure Selection

(1) Model Creation

First, we model the network. In this experiment, the network is modeled as shown in Figure 7.

Second, we analyze assets, threats, vulnerabilities and phases of target risks and usability as shown in Figure 2 and Figure 3. Then, we clarify measures to basic events based on Reference [12] and assign the probability of a basic event, the decrease in risk/usability caused by a measure and the implementation state of a measure, as shown in Table 1 and Table 2. Finally, we express risks and usability as STDs and deploy them on the network model with implemented security measures. As a result, the model was created as shown in Figure 9.

In this case, all of the event name, the state transition probability and the decrease in risk/usability caused by security measures are eliminated from Figure 9 in order to prevent the model from becoming complex. Most parts of the STDs about PC B are also eliminated because they were copied from PC A.

(2) Use of the Model for Simple Analysis and Correction of the Analysis Results

The created model can be used as an effective visualization tool, which can make it simpler to check and correct the results of risk/usability analysis. In the experiment, some results of the risk analysis and the implementation states of measures by using FTA were reconsidered at the STD model creation.

First, several phases were modified to expand their details because the model could not express several measures on an appropriate layer. The reason is that the phases of risks and the places to implement security measures become clear. Specifically, we added the state named “inappropriate application use” and redeployed the measure named “application update” from the host layer to the application layer. We also added the candidate measure “limitation of usable applications” at the transition between “PC access” and “inappropriate application use”. This measure, however, is not drawn in Figure 9 because we decided not to implement it.

Next, some of the state transition probabilities were modified. They had differed even though the phases were shared by certain risks. The probability of a particular phase should be equal regardless of previous or following phase. Similarly, some decreases in risk caused by a security measure were modified. These values had differed even though the measure was implemented in a common phase for certain risks. These modifications were made to address inconsistent results of risk analysis when combining STDs.

Furthermore, some measures which had already being deployed in a certain phase were copied to other phases. We found that a measure affects the specific targeted phase as well as other phases. The reason of this work is that we can visually clarify phases of risks and the layer where measures are implemented. For example, we found that the security measure “access rights” for reducing the risk of data leakage relates to control of virus infection and sending/receiving attached files in an e-mail; accordingly, we added the measure to appropriate places in the data layer.

Finally, measures that mutually affect certain phases of risks are added as follows: “web filtering”, “PFW preventing inbound access”, “PFW preventing outbound access” and “limitation of attached files in e-mails”. These measures were added so that we can consider whether some measures affecting several events. For example, “web filtering” affects three phases efficiently.

(3) Quantitative Assessment of Risks and Usability

Table 4 shows the probability of risks and the value of usability from the initial analysis using only FTA and from the second analysis using both FTA and STDs. We assessed the value of assets simply as shown in Table 5 and calculated the value of risks as shown in Table 6 from the risk probabilities and the values of the assets, which are the amount of damage when a risk event occurs. Note that although these results include some increased probabilities of risks and decreased usability, they mean not that we selected inappropriate measures, but that we analyzed the risk and usability more accurately.

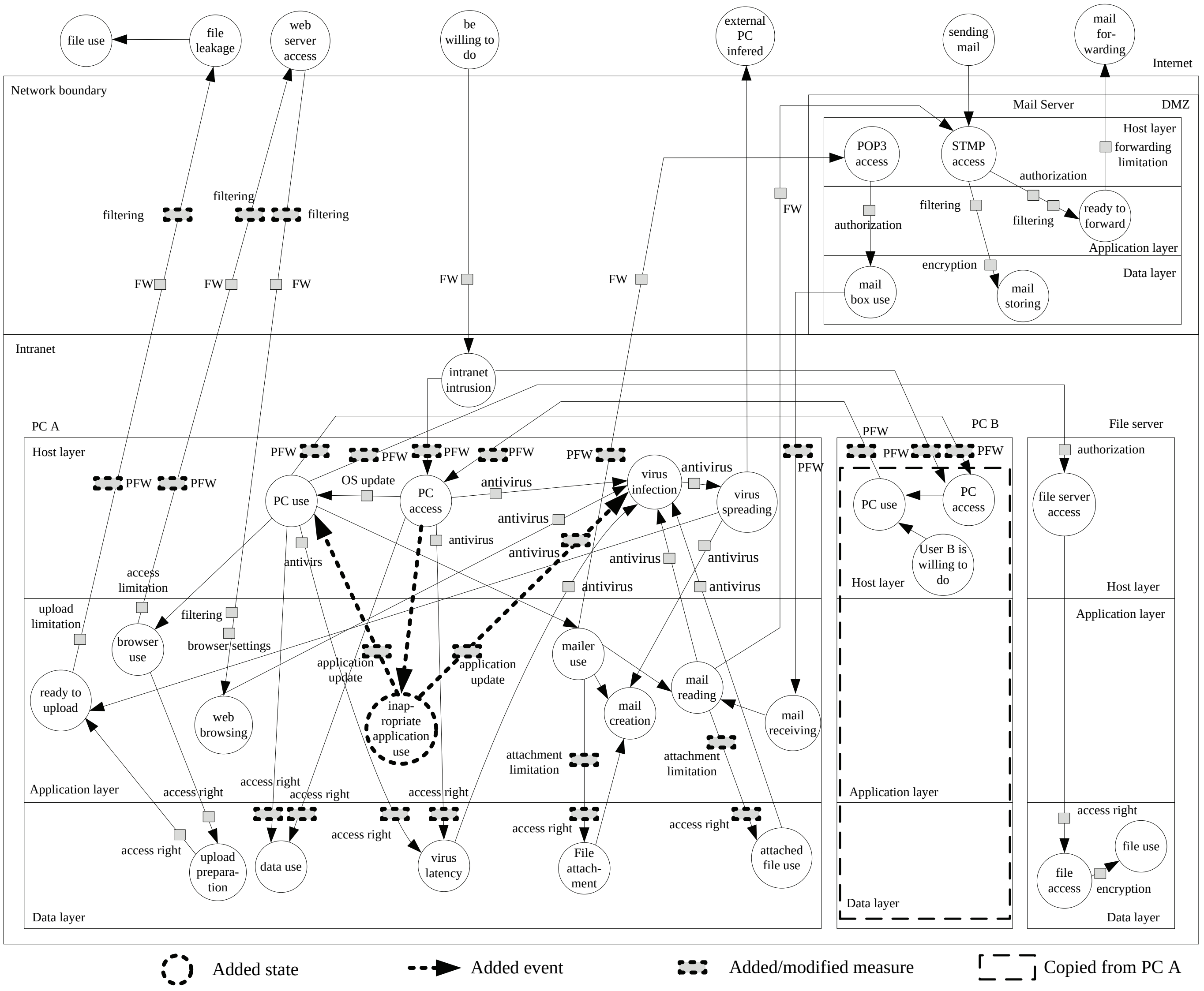

Figure 9: Model of risks, usability and security measures in the assumed network.

As a result, our method can be used to assess risks and usability quantitatively and to select security measures to reduce risks and improve usability.

5.3 Impact Estimates for Measures Control

Some measures must be modified to increase the security or usability by the plan-do-check-act cycle for improving of information security management systems. For reviewing or modifying security measures, identifying the resultant changes of security and usability is important.

Our method using FTA can calculate optimal measures by solving a discrete optimization problem with objective functions to minimize the increase in risk and the decrease in usability and constraint functions to maintain appropriate levels of risk and usability. We can recognize the impact of modifying measures visually by combining the above method with STDs.

We suppose that, for example, in the development of a software product, the user of PC A needs to communicate bidirectionally with an external system using a certain TCP/IP port, which is ordinarily closed. The user requests that the administrator open the port in the firewall. If the port is opened, the network risks being intruded more easily by attackers via the Internet. At the same time, this change causes an increased likelihood of reaching all states that follow from the state “intranet intrusion”.

The additional measures selected by calculation of the optimal measures and negotiation between the administrator and the user are as follows: (a) account lockout after login failure, (b) logging of PC access, (c) password protection of screen saver and (d) prohibition of using HTML e-mail [7]. Table 7 shows the risk probability, and the value of risks and usability, for typical network operation, network operation with the firewall port opened and network operation with implementation of the four above-mentioned security measures.

In this case, the firewall port open can be configured to affect only PC A. Therefore, all of the selected additional measures are implemented on PC A and they do not affect other users shown Figure 9. As a result, our method can select measures in consideration of their implementation layer and extent of effects.

Table 4: Probability and usability at the first analysis with only FTA and reanalysis with both FTA and STD.

Target of analysis		FTA	FTA and STD
(R1)	Unauthorized access	0.0285	0.0494
(R2)	Information leakage	0.0430	0.0198
(R3)	Virus infection	0.0181	0.0158
(U1)	Browsing websites	0.810	0.590
(U2)	Sending e-mail	0.590	0.372
(U3)	Reading e-mail	0.590	0.413
(U4)	Using files on the file server	0.729	0.510

Table 5: Assumptions regarding the value of assets.

(unit: yen)

User PC	1,000,000
Confidential files	
about product development	50,000,000
about customers	10,000,000
Not confidential files	100,000

In addition, another effective measure is “authentication for network access” (which is not drawn in Figure 9 because we decided not to implement it) deployed at the same transition as the firewall. This measure prevents intrusion into intranet. The other measure is “PFW” at the transition continuing directly from “intranet intrusion”. This measure prevents the state from transitioning to other states.

Looking at this analysis, we can see that the proposed method can identify potential states, which can occur by chain relations, by following STDs from a base state, which is directly caused by the transition that the modified measure had inhibited. Similarly, the method can also identify causes to raise the base state by tracing STDs back. At the same time, we can identify the effects on usability.

From a viewpoint of selecting measures, in order to maintain (or reduce) risks, the method can narrow down the candidate measures depending on the concept of preventing chains or resolving causes of the risks. On the other hand, in order to maintain (or increase) usability, the method can also narrow down the candidate measures to improve usability of chain phases or resolve causes of decreased usability.

5.4 Detecting Critical Points and Inferring Causes of Security Incidents

We focus on the state “PC A is usable”, which means unauthorized use of PC A, as an example. First, paths reversed from the state are extracted from the STDs shown in Figure 9. The results are shown in Figure 10. Note that Figure 10 includes measures which are not implemented and limits the states on the PC B to S6, S7 and related events. In addition, we connect an event directly from S2 to S7 in order to make the STD simpler, even though we should analyze events of accessing and intruding into PC B via the Internet.

Next, we change the state transition probability to conditional probability and attempt to infer causes of the incident.

Table 6: Value of risks calculated from the value of assets and risk probability.

(unit: yen)

	Object	FTA	FTA and STD
(V1)	User PC	46,551	65,245
(V2)	All files	2,581,968	1,188,176
	total	2,628,519	1,253,421

Table 7: Shift of risks and usability caused by modifying measures.

Probability and usability

	Usual operation	FW port opened	Additional measures added
(R1)	0.0494	0.0796	0.0518
(R2)	0.0198	0.0375	0.0269
(R3)	0.0158	0.0215	0.0195
(U1)	0.590	0.590	0.590
(U2)	0.372	0.372	0.335
(U3)	0.413	0.413	0.372
(U4)	0.510	0.510	0.510

Value of risk

(V1)	65,245	101,094	71,298
(V2)	1,188,176	2,251,166	1,619,260
total	1,253,421	2,352,261	1,690,558

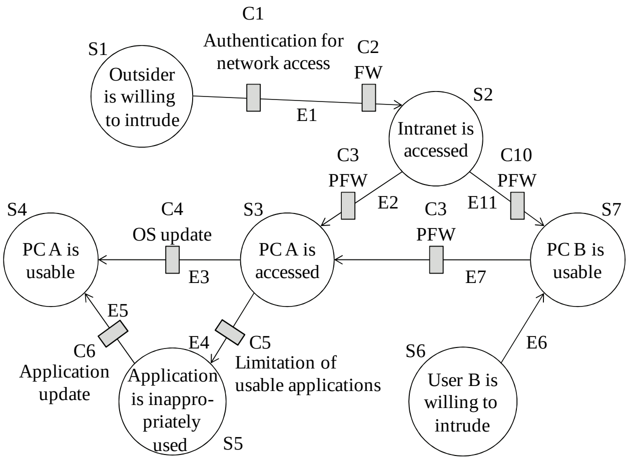
C1
Authentication for network access
C2
FW
S1
Outsider is willing to intrude
E1
S2
Intranet is accessed
C3
PFW
C10
PFW
E2
E11
S4
C4
OS update
S3
C3
PFW
S7
PC A is usable
E3
PC A is accessed
E7
PC B is usable
E5
C6
Application update
E4
C5
Limitation of usable applications
S6
E6
Application is inappro-priately used
S5
User B is willing to intrude

Figure 10: Candidate causes of unauthorized use of PC A.

The state transition/occurrence probabilities, the decrease in risk and the implementation states of measures were analyzed at section 5.2 as shown in Table 8.

Then, we infer the causes of S4. Table 9 shows the probability of each state that had occurred before S4 occurred during usual network operation, when the firewall port was opened (C2) and when “authentication for network access” (C1) was added.

During usual network operation, because the firewall protects against inappropriate access via the Internet, external users might be willing to intrude into the intranet (S1) but the probability of successful intrusion was inhibited (S2).

Table 8: Assigned values of states, events and measures in the analysis.

State or event	State transition /Occurrence probability	Measure	Risk decrease	State
S1	0.7	-	-	-
S6	0.4	-	-	-
E1	0.7	C1	0.9	0
		C2	0.7	1
E2	0.7	C3	0.5	1
E3	0.4	C4	0.7	1
E4	0.4	C5	0.3	0
E5	0.4	C6	0.7	0
E6	1.0	nothing	-	-
E7	0.7	C3	0.5	1
E11	0.7	C10	0.5	1

Table 9: Probability of causation of unauthorized use of PC A.

	Usual operation	FW port opened	Authentication added
P(S1|S4)	0.78	0.86	0.73
P(S2|S4)	0.38	0.77	0.15
P(S3|S4)	1.00	1.00	1.00
P(S5|S4)	0.72	0.72	0.72
P(S6|S4)	0.8	0.59	0.92
P(S7|S4)	0.9	0.78	0.96

On the other hand, the probability that the PC B was used (S7) and the user B was willing to intrude into the intranet (S6) were high. These probabilities mean that an internal user is more suspicious.

When the port of the firewall was opened, external users could access the intranet more easily via Internet. The probability of intrusion by external users (S2) increased considerably. This result means that an outsider became more suspicious.

When “authentication for network access” was implemented, the probability of intrusion by outsiders (S2) decreased notably. The probability that PC B was used (S7) and the user B was willing to intrude (S6) became extremely higher. These probabilities mean that an internal user is highly suspicious.

Note that the attacker had surely accessed PC A (S3) before he/she operated it without authorization (S4). On the other hand, intruding into PC A (S5) is entirely unrelated to whether vulnerabilities of the operating system or an application are exploited, that is, whether the transition from S3 to S4 goes through S5. Therefore, the following conditional probabilities are constant.

$$P(\mathrm{S3}|\mathrm{S4}) = 1,\quad P(\mathrm{S5}|\mathrm{S4}) = 0.72$$

As a result, our method can infer probabilistic causes of risks. Therefore, we can select measures to reduce the probability at the critical points. Furthermore, we can use the probabilities as information for selecting network monitoring points for proactive security measures and analyzing causes of incidents for reactive measures.

6 EVALUATIONS

6.1 Analysis of Risk and Usability with Chain Relations

In this experiment, we analyzed phases of risks and services use with FTA and converted the FT to an STD. We clarified the chain relations among risks and usability by combining the STDs. Moreover, the inconsistencies with the results of risk analysis by FTA are discovered and modified by using the combined STDs. Furthermore, our method can assess risks and usability by calculating the risk probability, the value of risks and the value of usability, as discussed in Section 5.2.

As a result, we confirm that our method can analyze risks and the usability of phases in consideration of chain relations.

6.2 Analysis of Relations among Risks, Usability and Security Measures

In the next experiment, we deployed the combined STDs on the network model based on defense in depth. We also implemented measures in the appropriate layer in the incorporated model presented in Section 5.2. We could recognize the layers related to risks and services use, as well as the place for implementing security measures. In addition, we could clarify the affects on risks and usability caused by modifying measures, as discussed in Section 5.3.

Therefore, the proposed method can be used to analyze visually and intuitively the relations among risks, usability and measures.

6.3 Selecting Optimal Measures and Inferring Causes of Security Incidents

When first selecting security measures in the experiment, we could find efficient measures for preventing certain targeted risks by analyzing the risks based on phases. We also visually found inconsistencies in the analysis results and a lack of required security measures.

When modifying measures, we could recognize the affects of risks and usability visually and quantitatively. We can select measures based on the concept of preventing causes or chains, meaning prior or latter phases. The measures can mitigate increases in risks and decreases in usability.

As a result, we confirmed that our method can select optimal measures visually and quantitatively when implementing and modifying measures.

On the other hand, we inferred probabilistic causes of a risk. We can detect incidents effectively and efficiently by monitoring events with a high likelihood of causing a security incident. We can also efficiently identify the causes of incidents by focusing primarily on such events.

7 CONCLUSION AND FUTURE WORKS

We have proposed a method for analyzing risks and usability and in turn selecting optimal measures in consideration of chain relations. In this method, risks and usability are analyzed by FTA. The FTs are converted to STDs, which are then deployed on a network model in accordance with defense in depth. The method can also be used to infer the causes of incidents by treating the STDs as a Bayesian network.

Through this study, we confirmed that the proposed method can be used quantitatively and intuitively (i) to analyze risks and usability, (ii) to select optimal security measures and monitoring points and (iii) to trace the causes of incidents.

The occurrence probability of a state, the state transition probability and the decrease in risk/usability caused by measures must be exact to assess risks and usability correctly. However, to assign proper values is difficult because these values may differ between environments or users. One solution to address this problem is to cycle risk analysis, assessment and review. The other solution is for stakeholders to decide the values through risk communication (e.g., [4]).

Moreover, Figure 9 is complex even though we consider only three risks and four services. When analyzing more risks and services, the number of states and transitions might become extremely large. On the other hand, the number of states might converge because the risks and usability related to a particular layer often have a common transition. Additionally, each state transition must be independent of the previous and next transitions in order to infer probabilistic causes. One way to achieve the independency of states is to parameterize each state and each event, such as the time of the transition and the person who causes the state transition. However, excessive numbers of the parameters may increase the number of states and transitions. In the future, we plan to study these problems further.

REFERENCES

[1] ISO/IEC 27002, http://www.iso.org/iso/home.htm.

[2] A. Zuccato, “A Decision Matrix Approach –to Prioritize Holistic Security Requirements in E-commerce, Security and Privacy in the Age of Ubiquitous Computing,” IFIP TC11 20th International Information Security Conference, pp. 35-49, Springer (2005).

[3] B.-C. Guan et al., “Evaluation of Information Security Related Risks of an Organization –the Application of the Multi-criteria Decision-making Method,” Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology, pp. 168-175 (2003).

[4] H. Yajima, et al., “Evaluation of the Participant-Support Method for Information Acquisition in the ‘Multiplex Risk Communicator’”, LNCS 4558, pp. 195-203 (2007).

[5] I. Kotenko and M. Stepashkin, “Attack Graph Based Evaluation of Network Security,” LNCS 4332, pp. 216-227 (2006).

[6] L. Wang, et al., “Measuring the Overall Security of Network Configurations Using Attack Graphs,” LNCS 4602, pp. 98-112 (2007).

[7] K. Kato and Y. Teshigawara, “A Proposal of Selecting Optimal Countermeasures with Security and Usability in a Special Network Use,” IPSJ Journal, Vol. 49, No. 9, pp. 3209-3222 (2008) (in Japanese).

[8] K. Kato and Y. Teshigawara, “A Proposal of a Risks, Usability, and Countermeasures Representation Model for Event Chain Clarification and Causal Inference,” IPSJ Journal, Vol. 50, No. 9, pp. 2243-2256 (2009) (in Japanese).

[9] J.D. Andrews and T.R. Moss, “Reliability and Risk Assessment - Second Edition,” Professional Engineering Publishing (2002).

[10] Microsoft TechNet, “Security Content Overview,” http://technet.microsoft.com/en-us/library/cc767969.aspx.

[11] Microsoft TechNet, “Chapter 3: Antivirus Defense-in-Depth,” http://technet.microsoft.com/en-us/library/cc162798.aspx.

[12] ISO/IEC 13335, http://www.iso.org/iso/home.htm.

(Received August 30, 2009)
(Revised June 23, 2010)

Koichi Kato received B.S., M.S. and Ph.D. degrees in Engineering from Soka University in 2005, 2007 and 2010, respectively. He is an Assistant Professor at Soka University. His research interests include risk management, digital forensics and privacy protection in ubiquitous space. He is a member of IPSJ.

Yoshimi Teshigawara received a doctorate of engineering from Tokyo Institute of Technology in 1970. He joined NEC Corporation in 1970, where he engaged in design and development of computer networks and he worked on international standardization. From 1974 to 1976 he was a Visiting Research Affiliate with the ALOHA System at the University of Hawaii. Since 1995, he has been a Professor at Soka University. His research interests include ubiquitous computing, groupware, e-learning and network security. He is a fellow of IPSJ and ORSJ. He is a member of IEICE, JASMIN, IEEE and ACM.