SPECIAL ISSUE PAPER

Threat scenario-based security risk analysis using use case modeling in information systems

Young-Gab Kim* and Sungdeok Cha

Center for Engineering and Education of Dependable Software, College of Information and Communication, Korea University, Seoul, Korea

ABSTRACT

Successful Security Risk Analysis (SRA) enables us to develop a secure information management system and provides valuable analysis data for future risk estimation. One of the qualitative techniques for SRA is the scenario method. This provides a framework for our explorations that raises our awareness and appreciation of uncertainty. However, the existing scenario methods are too abstract to be applicable to some situations and have not been formalized in information systems (ISs) because they do not explicitly define artifacts or have any standard notation. Therefore, this paper proposes the improved scenario-based SRA approach, which can create SRA reports using threat scenario templates and manage security risk directly in ISs. Furthermore, in order to show how to apply the proposed method in a specific environment, especially in a Broadband convergence Network (BcN) environment, a case study is presented. Copyright © 2011 John Wiley & Sons, Ltd.

KEYWORDS

security risk analysis; qualitative risk analysis; scenario method; use case modeling; Broadband convergence Network (BcN)

*Correspondence

Young-Gab Kim, College of Information and Communication, Korea University, 1, 5-ga, Anam-dong, SungBuk-gu, Seoul 136-701, Korea. E-mail: always@korea.ac.kr

1. INTRODUCTION

With the rapid explosion of Internet technology over the past few years, the incidence of security attacks has grown very rapidly. However, it is difficult to detect and prevent all security threats and security vulnerabilities in information systems (ISs). Therefore, there is an urgent need to analyze the risks posed by security threats and prevent them effectively. Security Risk Analysis (SRA) is a proactive approach that can identify and assess accident risks before they cause major losses. It enables us to develop secure information management and establish practical security policies for organizations. Furthermore, it provides valuable analysis data for future risk estimation [1]. In order to manage security risk, SRA involves identifying the most probable threats to ISs and analyzing the related vulnerabilities of ISs to these threats.

Security risk analysis techniques may be either qualitative or quantitative, and both types, ideally in combination, can be very effective in the process of SRA. The qualitative SRA prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. However, it does not provide specific quantifiable measurements of the magnitude of the security risks, therefore making cost–benefit analysis of any recommended controls difficult. On the contrary, the quantitative SRA provides a measurement of the risk’s magnitude, which can be used in the cost–benefit analysis of recommended controls. However, it has a disadvantage that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative risk analysis may be unclear, requiring the result to be interpreted in a qualitative manner.

The scenario method is a qualitative SRA that provides a framework for analyzing possible future events (cyber attacks) by considering alternative possible scenarios. Furthermore, it provides future strategies and appropriate countermeasures for security risks through the SRA. However, the normal scenario method is too abstract and informal because it is in the form of a narrative. That is, there is no standard notation or format for a scenario-based SRA [2]. Therefore, in order to address these problems, an enhanced scenario-based approach using the Unified Modeling Language (UML) use cases [3, 4] is proposed. It aims to provide systematic analysis of potential security issues at the start of risk analysis.

The rest of this paper is organized as follows: Section 2 presents background and related works about SRA and use case modeling. Section 3 presents an SRA based on a...
threat scenario using the use case model, which can effectively analyze security risks and provide countermeasures in ISs. In Section 4, in order to show how to apply the enhanced scenario method proposed in this paper, a case study is presented. Section 5 compares the existing qualitative approaches and the proposed method. Finally, Section 6 concludes the paper.

2. BACKGROUND AND RELATED WORKS

2.1. Security risk analysis

As mentioned previously, SRA is a technique used to identify and assess risk factors that may jeopardize ISs [5]. The SRA mainly involves three phases, as depicted in Figure 1.

Phase 1 (security requirements) is a step that defines the scope of the effort, the boundaries of the ISs, the resources and information, and the methodology for the organization. Phase 2 (risk analysis) is a step that identifies assets, threats, and vulnerabilities and measures the security risk. The important task in this phase is classifying and categorizing the assets, the threats, and the vulnerabilities. Furthermore, it includes the types of threats and vulnerabilities that exist for a specific asset and the probabilities that threats may occur. Finally, the security risk of the organization or the system is evaluated by summing up all the risks of the system components considering the existing threats in the core assets of the organization and the degree of vulnerability per threat. Once the risk analysis has been conducted, the management can use various risk mitigation techniques to complete the process in phase 3 (risk mitigation and evaluation). That is, phase 3 is a process that shows the list of current security countermeasures in the organization, selects suitable mitigation methods against the threats, and then shows their effectiveness.

In this paper, the following factors are considered in order to clarify the threat scenario, because each factor is a key aspect of information security: data integrity, availability, confidentiality, authenticity, and non-repudiation. Data integrity refers to the requirement that information should be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system as a result of intentional or accidental acts. Also, a violation of integrity may be the first step in a successful attack against system availability or confidentiality.

Availability is a property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to the performance specifications for the system. Ensuring availability involves preventing denial-of-service (DoS) attacks. Confidentiality refers to the protection of information from unauthorized disclosure. In order to support data confidentiality, cryptography techniques such as encryption, network traffic padding, and access control are required. Authenticity means that the data, transactions, communications, or documents are genuine. For authenticity, it is important to validate that both parties involved are who they claim they are. Non-repudiation implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

2.2. Use case modeling

The use case model is a means to understand and describe the functional requirements of a system. It defines a goal-oriented set of interactions between external actors and the systems under consideration. Furthermore, it consists of a use case diagram and a description of each use case using a template. A use case diagram in UML is represented by an actor, a use case, and an association line. The actors usually represent entities outside a system that interact with it in some manner, and the use case usually describes the possible courses of events that may occur in various scenarios. Finally, the actors and the use case in which they participate are connected by the association line. The use case description typically includes a normal scenario. Each

![Figure 1. Security risk analysis model.](image-url)
3. SECURITY RISK ANALYSIS BASED ON THREAT SCENARIOS

The scenario is the best available language for strategic conversation because it allows differing viewpoints while bringing people together to work toward a shared understanding of the situation. This enables decision making when the time comes to take action [15]. Therefore, we apply the scenario method to the SRA because we can obtain future strategies and appropriate countermeasures for security risks through the SRA. The steps of the proposed method in this paper are summarized as follows:

1. Identify actors representing malicious user classes such as (internal or external) attackers and malicious software or systems.
2. Identify use cases representing the many ways malicious user classes could cause harm in the service or the system. The goal of this step is to identify security threats and vulnerabilities for each of the functions, processes, data, transactions and assets involved in the use case. These can come from different potential security risks such as unauthorized access, DoS attacks, privacy violations, confidentiality and integrity violations, and malicious hacking attacks.
3. Show the associations between the actors and the use cases.
4. Identify and document scenarios for each use case. The goal of this step is to describe all possible threat scenarios for each use case and provide countermeasures for identified threats and vulnerabilities.

The core components of the scenario-based SRA proposed in this paper are the use case model and the threat scenario description. More detailed explanation will be presented in the following subsections.

3.1. Use case model for security risk analysis

As described earlier, the use case model for SRA involves three phases (phases 1–3). First of all, the actor(s) is identified. In the use case model for SRA, the actors may be hackers, malicious programmers, academics and security researchers, and inexperienced programmers and designers. Furthermore, the use cases can represent security hazards and attacks such as traffic analysis, masquerade, modification of message contents, and DoS attacks. In order to derive the use cases, threat trees [16] identifying threats and attacks unique to the application domain can be used. The use cases can also be translated to sequence diagrams [18,19]. The translation from a use case to a sequence diagram is the key to a successful implementation of user security requirements.

Figure 2 depicts an example of a use case diagram. There are two actors (service user attacker and service provider attacker) and five use cases (play user service, break legitimacy, play provider service, break integrity, and break privacy). Each use case can be mapped onto a scenario.

The first use case model describes an attack wherein a service user attacker plays a user’s service with unauthorized access and breaks legitimacy with malicious security attacks. The second one describes attacks wherein a service provider attacker plays a provider’s service, breaks integrity of service contents, and breaks privacy of service provider.

![Figure 2. Example of use case diagram.](image-url)
3.2. Threat scenario description

Scenario analysis is the process of analyzing possible future events by considering alternative possible outcomes (scenarios). The analysis is designed to allow improved decision making by considering the outcomes and their implications more fully.

As mentioned previously, the existing scenario analysis methods for SRA are ambiguous, abstract, and informal. Therefore, in order to describe more formally the scenario including many aspects of security risk such as security properties, security impact, sensitivity, countermeasures, and others, the enhanced threat scenario template is proposed as shown in Figure 5.

The proposed threat scenario template has been extended from the normal use case scenario description and has several elements: use case name, actor, security risk property, description, target, expected damage, pre-conditions, post-conditions, threat scenario, consideration, and countermeasure. Each element can reflect the context of the threat scenario sufficiently. The definitions of the 11 elements are as follows:

- **Use case name.** A use case represents security hazards and attacks. Each use case should have a unique name suggesting its purpose. The name should express what happens when the use case is performed.
- **Actor(s).** An actor(s) is someone or something that interacts with the use case. In a threat scenario, the actor is a malicious user such as a hacker, a cracker, or a malicious programmer.
- **Security risk property(ies).** A security risk property(ies) describes security attributes as one of the key factors affecting the system or the organization. These include confidentiality, integrity, availability, authenticity, and non-repudiation.
- **Description.** This is a set of simple explanations on the actions of the use case.
- **Target.** This is the aim of an attack (especially a victim of ridicule or exploitation) by some hostile actors (malicious user classes) or security attacks.
- **Expected damage.** This is the expected loss of assets such as information, hardware, software, human resources, and circumstances in ISs.
- **Pre-conditions.** These are the rules defining all the conditions that must be true for the trigger to meaningfully cause the initiation of the use case. That is, if the system is not in the state described in the pre-conditions, the behavior of the use case is indeterminate.
- **Post-conditions.** These are the rules defining all the conditions that must be true on successful completion of the use case. The post-conditions are not necessarily true if an exception course was taken.
- **Threat scenario.** These are the actions of the use case. A use case is defined as a set of sequences of actions (threat scenarios) a system performs that yield an observable result that is of value to a particular actor.
- **Impact.** This is the likelihood that a scenario event will occur. The following are simple definitions of the impact values:
  - **High impact—shutdown of a critical business unit that leads to a significant loss of business, corporate image, or profit.**
  - **Medium impact—short interruption of critical process or system that results in a limited financial loss to a single business unit.**
  - **Low impact—interruption with no financial loss.**
- **Sensitivity** is the likelihood that a scenario event will occur. The following are simple definitions of the sensitivity values:
  - **High sensitivity—very likely that the scenario event will occur by tomorrow.**
  - **Medium sensitivity—possible that the scenario may occur by tomorrow.**
  - **Low sensitivity—highly unlikely that the scenario will occur by tomorrow.**
- **Relationship** represents the relationship between threat scenarios. The following are simple definitions of the relationship values:
  - **Inclusive—if a scenario is described as inclusive, it allows all kinds of scenarios to belong to it.**
  - **Conflict—a conflict is a serious difference between two or more scenarios. If two scenarios are in conflict, they are very different.**
- **Consideration.** Anything of value in the SRA. **Countermeasure.** Controls or safeguards that could possibly eliminate the risk or at least reduce the risk to an acceptable level.

Generally speaking, the risk is the possibility of significant financial impact. In this paper, in order to assess the risk faced by the organization, the impact and sensitivity elements are included in the threat template. The identification of impact and sensitivity associated with a threat scenario is usually performed by engineers and actuaries, based on statistical data and expert judgment. In practice, many more threat scenarios can be added to the diagram. This gives the analyst a complete security risk profile of the ISs’ exposure to accidental damage.
4. CASE STUDY

In order to illustrate the motivation of our research, let us discuss an example application that will be enabled by a Broadband convergence Network (BcN) environment, as illustrated in Figure 3. In order to support BcN services, service requests and admission procedures are required. The detailed scenario description in Figure 3 may be described as follows:

1. **Service request.** To use the registered services, a user sends a service request message to the softswitch (SSW).
2. **Service profile check.** The SSW checks the service profile of the application server and identifies whether the user has a right to use the request service.
3. **Service provider search.** If the user has a valid right, the SSW looks for service providers supporting the user’s requested service. The service provider can be a server of a content provider or another user’s home terminal in case of interactive communication such as a video telephone. That is, the SSW retrieves the service provider connected to the current network and its location.
4. **Access route establishment.** In order to support the service to the user, the SSW establishes the access route and sends its information to the network transmission control systems such as routers, gateways (GWs), and signaling gateways (SGs).

In the BcN environment, attack scenarios are first depicted in Figure 4 by the use case diagram.

Given an actor and a home terminal attacker, there are four use cases that can occur for the home terminal attacker: Play User Service, Saturating the SSW, Modification of Session Message, Traffic Analysis.

As mentioned earlier, each use case can be a scenario wherein the use case is mapped onto the threat scenario. In this case study, the Modification of Session Message use case is mapped onto the threat scenario, as illustrated in Figure 5.

As described earlier, the key concept of our approach is use case modeling based on the threat scenario. The threat
scenario template is extended from the normal use case scenario description to deal with security aspects of SRA such as security property, threat impact, sensitivity, and relationship.

5. EVALUATION

In this paper, a method for analyzing the security risks in ISs using use case modeling and its threat scenario is proposed. The proposed method has different advantages from the existing qualitative approaches such as the scenario method, Delphi technique, ranking method, scoring method, and others. Table I compares the existing qualitative approaches and the proposed method in this paper.

First, the proposed method is easier to understand than the textual-based or expert-based qualitative SRA method. That is, from a user perspective, it is clear that the users do not need a strong security background. By examining the use cases, a user can establish what security threats can occur. By examining the actors, a user can establish exactly who will be involved in security hazards and attacks.

Table I. Comparison of the existing approaches and the proposed method.

<table>
<thead>
<tr>
<th></th>
<th>Understandability</th>
<th>Ambiguity</th>
<th>Standards compliant</th>
<th>Completeness</th>
<th>Operational technology</th>
<th>Measurability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario approach</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Delphi technique</td>
<td>Middle</td>
<td>Middle</td>
<td>Low</td>
<td>Middle</td>
<td>Middle</td>
<td>Middle</td>
</tr>
<tr>
<td>Ranking method</td>
<td>Middle</td>
<td>Middle</td>
<td>Low</td>
<td>Middle</td>
<td>Middle</td>
<td>Middle</td>
</tr>
<tr>
<td>Scoring method</td>
<td>Middle</td>
<td>Middle</td>
<td>Low</td>
<td>Middle</td>
<td>Middle</td>
<td>Middle</td>
</tr>
<tr>
<td>Proposed method</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Middle</td>
</tr>
</tbody>
</table>

Table: Use-Case Name | Modification of Session Message
Actor(s) | Home Terminal Attacker
Security Risk Property(ies) | Confidentiality, Integrity
Description | Home Terminal attacker breaks confidentiality and integrity of user service by modification of session message using session spoofing
Target | Network protocol between home terminal and local loop, private user information such as banking and currency
Expected Damage | Fabrication of user’s accounting, financial data, and private information
Pre-conditions
Post-conditions

– Threat Scenario

<table>
<thead>
<tr>
<th>No</th>
<th>Scenario</th>
<th>Impact</th>
<th>Sensitivity</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The home terminal attacker performs a spoofing attack against the connected session between the home terminal and the local loop using network scanning tools</td>
<td>Medium</td>
<td>High</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>The home terminal attacker communicates with an application server using the faked message against the spoofed session of the home user</td>
<td>High</td>
<td>Medium</td>
<td>-</td>
</tr>
</tbody>
</table>

– Consideration

Fabrication of the connected session requires advanced techniques such as understanding the application service layer, and attack skills and a fake service system. However, if this kind of attack isn’t protected by encryption of the session message in the application layer, there is no appropriate safeguard.

– Countermeasure

- Packets with an unauthorized IP address are blocked in the SSW
- Only an authorized user is allowed to service control equipments through user authentication of the request service
- In the case of protecting the traffic analysis in a specific BcN service, the service supports encryption of control messages in the home terminal.
Second, the proposed method aims to move from simple textual descriptions of security threat scenarios to more formalized SRA models. The captured use case diagram and threat scenario template for SRA deal with difficult security threats faced by users in a much more direct manner than a mere textual discussion of security threats. Furthermore, the proposed method uses the standard UML use case diagram, which is an industry standard collection of notations for analysis and design. The benefits of using the UML standard are sharing the best practices and setting benchmarks for performance, quality, and safety, so an SRA analyst can focus on evaluating a better SRA.

Third, the existing scenario approach does not consider security aspects such as the impact and sensitivity of threats. However, the proposed scenario-based SRA allows identification and prioritization of potential threats by estimating the impact and the sensitivity of threats. Therefore, the SRA can be conducted effectively and simply.

6. CONCLUSION

Scenario-based risk analysis allows us to investigate possible future accidents in detail. However, the existing scenario-based SRA methods are too abstract and informal, because they do not explicitly define artifacts or have any standard notation. Therefore, we proposed the threat scenario-based SRA method, which can create SRA models using use case diagrams and threat scenario templates, and managed security risk directly in the ISs. This starts with use case modeling, which can capture and analyze security risk in a simple manner. Thus, the proposed method makes it possible to use prototype user interfaces for capturing desired scenarios of SRA, as well as animating these scenarios for the purposes of validation using use case modeling. Furthermore, it can provide valuable guidance to decision makers and others responsible for the effective management of security risks.

ACKNOWLEDGEMENT

This research was supported by the National IT Industry Promotion Agency (NIPA) under the program of Software Engineering Technologies Development.

REFERENCES


