UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 3 : Issue 2 [ISSN 2250 – 3765]
Publication Date : 05 June 2013

Different Software Security Requirements in Engineering

Sarika Gupta
Department of Information Technology
Dronacharya College of Engineering
Greater Noida U.P,India
sarika.mittal0108@gmail.com

Priyanka Dabral
Department of Information Technology
Dronacharya College of Engineering
Greater Noida U.P,India
priyankadce4130@yahoo.com

Abhimanyu Kumar
Department of Information Technology
Dronacharya College of Engineering
Greater Noida U.P,India
kumar.abhimanyu375@gmail.com

Rana Pratap
Department of Information Technology
Dronacharya College of Engineering
Greater Noida U.P,India
ranapratap.5753@yahoo.com

Neeraj Raj Pal
Department of Information Technology
Dronacharya College of Engineering
Greater Noida U.P,India
neerajrajp@yahoo.com

***Abstract*- The goal of the software security requirements is to build better, defect-free software. But most requirements engineers are poorly trained to elicit, analyze, and specify security requirements, often confusing them with the architectural security mechanisms that are traditionally used to fulfill them. They thus end up specifying architecture and design constraints rather than true security requirements. This paper defines the basic of the security requirements and assets & threats in detail. And at last define the different types of security requirements as proposed by Firesmith [1] and provides associated examples and guildlines with the intent of enabling requirements engineers to adequately specify security requirements without unnecessarily constraining the security and architecture teams from using the most appropriate security mechanisms for the job.**
`

Keywords— Information System, Security Requirement Elicitation, Security Services, Security Mechanism, Assets, Threats, Identification and Prioritization.

I. INTRODUCTION

It comes as no surprise that requirements engineering is critical to the success of any major development project. Some studies have shown that requirements engineering defects cost 10 to 200 times as much to correct once fielded than if they were detected during requirements development [2, 3]. Other studies have shown that reworking requirements, design, and code defects on most software development projects costs 40 to 50 percent of total project effort, and the percentage of defects originating during requirements engineering is estimated at more than 50 percent. The total percentage of project budget due to requirements defects is 25 to 40 percent. Security Requirements is defined as a high level requirement that gives detail specification of the system behavior that is unacceptable such as all users' application can only access data for which they are properly authorized .

They differ from safety requirements which are domain specific and more suitable for control systems application. They are also kwon as shall not requirements but are not risks or threats..

Following are the points to be noted regarding security requirements:

. Security requirement are different from functional requirements which are derived from goals of system where as security requirements are objective resulting from threats on functionality or confidential data.

When security requirements are considered at all during the system life cycle, they tend to be general lists of security features such as password protection, firewalls, virus detection tools, and the like. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements, such as authenticated access. As a result, security requirements that are specific to the system and that provide for protection of essential services and assets are often neglected. In addition, the attacker perspective is not considered, with the result that security requirements, when they exist, are likely to be incomplete. We believe that a systematic approach to security requirements engineering will help to avoid the problem of generic lists of features and to take into account the attacker perspective.

II. ASSETS AND THREATS

Assets are the reason threats exist; an adversary's goal is to gain access to an asset. The security team needs to identify which assets need to be protected from an unauthorized user.

Assets can be either physical or abstract, i.e. employee safety, company's reputation etc. Assets can interact with other assets and, because of this, they can act as a pass-through point for an adversary.

A. Recognization of assets and priority processing

Assets are also identified along with their associated risks. We followed the procedure explained in [6] to identify and prioritize assets. As a first step, a brainstorming session is conducted and all the valuable assets are listed. Next step is to examine various existing documents for other important assets. Once all the assets are listed, the assets are categorized and prioritized with respect to security. To perform this, an asset is taken and viewed from different perspectives i.e. customer, administrator and attacker.

From each perspective, each asset gets assigned a number indicating the importance of confidentiality, integrity or availability for this asset. All the priorities of each asset are added and the asset with lowest sum is ranked as highest priority asset.

B. Specific Threats Identification

The second step, determining threats, is certainly the most challenging aspect of threat modeling. After the previous steps have been completed, it is time to think about the specific threats to the system. Threats may come from either inside or outside the system—from authorized users or from unauthorized users who masquerade as valid users or find ways to bypass security mechanisms. Threats can also come from human errors. The goal of this step is to identify threats to the system using the information gathered so far. A threat is the adversary's goal, or what an adversary might try to do to a system [7]. Sometimes a threat is also described as the capability of an adversary to attack a system. The best method for threat enumeration is to step through each of the system's assets, reviewing a list of attack goals for each asset. Assets and threats are closely correlated.

A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets. The process of correlating threats to an asset involves creation of adversary hypotheses.

C. Compartmentalization of all Threats

The output of threat identification process is a threat profile for a system, describing all the potential attacks, each of which needs to be mitigated or accepted. In general, threats can be classified into six classes based on their effect [7]:

. **Spoofing** is a term used to describe a fraudulent email activity in which the sender's address and other parts of the message header are altered so that the message appears to come from a different sender. Spoofing is commonly used for sending spam (unsolicited email) and phishing email (attempts to obtain sensitive information for fraudulent access to secure accounts)..

. **Tampering** refers to concept of altering data to mount an attack. All the attacks in which someone changes some information without permission fall into this category.

. **Repudiation** occurs when a user denies performing an action, but the target of the action has no way to prove otherwise. All the attacks in which someone denies a transaction that was performed are mapped into this category. For example, someone denying a purchase order after receiving the merchandise and denying the payment is classified as repudiation.

. **Information disclosure** refers to disclosure of information to a user who does not have permission to see it. All the attacks in which someone gets to see information she has no right to access can be termed as information disclosure.

. **Denial of service-** Reducing the ability of valid users to access resources. All the attacks in which someone breaks the system and prevent it from working normally and supplying the service it should fall into this category.

The fact that the system does not work can serve for the interest of the attacker (or the one who sent him).There a numerous ways to implement such an attack.

. **Aggrandisement of privilege** occurs when an unprivileged user gains privileged status. All the attacks in which

someone enhances their capabilities by raising their privileges fall into this category. Example is when the attacker manages to get administrative rights.

When identifying a threat, it is helpful to think of various attacks in terms of the above classification. On the other hand, security threats are breaches of confidentiality, integrity, or availability. Thus, threats could also be classified by these properties. This classification is useful in security requirements when deciding on a mitigation mechanism of a specific threat. For example, unauthorized modification of data en route to component B from component A poses a tampering threat which violates the integrity property. To mitigate this threat, it might make sense to apply integrity mechanism such as Secure Hashing Algorithm-1 (SHA-1) on the data being transferred.

III. DIFFERENT TYPES OF SECURITY REQUIREMENTS

The security requirements as proposed by Firesmith [1] are as follows -

A. Identification Requirements - An identification requirement is any security requirement that specifies the extent to which a business, application, component, or center shall identify its externals (e.g., human actors and external applications) before interacting with them.

Examples – . The main application shall identify all its client applications, human users before allowing them to use its capabilities.

. All persons should be identified before allowing them to enter.

B. Authentication Requirements

It is the security requirement that specifies that CBS should verify the identity of its externals. The typical objective of this security requirement is to ensure that externals are actually who or what they claim to be. Examples –

. Application shall verify the identity of all of its users before allowing them to do any interaction (message, transaction) with the system.

. Before permitting the personnel to interact with data center their identities should be verified.

C. Authorization Requirements

An authorization requirement is any security requirement that specifies the access and usage privileges of authenticated users and client applications. Examples –

. The application shall allow the customer to obtain access to his/her account information rather than of other customer.

. Application shall not allow intruders access the credit card information of customers.
. Application shall not allow users to flood the system.

D. Immunity Requirements

An immunity requirement is any security requirement that specifies an application shall protect itself from infection by unauthorized undesirable programs (e.g., computer viruses, worms, and Trojans). Examples –
. Application shall protect itself from infection by scanning data for viruses, worms, Trojan, and other harmful programs
. Application shall delete or disinfect the file found to be infected.
. Application shall notify the user if it detects a harmful program.

E. Integrity Requirements

This security requirement specifies ensures that its data does not get corrupted via unauthorized creation, deletion, modification. Examples -
. The application shall prevent the unauthorized corruption of emails that it sends to customers.
. The application shall prevent the unauthorized corruption of data collected from customers and other external users.
. The application shall prevent the unauthorized corruption of all communications passing through networks.

F. Intrusion detection Requirements

An intrusion detection requirement is any security requirement that specifies the extent to which an application or component shall detect and record attempted access or modification by unauthorized individuals..This security requirement specifies that if an application has been attacked by intruders then that can be detected and recorded so that the administrator can handle them. Examples
. The application shall detect and record all attempted accesses that fail identification, authentication, or authorization requirements.
. The application shall notify the security officer of all failed attempted accesses.

G. Non repudiation requirements

A nonrepudiation requirement is any security requirement that specifies the extent to which a business, application, or component shall prevent a party to one of its interactions (e.g., message, transaction) from denying having participated in all or part of the interaction. Examples
. The application shall make and store records of the following information about each order received from a customer and each invoice sent to a customer:
. The contents of the order or invoice.
. The date and time that the order or invoice was sent.
. The date and time that the order or invoice was received.
. The identity of the customer.

H. Privacy Requirements

A privacy requirement is any security requirement that specifies the extent to which a business, application, component, or center shall keep its sensitive data and communications private from unauthorized individuals and programs.Examples –
. Anonymity Privacy: - The application shall not store any personal information about the users.
. Communication Privacy: - The application shall not allow unauthorized individuals or programs access to any communications.
. Data Storage Privacy: - The application shall not allow unauthorized individuals or programs access to any stored data.

I. Security Auditing Requirements

A security auditing requirement specifies that an application shall enable security personnel to audit the status and use of its security mechanisms. Examples –
The application shall collect, organize, summarize, and regularly report the status of its security mechanisms including:
. Identification, Authentication, and Authorization.
. Immunity
. Privacy
. Intrusion Detection

J. Survivability Requirements

The security requirement specifies that that an application should work possibly in degraded mode even if some destruction has been there in the application.
Examples –
. The application shall not have a single point of failure.
. The application shall continue to function even if a data center is destroyed.

K. System Maintenance requirements

This requirement specifies that how the modifications can be done so that security fixes that have been detected can be resolved. Examples –
. The application shall not violate its security requirements as a result of the upgrading of a data, hardware, or software component.
. The application shall not violate its security requirements as a result of the replacement of a data, hardware, or software component.

L. Physical protection requirements

A physical protection requirement is any security requirement that specifies the extent to which an application or center shall protect itself from physical assault. The typical objectives of physical protection requirements are to ensure that an application or center are protected against the physical damage, destruction, theft, or replacement of hardware, software, or personnel components due to vandalism, sabotage, or terrorism. Examples
. The data center shall protect its hardware components from physical damage, destruction, theft, or surreptitious replacement.
. The data center shall protect its personnel from death, injury, and kidnapping.

IV. SUMMERY

Security requirement is very important to build better and defect free software. Security requirement is defined as a high level requirement that gives detail specification of the system.

Security requirement are different from functional and architecture requirements. These requirements are related to non-functional requirements like- correctness, interoperability, feasibility etc.

Security requirements engineering needs to identify those assets need to be protected from an unauthorized user. Assets can be either physical or abstract. For that we use assets identification & prioritization and threats identification process. The output come of the threat identification process is a threat profile. Generally threats are classified into six classes.

There are different types of the security requirements as proposed by Firesmith [1] like- identification requirements, authentication requirements, authorization requirements, immunity requirements, integrity requirements, intrusion requirements, non-repudiation requirements, privacy requirements, security auditing requirements, survivability requirements, system maintenance requirements and physical protection requirements.

The engineering of the requirements for a business, system or software application, component, or (contact, data, or reuse) center involves far more than merely engineering its functional requirements. One must also engineer its quality, data, and interface requirements as well as its architectural, design, implementation, and testing constraints. Whereas some requirements engineers might remember to elicit, analyze, specify, and manage such quality requirements as interoperability, operational availability, performance, portability, reliability, and usability, many are at a loss when it comes to security requirements. Most requirements engineers are not trained at all in security, and the few that have been trained have only been given an overview of security architectural mechanisms such as passwords and encryption rather than in actual security requirements. Thus, the most common problem with security requirements, when they are specified at all, is that they tend to be accidentally replaced with security-specific architectural constraints that may unnecessarily constrain the security team from using the most appropriate security mechanisms for meeting the true underlying security requirements.

V. REFERENCE

[1] Firesmith, D. G., .Engineering Security Requirements., Journal Of
Object Technology, 2003, Vol2, No.1, Pages 53-68.
[2] Boehm, B., W., Papaccio, P., N. .Understanding And Controlling
Software Costs. Ieee Transactions On Software Engineering 14, 10
(October 1988): 1462-1477.
[3] Mcconnell, S., .From the Editor - An Ounce of Prevention.. IEEE
Software 18, 3 (May 2001): 5-7.
[4] Gupta D., Agarwal A., "Security Requirement Elicitation Using View
Points For Online System", International Conference On Emerging
Trends In Engineering And Technology,Nagpur, July 2008.
[5] Gupta D., Agarwal A., "Guidelines and Case Study for Eliciting Security
Requirements".
[6] Martin, G. J., Tøndel, I. A., .Covering Your Assets in Software
Engineering., IEEE, 2008.
[7] Swiderski, F., Snyder, W., .Threat Modeling.. Microsoft Press., 2004.
[8] Robert J. Ellison, .Attack Trees. Software Engineering Institute,
Carnegie Mellonuniversity, 2005.
[9] Sommerville, I., .Software Engineering.. . ISBN - 8129708671. Pearson
Education. Seventh Edition 2003.
[10] Kotonya G., Sommerville I., .Requirement Engineering With View
Points., 1995.
[11] Davis, A. "The Art of Requirements Triage." IEEE Computer 36, 3
(March 20

.