# Security Engineering towards Building a Secure Software

Mohammad Nazmul Alam
World University of Bangladesh, Bangladesh

Subhra Prosun Paul
World University of Bangladesh, Bangladesh

Shahrin Chowdhury
Primeasia University, Bangladesh

## ABSTRACT

Information Systems Security is one of the most critical challenges presently facing nearly every one of the organizations. However, making certain security and quality in both information and the systems which control information is a difficult goal necessitating the mixture of two wide research disciplines which are typically separate: security engineering and secure software engineering. Security engineering has an extensive history, and has focused generally on providing advances in security models, techniques and protocols, but it remains in a steady state of the development. Secure software engineering, however, has emerged relatively recently, but is growing quickly and is paying attention on the integration of security into software engineering techniques; models and processes, in order to build up more secure information systems. In the study of security engineering, security described as the protection from harm.It presented the principles of security, the number of security mechanisms and the risk analysis to identify the risk. In the study of secure software engineering, it has been identified a number of challenges that need to establish for developing the secure software system. We also investigated a number of methods and languages that is modeling the security into software systems.

**General terms:** Cryptography, Computer Security, Modeling language, Information Security, Risk management.

**Keywords:** Security Engineering, Secure Software Engineering, Threat, Risk, Vulnerabilities.

## 1. INTRODUCTION

Every critical software system needs security. Just about all software controlled system faces threats from possible adversaries . Military, telecommunication, and hospital needs security features software to protect them from adversary [1]. Software engineer must aware of these threats while delivering value to customers. Weillustrates the security concepts and its definition in the context of information security. It also explains about security mechanism to identify the legitimate user of the system. Risk comes from malicious actors while they found the flaw in the system. Risk management used to identify analysis and evaluate these risks that normally occur in the business.

### 1 .1 Security concepts

Security is described as the condition of being protected from risk or danger [2]. The main aim of security is to protect assets from security threat [3]. The security is often given many meaning depending on the purpose and need of the circumstance. Therefore security is divided into different subtypes. Such as homeland security, financial security, social security etc. In this paper the investigation has done on one of those subtypes named information security. In order to do the investigation properly; related types of security such as computer security has also been considered.In the perspective of computer technology security is the prevention against unauthorized access to information and unauthorized modification, alteration and destruction of the information.

#### *1.1.1 Computer security*

Computer security is derived from computer technology and it leads to the information security that is applied to computer and network security.The main aim of computer security is to protect of information and property from stolen, damage, and or natural disaster.

#### *1.1.2 Information Security*

According to Anderson, security is defined as a secure system is a system, which does exactly what is desired and nothing that is unwanted, even when someone else tries to make it behave differently.

Security in information system is a high profile problem as hackers, malicious actors and adversary competitors. Software systems contain high sensitive information. Government and military confidential information, bank account, educational qualification and health record those needs to keep secret rather than option.

Thus the security information may also be regarded as a process oriented not as a condition indicated as in the definition by Anderson [4].As the view of the process oriented security maintains by protecting the assets from unauthorized modification, alteration and destruction.

According to Bishop more process oriented security information definition as Information security is the protection of information systems from unauthorized access to or modification of information, whether in storage, processing or transit, and from denial of service to authorized users or the provision of service to unauthorized users, including measures necessary to detect ,document and counter such threats[5].

However the main goal of security information is to protect information from harm. In that respect, there are three main principles in information security: Maintain the confidentiality, Integrity and availability of information resources [6].

**The CIA Triad**

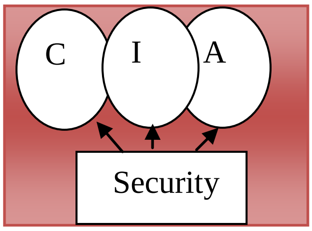

**Fig 1: CIA triad; C for confidentiality, I for integrity and A for availability**

The widely accepted elements of information security make up the, so called, CIA triad. These concepts are usually given the following meaning [7]: Confidentiality, Integrity and Availability.

### 1.1.2.1 Confidentiality

Confidentiality is the prevention of unauthorized disclosure of information. Confidentiality is related to the concept of privacy in that it is an essential for maintaining the privacy of the people whose personal information that the organization holds. A range of methods are used to protect information, including

**Access control mechanisms**: It is used to stop unauthorized individuals from accessing the system.

**File system security controls:** It is used tostop individuals authorized to use a system from exceeding their authority and reading confidential information they should not be allow to access.

**Cryptography:** Cryptography is used to encrypt the contents of sensitive files. It is probably the key enabling technology used to protect distributed systems. It is more power full techniques than access control and file system security control mechanisms.

### 1.1.2.2 Integrity

Integrity is the prevention of unauthorized modification or alteration, as well as changes by those who do not have the authorization to modify data and unauthorized modification completed by individuals usually permitted to modify the data. When data integrity is conserved, then it is called reliable.

### 1.1.2.3 Availability

Availability of guaranteeing the usability and accessibility of information or resources. That means information is available to use when it needs.

A balanced combination of three terms normally results in information control. Moreover, other aspects might also be adopted as elements of information security, for instance, Gollmann also mentions authentication, on-repudiation and reliability to be relevant security services of computerized systems. Basically which service to include in an information security strategy depends on the overall purpose, the risk factors involved, and the nature of the asset that requires protection.

## 1.1.3 Identification, Authentication and Authorization

### 1.1.3.1 Identification

Identification mechanisms let users to identify themselves to a resource. It can be a password to identify themselves to the resources. This is the most common identification mechanism now is used. Password can be a combination of user name and different letters.

### 1.1.3.2Authentication

Another most basic issue in improving security and enabling trust is to strengthen the provision of authentication. Computer use authentication to confidently associate an identity to a person. Authentication is thereby one of the basic building blocks of security. There are many authentication mechanism are exists to recognize the legitimate user. The passwords and the other range of techniques such as biometrics, access key, and encryption are normally used to authenticate the user.

There is another well known process to identify authenticate user is that the user have to present one or more of these evident to the system: Something the user knows for example the user given passwords, Something the user is that is identified by physical characteristics that we call biometrics measurement. It can be fingerprints, retinal scan or an iris scan. Another approach is something the user has it can be the physical device such as access card, some form of key etc..

The choice of authentication mechanism may vary to organization. It depends on the security policy and the level of access. A security policy can be defined as the set of rules that state which actions are permitted and which actions are prohibited. Thus we see the financial institution use different kind of security mechanism such as three factor authentication for transfer the fund where we can’t see in the manufacturing company.

### 1.1.3.3Authorization

Another approach is authorization. It is a process that is used to decide if a person or an entity is allowed to gain access to resource of a system, e.g., data, functionality or software. A computer system which has been designed to be used only by those who are authorized. Access to it therefore usually controlled by an authentication procedure before use is granted [8].

## 1.1.4 Security Process Engineering

Gollmann identifies two principle processes for the execution of computer security:

### 1.1.4.1 Risk Analysis

This is the process of defining what asset needs to protect, why and to what extent it requires protection. This issue we will broadly discuss in later of this section.

### 1.1.4.2 Protection

This process involves choosing, implementing, maintaining and evaluating the best possible means of protection. Typically protection is a process that includes three separate sub process:

-Prevention
-Detection
-Response

**Prevention** is a process where measures to prevent from being damaged are taken. This means that the attacker will fail to attack. Prevention usually involves execution of mechanisms that users can not make ineffective, and that are trusted to be implemented in a correct, unchangeable way so that the attacker cannot overwhelm the mechanism by altering it.

**Detection** is a process, which includes measures that allow for detection of when an asset has been damaged, how it has been damaged and who or what has caused the damage. Detection mechanism accepts the attack because of to identify the attacker and to report it.

**Response** defines a process of two forms of which the first one aims to bring to an end an attack, and to evaluate and fix any damage caused.

### *1.1.5 Risk management*

Risk management is the ongoing process in the business. Risk management is setup to reduce the risk in the business. Its aim to identify, analyze and evaluate the risks that occur in the business. This is called the risk analysis.

#### *1.1.5.1 Risk*

Risk has gained wide spread significance to many areas in the society. The risk areas are health insurance industry, military operations, traffic planning, and information security and many more. We will look at here the risk in the context of information security. One common view of the risk is the ‘chance of loss’ [9] and there is a common definition of risk within the information security domain [10] Risk is someone or something that creates or suggest an expected loss to individuals, institute, and organization.

Threats and vulnerabilities are the components of risk analysis. Threats are anything that may cause danger to the system. Some threats we are familiar that outside from information security such as severe storm, fire, theft and similar types of occurrence. However when we emphasis on the information security field then we must think about that hazard posed from hacker, electronic component failure, fault backup mechanisms and so on.

Vulnerability is another component for the risk. It is considered as a weakness of the system which allows user to break the integrity of that system. They can cause the loss of information, and reduce the value or usefulness of the system [11]. Mainly risk occurs from those two components-threats and vulnerability. And thus the security professional often describes risk by means of this equation:

Risk=Threat×Vulnerability

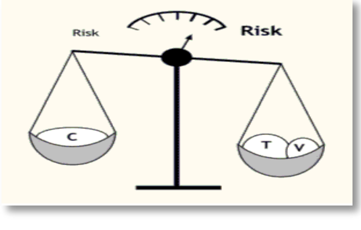

**Fig 2: Risk and vulnerabilities; C for Confidentiality, T for Threat and V for Vulnerability [12]**

A range of organizations need to work systematically on generating better founded knowledge and awareness about the risks, vulnerability, and threats they face in the digital world. On that basis, better informed decisions can be made.

## 2. PATTERNS FOR SECURE SOFTWARE DEVELOPMENT

There are different methods and patterns are currently using for capturing security in software development. Secure Quality Requirement Engineering (SQUARE) methods are used to identify security requirement engineering for extracting, analyzing and documenting security requirements for software engineering [13]. Various procedures and practice are used in this method. A misuse and abuse cases are used to describe from the position of the attackers circumstances. Attack trees as a method for describing a modeling attack to identify security requirements.

Security in the information system is not only technical problem but also human social environments involve in this problems. As a result social ontology is applied in the requirement engineering process for integrating security into a requirement driven software engineering process[14].The ***i**** agent oriented modeling framework evolve this issues to integrate the security in the agent oriented software development process.

Patterns are used to develop secure systems by considering whole software life cycle[15]. The main idea of this methodology is that security values should be applied at all stages of software life cycle and that can be tested for fulfillment with security principles.

Another pattern is that modeling security patterns using NFR (Non Functional Requirement) Analysis. This pattern is used to identify the non functional requirement and represent them as forces in the non-functional requirements framework [16]. Accountability, Confidentiality, Integrity, Availability, Performance, Cost, Maintainability and usability are the security related non- functional requirements in this model.

### 2.1 Modeling languages and methodologies for secure software development

Agile software development method can be used for secure software development. This method is distinguished by agility to swift changes, multiple incremental iterations and rapid development pace [17]. Security elements are identified in agile software development method to extend the security. These are: Security relevant subject where authorized person are identified in the organization and these persons are the security subject, Security relevant object where identified the key property of the organization and these property are the security objects. Security classification of subjects and objects determine which person will be authorized to access which object. They classify the object for examples, ‘top secret’, or ‘confidential’, or ‘unclassified’ and then the authorized person are assigned to access these assets .The final element is the risk management where risk are analyzed by identifying the threat scenarios.

There is another method that is called secure tropos which are used to modeling security and trust in agent oriented software development. This method incorporates two software engineering approaches; one is security-oriented process and another one is trust management process. This is the first attempt to reflect on security and trust issues in a solo software development methodology [18].

### *2.1.1 Access control specification in UML*

UML access control model shows the access control mechanism how to formalize the access control of the system. Access control is the typical approach to limit access to resources with restrictions. The restrictions include preventing principles from reading the contents of a file to protect the confidentiality of the data, or from modifying entries in a database to maintain the integrity of the data and trustworthiness of the information contained. Access control policies describe which states of the system are deemed acceptable, in which authorized principals can access entities in appropriate manner [19].

Role-based access control (RBAC) as the causal security model of our modeling language. RBAC is a model for access control where users and their privileges are decoupled by roles. This decoupling is not only conceptually useful, it also leads to significantly compacter access control policy descriptions.

RBAC model consists of five data types: users (USERS), roles (ROLES), objects (OBS), operations (OPS) and permissions (PRMS). A user is defined as a person or a software agent. A role is a job or function within an organization. It combines all privileges needed to fulfill the respective job or function. Privileges are expressed in terms of the permissions assigned to a role by entries to the relation Permission Assignment. Permission represents the authorization to execute an operation on one or more protected objects or resources. An object in this context is a system resource or a set of resources that are protected by the security mechanism. An operation is an action on a protected object that can be initiated by a system entity. The types of operations depend on the type of the protected objects. In a file system, for example, there might be permissions to read, write or execute files. The assignment of roles to users is defined by the relation User Assignment. The relation Role Hierarchy defines an inheritance relationship between roles. A relation r1 inherits r2 implies that all permissions of role r2 are also permissions of role r1 [20].

View–based Access control (VBAC) is an access control model specifically defined to support the design and management of access control policies in object oriented system [21].VBAC model consists of following data types: Subject which used to represent system users and the process that run on behalf of the users. Object used to represent the distributed objects in the system to which access must be controlled by a policy. Permission specifies a right to access an object. View groups a number of permissions belonging to the same object. Role represents the access control roles, which are assigned to subjects. A role can be played by several subjects, and a subject can play several roles.

## 3. SECURITY ENGINEERING IN AMBIENT INTELLIGENT (AMI)

Ambient Intelligent is an environment where people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects [22]. That type of environment is capable recognize and react to the needs of different individuals, mostly those technologies are seamless, unobtrusive and often invisible. Once they are in the home or work environment of user, it is important to evaluate the efficiency of their usage-how much do they make the life easier, how much are they user friendly, feasible and valuable for the daily life .AmI builds on three recent key concepts [23]: Ubiquitous computing, Ubiquitous communication, and intelligent user interfaces. Ubiquitous computing means integration of microprocessor into everyday objects like furniture, wrist watch, clothing, Bracelets, personal mobile display and so on. Ubiquitous communication enables these objects to communicate with each other and the user by means of ad hoc and wireless networking. Intelligent user interfaces enable the inhabitants of the AmI environments to control and interact with these environments in a natural (i.e., voice, gesture) and personalized way (i.e., preferences, context) [24].

### 3.1 Dependability and security in AmI world

A dependable theme of the scenario work is the requirement for a safe, consistent and secure AmI-world. The technologies should be tested to make sure they are safe and sound for use. On the one hand this refers to physical and psychological threats that the technologies might involve. On the other hand, the creation of a landscape of interoperating AmI devices focuses even greater prominence on the requirement for vigorous and dependable software systems. For this reason there is likely to be a promising importance on self-testing and self-organizing software and techniques based upon software components. It will also be essential to have AmI systems that are secure against intentional misuse. The scenarios presume techniques for secure ID authentication, micropayment systems and biometrics. These sorts of reliance technologies and sophisticated encryption techniques are sturdy requirements for both the dependability and the likely acceptance of nearly all of the processes, products and services based on the scenarios. Realistic and extensive use of micropayment is necessary for AmI according to some scenarios in which the AmI features are accessed and used on an ad hoc basis. But there is also the likelihood that many of these transactions will be bought on a subscription basis. In Information security, biometrics will be significant as a means of authentication based on measurable substantial characteristics that can easily be checked (fingerprints, iris scanning or speech) [25].

## 4. LIMITATION OF SECURITY INTO SOFTWARE ENGINEERING PRACTICE

There are some causes that should have to be conquered in the software system improvement to make the customer benefited secure software system. These are as follows:

### 4.1 Lack of security knowledge in individual developers in the system development

Lack of security knowledge of system developers causes security imperfection in the system development. Many software developers do not have adequate knowledge in computer security as a result they can not produce a desired security required solution. Secure software engineering methodologies ought to reflect on this issue and should make available methods and processes so that the system developers can follow that process even a non expertise in that field.

### 4.2 Need concrete guidelines for construction secure application

There are many patterns and frameworks in the market but most of them for specific scenario and concentrate on the specific stage on the development process for instance security requirement engineering. Security should consider in every phases in the system development such as requirement engineering to deployment of the system. Consequently it is very essential to build up new process and techniques that will give a proper guideline to construct a secure application. These should support formal modeling, security requirements and conversion of such requirements to a design model that will satisfy them. There will be also test and validation check before implementation on security perspective whether they meet the security or not.

## 4.3 Need standard tools for security aspects

Incorporating security in the system means add additional activities in the development process. Though it is very difficult task it is very important to generate tools to support the development process. These tools should not only support to modeling the analysis stage but also support to transform to design and throughout the process.

## 4.4 Need security analysis in correct way

The Widespread use of software makes necessary their security analysis especially with respect to the malware hazard [26]. Critical application requires powerful execution features and capabilities that may enable and favor the spread of new malware. Supposition risk assessment from the past experience should be carried out in the respect of attackers mind. This is an important role for security analyst for careful analysis of the entire system in view of potential attackers.

## 4.5 Unifying security expert people in software development team

As the Security engineering and software engineering is the different branch of study. So it is important to unify this two different background people while developing a system. Systems engineer analyze and select the market features. Security requirement analysis and risk assessment should be carried out by the security engineer that must need for market success and then it will be accumulate into security requirement in the system to function the security requirement as a prospective solution.

## 4.6 User doesn't understand their security related problems (understand wrong thing in correct way or correct thing in wrong way)

There is another problem is that the customer do not understand their security related problems most of the time. They don't know what their actually problems and what they need. It becomes a gap between user requirement and security functional requirement As a result the things are getting mismatch and this consequence the developer make the right thing in the wrong way and the customer get the wrong thing in the right way.

## 5. CONCLUSION

This work was devoted to different aspect of security in software engineering. The goal of those has been to investigate how the security can be integrated into software development system and how can be developed a secure software systems. Nevertheless, many works in the research areas of security in software systems have been done so far, but still is needed. Moreover managing security is a process not a product. And as such, the more knowledge one has, the better way onewill be able to manage from hostile behaviors in this area. In this paper different security mechanism has been presented to authenticate the legitimate user. However the concluding idea is not any concrete solution.The selfish and malicious people are always trying to get flaws inside the systems. This is not a product it's an ongoing process that we need to take care at all the times.

## 6. ACKNOLODGEMENT

At the outset we would like to pay our gratitude to Almighty for everything. We would like to extend our sincere thanks to Dr. Haris Mouratidis, Reader, University of East London School of Architecture, Computing and Engineering (ACE) for his guidance, support and invaluable feedback while preparing this paper. Also we feel like to show gratitude our friends and colleagues for their encouragement and support.

We are also gratifying to our parents, brothers and sisters for their everlasting support and love.

## 7. REFERENCES

[1] Premkumar T. Devanbu, Software Engineering for Security: a Roadmap, University of California, Davis, CA, USA 95616, 2000.

[2] A.Jacobsson**,** Privacy and Security in Internet-based Information Systems, Bleking Institute of technology, Sweden, Doctoral Dissertation Series No.2008:02, 2008.

[3] H. Mouratidis and P. Giorgini (eds), Integrating Security and Software Engineering: Advances and Future Vision, Idea group, IGI Publishing Group, 2006.

[4] R.Anderson, Security Engineering-A Guide to Building Dependable Distributed Systems, John Wiley & Sons, New York, NY.2001

[5] M.Bishop, Introduction to computer Security, Addison Wesley, Boston, MA, 2004.

[6] M.Chapple, the GSEC Prep Guide: Mastering SANS GIAC Security Essentials, John Wiley & Sons, New York, NY, 2003.

[7] D.Golmann, Computer Security, Second edition, Jhon Wiley & Sons, New York, NY, 2001.

[8] R.G. Smith, Authentication: From Password to public keys, Addison Wesley Proffesional, Boston, MA, 2002

[9] P.L Bernstein, Against the Gods-The remarkable Story of Risk, Jhon Wiley & Sons, Inc., New York, NY, 1998.

[10] T.R. Peltier, Information security Risk Analysis, Second edition,Auerbach publications, Boca Ranton,FL,2005.

[11] Ivan Victor Krsul, Software Vulnerability Analysis, PhD thesis, submitted to the Faculty of Purdue University, May 1998.

[12] Front Line Defenders : http://www.frontlinedefenders.org [Acc. 21 Sep 2013]

[13] N.R.Mead, Identifying security requirement engineering using of the security quality requirement engineering (SQUARE) method chapter iii, Integrating security and software engineering, Advances and future vision, idea group publishing, 2006.

[14] E.Yu, et al. A social ontology for integrating security and software engineeringchapter iv, Integrating security and software engineering,Advances and future vision, idea group publishing,2006.

[15] F.B.Fernandez, et al.A Methodology to develop secure systems using patterns, sectionII, chapterv, Integrating security and software engineering, Advances and future vision, idea group publishing, 2006

[16] M.Weissecurity pattern using NFR analysis, chapter disintegrating security and software engineering, Advances and future vision, idea group publishing,2006.

[17] M.siponen, et al.Extending security in agile software development methods section iii, chapter vi, Integrating security and software engineering, Advances and future vision, idea group publishing, 2006.

[18] H.Mouratidis, et al.Modelling security and trust with secure tropos chapter viii, Integrating security and software engineering, Advances and future vision, idea group publishing, 2006.

[19] M.Koch, et al.Access control specification in UMLchapter x, Integrating security and software engineering, Advances and future vision, idea group publishing, 2006.

[20] TorstenLodderstedt, David Basin, and Jürgen Doser, SecureUML: A UML-Based Modeling Language for Model-Driven Security, Institute for Computer Science, University of Freiburg, Germany, 2001

[21] Brose,G.,Access control management system in distributed object systems, PhD Thesis,FreieUniversitat Berlin,2001

[22] DušanŠimšík, AlenaGalajdová, ZlaticaDolná, Jana Andrejková ,The Ambient Intelligent and the assistive technologies for elderly, visually and hearing impaired users in Slovakia Technical University of Košice, Faculty of Mechanical Engineering, Department of Instrumental and Biomedical Engineering, Letná 9, 042 00, Košice, Slovak republic,2007

[23] Antonio Maña. (et al).Security engineering for Ambient Intelligence: A Manifesto, 2003

[24] A.Mana, et al .Security engineering for ambient intelligent: A Manifesto chapter xi, Integrating security and software engineering, Advances and future vision, idea group publishing,2006.

[25] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten& J-C.Burgelman, Scenarios for Ambient Intelligent in 2010, 2001

[26] Eric Filiol, Portable Document Format Security Analysis and malware Threats, Army Signals Academy-Virology and Cryptology Laboratory, France, 2008.