Modern Security Challenges

Conference Paper · May 2016

CITATIONS
0

READS
1,507

3 authors:

Rajeev Kumar
Shri Ramswaroop Memorial University
60 PUBLICATIONS **518** CITATIONS
SEE PROFILE

Suhel Ahmad Khan
Indira Gandhi National Tribal University
37 PUBLICATIONS **249** CITATIONS
SEE PROFILE

Prof. Raees Ahmad Khan
Babasaheb Bhimrao Ambedkar University
197 PUBLICATIONS **1,094** CITATIONS
SEE PROFILE

Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 5, Issue 4
April 2016

Modern Security Challenges

Rajeev Kumar[1], Suhel Ahmad Khan[2], Raees Ahmad Khan[3]

[1,3]Department of Information Technology, Babasaheb Bhimrao Ambedkar Central University, Lucknow, UP, India

[2]Department of Computer Application, Integral University, Lucknow, UP, India

Abstract: *As software applications are becoming more compound and distributed, need for security is increasing in every field. With the increasing complexity of software, developers are facing challenges in delivering software which fulfills customer's requirements but what if the software is not secure enough. It cannot be enough capable of handling the security threats and attacks in the real world. Hence, there is a need to focus on security, even now when customer's priority is having the secure software. In this paper software security is being focussed with the challenges which developer faces when employing it in software development. Software securities with its important terms are being discussed in this research. There are a generous of non-functional requirement, alongside with such characteristics as enactment and reliability, durability, availability. In this paper, there is a discussion about software security, security types, and its issues of upcoming threats of information technology territory and security contributions. This paper also describes challenges, problems of secure software in recent years.*

Keywords: Software Security, Software Risk, Security Vulnerability, Security Threat, Security Exploit.

1. INTRODUCTION

Digital technologies are now an essential part of our daily lives. Access to social networks, drop box, emails, and others are available from anywhere in the world. This fusion of computers and telephones into smart, mobile devices, and these practices are changing the concept of software. This much connectivity gives birth to different kind of viruses, threats, and vulnerabilities for PCs, laptops, and mobile phones[1]. This is now becoming the responsibility of developers to develop such kind of software or applications which secures itself from these viruses. The end user practices antivirus or same kind of applications to secure him from viruses. These viruses may harm his personal information or create business issues. Some of the organizations focus on end-to-end security while certain others have to move out the task inflexible even if the modules may collaborate.

Secure software development includes several characteristics, from security strategy definition, prescribed exhibiting, emerging security design and software prototypes, testing verification and confirmation, and finally estimation, certification, and authorization. It does not end at that time. The development stays through the software security life cycle. The task of consistently applying and authenticating high-level security strategies at a software level is a difficult and problematic whose derivations can be drawn support to the novel in computability results[2]. In this paper security challenges are discussed that have to be considered in building evolvable and flexible secure systems.

2. SECURITY FUNDAMENTALS

Security is one of the prevalent administration plans in the world, paying out thousands of billions of rupees per year. Security is the fragment of confrontation to, or protection from, impairment. It relates to any danger and appreciated ability, such as a person, dwelling, nation, or organization community. The Security curriculum's assistances contain leaving income, Medicare and Medicaid, information security, disability income, software cost and reliability and survivorship benefits. The prominence behind security is to certify confidentiality while defending personal or commercial documents. Some million devotee boomers are distinguished to multiply one of their furthermost essential financial choices of their lives, namely when to take security benefits[3].

There is no single taxonomy of security; it shows an inconsistency from “a narrow duration of avoidance of strength to a wide comprehensive opinion that recommends growth, social rights and traditional security

together." Opponents of the model of social security privilege that it protections almost the whole thing and that it is too wide to be the focus of research of security. There have also been denigrations of its experiment to the role of conditions and their domain. There are Security substances in general contexts given blow:

- Autonomy from risk or hazard that's means safety;
- Freedom from uncertainty, worry, or alarm; assurance;
- A set or branch of sequestered protectors;
- Processes approved by a government to prevent surveillance, interruption, or attack.
- Processes implemented to stop escape: Security in the secure is very close-fitting.

Security Fundamental in terms of IT Domain, Physical Domain, Political Domain and Financial Domain defined as the next term of paper.

3. CLASSIFICATION OF SECURITY DOMAIN

There is an enormous collected works on the examination and categorization of security. Security is categorized in four parts mainly, Information Technology, Physical, Political, Monetary shown in Figure 1.

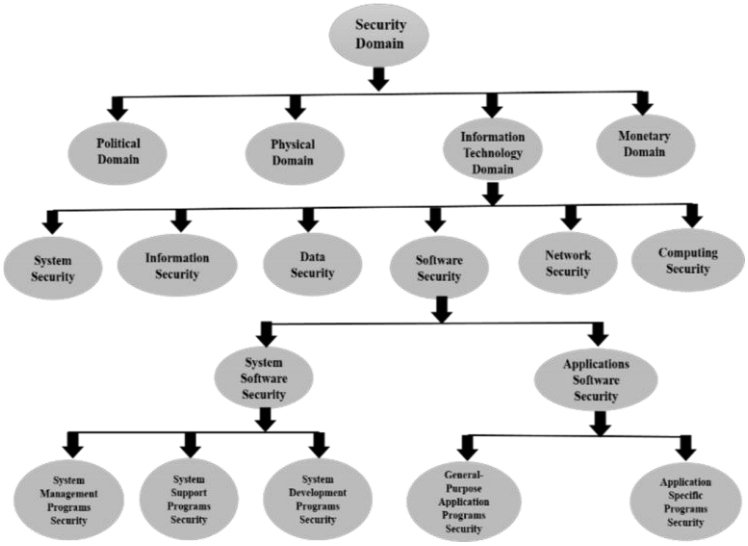

Figure 1: Classification of Security

I. Security in Context of Physical Domain

Physical security is termed as protection from personnel, programs and protection from physical circumstances and events that could cause serious hazards or damage to organization, agency or stakeholder[1]. This also includes protection from natural disasters like fire, terrorism and theft etc.

II. Security in Context of Political Domain

Political security is the defense beside some form of political domination. It is disturbed with people alive in a culture that nobilities their elementary human privileges[1]. Extradition is a means of preserving political security. Other than the security services established in terms of the Constitution, armed organisations or services may be established only in terms of national legislation. To give effect to the principles of transparency and accountability, multi-party parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 5, Issue 4
April 2016

III. Security in Context of Monetary Domain

Monetary security consists of the security of money and goods that are the assets of an organization. For security of money there are several ways one uses to secure[1]. Some of them are saving it in bank or like funds in funding companies. From the eye of thief it is kept safe by hiding it somewhere.

IV. Security in Context of Information Technology Domain

Information technology (IT) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data. Often in the context of a business or other enterprise[1]. The term is commonly used as a synonym for computers and computer networks, but it also encompasses other information distribution technologies such as television and telephones. Their definition consists of three categories: techniques for processing, the application of statistical and mathematical methods to decision making, and the simulation of higher-order thinking through computer programs.

An access control arrangement has the probable for impacting totally three principles of security (CIA). The main character is to safeguard the confidentiality of a source by confining access to the supply[1]. Furthermore, it will control the attributes of the contact, such as deliver, write and accomplish. For example, in the case of a data file, organizations may grant a user read access, but deny access to write or modify the data within the file. Here discussed of security in terms of information technology realm, which are directly or indirectly affects IT industry.

a) Information Security

Information security is not only a technological challenge but a human challenge as well, and needs human solutions first and foremost[1]. Bruce Schneier, one of the world's most well-known experts on security, once wrote that "security is a process, not a product." Indeed, with all the changing variables and players, security is a never-ending evolutionary process, wherein defenses change in response to new threats and new threats emerge with the introduction of new systems and defenses. This view only reinforces something that has been known for a while you cannot buy security off the shelf. In the case of Solaris, the operating environment provides a good set of proven security features and technologies, but they are useless if not correctly used and administered as part of an encompassing security process that tries to prevent security violations, detect them when they occur, apply corrective controls, recover from the incident, and improve it.

b) Software Security

As organizations worldwide increase their reliance on software controls to protect their computing environments and data, the topic of Software Security grows in importance. The tremendous potential costs associated with security incidents, the emergence of increasingly complex regulations, and the continued operational costs associated with staying up to date with security patches all require that organizations give careful consideration to how they address software security[1]. Application security is provided in some form on most open OS mobile devices. Thus, in viewed of the rapid cycles of development and obsolescence in the software world, any software of current interest will be confined by threats, internal and external attacks.

Criteria for protection include the requirement for the code to display uniqueness. In spite of the several advantages that software developed brings along with it, there are several concerns and issues which need to be solved before universal implementation of this application supposition happens. First, in software security, the user may not have the kind of control over information data or the performance of applications that may need, or the ability to stocktaking or change the processes and policies under which applications must work.

Software projects are almost always associated with the reengineering of business practices[3]. This results from the desire to adopt the best practices inherent in the chosen software solution rather than changing the software to match current business practices. Historically, traditional analysis and design projects had no reengineering and the software was written to match current practices. Additionally, a software

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 5, Issue 4
April 2016

implementation most always requires personnel to learn new programming languages and may also result in a transfer in on organization's security.

i. System Software Security

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords[4]. This deception is known as social engineering. In the world of information technology there are different types of cyber-attack–like code injection to a website or utilizing malware (malicious software) such as virus, Trojans, or similar. Attacks of these kinds are counteracted managing or improving the damaged product.

ii. Application Software Security

Software security means protecting information of software data, such as a database, from destructive forces and the unwanted actions of unauthorized users. From tarnished brand reputation to regulatory fines, the adverse impacts of data breaches are clear. Just a single incident of data loss can erode a business's competitive advantage, weaken consumer confidence, and result in fines or penalties from regulators. The problem is further exacerbated with rapid proliferation of mobile computing devices, widespread use of peripheral devices, and easy access to file-sharing software, all increasing the opportunity for data loss and theft.

Software-based security solutions encrypt the data to prevent it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offer very strong protection against tampering and unauthorized access[5]. Enterprise businesses and government agencies around the world face the certainty of losing sensitive data from a lost laptop, removable media or other plug-and-play storage device. This drives the need for a complete data protection solution that secures data on all common platforms, deploys easily, scales to any size organization and meets strict compliance requirements related to privacy laws and regulations.

4. SECURITY CHALLENGES IN SOFTWARE DEVELOPMENT

The three core requirements for developing secure software are as follows: **f**irst, people have to actually review the code; second, at least some of the people developing and reviewing the code must know how to write secure programs; third, once found, problems need to be fixed quickly and their fixes distributed[69].There are some challenges, though:

- Independent code review tends to be extremely expensive when one requires nondisclosure agreements.
- Free code review tends to be scarce with "source available" licensing, because people typically feel they're giving you something for nothing, whereas open source software is in many ways its own reward.
- Most of the best secure code writers understand that open code is the best way to get secure code (see Kirchhoff's), which might make it difficult to hire them if you plan to keep your code closed.
- Hiring and retention decisions in corporate development shops tend to ultimately rest in the hands of people who wouldn't know secure code if it bit them on their noses.
- Corporate responsibility lies with shareholder profits not the actual quality of software. This means that any time the ability to generate revenue or reduce costs conflicts with secure coding goals, the secure coding goals are likely to suffer. Considering the value of good programmers who know how to write secure code that means that severely limiting the money the human resources department is authorized to offer for new hire salaries is normal behaviour, which in turn limits the ability to hire the best programmers[10-11].
- Corporate responsibility is an important factor for patch distribution too; it is usually in a corporate vendor's best short term financial interest to downplay security vulnerabilities, which often involves

deferring development of security patches (sometimes indefinitely) and even hindering the ability of users to find reliable information about vulnerabilities and fixes.

- Identification, development, and testing of security fixes depends on the availability of developers and testers. Releasing software under the terms of an open source license tends to increase the number of available developers and testers significantly.

5. DISCUSSION

The traditional concept of security needs to be expanded in order to include the aforementioned information assets, whose combination is known as Information Systems Security. Security and information systems are therefore two closely linked terms, which is shown by the fact that any company's information is as good as the security mechanisms that are implemented over it. Unreliable information resulting from wrong security policies generates uncertainty and mistrust, and has a negative impact on every business area. Otherwise, secure information systems are a sign of certainty which contributes towards generating value both within and outside the company. Information Systems Security is a function whose mission is to establish security policies and their associated procedures and control elements over their information assets, with the goal of guaranteeing their authenticity, confidentiality, availability and integrity. Ensuring these four characteristics is the core function of Information Systems Security:

- Authenticity allows trustful operations by guaranteeing that the handler of information is whoever s/he claims to be.
- Confidentiality is understood in the sense that only authorized users can access the information, thus avoiding this information being spread among users who do not have the proper rights.
- Availability refers to being able to access information whenever necessary, thus guaranteeing that the services offered can be used when needed.
- Integrity is the quality which shows that the information has not been modified by third parties, and ensures its correctness and completeness.

Some of the current security challenges can be identified according to the innovative security approaches presented in this special issue. These security challenges could be grouped in the following security fields: Cryptography; Security in Small and Medium Enterprises; Privacy; Security and privacy in the Cloud and Internet; Security metrics; Forensics; Security standards.

6. CONCLUSION

There has been always an on-going discussion on the topic of security in every field. Because security of goods is as important as security of data, the issue takes a broader side. In today's world when 8 out of 10 people are connected to each other via some social networking sites, e-mails or simple networks for sharing data, security becomes an essential part of daily life. In this paper security is discussed in every field of life but focus is given on software security. There is a discussion on software security why it is important and how it can be achieved. This work may help a naïve customer, vendor or user to understand the security. So that one can give preference to security in its requirements when developer is going to develop software.

ACKNOWLEDGEMENT

This work is sponsored by UGC-MRP, New Delhi, India under F. No. 43-391/2014 (SR).

REFERENCES

1. Khan R. A., "From Threat to Security Indexing: A Causal Chain", Computer Fraud & Security, May 2009.
2. Boehm B., "Software Risk Management: Principles and Practices", IEEE Software, Vol. 8 (1), 1991, pp. 32-41.
3. Kumar R., Khan S. A., Khan R. A., "Revisiting Software Security Risks", British Journal of Mathematics & Computer Science 11(6): 1-10, 2015.

4. Kumar R., Khan S. A., Khan R. A., "Durable Security in Software Development: Needs and Importance", CSI Communications, pp. 34-36, October 2015.
5. Boban M., Pozgaj Z., Sertic H., "Strategies for Successful Software Development Risk Management", Management, Vol. 8, Issue 2, 2003.
6. Zubcsek P., Chowdhury I., Katona Z., "Information Communities: The Network Structure of Communication", Social Networks 38, P.P. 50-62, ©Elsevier B.V., 2014.
7. Yanyan W., "Research on e-commerce Security based on Risk Management", International Journal of Security and Its Applications Vol.8, No.3 2014.
8. Lee M., "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method", IJCSIT vol. 6, no1, February 2014.
9. Du S., Lu T., Zhao L., Xu B., Guo X, Yang H., "Towards An Analysis of Software Supply Chain Risk Management", Proceedings of the World Congress on Engineering and Computer Science 2013.
10. A Forrester Consulting Coverity, The Software Security Risk Report the Road to Application Security Begins in Development September 2012, Available at: http://www.coverity.com/library/pdf/the-software-security-riskreport.pdf last visit April 10 2015.
11. Patil S., Ade R., "Secured Cloud Support for Global Software Requirement Risk Management", IJSEA, Vol.5, No.6, 2014.