International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

Analysis of Information Systems Security Issues and Security Techniques

Rakesh Kumar[1], Hardeep Singh[2]
[1] Department of Computer Science and IT, Khalsa College for Women
[2] Department of Computer Science and Engineering, Guru Nanak Dev University Amritsar-143001

Abstract

Over the years, world witnessed a dramatically rise in count of the users who are in some way or other involved in data based software's use and development. A large pool of data and information is available over the internet for sharing. The social websites, personnel websites, banks database, NGO's data base, telecommunication company's data etc all are flooded with abundance of information. The rise is not single directional. The exposure to volumes of good and bad people has increased the risk of security of these software and information systems and hence the responsibility of developers has increased multiple times than their early companions. The time we are going through requires the software security and policies to be considered as early in development process so as to make them part of software architecture. In this paper we have qualitatively analyzed various security threats to information systems and various techniques for securing the information systems.

Keywords

Security techniques, attributes, threats, perspectives, software architecture.

1. Introduction

Now a day the software security has become a subject of great importance. The security of a software is mainly affected by software vulnerabilities. The hacker community may take advantage of a software vulnerability to compromise the three basic security properties, i.e., confidentiality, integrity and availability. These vulnerabilities when exposed may pose threats to systems and can have an impact on normal software functioning [3][4]. These vulnerability can be a defect that is an implementation or design error. It may lie dormant in software for several years and then surface in a fielded system with major consequences. It can also be a bug, which is an implementation-level software error. Bugs refer to low-level implementation errors that could be remedied by limited code analysis of the external environment, or it can be a flaw that is a subtle defect at a deeper level. It is important for a security software to be himself secure so as to ensure system security otherwise, it may contain software vulnerabilities, which could be exploited when attacked[8].

2. Security related issues

Given below is discussion of various related issues.

2.1 Security attributes

Security attributes define the aspects of a system that security is meant for. Major publication and studies have defined the composite notion of security as the combination of properties listed below.

1) Confidentiality: The prevention of unauthorized disclosure of information.
2) Integrity: The prevention of unauthorized modification of information (including accountability and nonrepudiation as sub-categories).
3) Availability: The prevention of unauthorized withholding of information.

2.2 Security threats and faults

All service failures originate to faults in the providing system. A service failure is defined as an event that occurs when the delivered service deviates from the correct service [6]. This deviation in the external state of the system is called an error, and the cause of an error is called a fault. Faults can be internal or external of a system. An external fault (malicious external faults are called attacks) causes an error, and possibly a subsequent failure; the internal fault that allows the external fault to harm the system has to pre-exist in the system [14]. These kinds of internal faults are called vulnerabilities. External attacks use vulnerabilities exploit the above listed security attributes like confidentiality, integrity and availability etc[5]. According to service architecture point of view, the prominent categorization of the faults is based on:

i) Creation time faults – Whether fault occurred during the development or the operation of the system.

ii) System boundaries- whether the faults have internal or external origins.
iii) Objective - whether introduced with malicious objective of causing harm, or non-malicious
iv) intent- whether faults are deliberately induced or by mistakes.
v) persistence- Whether bounded in time or persistent in nature.

2.3 The security Perspectives

A security goal is the ultimate security objective of a security property [13]. It is achieved as a result of the implemented security properties in the components. For example, a security goal could be defined as the integrity of an object or a piece of data; confidentiality of a message; authentication of an entity or user; authorisation for an operation on certain object or data; or non repudiation of a message and so on. Security perspective can be divided in three related categories:
i) The Security Expert's Perspective- These focus on the technical details of security of the component system such as cryptography, threats and security policies.
ii)The software composer's perspective- It covers implemented security properties and their impact on the composite system.
iii)The end-user's perspective- The ultimate security goals which are achieved in association with a particular functionality provided by a collection of components. A security goal is the ultimate security objective of a security property [9][15]. It is achieved as a result of the implemented security properties in the software. For example, a security goal could be defined as the integrity of an object or a piece of data, confidentiality of a message, authentication of an entity or user, authorization for an operation on certain object or data, or non-repudiation of a message etc [10].

3. Threats to data security

The act of authenticating an entity must be trustworthy if there is to be any security in the software system at all [17]. This means that the authentication facility must correctly identify the entity in all cases, regardless of the role played by the entity, the location of the entity, and the presence or absence of potential enemies[1][11]. The common threats to data security include Identity interception, Masquerade, Replay, Data Interception, Manipulation, Denial of service, Misrouting, Traffic analysis etc.

4. Various techniques for data security

Both the symmetric and asymmetric techniques are possible for encryption and decryption of data to make it secure from different threats mentioned earlier. Table below gives a comparative analysis made between different techniques depending upon factors like length of keys and number of rounds etc. The symmetric block ciphers like SDES (Simplified Data Encryption Standard), DES (Data Encryption Standard),2DES(Double Data Encryption Standard),3DES(2)(Triple Data Encryption Standard With Two Keys),3DES(3)(Triple Data Encryption Standard With Three Keys),IDEA (International Data Encryption Algorithm),BLOWFISH,RC5 (Rivest Cipher 5),RC2,CAST (Carlisle Adams and Stafford Taveres) are analyzed based upon above parameters [1][2].

4.1 Analysis of Symmetric and asymmetric security techniques

The description of these techniques is analyzed to produce following analysis.

Table 1: Analysis of symmetric block cipher techniques

Algorithm	Key Size	Level of Security	Application
SDES	10 bits	Less Secure	Encryption/ Decryption In hardware ,software
DES	56 bits	Less Secure	Encryption/ Decryption In hardware ,software, firmware
2DES	112 bits	Less Secure Than TDEA but Secure than DES	Strong Encryption/ Decryption in hardware and software
TDEA	168 bits	More secure Than DES	Very strong Encryption/ Decryption
DH	160 bits	Comparatively Secure	Encryption/ Decryption
ECDH	112, 160, 192, 156 bits	Well secure	Encryption/ Decryption
IDEA	128 bits	Resist-ant to Crypt analysis	Encryption/ Decryption

Blowfish	Variable up to 448 bits	Very Secure	Very strong Encryption/ Decryption
Cast-128	40 to 128	Secure	Encryption/ Decryption
RC5	Up to 2048	Highly Secure	Encryption/ Decryption
Vernam	Variable	Secure due to XOR operator	Encryption/ Decryption

Among the major asymmetric cryptographic techniques the best one are The Diffie-Hellman Key Exchange algorithm, Knapsack Algorithms, RSA, Pohlig-Hellman, Rabin, ElGamal

Table 2: Analysis of asymmetric block cipher techniques

Algorithm	Key size	Level of Security	Applications
Diffie-Hellman exchange	Same as message size to prevent brute force attack.	Truly Secure	Used for very fast Encryption/Decryption
Knapsack	Around half a megabit	Insecure	High speed encryption and decryption.
Elgamal	Of order 10000 bits	Semantically secure.	Encryption/Decryption
RSA	1024 bits.	Very secure due to property of prime numbers	Hardware and software Encryption /Decryption
Rabin	Has to be 256 bit.	Secure	Fast Encryption /Decryption

5. Conclusion

Best practice for incorporating security in an information system is to think and work it very early in development phases. The outcome of every phase should be checked for security concerns. Since the major work for information systems focus on the data management and retrieval, therefore it is recommended to use one of the security techniques, depending upon the usage requirements, so as to make every transaction a secure one. The architecture of information system also carries lot of importance when security is a point of concern. Effort will be made, in times to come, for establishing a relation between architecture of information system and its security.

Reference

[1] Schneier, Bruce. Applied Cryptography, 2nd Edition. New York: John Wiley and Sons, 1995.
[2] Stallings, W. Cryptography and Network Security: Principles and Practice, 2nd edition. Prentice Hall, 1999.
[3] Hoglund, G., McGraw, G., "Exploiting Software How to Break Code," Addison Wesley, February 17, 2004.
[4] Howard, M., LeBlanc, D., "Writing Secure Code," Microsoft Press- Microsoft Corporation, 2002.
[5] O. H. Alhazmi, Y. K. Malaiya, and I. Ray. Measuring, analyzing and predicting security vulnerabilities in software systems. Computers & Security, 26(3):219–228, 2007.
[6] S. Kumar and E.H. Spafford, "A Software Architecture to Support Misuse Intrusion Detection", Proceeding 18th Nat'l Information Systems Security Conf., National Inst. Standards and Technology, Washington DC, 1995, pp.194-204.
[7] Boehmer, W.; , "Toward a Target Function of an Information Security Management System," Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on , vol., no., pp.809-816, 2010.
[8] Chao-Qin Gao; Chuang-Bai Xiao; , "A Security Model for Information Systems with Multi-level Security," Computational Intelligence and Security (CIS), 2011 Seventh International Conference on , Dec. 2011.
[9] Boehmer, W.; , "Analysis of Strongly and Weakly Coupled Management Systems in Information Security," Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on , vol., no., pp.109-116, 18-25 July 2010.
[10] Leitner, M.; , "Security Policies in Adaptive Process-Aware Information Systems: Existing Approaches and Challenges," Availability, Reliability and Security (ARES), 2011 Sixth International Conference on , vol., no., pp.686-691, 22-26 Aug. 2011.
[11] Tvrdikova, M.;, "Information system integrated security," Computer Information Systems and Industrial Management Applications, 2008. CISIM '08. 7th, vol., no., pp.153-154, 26-28 June 2008.
[12] Pauli, J.J.; Xu, D.; , "Misuse case-based design and analysis of secure software architecture," Information Technology: Coding and Computing,

2005. ITCC 2005. International Conference on , vol.2, no., pp. 398- 403 Vol. 2, 4-6 April 2005.

[13] Alvi, A.K.; Zulkernine, M.; , "A Natural Classification Scheme for Software Security Patterns," Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on , vol., no., pp.113-120, 12-14 Dec. 2011.

[14] Sen-Tarng Lai; , "An Analyzer-Based Software Security Measurement Model for Enhancing Software System Security," Software Engineering (WCSE), 2010 Second World Congress on , vol.2, no., pp.93-96, 19-20 Dec. 2010.

[15] Gilliam, D.P.; Kelly, J.C.; Powell, J.D.; Bishop, M.; , "Development of a software security assessment instrument to reduce software security risk," Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings.

[16] Byers, David; Shahmehri, Nahid; , "Design of a Process for Software Security," Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on , vol., no., pp.301-309, 10-13 April 2007.

[17] Shaw, M. and P. Clements. 1996. A Field Guide to Boxology: Preliminary Classification of Architectural Styles for Software Systems. In Proceedings of the 1997 International Computer Software and Applications Conference, ACM, New York, NY.

Dr. Hardeep Singh is Professor, Department of computer science and Engineering and Director Placements, Guru Nanak Dev University Amritsar, Punjab,India. He is senior member Computer society of India, Punjab science congress and other eminent organization. He has been chairperson of many conferences of national and international level in the region. He has dozens of publications in international journals and conferences. His major area of research is Software Engineering.

Rakesh kumar received his B.Sc in computer science in 1999, the M.Sc (Mathematics) degree from G.N.D.U. Campus, INDIA, in 2002, M.Tech. (Information technology) From G.N.D.U. Campus, G.N.D.U., in 2004.He cleared UGC-NET in computer science and applications twice. He worked as lecturer at Dr. B.R.Ambedkar NIIT Jalandhar. He is doing Ph.D in computer science. His research areas include data security, information systems and software architecture. He has more than a dozen of publications to his credit.