Ind Jour Math & Comp Sc. Jhs. Vol. II - Pt I, 2013 Pg 26-30

Information systems security: A review

Amit Kumar Jain[1], Yashpal Singh[2] and Sachin Updhyay[3]
[1]NRCAF, Jhansi,[2]BIET, Jhansi, [3]BU ,Jhansi
[1]diggijain@gmail.com,[2]yash_biet@yahoo.co.in,[3]sachinupdhyayhcl@gmail.com
Recceived on 01/2/2012

ABSTRACT : The evolution of network-based computing has caused information security managers rethink their priorities and perceptions of risks. Studies have identified that security was not considered to be a major issue in the pre-Internet era, the early 1990s. But studies conducted in the mid-1990s revealed that managers were beginning to worry about open architectures and security issues posed by networks. But by the end of the 1990s, security was topping the list of major issues in IS. This change of perception has drawn greater attention to this issue; and this has eventually given birth to various IT control requirements and industry Standards that largely govern the process of security risk management today. The role of technology is paradoxical when it comes to security. Because, as seen earlier, technology is the one of the primary causes for the majority of security risks. For example, sophistication of technology adds to complexity and a steeper learning curve; and the complexity leads to oversights, thereby creating security holes. But paradoxically, most people turn to technology once again for solution to these security problems! Familiarity of the technology and being informed of the latest developments is one of the primary requirements of a security practitioner.

KEYWORD: network security / information system

Security of networked information system

The need to accommodate more complex business transactions over networks is changing the future of information security models (Fonseca and Lee, 2001). Security of an information system was considered to be a technical issue to be handled by the IT department until recently. But Fonseca and Lee reported (2001) that with the increased interaction between security and e-commerce, the line separating business and IT departments is continuing to blur. Lindstrom, cited by Fonseca and Lee (2001), states that "it's not just security folks that go to security conferences anymore; it's e-business directors and CIOs of pure-play businesses that want to be up to speed about what infrastructures are doing security-wise." A Gartner Group report (Witty et al., 2001) also re-emphsized this notion. The Gartner report estimates that about 90% of the current security spending is IT-related; however, it is forecasted that the non-IT portion would go up from current 10% to 40% by 2014.

Although business or non-IT components are playing an increasingly prominent role in the security model of an organization. The need to authenticate and validate users is one of the top components of an information security model. PKI (Public Key Infrastructure) is one of the most important components of user authentication and validation. Most security comes with controls, and DO's and DON'Ts. But it is important to identify the right balance of security measures and controls such that the right people access the right information at the right time. However, Lewis (2000) pointed out that achieving that balance is a challenge given the simple dynamics of e-business, a system is required to serve hundreds of thousands of end-users with potentially diverse computer platforms and requirements.

When does a security issue become a risk?

Technically, risk is the probability associated with losses or (failure) of a system multiplied by the dollar loss if the risk is realized (Straub and Welke, 1998). By this definition, it is evident that risks are subjective. It is up to the management to assess risks and to classify them based on their severity. The economic aspect of managing risks also plays a role in it, because sometimes the benefits from mitigating a risk may not justify the costs involved. At the same time, chances of occurrence of some risks may be less than the others. In general, Straub and Welke's definition of risk can be used as a simple gauge of measurement.

What role does the network play in the security of the information system? And how has the evolution of the global network changed the security of information systems?

A clear indication that security was not perceived to be a serious issue before the advent of the Internet can be seen Delphi study conducted by Society for Information Management (SIM) in the United States on the key issues in Information Systems Management. In the survey, SIM institutional and board members were asked to consider what they felt were the most critical issues facing IS

executives over the next 3 to 5 years, they found security to be of markedly lower priority, and decided to drop it from the list of issues (Brancheau et al. 1996).

However, it is interesting to observe that another study was conducted in Australia around the same time specifically on security issues (Fink, 1995), probably because security was considered to be a significant issue in that part of the world. A convincing explanation for this inconsistency in IS executives' perceptions can be found in another study (Watson, et al., 1997). Watson and his team compare and contrast the findings of 10 information systems management studies in 10 countries, and the SIM Delphi study mentioned above. They discovered that the possible reasons for these differences are cultural, economic development, political/legal environment, and technological status of these nations. According to recent studies (conducted by Sisco) security is the biggest challenge facing small and medium-sized businesses. Ever-changing security threats from both inside and outside the business network can severely impair business operations, affecting profitability and customer satisfaction. In addition, small and medium-sized businesses must comply with new regulations and laws formulated to protect consumer privacy and secure electronic information.

Coming back to the point, the Australian Delphi study (Fink, 1995) mentioned above was conducted to identify key IS security issues by surveying IS managers of the 198 largest companies operating in the Australian Stock Exchange. The results of this study provided a ranking of IS security issues in terms of their perceived importance in the middle 1990s, as shown in Table 1.

A quick look at the results of the Top Five IS security issues of the mid 1990s clearly indicate that the IS executives were beginning to get concerned about the security issues of open architecture and networks that would become the Internet, and an organization's vulnerability to errors and crime that would become so common by the end of 1990s. It is to be noted that there were about 9 million Internet hosts by the end of 1995, whereas the number of Internet hosts today stands well over 100 million (ISC, 2000).

The open nature of the Internet provides an ever-growing list of vulnerabilities that every enterprise needs to address. As companies move a greater percentage of their revenues to Internet/e-business channels, the degree of security risks increases and the number of controls implemented rises.

The Gartner group estimates (Witty et al. 2001) that in 1999, 75% of all enterprises were Internet-isolated. But by 2004, they estimate that 80% of enterprises will be using the Internet as an integral part of their business processes. In other words, this finding means that security risks of using the Internet will be faced by 80% of all enterprises. It was seen earlier that 85% to 90% of all businesses on the Internet reported some form of security incident in 2000 (CSI, 2001, Fogarty, 2001; Gaudin, 2001; Veysey, 2001).this finding reveals a potentially dangerous situation.

In other words, approximately 72% of all businesses in world will be under threat of security risks by the next three years from the Internet alone, unless adequate measures have been taken.

Table 1 : Top five IS security issues (Fink, 1995)

Rank	Description
1	**Access Control:** Controls need to be devised to limit access to resources of a system only to authorized persons, as the move to open systems architecture has made this a complex task.
2	**Disaster Recovery:** Organization need to identify potential threats and have procedures in place to overcome disasters, when they occur.
3	**Networks:** Knowledge needs to be gained on the complex security requirements of networks.
4	**Security Management:** Deliberate management action should be taken to reduce the organization's vulnerability to disasters, errors, and crime.
5	**Security Awareness:** IS managers should consider using marketing methods to raise awareness of security issues.

IT Control Requirements

As vulnerabilities and risks associated with Information Systems increase, corporates are faced with an ever -longer list of controls to be implemented to protect their businesses.

The seven **IT** control requirements needed to adequately and comprehensively protect an enterprise are defined as authentication, authorization, confidentiality, integrity, privacy, non-repudiation and availability. The Gartner Group identifies an eighth requirement titled ''Non-interference'' that addresses someone trespassing within an enterprise, which, for example, may be used as a launch pad to another enterprise.

Table 2 below describes the eight IT control requirements and possible security control tools currently available for each of them.

Table 2 : IT Control Requirements

Requirement	Definition	Security Control
Non-Interference	Ensure that control is exercised over the entry and use of an enterprise's electronic assets.	▪ User ID/ Password ▪ Firewall ▪ Nondisclosure of Passwords
Authentication	Ensures that users and applications appropriately identified before gaining access to information assets.	▪ User ID/ Password ▪ Token ▪ Biometrics Device ▪ PKI Credentials
Authorization	Ensures that a properly authenticated user/application can access only those IT resources to which the information owner has given approval.	▪ Access Control List ▪ Attribute Certification
Confidentiality	Ensure that only those people who have a need to see information are able to see it.	▪ Encryption
Integrity	Ensure that it can be identified if a transaction has changed between the sender and the receiver.	▪ Message Authentication Code (MAC)/ Hash
Privacy	Ensures that information provided by employees, customers and other is protected so that the information is used solely for the stated purpose of the enterprise's customer privacy policies, the person has authorized such use and its use is in compliance with all local privacy regulations.	▪ Policies & Procedures ▪ Encryption ▪ Policy Management Tools
Non-Repudiation	Ensure that both the sender and receiver of information can unequivocally prove that the exchange occurred.	▪ Digital Signature ▪ Time Stamp
Availability	Ensure that an enterprise's IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks.	▪ Redundancy ▪ Load Balancing ▪ Policies & Procedures ▪ Business Continuity Plan ▪ Alternate Processing Site

Source: Gartner Research (Witty, et al., 2001)

Security principles from the industry leaders

The following are the components of Deloitte's guiding security principles for the design of information security architectures, which are particularly relevant to the case being investigated in this project:

Intrusion: Ensures that access to systems and inforn1ation can only be gained through authorized access methods.

Authentication: Ensures that only authorized personnel are able to access the systems and information.

Authorization: Ensures that access to systems and information is restricted to those with an authorized requirement for such access.

Encryption: Protecting information in transit and in storage through the use of encryption.

Accountability: Ensures that access to systems and information by users is appropriately recorded.

Availability: Ensures that systems and information are available to authorized users whenever required.

Endurability: Ensures that security risks are maintained at acceptable levels over time.

Security Policies

Imposing network and systems security is only a part of the overall security strategy. The literature refers to the policies as another important aspect of security.

As seen earlier (Lewis, 2000), a critical component of managing risk is to assign and manage liability clearly. Lewis points out those authentication systems allow

organizations to assign liability to an account, and the person owns that account. Such dependencies can be articulated in the security policies of the organization. Lewis suggests that security policies can also explicitly define what people can do and when they can do it, and policy conditions under which they are operating, assigning, sharing or disclaiming any liability associated with their actions. Non-repudiation, or the use of logging and auditing functions to prove that something actually happened, can also be used as tool in the case of an incident.

Usage of insurance instruments is also proposed as part of the policy measures to indemnify businesses (Lewis, 2000). The author observes that the insurance industry is coming up with a completely new set of instruments targeted at this area.

In addition to this, to effectively deal with system and security risks, Straub and Welke (1998) propose that managers should initiate a theory-based security program that includes (1) use of a security risk planning model, (2) education in security awareness, and (3) countermeasures matrix analysis.

Perhaps the most important aspect is defining and imposing an acceptable security policy framework for the organization as far as usage of information systems are concerned. It has been observed that insider attacks, or attacks from the employees, attribute to a major proportion of network attacks (Ehinger, 2000). Ehinger observes that effective implementation of network resources use policies could prevent such events to an extent. Examples include policies on using modems in the corporate networks, telecommuting, and usage of Email and the Internet.

People and security risks

The people aspect of systems security is an area not to be overlooked. Long (2001) stressed the importance of background checks of people before employing them and assigning them to work on critical information systems. Long pointed out that lowering applicant screening standards may result in putting the wrong person on the payroll and open the road to work-related crime and related issues.

Some researchers believe in the importance of ethical issues associated with accessing and using confidential information (Smith et al., 1996; Kreie and Cronan, 2000). Today's information technology makes vast amount of information accessible to businesses and their employees. The authors point out that this creates the potential for misuse of information technology, and businesses are to be concerned about the ethical behaviour of their employees and the security of their information systems. Smith, et al (1996) point out that information privacy has been called one of the important ethical issues of the information age. Kreie and Cronan (2000) believe that **in** certain situations, external influences such as company standards are likely to affect employees' behavior. The proposed solution to this issue is to encourage ethical decision making by having a written code of ethics and providing ethical training.

Countermeasures of risks

What can be done to reduce the effect of security risks of an information system? It is widely accepted that countermeasures or strategies adopted to reduce security risks, fall into four categories of sequential actions (Straub and Welke, 1998), namely: (1) deterrence, (2) prevention, (3) detection, and (4) recovery. Straub and Welke notes that a certain portion of the potential system risks can be prevented by "deterrent" techniques, such as policies and guidelines for proper system use and by reminders for users to change their passwords, etc.

If users choose to ignore deterrents, the next line of system defense is "preventives," such as locks on computer room doors and password access controls. The literature refers to preventive measures as active countermeasures with inherent capabilities to enforce policy and prevent illegitimate use (Straub and Welke, 1988).

If abusers successfully penetrate through the first two levels of defense systems, the organization needs the ability to "detect" the misuse. Examples for this mechanism include activity reports and system audit trails. The primary purpose of this security response is to gather evidence to identify the abuser.

Finally, an effective security program should be able to help "recover" from the harmful effects of a harmful act and to punish the offenders.

References:

1. Brancheau, J.C., Janz, B.D. and Wetherbe, J.C. 1996. "Key issues in information Systems management: 1994-95 SIM Delphi results," *MIS Quarterly*, Minneapolis; Jun, Vol. 20, Iss. 2, pg. 225
2. CSI. 2001. Financial losses due to Internet intrusion, trade secret theft and other cybercrimes soar, *Sixth-annual Computer Security Institutes/FBI computer crime and security survey, (press release),* URL:
3. Ehinger, D.P. 2000. Considerations for an acceptable use policy for a commercial enterprise, *SANS Institute*. URL:
4. Fink, D. 1995. "IS security issues for the 1990s: Implications for management," *Journal of systems Management*, Cleveland: Mar/Apr; Vol. 46, Iss. 2, pg. 46
5. Fogarty, K. 2001. "Better Part of valor?"

Computerworld, 2001. Framingham; Jul 16; Vol. 35, Iss. 29; pg. 38

6. Fonseca, B. and Lee, S. 2001. "Changing face of security," *InfoWorld,* Framingham; Apr 16; Vol. 23, Iss. 16; pg. 8
7. Gaudin, S. 2001. "Cost of computer crime explodes, survey says, *Network World*, Framingham. Mar 12; Vol. 18, Iss. 11, pg 1 http://www. sans.org/infosecFAQ/policy/considerations.htm [11 Sep 2001]
8. ISC. 2000. Internet domain survey: Number of Internet hosts. *Internet Software Consortium Survey Results*, URL: http://www.isc.org/ds/host-count-history.html [29 Jan 2001]
9. Kreie, J. and Cronan, T.P. 2000. "Making ethical decisions," *Communications of the ACM*, New York; Dec; Vol. 43, Iss. 12, pg 66-71
10. Lewis, J. 2000. "Security strategy must focus on business issue of managing risk," *InternetWeek*, Manhasset; Oct 2; Iss. 831, pg. 41
11. Long, J.W. 2001. "Background checks step by step," *Security Management*, Arlington; Feb; Vol. 45, Iss. 2, pg. 72
12. Smith, S.J., Milberg, S.J. and Burke, S.J. 1996. "Information privacy: Measuring individuals' concern about organizational practices," *MIS Quarterly*, Minneapolis; Jun; Vol. 20, Iss. 2; pg. 167
13. Straub. D.W. and Welke, R.J. 1998. "Coping with system risk: Security planning models for management decision making," *MIS Quarterly*, Minneapolis; Dec; Vol. 22, Iss. 4; pg. 441-469
14. Veysey, S. 2001. "E-commerce risks about for companies," *Business Insurance*, Chicago; Apr 9; Vol. 35, Iss. 15, pg. 15
15. Watson, R.T., Kelly, G.G., Galliers, R.D. and Brancheau, J.C. 1997. "Key issues in information systems management: An international perspective," *Journal of Management Information Systems*, Armonk; Spring; Vol. 13, Iss. 4, pg. 91-115
16. Witty, et. al. 2001. The price of information security. *Strategic Analysis Report: Gartner Research*, June 8; Note Number: R-11-6534

Ind Jour Math & Comp Sc. Jhs. Vol. II - Pt - I, 2013 Pg 31-36

An Analysis of a queue with length distribution according to its priorities

RAM KHILAWAN TIWARI, DR. DHARMENDRA BADAL*
Department of Mathematics, G.B.S. College, Mauranipur
*Department of Mathematical Sciences and Computer Application, Bundelkhand University, Jhansi (U.P.)
*E-mail: dr_dbadall@yahoo.co.in

ABSTRACT : Abstract. We consider a single server multi-class queueing model with Poisson arrivals and relative priorities. For this queue, we derive a system of equations for the transform of the queue length distribution. Using this system of equations we find the moments of the queue length distribution as a solution of linear equations.

Introduction

We consider a multi-class queueing model with relative priorities. In the relative priority service discipline for a single server (processor) system with K classes of customers, if at some service completion there are n_j customers of class j, j = 1, . . . ,K, then the next customer to commence service is selected from class i customers with probability.

$$\frac{n_i p_i}{\sum_{j=1}^{K} n_j p_j},\ i = 1,..., K.$$

Once a customer has started service, it is served without interruption until completion.

Relative priority model is related to the well-known model of discriminatory processor sharing (DPS), see the recent survey [2]. An essential difference with DPS is that for DPS all customers in the system are served simultaneously by a single processor, whereas in relative priority model, the processor serves customers one at a time until their service has been completed.

A single server multi-class queueing model with relative priorities was first suggested in [4]. For the analysis of queueing model with relative priorities it seems that Haviv and van der Wal [5] is the only known result in open literatures. Haviv and van der Wal [5] obtained the mean waiting times for the M/G/1 queue with relative priorities.

In this paper we consider a single server multi-class queueing model with Poisson arrivals and relative priorities. For this queue, we derive a system of equations for the transform of the queue length distribution. Using this system of equations we find the moments of the queue length distribution as a solution of linear equations. Besides, numerical examples are given.

Transform of the queue length distribution

We consider an M/G/1 queue with relative priorities and K classes of customers. Each class i customer has a positive priority parameter $p_i, i = 1,...., K.$ Customers of class i arrive in a Poisson stream with rate λ_i. The overall arrival rate is $\lambda = \sum_{i=1}^{K} \lambda_i$. The service times of class i customers, denoted by random variable X_i, have an identical distribution function $B_i(t)$ with Laplace-Stietjes transform $B_i^*(s) = \int_0^\infty e^{-st}\, dB_i(t)$. The traffic intensity for class i customer is $\rho_i = \lambda_i E[X_i]$ and the total traffic intensity is $\rho = \sum_{j=1}^{K} \rho_j$.

Let $N_i(t), i = 1...., K,$ be the number of class i customers in the system at time t. Let τ_n be the nth departure epoch. Then $\{(N_1(\tau_n +),...., N_K(\tau_n +)): n = 1,2,...\}$ is a Markov chain, called an embedded Markov chain (EMC). We observe that

$$P((N_1(\tau_{n+1} +),..., N_K(\tau_{n+1} +)))$$
$$= (l_1,....,l_K) \mid (N_1(\tau_n +),...,N_K(\tau_n +)) = (n_1...,n_K)$$

$$= \begin{cases} \sum_{i=1}^{K} \frac{\lambda_i}{\lambda} b_i(l_1,...l_K) \text{ if } (n_1...,n_K) = (0,...,0), \\ \sum_{i=1}^{K} \frac{n_i p_i}{n_1 p_1 + ... + n_K p_K} b_i((l_1,....,l_K) - (n_1,...,n_K) + 1_i) \\ \qquad \text{if } (n_1,....,l_K) = (0....,0), \end{cases}$$

2.1