A Framework of 'Enabling Security Systems' for Organizations

Saleh Al-Zharani
Department of Information Systems
Imam Mohammad Bin Saud University
Riyadh, Saudi Arabia

Pit.Pichappan
Imam Mohammad Bin Saud University
Riyadh, Saudi Arabia
Department of Information Systems

Abstract:
Increasing information security threads lead the Information Technology Systems to the strategic level. The organizations' information systems need to be protected from many possible attacks such as computer viruses, trojans, worms, and other debilitating networked-based attacks. Consequently, it is imperative that technologies be examined and adopted from an Enterprise-wide perspective, and that priority is given to technologies that facilitate System-wide improvements. Our survey has provided an opportunity to review and reflect on broader infrastructure requirements to ensure system security. Security systems can operate at different levels, and every effort needs to be made to ensure that security issues never compromise. In particular, for a system to be made operational under the best possible circumstances, the initial launch of a system must conform to strict quality assurance guidelines. These same guidelines will provide the basis for assessing the systems state at the time of change and can also be referenced to assess future performance. A deployment assurance procedure must be introduced to ensure optimal performance of operating systems. This will involve both initial testing as well as ongoing operational procedures.
In order to ensure a comprehensive information security policy, we have surveyed the existing security system by using the following variables. They are Unit testing, Functional/System testing, Environment testing, Data conversion testing, Actuarial certification testing, User acceptance testing, Volume/Stress testing and Version upgrade testing. The use of the above variables ensures an improved security for organizations. The results of the study are discussed in this work.

Key words:
Enabling Security Systems, Organizations, Framwork

1- Introduction

Threats to information technology are ever increasing and many organizations are spending much money and time in attempting to fix security problems. As more people, systems and network go online, the security threat increases alarmingly. Increasing information security threads lead the Information Technology Systems to the strategic level. The organizations' information systems need be protected from many possible attacks such as computer viruses, trojans, worms, and other debilitating networked-based attacks. The major recent attacks are found to be emerged from the networked systems. Consequently, it is imperative that technologies be examined and adopted from an Enterprise-wide perspective, and that priority is given to technologies that facilitate System-wide improvements.
Digital information transactions are subject to multiple information security threats. For example, the most critical threat for HIS is the power failure (Ganthan Narayana Samy, Rabiah Ahmad, and Zuraini Ismail 2009). However, Modern technologies such as networks, Internet, and electronic services demand private and secure communications for a great number of everyday transactions. Security and cryptography provide a huge set of primitives, methods, and operation modes to support the special needs of data transmission (Nicolas Sklavosa, 2010). The organizations reliance on digital information transactions is influenced by perceived information security and distinguishes it from the objective assessment of security threats. The mechanisms of encryption, protection, authentication, and verification are the antecedents of perceived information security and we need to look after the security beyond the above parameters. These mechanisms are derived from technological solutions to security threats that are visible to organizations and hence contribute to the real perceptions of organizations.
As the modern information and communication technologies become a critical component of organizations' infrastructures and information establishes itself as a key and potential resource as well as driver, users have realized that there is more than the functionality of the new information systems that is significant. The organizational transactions over new system require stability, one factor of which is information security. Information systems development practices have changed in line with the evolution of technology offerings as well as the nature of systems developed. Through this paper we articulated that most of the contemporary development practices do not accommodate sufficiently security concerns. Beyond the

Manuscript received October 5, 2010
Manuscript revised October 20, 2010

literature evidence, reports on empirical study results indicating that practitioners deal with security issues by applying conventional risk analysis practices after the system is developed. In fact, System security involves decisions in at least three areas, identification of well-defined security policies, selection of cost-effective defense strategies, and implementation of real-time defence tactics. Unfortunately, there is no comprehensive tool that can integrate them to provide a single efficient model for safeguarding a network (Huaqiang Wei,etc 2008). Therefore, organizations formulate different security policies and there is a need for a way to incorporate these policies into the system independently from the design of the application. We also advocate that for security concerns integration in systems development by using field study results recording development practices that are currently in use to illustrate their deficiencies are incremental to our efforts in building security. Recording the required enhancements of practices and to propose a list of desired features that contemporary development practices should incorporate and will benefit the security concerns.

2- Background

The last few years have witnessed a rapid growth in cyber attacks, with daily new vulnerabilities being discovered in computer applications. Various security-related technologies, e.g., anti-virus programs, Intrusion Detection Systems, firewalls, etc., are deployed to minimize the number of attacks and incurred losses. However, such technologies are not enough to completely eliminate the attacks to some extent; they can only minimize them. Therefore, software assurance is becoming a priority and an important characteristic of the software development life cycle (Sanjay Rawat and, Ashutosh Saxena 2009). In Fact the word of information security is complex, not solely because of technology consideration but also because of information security practitioners must understand how to sect relevant controls and equipments from a diverse set of information security standards and guidance (Toby D.Sitk 2008).

Our views and documentations have provided an opportunity to review and reflect on broader infrastructure requirements to ensure system security. Security systems can operate at different levels, and every effort needs to be made to ensure that security issues never compromise. Policy integration and inter-operation is often a crucial requirement when parties with different access control policies need to participate in collaborative applications and coalitions. Such requirement is even more difficult to address for dynamic large-scale collaborations, in which the number of access control policies to analyze and compare can be quite large. Existing approaches to the problem of analyzing and comparing access control policies are very limited, in that they only deal with some special cases (Dan Lin et al., 2010).

In particular, for a system to be made operational under the best possible circumstances, the initial launch of a system must conform to strict quality assurance guidelines. These same guidelines will provide the basis for assessing the systems state at the time of change and can also be referenced to assess future performance. A deployment assurance procedure must be introduced to ensure optimal performance of operating systems. This will involve both initial testing as well as ongoing operational procedures.

In order to ensure a comprehensive information security policy, we have analysed the existing security system by using the following variables. They are Data conversion testing, User acceptance rating, Environment testing, Vulnerability Assessments, Assessment tools and the reporting patterns. The use of the above variables ensures an improved security for organizations. The results of the study are discussed in this work.

In many security systems, two principal security measures are deployed which consist of authentication and authorization. Authentication verifies who and where a user is. Authorization involves checking the privileges of an authenticated user. This distinction can be useful in a distributed system where applications may run at different locations. Users can be authenticated from a central login application so they do not have to re-enter a password for each application. Authorization can be performed on operations as needed for each application.

A significant way for reusing security code is to create a library of pluggable security components and a framework for incorporating these components into applications. However, the algorithm for putting together components will almost always be overridden, making the framework difficult to generalize. Another approach is to create configuration options that allow small parts of the algorithm to be turned on and off.

Authentication solutions for Virtual Organizations environments should have the following characteristics (Butler, R., et al.200).

○ *Single sign on*. Users must be able to "log on" (authenticate) just once and then have access to multiple Grid resources defined in the Fabric layer, without further user intervention.

○ *Delegation:* User delegation is a mechanism for assigning access rights available to one user to another user. A delegation can either be a grant or transfer operation. (Jason Crampton and Hemanth Khambhammettu, 2008). The identity delegation makes good use of trust relationships among users of a particular environment and offers the possibility of improved usability. Although identity delegation might violate the

principle of least privileges, in practice it could increase the overall security of a nomadic environment where users need to delegate their duties frequently (Naveed Ahmed, Christian D. Jensen 2009) according to (Foster, I., Kesselman, et al 1998, Gasser, M. and McDermott,1990, and Howell, J. and Kotz, D., 2000) A user must be able to endow a program with the ability to run on that user's behalf, so that the program is able to access the resources on which the user is authorized. The program should (optionally) also be able to conditionally delegate a subset of its rights to another program (sometimes referred to as restricted delegation).

○ *Integration with various local security solutions*: Each site or resource provider may employ any of a variety of local security solutions, including Kerberos and Unix security.
Grid security solutions must be able to interoperate with these various local solutions.
They cannot, realistically, require wholesale replacement of local security solutions but rather must allow mapping into the local environment.

○ *User-based trust relationships*: In order for a user to use resources from multiple providers together, the security system must not require each of the resource providers to cooperate or interact with each other in configuring the security environment. For example, if a user has the right to use sites A and B, the user should be able to use sites A and B together without requiring that A's and B's security administrators interact.

Grid security solutions should also provide flexible support for communication protection (e.g., control over the degree of protection, independent data unit protection for unreliable protocols, support for reliable transport protocols other than TCP) and enable stakeholder control over authorization decisions, including the ability to restrict the delegation of rights in various ways.

Globus Toolkit: For an effective security assessment the grid architecture plays an important role. The Internet protocols listed above are used for communication. The public-key based Grid Security Infrastructure (GSI) protocols are used for authentication, communication protection, and authorization. However, Dierks, T. and Allen, C. (1999) claimed that GSI builds on and extends the Transport Layer Security (TLS) protocols to address most of the issues listed above: in particular, delegation, integration with various local security solutions (including Kerberos and user-based trust relationships (Steiner, J., Neuman, B.C. and Schiller, J., Kerberos 1999).

3- Data conversion testing

In framing and implementing security layers, people often attach more significance to the technology rather than data. Data control and access have more value if they the process are properly and systematically planned.
While designing the security system, granting permission during the set up process to permit certain information access or to allow certain actions to be taken implies the need of temporal logic and control. The precedence relationships of various types of events will have to be used to establish temporally related control systems. An access may lead to a sequence of access activities. These chained activities will require the data security system to have propagation transaction controls.
Layered authentication of data offer more promises. The layered data authentication works by correlating the basic data in a problem environment with the basic data already stored in the database. The validity of this security is increased as the base data is compared empirically.
Information security can be viewed as the efficient control of uncertainty arising from malicious acts intended to exploit valuable assets and in the context of information systems the valuable assets under consideration are data. A large part of information security approaches is technical in nature with less consideration on people and organizational issues (Ioannis Koskosas, 2008). In many security control systems, the authentication and authorization process are controlled only technologically. However we advocate the deployment of data verification. This is possible by the following way.
The preliminary data for a secured information transaction is stored in the database which is available with the authentication request. The authentication request is first analyzed for security using formal mechanisms of security and then in order to ensure trust, the basic data is verified in the database. The database has inbuilt preliminary authentication questions for each record which are directed to the authenticated users who sought data. Correlation between the authenticated users-fed data and the basic data stored in the database is based on the concept interactive trust. The basic data observed from a base data set by authenticated users describe a variety of environments such as physical features, early fundamental data that get correlated in a problem situation and other conditions. Such a system ensures access to protected data from remote locations with security. The authenticated users are then granted access to the second level data.

4- Concept of broker server

The broker server is an additional security server that performs the data correlation between the any attempt for data access and the base data set. The broker server is

different from network server and data server. The broker server verifies the data access request at different layers. The broker server was initially suggested in (Chao-Hung Lin et al., 2007).

The broker server performs the following tasks.

a) Authenticate only designated requests and services
b) Adhere to all formal security variables
c) Monitor regularities in data access pattern

The role of the broker server is illustrated in the figure 1. The broker server acts as a controlling device that has a database of the users' description and the access data. It has the user control description where each user is permitted to enter into specific operation circles. Each user visits after authentication by the broker server, is correlated by it for *http* description, the extent of the use of permissible rights etc. If a specific user tries to exceed the right and when it happens with more threshold, the broker server monitors and control it. The broker can manage any number of users. The broker server is entrusted with the activities such as data access, data control and data validation.

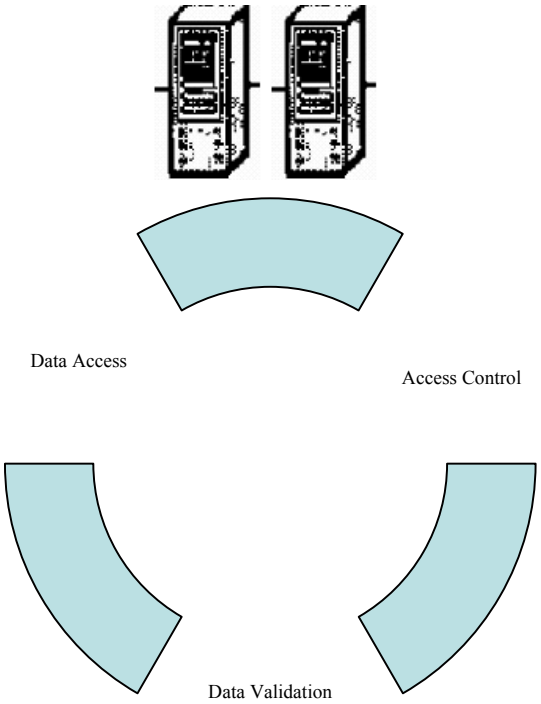

Figure 1: The role of a broker server

The broker server validates the request (including professional credentials check) and transmits the authentication to the data server. The data server then approves and delivers the digital certificate to the node. Once the formal security mechanisms validate the node user, the node user can enter the user ID and password to log into the data server. The data such as *http, ip, user id* and other similar description about the computer programs and the accounts of remote-monitoring users are stored in the database.

Our preliminary investigation results are encouraging. The proposed security design is validated first in a stimulated environment followed by the selection of a random trail. The random trial of 257 requests was routed through broker server with a mean frequency of 25 access attempts. The nodes used in the operations include remote location mobile and other related hand held devices. Out of the 25 nodes, 17 are designated and the remaining are intruders. Each of the nodes tries to enter into the data server including intruders. The security measures as well as broker validation are tested for the efficiency of the proposed design.

Over the evaluation period, 257 requests from the 25 nodes have applied for data access. In the first level, that is at the formal security measures, all the 17 valid users and two intruders were successful to get validated. The intruders' access is planned in an optimized way that they can break the security measures.

The 17 nodes were successful in each of the broker validation system. The 8 intruders requested for access by possessing false claims with the optimized authentication. It was found that two highly powerful intruders are able to break the firewall and encryption security.

5- Comparison

We compare the successful intruder attempts in both the systems, viz., A) firewalls and encryption and B) the above with the broker server validation. The access in these two systems consists of prioritized scores, which denote the rate of prevention. The attained scores indicate that there is a difference in the level of information security between the two systems, 'Broker data validation' and 'Normal security measures'.

From our earlier trials, the degree of the success of the two systems was calculated as the scores in this case reveal, the 'broker data validation' and the 'Normal security measures'. The broker data validation has scored more than the normal security measure in all attempts.

Thus the tractability of data access activities will have to be required for the establishment of authenticated access. The system must be able to maintain a trace of data access activities. The trace should be able to tell who generated and accessed what information and when in order to

determine individual user's legal and professional responsibilities. The results suggest that security measures are not confined to systems alone but data correlations offer much promise for developing a secured health care information system. (Pit Pichappan and Saleh Al-zharani, 2007).

6- User acceptance rating

A- User's role in information access and control

Information security functions and features must be developed within the domain of information delivery application. The delivery of validated information plays an important role in information access and control. The access of information can not just be based on the trustworthiness of the user but more on the user's need for information in order to perform the user's professional functions and duties.

Information security control must be developed as an integral part of the application. The semantics of security requirements must reflect data semantics germane to the data delivery application and relevant to the user's role. The data delivery system is considered effective and secure if it will provide the needed and timely information to all legitimate users for accomplishing their professional responsibilities and it will prevent all individuals from the unauthorized access of information.

B- Testing Environment Configuration

The ideal environment to assess the security basically is a safe configuration. However, it is also desirable to have all connecting components and functionality available in order to confidently assess full system interoperability. This includes everything from the Inter-Communication Protocol link to the Remote Terminal Unit connectivity. The ICCP is the international standard for real-time data communication between control centers. An Remote Terminal Unit connectivity is used in security systems at a remote location to collect code and transmit data back to the control station, as well as receive and implement commands from the control center. Ideally, these components are configured with actual signals for the assessment, although emulators and simulators may be necessary.

The ability to establish a typical security installation allows the assessment team to more accurately test and make recommendations on the configuration and deployment of a production system. Mirroring the connections to external systems is vital when replicating this configuration. The assessment team must know where and how a security system element typically connects to such things as the Internet, ICCP servers, and RTUs. Any of these elements being accessed from outside the security network, should be tested based on its position in the network. Firewall and intrusion detection system (IDS) configurations should be duplicated in order to test the effectiveness of the perimeter security they provide.

C- Vulnerability Assessments

Vulnerability is very essential in information security related mechanisms. The usage of this vulnerability is to identify the attacks over the cyber space system. This term becomes more popular as the challenges in cyber space system in large areas. In additional, Interdependencies between computer communication system and the physical infrastructure also become more complex as information technologies are further integrated into devices and networks. (S. Suma Christal Mary, 2010).

In many security breaches invaders penetrate the security rings, and thus the penetration testing is required as a part of the system. Penetration testing must be conducted from a machine that is not part of the network system unless otherwise defined in the assessment plan (i.e., an insider threat). This replicates a typical attack scenario where the attacker must penetrate the system from a remote computer. Placement of the attack computer depends on what is being tested and where the attack scenario originates.

Sophisticated attacks are often system specific and tailored to the target computer’s architecture. Therefore, the attacker needs a similar computer to create and test malicious code. For example, if 64-bit processors are used in the target security system, the assessment team may need equivalent hardware and software for developing exploits specific to that architecture. Although in a test environment there is direct access to the target system, its configuration should not be altered. A separate machine is needed to install required software such as compilers, debuggers, and other tools.

It may not be feasible to obtain test computers for each represented hardware or software configuration on the security system, but doing so would improve the assessment time and results.

Dedicated assessment equipment is also necessary for the assessment to be conducted without interruption. An attack machine with all the tools needed to perform the vulnerability assessment should be available for this work. In addition, a reliable Internet connection for research in the test area makes work more efficient.

D- Assessment Tools

Vulnerability assessment tools, in general, work by attempting to automate the first three steps often employed by hackers. The vulnerability assessment tools evaluate network attached devices (servers, desktops, switches, routers, etc.) for vulnerable or potentially vulnerable situations. Often the vulnerabilities that are

identified by these tools are programming flaws; however, some tools provide enough data that an analyst can uncover design, implementation, and configuration vulnerabilities (Yyan, Skousen 2009).
Deploying several assessment tools is the integral part of the security enforcement. Many open source and commercial tools are useful for assessing security systems. It is important to note that these scans and exploits are being run in a controlled lab environment. Any of these used on a production system could cause it to malfunction or stop operating. Legal restrictions on using scanning tools and exploits across a public network or your own computing systems vary.
Therefore, it is imperative to check with the assessment tools so that the infrastructure created would reinforce security measures.

E- Logs

System logs should be saved during testing because they can be used to indicate intrusions. Information gathered during testing can later be used for discovering these attacks on a production system.

F- Reporting

Detailed reporting of all tools used against the security system and the associated steps, findings, and system response is invaluable. This includes archiving the test tools and scripts used. Documenting this information as quickly as possible assures that no information is forgotten and saves time when trying to duplicate the attack. This information can then be used in the future for writing reports and validating which tests were conducted and whether the system was susceptible to them. Reports also provide a way to reproduce an attack when confirming that the hole was fixed in the next version of the software. The goal for this process should be to document to the level where someone skilled in the area could duplicate the results.

G- Metrics and Scoring

It is important to have a way to quantitatively measure the security of a system to determine its risk level, measure risk reduction due to security enhancements, and evaluate how it compares to other systems. Since there is no tool to perform these tasks, the best way to do it is to seek the opinion of cyber security experts. This is somewhat subjective, however. The Department of Homeland Security (DHS) is currently working on a risk-based decision methodology that can be used to calculate risks associated with potential terrorist acts that utilize control systems (George Beitel and Alessi, Sam, 2005).
Information Technology (IT)-based scoring systems do exist. Experience using these tools shows that it is important to decide on a scoring system before the assessment is performed. This ensures that the necessary data can be gathered for more meaningful scoring.

7- Conclusion

Methodologies for performing vulnerability assessments of SCADA systems are being developed through ongoing research, with the goal of improving the security of the nation's critical infrastructure. This experience can be leveraged to refine the assessment process and provide industry with better options to secure their section of the infrastructure.
Lessons learned in a laboratory environment can be taken advantage of in other environments as well. Those sites which operate with backup and test systems can perform vulnerability assessments on these systems. Many hacking tools and resources are available for sale or as free downloads off the Internet. These tools do require some computer skills and therefore should only be performed by a qualified IT/cyber security professional.

References

[1] Butler, R., Engert, D., Foster, I., Kesselman, C., Tuecke, S., Volmer, J. and Welch, V. Design and Deployment of a National-Scale Authentication Infrastructure, IEEE Computer, 33 (12) 60-66. 2000.
[2] Chao-Hung Lin , Shuenn-Tsong Young , Te-Son Kuo,. A remote data access architecture for home-monitoring health-care applications, Medical Engineering & Physics. 29, pp 199–204,2007.
[3] Dan Lin, Prathima Rao, Elisa Bertino, Ninghui Li and Jorge Lobo. Acomprehensive environment for the analysis of access control policies. International Journal of Information Security .Volume 9, No 4, 253-273, 2010
[4] Dierks, T. and Allen, C. The TLS Protocol Version 1.0, IETF, RFC 2246, 1999, http://www.ietf.org/rfc/rfc2246.txt.
[5] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S. A Security Architecture for Computational Grids. In: ACM Conference on Computers and Security, 83-91, 1998.
[6] Ganthan Narayana Samy, Rabiah Ahmad, Zuraini Ismail, Threats to Health Information Security. Fifth International Conference on Information Assurance and Security , vol. 2, pp.540-543, 2009.
[7] Gasser, M. and McDermott, E., An Architecture for Practical Delegation in a Distributed System. In: Proc. 1990 IEEE Symposium on Research in Security and Privacy, IEEE Press, 20-30, 1990.
[8] George Beitel and Alessi, Sam, Control Systems Risk Decision Methodology, INL/EXT-05-02585, Rev. 1, US Department of Homeland Security, Idaho Falls, Idaho, March, 2005.
[9] Howell, J. and Kotz, D., End-to-End Authorization. In: Proc. 2000 Symposium on Operating Systems Design and Implementation, USENIX Association,2000.
[10] Huaqiang Wei, Jim Alves-Foss, Terrence Soule, Hugh Pforsich, Du Zhang, Deborah Frincke. A Layered Decision

Model for cost-effective system security. International Journal of Information and Computer Security 2008 - Vol. 2, No.3 pp. 297 - 324, 2008.
[11] Ioannis Koskosas. Goal Setting and Trust in a Security Management Context . Information Security Journal: A Global Perspective, Volume 17, Issue 3,pp 151 – 161, 2008.
[12] Jason Crampton and Hemanth Khambhammettu. Delegation in role-based access control International Journal of Information Security. International Journal of Information Security. Volume 7, No 2, 123-136, April 2008
[13] Nicolas Sklavosa, On the Hardware Implementation Cost of Crypto-Processors Architectures . Information Security Journal: A Global Perspective, Volume 19, Issue 2, pp. 53–60, 2010.
[14] Pit Pichappan and Saleh Al-zharani, Interactive Trust Negotiation-based security of EHR access in health information system, Journal of Information Assurance and Security, Vol. 2, No. 1, 2007.
[15] S. Suma Christal Mary. Evaluation of vulnerability assessment form hackers in cyber security. International Journal of Engineering Science and Technology, Vol. 2, No 7, pp 3213-3217, 2010.
[16] Sanjay Rawat, Ashutosh Saxena .Application security code analysis: a step towards software assurance. International Journal of Information and Computer Security . Vol. 3, No.1, pp. 86 - 110, 2009.
[17] Steiner, J., Neuman, and Schiller, J., Kerberos: An Authentication System for Open Network Systems. Proceedings of the Usenix Conference, 191-202, 1990.
[18] Toby D.Sitko. Information Security Governance: Standardizing the practice of Information Security. Education Center for Applied Research. Georgia State University. Vol. 2, No. 17. August 19, 2009.
[19] Yyan, Skousen .Information Assurance Tool Report-Vulnerability Analysis. Fifth education, The Information Assurance Technology Analysis Center. Sponsored by the Department of Defense. September 25, 2009.