Security in In-House Developed Information Systems: The Case of Tanzania

Magreth MUSHI
Institute of Educational Technology, The Open University of Tanzania (OUT),
Dar es Salaam, Tanzania
And

Jabiri BAKARI
Institute of Educational Technology, The Open University of Tanzania (OUT),
Dar es Salaam, Tanzania

ABSTRACT

In this 21st century**,** the world is moving more and more into the information economy; and information held by organization's information systems is among the most valuable assets in the organization's care and is considered a critical resource, enabling the organizations to achieve their strategic objectives. In-house developed information systems meant to enable organizations to achieve their strategic objectives, are on the increase and security has become a major concern in recent years. Hackers are using new techniques to gain access to sensitive data, disable information systems and administer other malicious activities aimed at the information systems. The need to secure an information system is imperative for use in today's world. Until recently, information systems security was an afterthought; developers were typically focused on functionality and features, waiting to implement security at the end of development. This approach to information systems security has proven to be disastrous because vulnerabilities have gone undetected allowing information systems to be attacked and damaged. A survey done in three (3) organizations in Tanzania has proved that most of the information systems developers have drawn their background from traditional systems development without the sense of implementing security in the early stage of information system development. This paper attempts to identify in-house developed information system's security deficiencies and related risks to organizations, the paper also attempt to establish technique that can be used to detect those deficiencies. Lastly the paper provide guidance that can be used by organizations to mitigate the risks.

Keywords: In-house, information system, Security, Source code scanner

1. INTRODUCTION

In-house developed information systems security has become a major concern in recent years. Hackers are using new techniques to gain access to sensitive data, disable information systems and administer other malicious activities aimed at the information systems. Until recently, information systems security was an afterthought; developers were typically focused on functionality and features, waiting to implement security at the end of development. This approach to information systems security has proven to be disastrous because vulnerabilities have gone undetected allowing information systems to be attacked and damaged; therefore, the need to secure in-house developed information systems is imperative for use in today's world.

A study done by Mushi [8] in Tanzania clearly shows that, developers are not effective in ensuring security is implemented in in-house developed information systems, and at the same time most IT professionals (84.5%) employed in organizations in Tanzania have no background in information systems development or information systems security, therefore appeared to be insufficient to ensure that the information systems developed and installed in their organizations are secure.

In making effective planning and good decisions, organizations rely not only on accurate, timely, relevant and easily accessible information, but also on information that is presented in a meaningful way. According to Sadowsky [11] information is now being regarded as a fourth factor of production and therefore an input resource in any production process besides raw materials, capital and labor. The above views logically lead to the following conclusions:

i. Information is a resource,
ii. Any resource has value, and
iii. Any valuable thing must be protected.

Factors Contributing to Poor Performance in Securing In-house Developed Information Systems

Swanson et al [12] pointed out examples of causation factors, contributing to poor control implementation and effectiveness in in-house developed information systems security. The factors are also adopted here:

- ***Resources:*** Insufficient human, monetary, or other resources. Unfortunately, many organizations will find that they do not have sufficiently skilled resources available internally to cope with information systems security. As a result of lack of skilled and well-trained personnel, organizations are forced to hire expatriate staffs, who in turn lack knowledge about local organization's cultures and thus they design and deploy poor systems.
- ***Training:*** Lack of appropriate training for the personnel installing, administering, maintaining, or using the

information systems. This is also another hindrance which resulted into inability by managements to properly evaluate the cost versus benefits for implementing protection measures.

- ***Policies and Procedures:*** Lack of policies and procedures that are required to ensure existence, use, and audit of required security functions. Jan [6] attributed the problem as due to lack of well formulated and implementable information systems security policies binding both employees as part of conditions of employment and the management as a whole in an organization. Employees are expected to act in a manner that will ensure the information which they are authorized to access, is protected from unauthorized access, unauthorized use, invalid changes or destruction.
- ***User Involvement:*** The need to involve users at all levels during the designing and implementations of in-house developed information systems. It is not proper the way many organizations hire experts to handle systems implementation without the necessary involvement of the users (employees and the management). Without necessary users' involvement, hired experts end up developing information systems based on what the experts believe their customers need rather than what they actually need. The resulting designs become 'Solutions looking for problems'.

Challenges of Protecting In-house Developed Information Systems

Hackers tend to go where the targets are the most attractive, and the defenses are the weakest; therefore, it shouldn't be surprising that organization in-house developed information systems are increasingly coming under attacks.

Most large organizations have already installed antivirus applications, firewalls and even Intrusion Detection Systems (IDSs) to protect their networks and host operating systems. But by comparison, in-house developed information systems have received relatively little attention, on the assumption that they are protected by firewalls and other defenses at the network perimeter. Yet these information systems are the major reason organizations invest in IT in the first place, and the data they contain are often the organization's most valuable assets.

Though a critical component of a layered defense, firewalls cannot detect and stop the new class of threats now being directed at in-house developed information systems. Another widely deployed tool, intrusion detection systems, performs only passive monitoring and after-the-fact forensics rather than preventing attacks. Attacks have moved to the information systems, circumventing network-based firewalls; worms propagate so quickly that signature-based antivirus protection is useless; intrusion detection systems do not provide protection, only faster notification that your security has failed.

Under the above assumption, organization's in-house developed information systems are often developed and used without a focus on securing them. This happens for several reasons:

- ***Ignorance:*** Both designers and the users do not know about the need for security;
- ***Low priority:*** Until now, security issues do not have the visibility that they deserve, as a result, even people who knew about security issues chose to ignore them;
- ***Time and expense:*** Some people think that it is more expensive and time consuming to implement and test for security issues during the information system development process and lifetime;
- ***Sloppiness:*** In some programming efforts, the same mistakes are made repeatedly, some of these mistakes make security breaches possible.

Organizations need to bring the same level of protection to in-house developed information systems as they apply to servers and networks, with solution that is permanent and can detect and respond to information systems threats in real time, and that are granular enough to provide access for customers and business partners while keeping attackers out.

2. OBJECTIVES

The main objectives of this paper are:

- To identify in-house developed information system's security deficiencies.
- To establish in-house developed information systems related risks to organizations.
- To establish technique that can be used to detect the in-house developed information systems security deficiencies.
- Provide recommendations on how to reduce the risks.

3. METHODOLOGY

The study done by Mushi [8] was divided into two main phases, namely: initial investigations, which is a fact-finding stage and development of an in-house developed information systems security analyzer. Initially raw data was collected from the fields using both open ended and closed ended questionnaires and interviews.

Secondary data was collected from published studies in order to compare the effect and size of In-house developed information systems users in implementing in-house developed information systems security. Data about installation, running and maintenance of in-house developed information systems were also collected mainly from systems administrators, analysts, developers, and general and senior members of the management of the randomly selected three organizations. A Sample of 45 respondents was drawn from three (3) organizations. Java compiler for compiling source codes was used and a database which will hold options for the system to choose from, was developed.

Data Analysis

Quantitative research approach was used to describe the relationship between the variables, where data from the field was analyzed using SPSS 13.0 and sample in-house developed information systems for testing the analyzer.

4. SECURITY ISSUES IN IN-HOUSE DEVELOPED INFORMATION SYSTEMS

According to Ollmann [9], most initial attacks against systems were likely to focus upon the systems infrastructure and commercial information systems, as there is where most of the exploit material and methodologies were likely to work. Due to this fact, attackers have changed their target and moved to in-house developed information systems. Depending upon the skills or resources, if your systems are well secured and up-to-date with the latest bug-fixes or patches, the attacker may either resort to social engineering (Why try to crack a password when you can just call the helpdesk and have it reset?) or focus upon the manipulation of the vulnerabilities inherent in the information systems, or sub-components.

Although in-house developed information systems can be vulnerable to a number of attack methodologies, the following are most prevalent as adopted from OWASP [10]:

Input is not validated before use: Information entered by the user to the web information system is not validated before being used by the in-house developed web information system. Attackers can use these flaws to attack backend components through a web information system by entering codes which will allow them access through the input box.

Access Control: Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.

Management of Identification and Authentication: Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.

Cross Site Scripting: The web information system can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

Buffer Overflow: Information systems components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web information systemserver components. This is compared to pouring 1000mls of water into 500mls jar, for sure the remaining 500mls will spill out and cause a mess.

Injection Flaws: This happens when information systems pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the information system.

Poor Error Handling: Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the information system does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

Insecure Storage: In-house developed web information systems frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.

Information system Denial of Service: Attackers can consume information system resources to a point where other legitimate users can no longer access or use the system. Attackers can also lock users out of their accounts or even cause the entire information system to fail.

Insecure Configuration Management: Having a strong server configuration standard is critical to a secure information system. These servers have many configuration options that affect security and are not secure out of the box.

5. ADDRESSING IN-HOUSE DEVELOPED INFORMATION SYSTEMS SECURITY ISSUES

In order to ensure that organizations achieve their targets, there must be a cost-effective means of ensuring that the in-house developed information systems installed in the organization's computers are secure enough to provide accurate and reliable information. This can be achieved by integrating source code scanners in the early stages of information systems development life cycle.

Coding is tough enough, and coding right can sometimes seem an almost impossible task. Between design constraints, deadlines and making it work in the first place, it's difficult to get your code secure. Security concerns, however, can be helped by scanners.

For sure we know that, source code scanners aren't a replacement for manual checks and edits, but tools like MegApplicationScanner, Flawfinder, RATS and ITS4 can point you to the right direction. Source code scanners are nothing new. Tools like **lint** have been around for many, many years to help you find errors in your C code.

Source code audits are also great things, things like the Linux Auditing Project. However, audits can take a lot of time and money if one outsources them, though the payback is well worth the investment.

Typically, the scanners are designed to be run over the source code several times during development, each time fixing or investigating the major problems. When coding, it's easy, initially, to forget to use a more secure function like strncpy(), and these tools help reinforce improved habits. When examining outside sources of code, scanners help highlight areas of code that may be problematic. In either case, these scanners help show you where to focus your attentions, and they cover many of the basic, common coding errors that lead to faulty code or, worse, security issues.

All of these tools are quite fast, operating on about 100,000 lines of input in less than one second. Simply put, you'll spend more time trying to figure out the meaning of the output than you will, running the checker itself.

6. IN-HOUSE DEVELOPED INFORMATION SYSTEMS SECURITY ANALYZER

The use of in-house developed information system security analyzer will provide a technical and non-technical security review of in-house developed information systems to determine security weaknesses, and provide detailed recommendations for remediating any vulnerability discovered. This will enable organizations to have reliable information, prevent information systems downtime, and therefore improve productivity which according to Transport Research Board (TRB) Committee A5001 (1994) can be measured in terms of:

- *Reduced cost of organizations research, technology development and operations:* Reducing cost is one of the primary goals of a quality and well accessible information and data.
- *Quicker implementations of innovations and time savings:* Quality information saves time in numerous ways, by avoiding duplicative efforts, stopping

unproductive activities, modifying designs approaches, or correcting bad information.

- *More effective decision-makings at all level of the organization:* In today's competitive markets, knowing what others are doing in the business or how they are confronting similar challenges is very important in order to equip the management with adequate knowledge necessary for appropriate course of action to be taken.
- *Increased customer satisfaction:* Although many organizations cannot quantify the value of information or information services, the perceived value among users is high. Users discuss the value in terms of whether, and to what extent the data and information provided meets their expectations and needs.

7. CONCLUSION

From the analysis and discussions of the findings of the study done in three (3) organizations in Tanzania, the following conclusions were derived:

- It is clear that, currently, in-house information systems developers are not effective in ensuring information systems security; and therefore in-house developed information systems are the number one sources of information system flaws as described above.
- Professionals employed in organizations do not have background in information systems security and enough experience to ensure that the information systems developed and installed in their systems are secure. This can be one of the contributing factors, as they lack ICT security knowledge and the consequences to business.
- Management has no idea of the connection between possible risks posed by such systems and how such risks can affect organizations in achieving their strategic objectives.

Static analysis for software defect detection has become a popular topic, and there are a number of commercial, open source and research tools that perform this analysis. Unfortunately, there is little public information about existence and the experimental evaluation of these tools with regards to the accuracy and seriousness of the warnings they report. Commercial tools are very expensive and generally come with license agreements that forbid the publication of any experimental or evaluative data.

Introducing security requirements, testing, and remediation at the earliest possible points in the development lifecycle to ensure the best possible quality at the lowest possible cost is inevitable. It is required to identify and bridge the gap that currently exists between software developers and security professionals by offering specific organizational approaches and process improvements to embed security into the information systems development lifecycle. Organizations should implement source code security scanning tools as part of the software development life cycle to find and fix the highest number of security issues early in the project. This will result in a higher-quality product and lower overall information system life cycle costs.

Source code scanners specifically designed to look for security flaws are obviously of help. However, there are two major limitations which need to be addressed in the future. Firstly, Scanners are limited in the programming languages they understand. This definitely limits their utility. Secondly, most scanners are available for commercial application only, prohibiting their use by many Linux developers and researchers, who didn't always place user friendliness high on their lists of goals.

8. REFERENCES

1. Bakari, J.K. and Mboma, L. (2001) *The current status of ICT at the University of Dar es Salaam*. Status report, Directorate of Planning and Development (DPD), University of Dar es Salaam.
2. Caelli, W. Longley, D & Michael Shain, M. (1991) *Information Security Handbook.* Macmillan Publisher Ltd.
3. Chacha , M. K. L. (2000) *The Impact of Information Technology on Internal Auditing in Tanzania Organizations*. Masters of Business Administration thesis. University of Dar es Salaam.
4. Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in Computing*, **Publisher:** Prentice Hall, Hardcover, 3rd edition, Published 2002, **ISBN** 0130355488
5. Christopher Alberts, Audrey Dorofee, *Managing Information Security Risks: The OCTAVE (SM) Approach*, **Publisher:** Addison-Wesley, Published 2002, ISBN 0321118863
6. Jan, C.A. van der Lubbe, "*Information Security and Privacy in Practice"*, Delft University of Technology press, August 2005.
7. Matt Bishop, *Computer Security: Art and Science*, **Publisher:** Addison-Wesley, Hardcover, Published 2002, **ISBN** 0201440997
8. Mushi M.J, *Development of In-house Applications Security Analyzer (IASA)*, Masters Thesis, Department of Computer Science, University of Dar es Salaam, Tanzania **Publisher**: Dar es Salaam University Press, Published Jan 2008.
9. Ollmann G, 2005, "*Advice on Assessing your custom Application*", http://www.technicalinfo.net/papers/index.html , Date accessed: 4th March 2010.
10. OWASP Top Ten project: *List of Top Ten Application Security Flaws in 2004.* http://www.owasp.org/index.php/Top_10_2004. Date Accessed 5th March 2010.
11. Sadowsky, G., James, X. Dempsey, A.G, Barbara, J. M., Schwartz, A., *"Information Technology Security Handbook",* ISBN 0-9747888-0-5, Office of the publisher-World Bank, 2003.

12. Swanson M, Bartol N, Sabato J, Hash J, and Graffo L, 2003, "*Security Metrics Guide for Information Technology Systems*" http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf, Date accessed: 26th Feb 2010.