Nigerian Journal of Technology (NIJOTECH)
Vol. 34 No. 4, October 2015, pp. **788 – 792**

University of Nigeria, Nsukka, ISSN: 0331-8443
www.nijotech.com
http://dx.doi.org/10.4314/njt.v34i4.17

SYSTEM HARDENING ARCHITECTURE FOR SAFER ACCESS TO CRITICAL BUSINESS DATA

A. E. Ibor[1, *] and J. N. Obidinnu[2]
[1, 2] DEPT OF COMPUTER SCIENCE, CROSS RIVER UNIVERSITY OF TECHNOLOGY, CALABAR, CROSS RIVER STATE. NIGERIA
Email addresses: [1]*ayei.ibor@gmail.com,* [2]*obijulius@yahoo.com*

ABSTRACT
This paper affirms that the total cost of cybercrime to society is significant, and the threat is growing faster than the potential victims can deal with. One of the factors fueling this rapid growth is the confining of the security of a system to a specific security function. The paper therefore, presents a system hardening architecture to guide system administrators towards implementing multi-layers of in-depth protective mechanisms around stored data. System hardening is a defence strategy, where several different security measures are applied at various layers, all of which must be defeated before a module can be compromised. The protective mechanisms in this architecture are applied to the host, application, operating system, user, and the physical layers. This architecture is proposed on the premise that organisations implementing system hardening security approaches experience safer access to data, as well as decrease in the number of security breaches.

Keywords*: System Hardening, Security, Cybercrime, Cyber attack, defence in-depth strategy.*

1. INTRODUCTION
Cybercrimes or cyber-attacks represent a range of criminal activities conducted using computers, with or without the Internet. A person who perpetrates cybercrime is a cybercriminal. Cybercriminals go after information assets that are of value to individuals, governments or business organisations. The objective of any cyber-attack is either to steal information from a computer system or to inject malicious code into it, aimed at causing harm to the entity.

Some specific examples of what cybercriminals seek include: disrupting a country's critical national infrastructure (nation-state-sponsored terrorism and attacks), confiscating online bank accounts (credit/debit card data), creating and distributing viruses on other computers (leading to Denial of Service (DoS)), stealing an organisation's intellectual property, and posting confidential business information on the Internet. These could eventually drive an organisation out of business.

Over the years, the numbers of cyber-attacks and associated losses have continued to grow [1], [2]. Furthermore, [3] asserts that the growth of the threat of cybercrime is growing faster than the potential victims can deal with, thereby imposing considerable risks on the targets. In the same vein, [4] affirms the foregoing, that the total cost of cybercrime to society is significant.

However, [5] indicates that the root causes of the breaches in information security emanate largely from the weaknesses in information systems. More so, [6] refers to security weaknesses in information systems as vulnerability. Vulnerability is a fault in a system, which a cybercriminal discovers and exploits. In other words, there cannot be a cyber-attack without the presence of vulnerability. Vulnerability can exist in operating systems, network devices, firewalls, encryptions, password protections, embedded systems, and any software driven products.

In a related study, [7] recommends countermeasures such as adopting defence in-depth strategies, where several different security measures are applied at various layers, all of which must be defeated before a module can be compromised. Sharma et al. in [8] refer to this strategy as system hardening, which [9] defines as a multi-layered system of defence to enhance the security of an information system. The results of the study in [5] indicate that, organisations implementing system hardening security approaches experience safer access to stored data, and therefore, decrease in the number of security breaches.

This success indication in [5] therefore, drives this paper to introduce a system hardening architecture for creating additional layers of security around stored data. The model comprises of in-depth protective mechanisms built into the host, application, operating system, user, and the physical layers. This architecture is developed on the premise that, the more time and resources an attacker expends on a system without success, the more discouraged (s)he becomes in continuing with the process, as opined in [6].

It is then our position that, security issues remain a continuous war situation between attackers (cybercriminals) and the defenders (owners). While an attacker needs to find only one vulnerable opening to perpetrate an act, a defender needs to proactively find and fix all openings, or react after an exploit, thereby suffering maximum damage there from. Since the security of a system cannot be localised to a specific place, the defender should be guided towards implementing more comprehensive security architecture. This is the objective of this paper.

***Corresponding author, Tel: +234-815-421-3807**

2. LITERATURE REVIEW

Several threats exist against critical data in business. Threats to data security have been on the increase and several efforts have been made by the computing community to proffer solutions to these security risks. For instance, data processed through e-business and e-services have been identified to be at the risk of compromise due to the ubiquitous nature of computer networks. As described in [10], e-business and e-commerce have tremendously imparted on corporate services, including the sharing of information. When information is shared, especially through unsecure channels, there is the likelihood of security breaches that have the capacity to intercept, modify or steal sensitive data meant for business decisions and the protection of proprietary information. As a consequence, many organisations suffer a lot of losses in data and revenue including business intelligence and intermediate data for control of business.

Security breaches are happening because, in recent times, ease of use has been more popular than hardened security measures for various devices [7]. In this context, default security configurations for computer systems and other computing devices are usually not enough to allow for the secure storage of critical data. System hardening is undertaken to build systems that can withstand adverse computing conditions such as errors, attacks and compromise [11]. To make this possible, system hardening involves the secure configuration of a computer system or network in order to reduce the likelihood of exposure to security risks [12]. Security risks trigger vulnerabilities, which usually come along with a plethora of computer products owing to the default settings available on these devices.

Conventional methods of storing data include: the dumping of data on a storage medium (hard drive, tape drive, etc.) and putting the storage medium under lock and key. In another perspective, passwords or some other form of authentication such as pass codes and personal identification numbers (PINs), used during operating system logins, are adopted without an added security layer to harden the process of accessing stored data. These have continued to prove to be inadequate.

3. METHODOLOGY

We develop a system hardening architecture, which integrates several security functions into a module. These functions are applied independently and separately, but are expected to be providing their own level and method of protection at their own location in the system. Consequently, if an attacker breaks the first wall of protection, (s)he is bound to encounter another level of protection without having access to the stored data yet. Breaking the second wall introduces the third barrier, and so on.

The higher the number of protective mechanisms applied to stored data, the more difficult it will be for the potential intruder to succeed. This position derives from [6], who insists that hardening an information system will make attackers spend more time and resources trying to conduct their malicious act. Spending more time and resources could evoke the fear of being noticed, and be discouraged from attacking such a system. The attacker might just decide to look for easier targets for the feeling of success.

The system hardening security functions are grouped into two categories: (i) software oriented, and (ii) physical level. The software oriented functions are applied to the various software making up the system, while the physical level comprises of the physical barrier systems, such as perimeter fencing, etc.

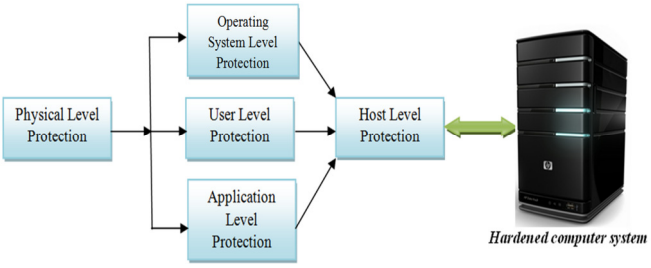

Figure 1: System hardening architecture for safer access to critical business data

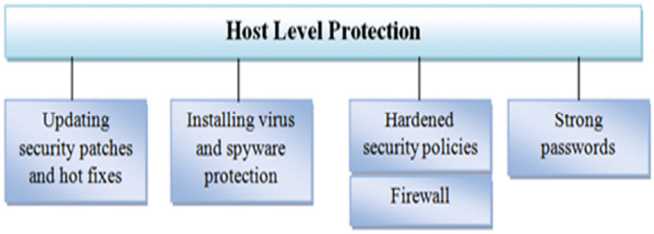

Figure 2: Host level protection for systems hardening

3.1 Software Oriented Hardening Functions

The software oriented hardening functions are defined at different layers to deliver robust defence-in-depth protections. The layers include:

i) Host level protection
ii) Application level protection
iii) Operating system level protection
iv) User level protection and

The architecture integrating these layers, including the physical security layer is presented in Figures 1.The layers depicted in Figure 1 are discussed in the following sections.

3.1.1 Host Level Protection

As shown in Figure 2, a typical computer system requires a series of protective measures to keep its data and programs safe. Host level protection entails the following activities:

i) Updating security patches and hot fixes: most software vendors provide security patches and hot fixes for their applications. It is important to regularly update applications using the patches and hot fixes available in order to close security holes (flaws) that can allow an attacker to have unauthorised access to critical data in a particular host. Applying security patches and hot fixes also comes with the constant monitoring of security bulletins applicable to a host's operating system and applications. As shown in [13], the Computer Emergency Response Team (CERT) of the United States of America periodically publishes security

bulletins and advisories with details of available security patches for most operating systems and applications. Nordlanderin [12] opines that the use of software patches and hot fixes should be able to address appropriate security issues, and as such only tested patches, which are not likely to degrade performance and reliability should be used.

ii) Installing virus and spyware protection: anti-virus and spyware protection programs are useful for protecting a host system from viruses and spyware. Viruses are known for attaching themselves to files, programs and the boot sectors of disk drives in order to replicate [14].When viruses are allowed to replicate, they usually have harmful effect on infected hosts, which can lead to data theft, distortion, corruption and loss. The effect of such malicious activities can destroy the contents and integrity of business data. Similarly, [15] asserts that spyware has harmful effect on a host system and network. Spyware is software that allows for the unauthorised stealing and transmission of sensitive data including the ability to have control over a host without the user's consent. Protection against spyware can be achieved with anti-spyware programs such as PC Tools Spyware Doctor and Spybot – Search and Destroy.

iii) Using hardened security policies: security policies define the constraints that should be imposed on a host's functions and data use as well as processes within the system. Such constraints allow for the secured use of the data and processes in the system while enhancing integrity and confidentiality. Policies such as password policies for local users of a system should be hardened through periodic changes including the duration of use and format. As discussed in [12], security policies should be strict and their implementation flexible enough to allow for their refinement with time.

iv) Using a firewall: a firewall is useful for controlling the packets (network traffic) that arrives or departs a network to which a host is connected. Firewalls are network security appliances that help to create barriers between secure and insecure network channels. Usually, packets that arrive at a firewall from an external source are filtered based on applicable access control lists, which determine how the packets are treated on arrival. Similarly, outgoing packets are filtered according to outbound rules. Nordlanderin [12] proposed the use of a smart firewall design that deploys a Virtual Private Network (VPN) to help segment a network in such a way that allows for the elimination of threats to network and computer resources. Sharma et al. in [8] recommend the use of firewalls with strong filters as an effective way to harden a computer system and reduce the likelihood of threats to resources including data.

v) Using strong passwords: passwords are commonly used to secure authentication interfaces and protect data from unauthorised access and modification. However, most users make use of default or weak passwords such as using their date of births, surnames, pet names, and the like. A good password usage practice provides that there should be a good combination of alphanumeric characters including special characters to create a password. A password should also be of reasonable length, simple to recall by the owner but difficult to guess by an adversary. The use of strong passwords should also include password aging policies that allow a password to expire over time. Users should be made to change their passwords regularly in order not to create an avenue where intercepted passwords can be used against protected systems and networks.

3.1.2 Application Level Protection

Application security is vital to the security of the data accessed by such applications. When applications that use data are vulnerable; there is the propensity for the data processed by such programs to be exposed to intrusive activities. Some of the activities that can allow for application level protection, as depicted in Figure 3 include:

i) Disabling file sharing: file sharing allows different users and programs to have access to data and/or programs including multimedia (audio, images and video) held on storage devices especially the hard disk and databases. As highlighted in [8], disabling file sharing limits the access level of users and applications, and can help to reduce security risks and threats to critical data such as the spread of viruses and spyware, unauthorised access and modification of data, data theft and loss.

ii) Disabling cookies: cookies are used to store browser entries containing information about the activities of a user or application on the web. Information stored by cookies includes usernames and passwords, credit card details, and addresses. When cookies are not disabled, these data can be accessed by a malicious user, who can in turn use the information to gain access to critical data and perform various degrees of harmful actions. Data used by applications can be affected, leading to erroneous results in computations and reporting of transactions. Assuming a hacker is able to access the authentication details of a credit officer through a cookie, then, it is possible to modify account balances so that the banking applications that rely on the data processed through daily transactions will report unreliable results that may affect the integrity of the credit officer as well as the bank's reputation. Loss of confidence is likely on the part of the customers, who may also decide to shift their accounts to other competitors.

iii) Application security testing: the security of applications through design, development, deployment and maintenance should be hardened in order to ensure that applications behave normally in the face of malicious attacks. In [16], a risk-based approach to software security testing is proposed. The core elements of this approach are meant to enable the testing professionals to proffer solutions to security issues arising from software development

and deployment. Stytz and Whittaker in [17] assessed security testing as a measure of requirements verification for application behaviour and usage while detecting and managing security risks.

Figure 3. Application Level Protection for Systems Hardening

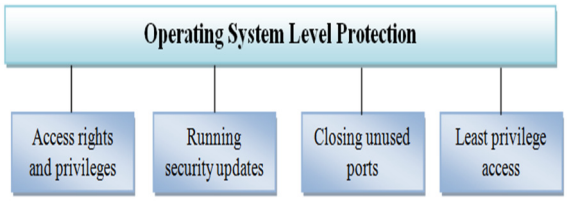

Figure 4. Operating System Level Protection for Systems Hardening

3.1.3 Operating System Level Protection

The activities and processes of every computer system are controlled and monitored through an operating system. For an operating system to adequately supervise other programs and hardware, a number of security measures must be applied to it. One of such measures is the application of patches and updates when available.

Though many computer users and professionals tend to trivialise the importance of security updates in an operating system, [12] asserts that when an operating system is not hardened, it is likely to exploit services and vulnerabilities in it that can allow an attacker to gain access to applications and services running on that operating system. He states that more harmful effects to an un-patched operating system include viruses and Trojans as well as other malicious code that can cause the operating system to malfunction including system crashes.

Running security updates can as well indicate the protection of services, applications, and processes running on a computer system viz-a-viz a network. Most operating systems allow for options on manual and automatic updates. It is advisable to set updates to automatic in order to allow your operating system to check for updates and apply them whenever necessary.

Another hardening strategy for an operating system is the closing of unused ports. Ports allow for local and external connections to services, applications and processes. Closing unused ports limits the ability of an intruder to exploit such ports for malicious intent [8]. Other hardening strategies include the least privilege access, in which the user is allowed access to the functions sufficient for his/her daily job roles. Generally, as shown in Figure 4, access rights and privileges must be well defined in order to control access to programs and data.

3.1.4 User Level Protection

At the user level (Figure 5), users' data and account information should be protected from unauthorised access and modification. User level protection can include the encryption of data (transmitted and stored) and the uninstalling of unused programs and user accounts.

i) Data encryption: encrypting stored and transmitted contents controls the way data can be intercepted and manipulated. Encryption only gives access to the data owner who has the secret key to decrypt the encrypted contents. In encrypting data, however, fast encryption algorithms should be used. According to [8] and [12], encryption is useful for providing an added layer of security over data, file systems, applications and network connections. Some common encryption algorithms such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES), which deploy symmetric key encryption, that is, the same key is used for encrypting and decrypting data, can be used. Intercepting an encrypted message or data creates more difficulty to the attacker, who must have to decipher the encryption key in order to decode the original message or data. This is computationally expensive, and sometimes infeasible in real time. Creating cryptographic hashes of data also creates a level of security for the data and its users. A cryptographic hash enhances message integrity and is useful for determining the extent to which data has been modified or changed. Capturing the hash of stored or transmitted data is achieved through hash functions such as Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1 and SHA-256) [18]. A change in a single bit of the original data can be detected by comparing the hash of the original data and its image. This enforces integrity on the originally stored and transmitted data.

ii) Uninstalling unused programs and user accounts: unused programs and user accounts are usually targets for exploitation by hackers. It is advisable to uninstall all unused programs and user accounts such as anonymous and guest accounts with default passwords. This is to ensure that only users with valid and strong authentication credentials are granted access to data and other resources.

iii) Creating regular backup of data: there is need to regularly backup critical data in the event of a system failure or crash, natural disaster, data distortion and loss, and unauthorised access and modification of stored contents.

3.2 PHYSICAL LEVEL HARDENING FUNCTIONS

Figure 6 indicates the physical level hardening functions, which include (i) Use of locks and keys (ii) Access control barriers/doors (iii) Use of closed circuit cameras (CCTV) (iv)Incident alarms (v) Physical barriers and fencing (vi) Restricted access technology (vii) Perimeter intrusion detection.

The physical level hardening functions are defined in the physical level protection layer. The architecture for the physical level follows the same pattern as presented in Figure 1, except that the functions making up this layer

are different. These functions are all relevant in enhancing physical security [19].

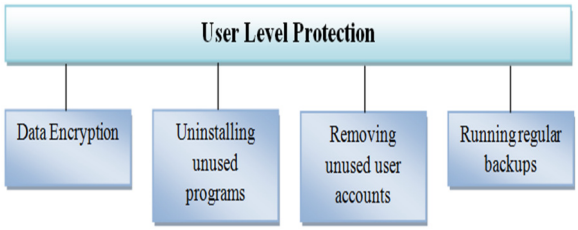

Figure 5. User Level Protection for Systems Hardening

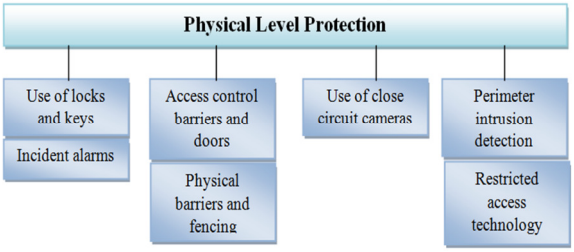

Figure 6. Physical Level Protection for Systems Hardening

4. CONCLUSION

Security issues remain a continuous war situation between attackers (cybercriminals) and the defenders (owners). In this situation, the defender needs to proactively find and fix all vulnerable openings; otherwise a cybercriminal could discover only one of the unfixed openings and exploit it, thereby inflicting maximum damage there from.

There cannot be a cyber-attack without the presence of vulnerability. Vulnerability is a fault in a system, which a cybercriminal discovers and exploits. A vulnerable system is a system having vulnerability. Vulnerable systems and networks pose great danger to the security of an organisation's data, including the ability of intruders to steal data and circumvent security measures to suit their malicious intents.

The threat of cybercrime is growing faster than the potential victims can deal with, thereby imposing considerable risks on the targets, and the total cost of cybercrime to society is also significant. However, one of the factors fueling this rapid growth is the confining of the security of a system to a specific security function.

To this effect, organisations implementing system hardening security approaches experience decrease in the number of security breaches. System hardening is a defence in-depth strategy, where several different security measures are applied at various layers, all of which must be defeated before a module can be compromised. The more time and resources an attacker expends on a system without success, the more discouraged (s)he becomes in continuing with the process. It is common knowledge that not many computer users, including most professionals, pay much attention to basic computer security principles, which are able to prevent security breaches on critical data. This paper has therefore highlighted some of these measures, most of which do not require extra overhead expenses for implementation and can be effected even by nominal computer users.

6. REFERENCES

[1] Singleton, T. "IS Audit Basics: Understanding the Cybercrime Wave", *ISACA Journal*, vol. 1, 2014.

[2] Nikhita Reddy, G. and Ugander Reddy, G. J. "A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies", International *Journal of Engineering and Technology*, Vol. 4, Number 1, 2014, pp 48-51.

[3] Rotich, E. K., Metto, S. K., Siele, L. and Muketha, G. M. "A Survey on Cybercrime Perpetration and Prevention: A Review and Model for Cybercrime Prevention", *European Journal of Science and Engineering*, Vol. 2, Number1,2014, pp 13-28.

[4] Shaik, A. and Shaik, S. B."Cybercrime is a Global Problem: Increasingly Social and Mobile", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Number 1, 2014, pp 4993-5001.

[5] Alshboul, A. "Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks", Communications of the IBIMA, 2010.

[6] Obidinnu, J. N. and Duke, O.S. "Deploying Security-Aware Software Systems Using Source Code Vulnerabilities Analysis", *African Journal of Computing & ICT*, Vol. 6, Number 5, 2013, pp 171-180.

[7] Bacic, E. and Maxwell, G. "Software Hardening &FIPS 140", In *Physical Security Testing Workshop*, June, 2013.

[8] Sharma, S., Singh, G. and Singh, P. "Security Enhancing of a LAN Network Using Hardening Technique", *International Journal of Innovative Technology and Exploring Engineering*, Vol. 2, Number 3, 2013, pp. 174-181.

[9] Clemente, N. "System Hardening: The Process of Defending and Securing Today's Information Systems", *Journal of Security Education*, Vol. 2, Number 4, 2007, pp. 89-118.

[10] Damanpour, F. and Damanpour, J. A."E-Business E-Commerce Evolution: Perspective and Strategy", Managerial Finance, Vol. 27, Number7, 2001, pp 16-33.

[11] Anderson, R. "Security Engineering", New York: John Wiley & Sons, 2008.

[12] Northlander, P."Architectures and Standards for Hardening of an Integrated Security System", Chalmers University of Technology, Sweden, 2010.

[13] Smith, R. E. "Sidewinder: Defense In-Depth Using Type Enforcement", *International Journal of Network Management*, Vol. 5, Number4, 1995, pp 219-229.

[14] Tropeano, G. "*Examining Viruses", Code Breakers Journal*, Vol. 1, Number 2, 2006.

[15] Xiaoling, S."The Study on Computer Network Security and Precaution", *International Conference on Computer Science and Network Technology, Harbin, China*, Vol. 3, 2011, pp 1695-1698.

[16] McGraw, G. "Software Security*", Security & Privacy, IEEE*, Vol. 2, Number2, 2004, pp 80-83.

[17] Stytz, M. R. and Whittaker, J. A. "Software Protection: Security's Last Stand", *IEEE Security and Privacy*, January, 2003.

[18] Gupta, P. and Kumar, S. "A Comparative Analysis of SHA and MD5 Algorithm", *International Journal of Computer Science and Information Technologies*, Vol. 5, Number 3, 2014, pp 4492-4495.

[19] Gollmann, D. "*Computer Security (3rd Ed.)"*John Wiley & Sons, New York, 2006.