

EFFECT OF POOR SOFTWARE DEVELOPMENT PRACTICES ON COMPUTER SOFTWARE SECURITY

EMILY GAKII MURERWA
CHUKA UNIVERSITY
P.O. BOX 149
CHUKA 60400.
KENYA.
emilymurerwa2012@gmail.com

ABSTRACT

We are in what is known as the digital age. Almost every aspect of life is in one way or another affected by computers. There has been seen an increase in the availability of computer hardware and software. Computer hardware has become rampant with devices such as mobile phones, tablets and laptops making it possible for people to easily carry and move with the computing device which has in essence contributed to computer usage. We use computer software otherwise known as computer systems for communication, for online shopping and purchasing, for business transactions, for remote medical services, for government services and for education purposes among many other uses. It is right to say that computers have revolutionized the way we live. Computer systems are obtained through a process known as programming. Computer programmers also known as developers work either as individuals, as members of a team or in employment by a software development company. But as computer usage increases so has a type of criminals known as cybercriminals perpetrating what are known as cybercrimes. Cybercrimes are intended to disrupt computer usage and cause damage to individuals, organizations and even governments. Software creators need to be keen so that they can develop software that is secure and which makes it hard to manipulate by criminals. This research considers some of the practices ignored or in some cases taken lightly by software developers which in return lead to less secure software. The research also recommends what software developers need to do in order to secure software.

Keywords:

Software, Cyber Space, Security, Cyber Security, Cyber Crime

1.0 INTRODUCTION

The advent of the internet and web technologies has created a totally new platform for interaction known as the cyber space. Computer hardware, software and networks play a crucial role in cyber space. Through the cyber space, individuals interact socially and influence one another. Businesses are setup and carried out through eBusiness and eCommerce, learning opportunities are offered through eLearning, government technologies offered through eGovernment. Banking has also been revolutionized with mBanking and internet banking being a force to reckon with. Komen (2016) broadly reviews MPESA, a world reknown telephony money implementation; a trendsetter in mobile money transactions which has completely changed the banking and business sectors in Kenya and in a way the world at large.

Computer Software

Computer software are the instructions that drive the computer. Computer software are also referred to as computer systems, software or systems. Computer software are primarily classified into two broad classes. There are System software and Application software. System software are the most important software of a computer. They must be there, must have software. These are software that bridge the gap between computer hardware and computer users. System software includes Operating System software and Utility software. Application software are software used to carry out specific functions in a computer. These include word processing software, spreadsheet software, database management software as well as software for any other specific application. Software is created through a process known as programming or development. This is done by computer programmers as well referred to as software developers. A programming language is used as the platform for the creation of software.

Types of Software

There are many types of software including desktop applications, database driven software, web based software and mobile applications commonly known as apps. A desktop application is one that runs stand-alone in a computer. It can only be accessed from the computer on which it has been installed. Database driven software has a database onto which data and transactions are accessed. Web based software primarily websites and web applications and stored on a web server from which users access via a Uniform Resource Locator on a browser.

To program, computer programmers make use of programming languages. These can be either open source or proprietary. The resultant systems could also be either open source free software or proprietary software. Open source software are those whose source code is free available on the internet. Proprietary software is that which is owned either by an individual or by a company which developed it. Source code for proprietary software is closely guarded.

2.0 SOFTWARE SECURITY CONCERNS

However, with the advent of so much happening on the cyber space there have also arisen threats taking advantage of the new technologies. This introduces what is known as cyber security. Thakur et al., (2015) compares cyber security to information security. They shed light on three factors that cyber security is concerned with. Included are the methods of protecting Information Technology (IT), the data being processed and transmitted together with physical and virtual setup, the level of

protection obtained by applying such measures and the professional aspects associated. Threats to cyber security are hence threats that touch any of these. The section that follows discusses some of these security concerns.

The first and most commonly known cybercrime is hacking. Hacking is the process of using system which one is not authorized access. Mostly users of a computer system are defined and stored from which the system references who to allow access or not. Hackers are primarily classified as white hat hackers, black hat hackers and grey hat hackers. White hat hackers the so called ethical hackers are also known as security professionals who hack computer systems with an intention to find vulnerabilities which an ill-intentioned person could take advantage of. These hackers hack to help, they hack to advice. Black hat hackers hack to harm. Such hackers if they are able to gain access to a computer system wreak havoc. They delete data, edit data, crash systems, and introduce bad software among many other ills. Grey hat hackers are those hackers without a stand. They can be black hat or white hat depending on what suits them. Computer software must have mechanisms in place to defeat hacking attempts. Identity theft is another cybercrime. It is also known as impersonation. This is where someone steals personal details of another and pretends to be them. Computer systems store a lot of identification data which if it falls into wrong hands could be used for illegal purposes such as fueling illegal immigration and cyber terrorism. Commercial identity theft where someone transacts by pretending to be another greatly impacts the economy of a country. Another criminal activity associated with the cyberspace is Cyber stalking. This is a crime akin to emotional torture is where someone uses internet technologies and the web to cause harassment to another. False accusations, trolling are among crimes associated with cyber stalking. Terrorists also take advantage of the internet and the World Wide Web to effect Cyber terrorism. The nature of this crime is that terrorists manipulate computer software, systems and computer networks to effect works of terrorism. Activities range from disabling services, tarnishing institutions including government institutions, spreading of propaganda, use of computer systems for training recruit as well as experienced terrorists, for communication among terrorists just to mention but a few.

A number of researchers have pointed out security concerns over software applications. Bayse (2004) presents a checklist for consideration while developing web applications among them security considerations. When software developers are creating software there are some practices they take which can be considered to effect security of the software being created. Booch (1998) presents a write-up on software development best practices. He address practices to consider to mitigate among others poor quality software and software flaws.

Developer Practices affecting Software Security

Use of Open Source Software - A common practice by young software developers is the download and use of open source software platforms and frameworks for use in creating own software. Open source platforms are a preference in this case because most are in essence free, with availability being easy and fast due to their presence on the internet. No cash is needed to acquire these platforms and if any is required it is mostly quite affordable. Open source platforms too have quite an online support with online fans ready to help where a need arises. Nevertheless the learning curve too is considered fast. However there are issues of concern touching on open source free software. Vadalasetty (2004) highlights some of the security concerns with use of open source

software in a production environment. He points out that the availability of open source software to a wider mass of reviewers may be to its disadvantage welcoming even unqualified reviewers. When open source software is published, other developers could make changes to the software introducing a possibility for implementation of security concerns Rantala, Chuan and Jiao (2013). A developer should be careful to audit the source of the free software as well reading available materials, responding to security concerns from the online community.

Upgrades and Patching - Lack of development platform upgrade is another identified practice that impact negatively on developed software. It is a common practice for platform developers to times and again release version upgrades and patches to address vulnerabilities and bugs identified in the developing platforms. If a software developer is not keen to keep trace of releases and thereafter upgrade platform as advised, then the platform is left unprotected which spills over to the system being developed of which cyber criminals can take advantage of.

Not changing Default Configurations- Another identified shortcoming practice is that of sticking to default configurations. Some development platforms come with default authentication configurations which may be all too well known by everyone cyber criminals included. Example is the MySQL server administrator login whose user account is root with no password. A software developer who makes use of a platform or framework but ignores changing the default settings is courting trouble. Any cybercriminal can easily use the already well known configurations to access and carry out damage on the developed software.

Not Following a Development Methodology - Software development is not a haphazard process rather one that is well thought of. Any software creation endeavor could do well to follow any of the well-defined software development methodologies. These include the waterfall methodology, agile and rapid prototyping just to mention a few. All these approaches take into consideration a clear understanding of the problem for which a computer solution in form of a computer software is being sought, interacting with users to understand system procedures and other considerations including security, testing the developed system for functionality and usability; the so called functional and non-functional system requirements and many other steps. Developing by following a methodology will be able to note points of concern especially as highlighted by users but also those discovered during the analysis stage which the development can then address to ward off abuse by cyber criminals.

Ignoring System Users - It is a good practice to involve the software users throughout the development process. At the initial stages, users are involved to shed light on how the current system works and moreover offer advice on the user expectations of the software being developed. According to Emam, Quintin and Madhavji (1996), during software development, the users are typically involved in early phases of development for requirements elicitation and feedback. Ultimately the software is being developed for the user. Users are involved at the final testing stage to confirm if the developed software meets the defined or expected requirements. Involving users throughout the development but moreover at the initial and final stages increases the chances of capturing major bugs that could be introduced through unnecessary oversights. Kujala *et al.*, (2005) also argue that involving users in software development positively affects the success of the system.

User Training - Another good practice which overlooking it contributes to insecure software is that of training users. The weakest security link in any system is the system users. Cyber criminals commonly utilize what are known as social engineering to gain access to secured systems. Social engineering is a set of soft techniques whereby the cyber criminals play on the humanity of users through diverse ways aimed at gaining trust with the user such that the user reveals access credentials. Software developers should plan to train users on functionality and cyber security concerns. User training however should not be a one-time activity, rather should be incorporated as an ongoing maintenance activity.

No Security Policies - Software developers in partnership with system administrators and network administrators should plan for security policies. Simple basic policies like password policy, login policy among others should be put in place. If none are in place, the developer should create one.

Laxity in System Maintenance - Laxity in system maintenance is also a contributor to software insecurity. Some developers ignore or take lightly software maintenance. Generally after a system is developed and deployed, there comes system maintenance which is an ongoing process. Activities inclusive of maintenance are log checks, system upgrades, system backups and user training. Logs include System, Security and Application logs. Checking the logs would alert of any attempt to login illegally as well as any other alert from the computer on what is going on with the software. Preventive and / or corrective actions can hence be taken. Lack of checking logs is courting disaster.

3.0 RECOMMENDATIONS

Tenets of computer security highlight three major areas by which security in computer systems is measured.

Computer systems must offer confidentiality such that data which the system transacts with is kept confidential as well as information flow through the software. Systems should apply the must know principle for data, information and transactions through them. Secure computer systems are also expected to assure the integrity of the data, information and transactions within and through them. Consumers of the information are expecting that no changes have happened mid-way and that what the recipient is getting is exactly as the sender intended with no subtractions, no additions, and no changes whatsoever. Availability is another expectation of a secure computer system. The software itself is expected to be always available for use when needed by the user. Data and information are also expected to be availed as and when needed.

Security breaches by cyber criminals interfere with this triage. Breached software are not confidential, do not have integrity and may not be available.

This paper recommends that software developers consider the practices highlighted above and make efforts to reference during and after the software development process.

Developers are advised also to seek memberships in online and physical groups that focus on matters security. Attending of seminars, workshops, free and paid security trainings is also advisable to keep up to date with new tricks used by cyber criminals as well as learn new techniques to ward off the criminals. Information is power. An informed developer is a prepared developer.

Another recommendation is for developers to consider third party technologies specially created for protecting software creations. These may not be part of the platform per se but can be enabled or installed as add-ons.

REFERENCES

1. Leah Jerop Komen (2016), M-PESA: A Socio-Economic Assemblage in Rural Kenya, Networking Knowledge, Standard Issue(2016)
2. Kutub Thakur, Meikang Oiu, Keke Gai, Liakat Ali(2015), 15 Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud) Pages 307-311
3. Gail Zemanek Bayse (2004), GIAC Security Essential Certification, SANS Institute Reading Room
4. Grady Booch (1998), "Leaving Kansas," IEEE Software 15(1) Jan.–Feb. 1998, pp. 32–35.
5. Sreenivasa Vadalasetty (2004), Security Concerns in Using Open Source Software for Enterprise Requirements, SANS Institute Reading Room
6. Oskari Rantala, Hu Chuan & Huang Jiao (2013), Security Issues of Open Source Software
7. Khaled El Emam, Soizic Quintin and Nazim H. Madhavji (1996), User participation in the requirements engineering process: An empirical study, Requirements Engineering, 1996, Volume 1, Number 1, Page 4
8. Kujala S, Kauppinen M, Lehtola L and Kojo T (2005), The role of user involvement in requirements quality and project success, 13th IEEE International Conference on Requirements Engineering (RE'05)