EFFECT OF POOR SOFTWARE DEVELOPMENT PRACTICES ON COMPUTER SOFTWARE SECURITY

EMILY GAKII MURERWA
CHUKA UNIVERSITY
P.O.BOX149
CHUKA60400.
KENYA.
emilymurerwa2012@gmail.com, emurerwa@chuka.ac.ke

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 hardwareand software. Computer hardware has become rampant withdevices such as mobile phones, tablets and laptopsmaking it possible forpeopleto easilycarryand movewiththecomputingdevicewhich has in essence contributed to computer usage. We use computer software otherwise known as computer systems for communication, for online shopping and purchasing, for businesstransactions, 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 knownas cybercrimes. Cybercrimes are intended to disrupt computer usage and cause damage to individuals, organizations and even governments. Software creators need to be keenso thattheycandevelop softwarethat 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,CyberSpace,Security,CyberSecurity,CyberCrime

1.0 INTRODUCTION

The advent ofthe internet and web technologies has created atotally new platform for interaction knownas the cyber space. Computer hardware, software and networks playa crucial role in cyber space.Throughthecyberspace, individualsinteractsociallyandinfluenceoneanother.Businesses are setup and carried out through eBusiness and eCommerce, learning opportunities are offered throughe Learning,governmenttechnologiesofferedthroughe Government.Bankinghasalsobeen 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.

ComputerSoftware

Computer softwareareetheinstructionsthat drivethecomputer.Computer softwareareal so 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 ofa computer. The must be there, must have software. These are software that bridge the gap between computer hardware and computer users.System software includes OperatingSystemsoftwareandUtilitysoftware. Applicationsoftwareareusedto carryout specific functions in a computer. These include word processing software, spreadsheet software, database management software as well as software for anyother 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.

TypesofSoftware

There are many types of software including desktop applications, database driven software, web basedsoftwareand mobileapplicationscommonlyknownasapps. Adesktopapplicationisonethat runs stand-alone in a computer. It can only be accessed fromthe computer on which it has been installed.Database driven software has a database onto which data and transactions are accessed. Web basedsoftwareprimarilywebsitesand webapplicationsand storedonawebserver from which users access via a Uniform Resource Locator on a browser.

Toprogram,computerprogrammersmakeuseofprogramming languages. Thesecanbeeitheropen source or proprietary.The resultant systems could also be either open source free software or proprietarysoftware. Open source software are those whose source code is free available on the internet. Proprietarysoftware is that which is owned either byan individualor bya companywhich developed it. Source code for proprietary software is closely guarded.

2.0 SOFTWARE SECURITYCONCERNS

However, with the advent of so much happening on the cyber space there have also arisen threats takingadvantageofthenewtechnologies.Thisintroduceswhat isknownascybersecurity. Thakur et al., (2015) compares cyber securityto informationsecurity. Theyshed light on three factorsthat cyber security is concerned with. Included are the methods of protecting Information Technology (IT),the data being processed and transmittedtogether withphysical and virtualsetup, the levelof

protection obtained byapplying such measures and the professionalaspects associated. Threatsto cyber securityare hencethreatsthat touchanyofthese. Thesectionthat followsdiscussessomeof these security concerns.

The first and most commonlyknowncybercrime ishacking. Hacking istheprocessofusingsystem whichone is not authorized access. Mostlyusers ofa computer systemare defined and stored from which the systemreferences who to allow access or not. Hackers are primarily classified as white hat hackers, black hat hackersand greyhat hackers. White hat hackerstheso called ethicalhackers are also known as securityprofessionals who hack computer systems with an intention to find vulnerabilitieswhichan ill-intentioned personcouldtake advantageof. These hackershack to help, theyhack to advice. Black hat hackershack to harm. Suchhackers iftheyare able to gainaccessto a computer system wreak havoc. Theydelete data, edit data, crash systems, and introduce bad software among many other ills. Grey hat hackers are those hackers without a stand. Theycan be black hat orwhite hat depending onwhat suitsthem. Computer software must have mechanisms in place to defeat hacking attempts. Identitytheft is another cybercrime.It is also known as impersonation. This is where someone steals personal details of another and pretends to be them. Computer systemsstorealot ofidentificationdatawhichif it falls into wronghandscould beused 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 economyof a country.Anothercriminalactivityassociatedwiththecyberspace isCyberstalking.This isacrime akin to emotionaltorture is where someone uses internet technologies and the web to cause harassmentto another. Falseaccusations, trollingareamongcrimesassociatedwithcyberstalking. Terrorists also take advantage ofthe 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 institutionsincludinggovernment institutions,spreadingofpropaganda,useofcomputersystems 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 securityconsiderations. Whensoftwaredevelopersarecreatingsoftwaretherearesomepractices theytake whichcan be considered to effect securityofthe 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.

DeveloperPracticesaffectingSoftwareSecurity

UseofOpenSourceSoftware- Acommonpracticebyyoungsoftwaredevelopers isthedownload and use ofopen 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 mostlyquite affordable. Open source platforms too have quite an online support with online fans readyto 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 ina productionenvironment. He points out that the availability ofopensource software to awider massofreviewers maybeto itsdisadvantagewelcoming evenunqualified reviewers. When opensourcesoftwareispublished,other developerscould makechangestothesoftwareintroducing a possibility for implementation of securityconcerns Rantala, Chuan and Jiao (2013). A developer should be careful to audit the source ofthe free software as wellreading availed materials, responding to security concerns from the online community.

UpgradesandPatching- Lackofdevelopment platformupgrade isanotheridentifiedpracticethat impact negativelyon developed software. It is a common practice for platformdevelopers to times and againrelease versionupgrades and patches to address vulnerabilities and bugs identified inthe developing platforms. If a software developer is not keen to keep trace of releases and thereafter upgrade platformas advised, then the platform is left unprotected which spills over to the system being developed of which cyber criminals can take advantage of.

NotchangingDefaultConfigurations- Another identifiedshortcomingpractice isthatofsticking to default configurations. Some development platforms come with default authentication configurationswhichmaybealltoowellknownbyeveryonecybercriminals included. Example is the MySQL server administrator login whose user account is root with no password.A software developer who makes use ofa platformor framework but ignores changing the default settings is courting trouble. Anycybercriminalcaneasilyusethealreadywellknownconfigurationsto access and carry out damage on the developed software.

Not Following a Development Methodology - Software development is not a haphazard process ratheronethatiswellthought of. Anysoftwarecreationendeavor coulddo welltofollowanyofthe well-defined software development methodologies. These include the waterfall methodology, agile and rapid prototyping just to mention a few. Allthese 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 functionalityand usability; the so called functionaland non-functionalsystemrequirementsand manyothersteps.Developingbyfollowing a methodologywill be able to note points of concern especially as highlighted byusers but also those discovered during the analysis stage which the development can then address to wardoff 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 systemworksand moresoofferadviceontheuserexpectationsofthesoftwarebeingdeveloped. 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. Ultimatelythe software is being developed for theuser. Users are involved at the finaltesting stage to confirm if the developed software meets the defined or expected requirements. Involving users throughout the development but moreso at the initialand final stages increases the changes of capturing major bugsthat couldbe introducedthroughunnecessaryoversights. Kujala*et al*.,(2005) alsoarguethatinvolvingusersinsoftwaredevelopmentpositivelyaffectsthesuccessofthesystem.

UserTraining-Anothergoodpracticewhichoverlooking it contributestoinsecuresoftware isthat of training users. The weakest security link in any system is the systemusers. Cyber criminals commonlyutilize 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 humanityof 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. Usertraining however should not be a one-time activity, rather should be incorporated as an ongoing maintenance activity.

NoSecurityPolicies- Softwaredevelopers inpartnershipwithsystemadministratorsandnetwork administrators should plan for securitypolicies. Simple basic policies like password policy, login policy among others should be put in place. Ifnone are in place, the developer should create one.

Laxity in System Maintenance - Laxity in system maintenance is also a contributor to software insecurity.Somedevelopersignoreortakelightlysoftware maintenance. Generallyafterasystemis 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, Securityand Application logs. Checking the logs would alert of any attempt to login illegally as wellas anyother alert fromthe computer on what is going on with the software. Preventiveand/orcorrectiveactionscanhencebetaken.Lackofcheckinglogsiscourtingdisaster.

3.0 RECOMMENDATIONS

Tenetsofcomputersecurityhighlightthreemajorareasbywhichsecurityincomputersystems is measured.

Computer systems must offer confidentiality such that datawhich the systemtransacts with is kept confidentialaswellas informationflowthroughthesoftware. Systemsshouldapplythe must know principle for data, information and transactions through them. Secure computer systems are also expected to assure the integrityof the data, information and transactions within and through them. Consumersofthe informationareexpectingthat nochangeshave happened mid-wayandthat what the recipient is getting is exactly as the sender intended with no subtractions, no additions, and no changeswhatsoever. Availabilityisanother expectationofasecurecomputer system. Thesoftware itself is expectedto be always available for use when needed bythe user. Data and informationare also expected to be availed as and when needed.

Securitybreachesbycybercriminals interferewiththistriage. Breachedsoftwarearenot confidential, do not have integrity and may not be available.
Thispaperrecommendsthat softwaredevelopersconsiderthepracticeshighlightedaboveand 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 securitytrainings is alsoadvisableto keepuptodatewithnewtricksusedbycybercriminalsas wellas learnnewtechniques to ward off the criminals. Information is power. An informed developer is a prepared developer.

Anotherrecommendationisfordeveloperstoconsiderthirdpartytechnologiesspeciallycreatedfor protecting software creations. These may not be part ofthe platformper se but can be enabled or installed as add-ons.

REFERENCES

1. LeahJeropKomen(2016),M-PESA:ASocio-Economic Assemblage inRuralKenya, Networking Knowledge, Standard Issue(2016)
2. KutubThakur,MeikangOiu,KekeGai,Liakat Ali(2015),15Proceedingsofthe2015IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud) Pages307-311
3. GailZemanekBayse(2004),GIACSecurityEssentialCertification,SANSInstituteReading Room
4. GradyBooch(1998),"LeavingKansas,"IEEESoftware15(1)Jan.–Feb.1998,pp.32–35.
5. Sreenivasa Vadalasetty(2004), SecurityConcerns inUsing OpenSourceSoftware for Enterprise Requirements, SANS Institute Reading Room
6. OskariRantala,HuChuan&HuangJiao (2013),SecurityIssuesofOpenSourceSoftware
7. KhaledElEmam,SoizicQuintinandNazimH.Madhavji(1996), Userparticipationinthe requirements engineering process: An empirical study, Requirements Engineering, 1996, Volume 1, Number 1, Page 4
8. KujalaS,KauppinenM,LehtolaLand Kojo T(2005),Theroleofuser involvement in requirements quality and project success,13th IEEE International Conference on Requirements Engineering (RE'05)