ON COMBATING CURRENT AND EMERGING CYBERCRIMES IN KENYA

Fredrick Mugambi Muthengi
Department of Computer Science
Chuka University
109 - 60400,
Chuka
fremugambi@gmail.com

ABSTRACT

Communities are increasingly embracing information technology in its many various forms due to its increased efficiency in service delivery. Currently, information technologies rely entirely on interdependency of cyber infrastructures that is faced with an immense share of challenges. Cybercrime comes in has number one. This crime is often rampart on Web-based systems that are accessible online via the Internet. Generally, cyber-attacks are on the rise. Users need awareness in the devastating effects of the ever increasing cybercrimes. This paper proposes measures to address current and emerging cyber security issues in the Kenyan context. Further, the paper discusses a model/platform for knowledge sharing (on cybercrimes as they are noticed) among organizations. Research institutions can then pick from the knowledge pool on specific attacks and initiate research tasks to address them.

Key words: *Information technology, cybercrime, web-based system, security, cyber-attacks, online*

1.0 INTRODUCTION

The general definition of cybercrime may be unlawful actions where the computer is used as a tool, a target or both that threaten a nation's security and financial health (Chavan et. al, 2010; Halder & Jaishankar, 2011). Both governmental and non-governmental criminals engage in cybercrimes ranging from espionage, financial theft and other cross border crime. Simply put, cybercrime refers to any criminal activity carried out with the aid of a computer system.

Security is a primary and widespread concern for software systems especially web-based software systems (Romero-Mariona et. al, 2009). The ease of performing cyber-attacks has tremendously increased with the drastic changes in information technologies. These cyber-attacks are becoming increasing complex. Many software systems quality attributes at the moment have security topping the list. Cyber-attacks and other cyber threats can cause disastrous impacts in a community, especially for a coordinated attack targeting multiple critical infrastructures. This crime is often rampart on Web-based systems that are accessible online via the Internet. Some institutions/organizations in fear of this attack have chosen to shelve online processing to more secure intranets that only allow accesses on their local area networks.

As communities embrace information technology for efficient service delivery, the bad elements in the society are constantly exploiting the same technology for illegitimate gains. Criminals are exploiting the Internet and other networks to advance the illegal business. As result, cybercrime is on the increase. Just as technology is advancing, cyber-attacks are getting more sophisticated (Poonia, 2014). The fast growth in cyber security challenges requires a robust framework to address the menace. Poor or no cyber safety measures lead to massive loss of critical data and financial assets.

The Internet structure lacks a single central control (Peisert et. al, 2014). Therefore, anyone connected online can carry out legitimate or malicious tasks. Cybercrimes exploit this unstructured nature of the Internet. In addition, individuals with expertise on programming and other complicated computing skills are the majority involved in compromising the security of the computer users. Currently, there are many online tools that are misused. Software developers who contravene software engineers' professional code of ethics (Summerville, 2011) can be cited as the source of cyber-attacks. The primary target of most reported cybercrimes in Kenya (in 2014) targeted key government institutions' websites. Successful cyber-attacks in Kenya are blamed on poor detection tools and a lack of capacity to address the crime. This paper explores the various cybercrimes prevalent in Kenya, proposes measures to address /minimize or eradicate them. It also proposes an information sharing model to allow IT research experts and organizations take up the issue and facilitate research tasks to curb the crime.

2.0 FIVE PREVALENT CYBERCRIMES IN KENYA AND MEASURES TO ADDRESS THEM

Generally, cybercrimes are criminal/and unethical activities performed using computers and/or computer networks especially the Internet. Reported cyber-attacks in Kenya (especially by the Kenyan media) range from denial of service (DoS) attacks to breach of confidentiality thus leading to online impersonation among others. General Cyber security awareness and knowledge on cyber-attacks is beneficial to all computer users as it prepares them to prevent inherent online threats. Some of the attackers are basically in a learning session and experimenting what would become by carrying out some of these actions. Deploying Security Intelligent Agent (Security Intelligent Checkers) to an existing intrusion detection system would facilitate detection of successful attacks through independent monitoring of physical processes (Sabaliauskaite&Mathur, 2014).

2.1 Malware

Malware refers to malicious software that finds their way to a computer system especially from the Internet. They could be viruses, trojans worms, and other software that get installed in a computer without the user's knowledge. In several cases, the software will pretend to be legitimate software. Malware's intentions are diverse ranging from spying on your work, phishing/password sniffing, monitoring web sites visited, access to confidential data, and denial of service, among others.

Hackers capitalize on malware to gain access to government sites. At the extreme, they may bring down an entire web site. Whatever the motivation of attack, it is important that users avoid installing pirated software, downloading software from non-trusted sites, and maintain an up-to-date anti-malware protection. Although not common, users should ignore any payment requests for transactions they have not initiated. General awareness on computer software security issues can go a great mile in reducing cases of malware attacks.

2.2 Identity theft / Fraud

Cybercriminals obtain personal and confidential data belonging to someone or an institution they are targeting. This information can be obtained through social engineering, email phishing, purchase the data on the black market, or use tools and techniques to search. A majority of personal data is the open access in the Internet especially in this era of socializing sites. An attacker may befriend a non-suspecting individual and obtain all the information they needed to launch an attack or entice them to perform some action.

Identity theft typically succeeds when a cybercriminal gets an individual's personal identification information. The crime is motivated by the likely financial reward or corruption done on accessed data. Therefore, identity theft is a gateway for fraud cases such as credit-card fraud and other related cases.

The only sure way to avoid this crime is to ignore in attempts by strangers to initiate conversations either via phone calls, online chats, emails or other means of communications on disclosure of private information. However, once a victim realizes success in an attack, it will be safe to notify relevant authorities. It is also important to keep a record of any conversations made especially text messages.

2.3 Cyber stalking

Simply defined, cyber stalking is the use of technology to harass someone. An attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), phone calls or posting messages on chat forums/discussion groups or social sites. A cyber stalker will hide in the Internet for anonymity to avoid detection. The stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. The messages sent range from sexual harassment, threats to one's security and safety, posting of false information for defamation or just annoying attention to an individual's private life and family activities. Unlike general cyber harassment, cyber stalking poses a credible threat to the victim. In Kenya cyber stalking takes many forms such as defamation or libel, falsification, fraud, intimidation, offensive comments, personal attacks, graphic violence and violation of rights to privacy.

Cyber stalkers will go to great lengths to try to monitor a victim's online activity. This may include infecting a person's computer with malware that is able to log computer activity. They may contact a victim's colleagues, friends and other online contacts in an effort to slander them or extract personal information from them. Cyber stalkers are also known to continually harass their potential victims.

To deal with cyber stalking some of the drastic measures are to block contacts of the perpetrator, unfriend their contacts, or report the crime to the police. However, generally, lack of legislation on dealing with cybercrime retards the efforts of reporting. Some victims may even chose to ignore the attack and move on. General knowledge on cyber-attacks may also help individuals identify a potential attacker and take necessary measures.

2.4 Ransomware

Ransomware built from two words, *ransom* and *malware* it's a kind of malware attack that demands payment in exchange of stolen computer functionality. Most attacks of this nature make use of encryption as means of extortion. Basically encrypting files on computer's hard drive and then asking for financial favours to decrypt them back for the victim to have them back. It's a form of denial of service attack (Gazet, 2010). A majority of the people will go dramatic lengths in order to access locked information or to prevent sensitive information from being leaked to the public. Ransomware is a crime in the rise and it's projected as the favorite cybercrime of the future ("5 cybercrimes on the rise in 2015", 2015).

Awareness education is the key to ransomware prevention (Luo & Liao, 2007). Efforts to make backups in the "*cloud*" are gaining popularity. However, this measure is constrained by the privacy policy a client has to sign or accept. Since some of the content is highly confidential some individuals find it hard to make these online backups.

2.5 Attack on Mobile money payment systems

Cybercriminals have their eyes on the M-Pesa (in Kenya) platform. Users therefore need to exercise great caution and use common sense in the event of potentially fraudulent transactions. Over the years, since mobile money transactions services such as M-Pesa gained ground, criminals have always devised ways of gaining access to individual's accounts. The tremendous growth in the mobile payments also offers a great opportunity for money laundering. Apparently, most of the mobile money transactions are not monitored via banking regulations. The lack of thorough testing on mobile money transactions platforms offers a major vulnerability easily exploited by cybercriminals. Various malware families may take advantage of this situation and cause serious losses to mobile money transaction clients. Mobile money transaction users will therefore

3.0 MOTIVATIONS OF CYBERCRIME

There are a number of general motivations for cybercriminals to continue in their endeavors:

- Lack of legislation touching on cyber-attacks.
- Poor detection techniques. Mechanisms of tracking the culprit are much behind.
- Lack of capacity to respond to the crime. This exposes vulnerability of systems (in Kenya).
- Attackers are also capitalizing on the naivety of some of the Internet system users. Numerous "mouse click events" without thought of what is likely to happen next. Solution to every problem begins from analysis of consequences. This ought to be the case for Cyber security.

4.0 CYBERCRIME INFORMATION KNOWLEDGE SHARING MODEL

Companies start a common platform for sharing cybercrime information. This sharing would increase preparedness and help in collaborative efforts to combat cybercrimes in their various evolving forms. As such, it is important that companies embrace a multi-faceted approach on dealing with cybercrime. The public and the private sector need a common ground to tackle this menace by devoting more resources to secure cyber space.

Invest heavily on computer network security: specialized training for system administrators; crime awareness forums in learning institutions especially universities; encourage computer and Science

and IT students to undertake specific lecturer/researcher coordinated teamwork projects on cyber security – securing software systems.

The Community Cyber Security Maturity Model (CCSMM) was proposed to help communities establish viable and sustainable cyber security programs (White, 2011). Information Sharing is one of the key areas emphasized in the CCSMM but there are significant aspects to be explored. Collaborative information sharing helps a community detect potential risks and prevent cyber-attacks at an early stage. Other than creating awareness groups, the public and private sectors need to establish a partnership on disseminating knowledge on cyber-attacks and upcoming threats. Discussion forums leading to mutually funded projects would boost efforts on addressing this crime. In the forums, various stakeholders can pre-empt on the possible effects of any successful attack thus enabling the categorization of the level of the crime that warrants concerted efforts to counter the threat or stop a crime from being repeated.

5.0 Conclusion

Cyber-attacks are real in our communities. The level of preparedness for cyber-attacks plays a major role in addressing cybercrime. Currently, cybercrime is advancing with the ever changing technology. As such, the crime has become one of the biggest threats facing organizations and individuals. Some of the routine measures that need reinforcement include maintaining updated security software and updated software in a computing equipment; good password management practices - change your online accounts passwords frequently. In most cases, attackers capitalize on the vulnerability of their victims. Basically, attackers make use of opportunities got from victim's exposure. While the five attacks are expected to thrive in the cyber security landscape, information sharing and analysis, awareness campaign (especially on phishing scams), and two-factor authentication, would go great lengths in combating the problem.

REFERENCES

1. Poonia, A. S. (2014), Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN*, 2278-6856.

2. Chavan, G. R., Rathod, M. L., &Naik, N. (2010). Cyber Crime: A Study. *SRELS Journal of Information Management*, *47*(4), 465-472.

3. Halder, D. &Jaishankar, K. (2011). *Cyber crime and the victimization of women: laws, rights and regulations*. Information Science Reference.

4. Hassan, A. B., Funmi, D. L., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, *2*(7), 626-631.

5. Arora, M., Sharma, K. K., &Chouhan, S. (2014). Cyber Crime-The review.

6. Zhao, W., & White, G. (2014, January). Designing a formal model facilitating collaborative information sharing for community cyber security. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 1987-1996). IEEE.

7. Sabaliauskaite, G., &Mathur, A. P. (2014, July). Design of Intelligent Checkers to Enhance the Security and Safety of Cyber Physical Systems. In *Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International* (pp. 7-12). IEEE.

8. Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. (2014). A Dutch Approach to Cybersecurity through Participation. *Security & Privacy, IEEE*, *12*(5), 27-34.

9. Peisert, S., Margulies, J., Nicol, D. M., Khurana, H., &Sawall, C. (2014). Designed-in Security for Cyber-Physical Systems. *Security & Privacy, IEEE*, *12*(5), 9-12.

10. Summerville I., (2011), *Software Engineering*, *9*th Ed. Pearson Education, Addison Wesley

11. Romero-Mariona, J., Ziv, H., Richardson, D. J., & Bystritsky, D. (2009, April). Towards usable cyber security requirements. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (p. 64). ACM.

12. Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in computer virology*, *6*(1), 77-90.

13. Luo, X., & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. *Information Systems Security*, *16*(4), 195-202.

14. White, G. B. (2011, November). The community cyber security maturity model. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (pp. 173-178). IEEE.

15. Five Cyber Crimes on rise in 2015: http://www.forensicscolleges.com/blog/resources/cybercrime-on-rise-2015