International Journal of Data Science and Analysis
2017; 3(2): 13-17
http://www.sciencepublishinggroup.com/j/ijdsa
doi: 10.11648/j.ijdsa.20170302.12

Research/Technical Note

Developing Countries Based End-User Computing Security Issues: Threats, Holes and Solution Prospects

Tibuhinda Ngonzi

Department of Accountancy and Finance, Saint Augustine University of Tanzania, Mwanza, Tanzania

Email address:
rigonzizk@gmail.com

To cite this article:
Tibuhinda Ngonzi. Developing Countries Based End-User Computing Security Issues: Threats, Holes and Solution Prospects. *International Journal of Data Science and Analysis*. Vol. 3, No. 2, 2017, pp. 13-17. doi: 10.11648/j.ijdsa.20170302.12

Received: June 7, 2017; **Accepted**: July 14, 2017; **Published**: August 3, 2017

Abstract: Security concerns comprise a prominent phenomenon in industrial computing. Software counterfeiting, hardware cloning and loss of data are always at the center of IT professionalism's thinking as it works to counteract those threats in the workspace. Still lacking however, is the awareness on security holes to industrial and personal computing, emanating from human behavior related to the end-users in the IT consumer blocks of the world, specifically the block of developing countries in Africa. In that context, the main purpose of this paper is to espouse the security holes from the end-user dimension as a way of sensitizing for inclusive security thinking among IT experts. The significance of the paper derives from at least two facts. One: while industrial computing is dominantly important, personal computing is also gaining prominence worldwide. As a result, complacency on security issues at this stage is no longer without felt consequences in industrial and mainstream computing. Two: as mobile technology use grows, so does the number of threats facing mobile data and platforms, as well as security vulnerability at personal computing level. This goes beyond the traditional data, software, and hardware concerns in industrial computing. It is noted that the level at which security concerns are stated makes a difference in the contemplation of solution options.

Keywords: End-User Computing, Industrial Computing, Mainstream Computing, Security

1. Introduction

Currently, the concerns of the developers and providers of information technologies (ITs) in the socio-technically advanced block of the world are software counterfeiting, hardware cloning and loss of data in the corporate world [14, 15]. However, the issues are different in the paradigm of consumers in the underdeveloped block. Ironically the consumers in this other block happen to be the main benefactors of the otherwise concerns of the IT developers' block. For them, the software counterfeits for instance, provide a cheap source of software resources such as operating systems (OS) for secondhand devices. Any problem with that? - Debatable. The obvious problem however, is where counterfeits are used to replace the original OS in stolen devices to over-write identity. This is real and rampant. This writer is familiar with the scenario in Africa, while admitting that the theft of computing devices is not confined to Africa alone. Reference to Hill and Alan [6] for instance, reveals a study conducted in 2008 which shows that more than 800,000 laptops slip off their owners' hands through theft and other factors each year at airports in the US and Europe, leading to tremendous breaches of confidential data. The point made however is that, the impacts of thefts are differentiated and relative to places, thus calling for differentiated solution technologies.

For the underdeveloped block, the loss of a personal computing device such as a laptop, a tablet, or a smartphone through theft has two consequences. The first is related to denial of service to the victim. In essence, it is a reality of the time that the relationship between electronic devices and their owners in personal computing increases in prominence with the age of ownership of a device. In the other words, overtime, each device gets uniquely related to its owner, changing its owner's perceived value exponentially in the process. This is due to the personalized features that are built such as information build-up in the device, enhancements, access to internet based subscriptions and resources, and so many other things. It means therefore, that it is not just a replacement of a stolen device with another, or having a data backup strategy in

place, that can effectively counteract the damage related to any loss of a device. Also serious, is the second consequence which is a derivative of the loss of a personal computing device. This is the propagation of security threats in the computing mainstream which is further elaborated in the sections ahead. Before then however, are some working definitions.

The text definition of '*end-user*', from the computing point of view, is an individual using an own [personal] computing device for personal or corporate related operations. This is evolved from the definition on 'end-user computing' as provided by Hill and Alan [6 p. 67]. In the same context is *'personal computing'*. This is a term used to refer to computing processes carried out by an end-user from a personal computing device such as a lap-top, iPad, smartphone, or tablet for personal ends. '*Mainstream computing'* is another terminology in the text, that applies to the context of IT professionalism and practices. It involves developers, providers and security experts.

In the sections below, the paper constructs security risk in the end-user computing dimension, followed by a brief discussion of the security concerns and developments in industrial computing in the corporates' perspectives with respect to corporate data. The context of corporates is hereinafter referred to as '*industrial computing*'. The discussion on concerns is followed by the conceptualization of the end-user security issues at large and their functioning as security threats gateway for industrial and mainstream computing. The fifth section is a challenge of 'design science' on HW security technological capabilities for end-user computing, followed by concluding remarks in the last section.

2. End-User Computing Security Risk Modeling

Security in IT is the "defense of digital information and IT assets against internal and external malicious and accidental threats" [17]. In industrial security analysis, as presented by Byres and Lowe [2], "security risk faced by an organization is a function of the likelihood of successful attack (LAs) against an asset and the consequence (C) of such an attack". The authors estimate 'consequences' in terms of financial loss, acute health effects, and environmental impacts on organizations, while in terms of Tan [20], the list can be extended to include sectorial consequences such as energy, water, finance and banking, government, healthcare, information communications, security, emergency services, and transportation [20 p.20].

Following the American Institute of Chemical Engineers' (AICE) guidelines, Tan [20] presents that the LAs variable is further broken down into three sub-variables as: Threat (T) - Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset; Vulnerabilities (V) - Any weakness that can be exploited by an adversary to gain access to an asset; and Target Attractiveness (Ar) - An estimate of the value.

The industrial security risk analysis presented above is used in this text to express for understanding of end-user computing security risk consequences in terms of loss of privacy on data, denial of access to internet resources and propagation of counterfeiting.

To likelihood of successful attack in the context of end-user computing, this paper benchmarks against the specified three sub-variables as per the AICE guidelines:

Threat (T) this applies to end-user computing without modification.

Vulnerabilities (V) this will refer to the access in terms of the software, where the felon or third party (the buyer of the stolen device) is enhanced the re-use of a device by flashing and installing it with a counterfeit OS, or side - installing it with another OS.

Target attractiveness (Ar) computing devices are on the high end of value worldwide. They are quick to sell in the underworld market. The felons can sell the devices at extremely low prices relative to their actual costs, causing terrible losses to their genuine owners.

3. The Security Concerns and Developments in Industrial Computing

Security in the cyber space is an ever evolving and expanding conceptual phenomenon, thus outgrowing the defense provided by the aged technologies of back-ups and firewalls. Mobile computing, cloud computing, smartphones and tablets, are changing the business landscape, where personal computing is gradually getting integrated in business processes. Consequently, risks related to data tampering, integrity, confidentiality, loss, theft and authentication of devices requesting services [19] are increasing in intensity.

With time, security issues have developed complexities, necessitating for the development of new reasoning and imagination dimensions. Literature is rich with security issues and threats as perceived and tackled by IT professionals in relation to software, hardware, and corporate data. The professionals and providers of technology, such as developers of SW and electronic devices, are rigorously active in devising defensive strongholds for their ingenuity and their corporate clients. Software piracy, hardware cloning, counterfeiting, and side-channel attacks as outlined by Rose, McDonald, Yan and Wysocki [14] or Rostami, Koushanfar, and Rajendara [16] are the common issues of concern for developers. The study involving organizations' IT professionals conducted by the Computer Economics [3], in the fourth quarter of 2006 identified malware, phishing, pharming, spam, denial of service and unauthorized access by outsiders and insiders as the prevalent security concerns of business organizations. Others are sabotage and fraudulent transactions. Relatively recent are the security risks paralleling cloud computing and cloud sourcing in the cyber space [10, 19, 20, 21]. According to the study report by the Computer Economics above, organizations did not think the physical loss or theft of

computer hardware to pose as a serious threat. This can be explained by the fact that most of the computing devices at the time of the study were stationed in facilities such as office buildings which could be physically protected. The situation is different with personal computing as it can be seen elsewhere in this text.

In the organizational settings, the challenges to chief security officers (CSO) or chief information security officers (CISO), the corporate executives responsible for the protection of people, assets, infrastructure, technology, and implementation of information security programs, include maintaining proactive mechanisms for thwarting security threats to their organizations. The officers are expected to always think ahead of time, and never ignore any security alarm. For instance, it is not a surprise that the impacts of the '*Wanna Cry*' ransomware attacks [1] are hinged on the misuse of '*blockchain*', the source code of '*bitcoin*' technology capabilities that provide "a way to record transactions as automated trusted activity among digitally networked peers" [11].

Good for industrial computing, there is a constant watch on security issues by the security experts in IT. This is evidenced by literature and a multitude of websites dedicated to gathering, expert sharing, and dissemination of information on emergent threats and possible solutions such as the Computer Weekly. com, Tech Target, Search CIO. com and many others. What is the situation at personal computing level? This question is attempted in the next section.

4. The Conceptualization of End-User Security Issues in Developing Countries

Security concerns emanating from the context of end-users computing in developing countries is a factor of human behavior outside computing processes. This means, unlike in the crafting of viruses, Trojans or other malicious software and data hacking attempts, it is human action such as theft and facilitation of dispossession of hardware that poses serious cyberspace threats in developing countries, especially in Africa. Elaboration on the phenomenon is provided here under by focusing on end-user computing levels first, then how security threats therefrom impact on industrial and mainstream computing.

Human Behavior in End-user Computing Levels

End-user computing is at two levels. The first is where employees of organizations use their mobile personal computing devices for undertaking organizational business processes [6]. In this case, what happens to the end-user's device may pose a direct or indirect threat to the respective employee's organization data. Here the device plays the third-party resource role, leading to 'third party' security risk [19]. A case in point is where, for instance, a device gets stolen. The felon can access any stored files by simply installing the device with a parallel Open Source Operating System, if the formally resident OS was any vendor provided resource. The scenario is observed in one of IBM's white paper as thus; "in today's '*industrial computing*' (the original term was '*mobile enterprise'*), the lines are blurred between personal and corporate assets, and IT organizations have to do much more than simply protect a corporate-owned device" [7].

The other level is where the end-users use personal computing devices for personal transactions. This may range from accessing personal email accounts, to participation in social media, politics, and e-governance, and to conducting financial transactions. As observed by James & Versteeg [8], personal computing has of long been a crucial mode of communication and welfare enhancement in poor countries. Reports are plenty on how the phenomenon has actually become a potential changer of lives in the areas of finances, education, health, activism, agriculture and others [10]. Personal computing has significantly promoted 'digital economy' on the continent of Africa in the tone of 6.7 per cent of GDP in the year 2016, and projected to increase to about 7.6 per cent by the year 2020 according to the GSMA report [5]. The report further states that 46 per cent of the population of Africa, that is about half a billion people, is subscribed to mobile computing services. In essence, mobile services are inseparable with personal computing in Africa.

Side two of the coin is the fact that there is a software industry driven factor that is progressively impacting on human behavior by developing relationship bonds of intimate type between users and their personal computing devices. It can be easily observed that the 21st century kind of relationship between computing devices and their owners is far different from the 20th century and before. Two factors explain the scenario: (1) there is a lot of data build up in the personal computing devices. They include passwords, sensitive data such as banking and transaction records, and other attributes which tend to connect users to services automatically. (2) The design side is continuously binding owner-users to their devices through advancements in software technology. In advanced computing environments, devices tend to learn the attributes of their users such as passwords and email accounts. Cases are there for instance, that it is impossible to log into personal email accounts from different devices other than own. In addition, the progresses being made in cloud computing are requiring for more to justify connectivity to include the identity and authenticity/genuineness of login to the cloud at the levels of HW, SW, and '*perhaps a user in person in the future'?*

Obviously, as the digital economy continues to grow rapidly in Africa, the post IT adoption issues among the technology stakeholders globally are also evolving beyond the ordinary digital divide. In the contemporary, the advocacy of the Technology Acceptance Model (TAM): perceived usefulness and perceived ease of use [4] as pushers of technology into communities remain relevant but phasing out. Thanks to the 'evolving' nature of the 'information society' concept of the WSIS [22] which takes it to different levels with phenomenal progresses. It includes in its targets, "to address new challenges of the Information Society, at the national, regional and international levels" [22, 23]. This guarantees the taking security concerns of the nature in

context on board of the international forum.

End-user Based Security Threats to Mainstream Computing

Theft is the number one human behavior threat in the cyber space of the developing world. This was shown to be a potential opening for breach of data in industrial computing elsewhere in the document. On the other side, the theft of personal computing devices in the low income population of the world, or the developing countries, is an opening for the security concerns of IT developers and providers in *mainstream computing* as well. To the poor end-user in developing countries, the theft of a device has an added factor to the loss of property, and that is the propagation of the continued use of counterfeited objects such as hardware and software. This works as follows: (1) Cloned hardware provides a cheap source of replacement for the victims of theft. As simple as that. (2) Counterfeit software are used by the culprits in the theft chain. The thieves install such SW on stolen devices to overwrite or destroy the authenticity of the genuine owner and facilitate the re-sale of the stolen devices. The process is simple because, by assumption, there appear to be lack of at least authentication/authorization mechanisms to prevent rogue control at the hardware layer, or resist the illegal installation.

5. Scaling on HW Security Technological Capabilities: Some Optimism

There is a pack of initiatives in place already to provide protection against human malpractices in cyber space. Tracking technology such as offered by Preyproject [12], Insurance of mobile devices [13], back-ups and so on, cite examples. However, the features of these measures are such that they are built on reactive perspectives. This paper suggests that the IT security professionalism should aggressively push towards the intersection of two knowledge spheres: the knowledge of the properties of physical objects, and the knowledge of human behavior. For instance, it makes a difference if the would be culprit knows that it is impossible to re-use a device with changed features such as OS.

Standing on the progress so far made in the field of hardware based security techniques such as expressed by Majzoobi, Koushanfar and Potkonjak [9], this paper calls on design science to build technology with appropriate security tests for owner authentication before any changes such as disk formatting, installation of a parallel OS or reading the stolen device's HDDs can be accepted, failure of which the device is self-destroyed. The effect of such measures is not only to discourage theft for anticipation of easy re-use, but also to soothe the victim by knowing that it is not possible to benefit from the crime apart from loss of data and intimacy.

The concept related to specific unique identification of HW [14] or the technology used in 'microcontrollers' which use technology that "prevent unauthorized user from reading or modifying selected sections of its memory" [15 p. 1283] are the cases in point which could revolutionize end-user security tremendously. The unique identification of HW technology in mainstream computing could be made to function at the end-user layer between a device and the user. In the same manner, it is possible to develop HW based technology for the prevention of unauthorized access to devices' memory in levels. For the sake of scope limit, the reader is referred to the original works respectively for a detailed coverage. In essence, this paper sees HW security technology as bringing with it the possibility for designing a security model with mechanisms to hold and test security parameters that can restrict un-welcome malicious overwrites in unlawfully appropriated devices.

6. Conclusions

The main issue in this paper was to sensitize for security concerns at the level of end-user and personal computing. The paper used the American Institute of Chemical Engineers' guidelines to conceptualize for security risks in end-user computing dimension, then used the framework to explicate security exposures towards industrial and mainstream computing planes.

The paper went on to explore the contemporary potentials of technology to contribute towards improving end-user protective security, then challenged the design science class of IT for HW based security technology that would impose stringency on human malice to propagate security threats, as a way of reducing vulnerability of electronic devices at the human layer in the computing world.

In the end, the paper points at taking technological security issues developed in this paper as the future practical work in IT design science.

References

[1] BBC NEWS. (n. d). WannaCry ransomware cyber-attacks slow but fears remain - BBC News. Retrieved May 16, 2017, from http://www.bbc.com/news/technology-39920141.

[2] Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*. Retrieved from http://www.jstor.org/stable/249008.

[3] Computer Economics, (2007). *Trends in IT Security Threats: Executive Summary*. Retrieved from http://www.computereconomics.com/article.cfm?id=1214.

[4] GSMA. (2016). The Mobile Economy: Africa 2016. *GSMA Annual Report*, 1–66. Retrieved from https://www.gsmaintelligence.com/research/?file=3bc21ea879a5b217b64d62fa24c55bdf&download.

[5] Hill, M. C, & Alan, B. W. (2011). End-User Computing Applications. *The CPA Journal*, *7*, 67–71.

[6] IBM. (2017, April 27). A solution that addresses 4 key mobile security challenges. *Data Center and Virtualization Media Group*, p. 6. Retrieved from http://www.bitpipe.com/fulfillment/1481916529_964.

[7] ITU. (2011). *Measuring the WSIS targets - a statistical framework*. *ITU*.

[8] James, J, & Versteeg, M. (2007). Mobile phones in Africa: How much do we really know? *Social Indicators Research*, *84*(1), 117–126. https://doi.org/10.1007/s11205-006-9079-x.

[9] Majzoobi, M, Koushanfar, F, & Potkonjak, M. (2008). Testing techniques for hardware security. *Proceedings - International Test Conference*, 1–10. https://doi.org/10.1109/TEST.2008.4700636.

[10] Ogunlesi, T; & Busari, S. (n.d.). Seven ways mobile phones have changed lives in Africa. Retrieved May 29, 2017, from http://edition.cnn.com/2012/09/13/world/africa/mobile-phones-change-africa/.

[11] Olavsrud, T. (n.d.). Top 4 security trends of 2016 | CIO. Retrieved May 16, 2017, from http://www.cio.com/article/3152347/security/top-4-security-trends-of-2016.html.

[12] Preyproject. (n.d.). Device tracking and protection. Retrieved May 17, 2017, from www.preyproject.com.

[13] Ratemo, J. (n.d.). Kenya's smartphone owners turn to insurance. Retrieved June 6, 2017, from http://www.biztechafrica.com/article/kenyas-smartphone-owners-turn-insurance/9522/.

[14] Rose, G. S; McDonald, N; Yan, L. K; & Wysocki, B. (2013). A write-time based memristive PUF for hardware security applications. *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 830–833. https://doi.org/10.1109/ICCAD.2013.6691209.

[15] Rostami, M; Koushanfar, F; & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, *102*(8), 1283–1295. https://doi.org/10.1109/JPROC.2014.2335155.

[16] Rostami, M; Koushanfar, F; Rajendran, J; & Karri, R. (2013). Hardware security: Threat models and metrics. *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 819–823. https://doi.org/10.1109/ICCAD.2013.6691207.

[17] Rouse, M. (n.d.). Security. Retrieved June 6, 2017, from http://searchsecurity.techtarget.com/definition/security?utm_content=control&utm_medium=EM&asrc=EM_ERU_76877080&utm_campaign=20170510_ERU Transmission for 05/10/2017%28UserUniverse:2366898%29&utm_source=ERU&src=5633804.

[18] Sparapani, J. (n. d). Signs point to cloud future at Red Hat Summit 2017. Retrieved May 10, 2017, from www.searchcio.techtarget.com.

[19] Subashini, S, & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. Retrieved from http://www.sciencedirect.com/science/article/pii/S1084804510001281.

[20] Tan, B. (2016). Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective. In C. Heinl & E. Tan (Eds.), *Cybersecurity: Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond* (pp. 19–26). Singapore: RSIS.

[21] Wang, E. K; Ye, Y; Xu, X; Yiu, S. M; Hui, L. C. K; & Chow, K. P. (2010). Security Issues and Challenges for Cyber Physical System. *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, 733–738. https://doi.org/10.1109/GreenCom-CPSCom.2010.36.

[22] WSIS-03/GENEVA/DOC/9-E. (2004). *REPORT OF THE GENEVA PHASE OF THE WORLD SUMMIT ON THE INFORMATION SOCIETY GENEVA - PALEXPO, 10 - 1 2 DECEMBER 2004*. Geneva. Retrieved from https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009!R1!PDF-E.pdf.

[23] WSIS-05/TUNIS/DOC/9(Rev.1)-E. (2006). *Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16-18 November 2005*. Tunis. Retrieved from http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf.