УДК 004.051

ОБЗОР ЗАДАЧ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

ТИАМИЙУ А. ОСУОЛАЛЕ

Еще недавно цифровая безопасность не рассматривалась в качестве дела, затрагивающего каждого, но в наши дни всякий осознает важность безопасной работы вычислительных и сетевых систем. Это имеет важное значение, т.к. многие стороны нашего бизнеса и частной жизни опираются на вычислительные и телекоммуникационные сети. Безопасность телекоммуникационных сетей способствует доверительным отношениям между заинтересованными сторонами. В статье представлен обзор задач, стоящих перед безопасными телекоммуникационными сетями, и предлагаются пути решения обозначенных задач.

сетевая безопасность; кибербезопасность; электронная коммерция; информированность и подготовка в области безопасности.

AN OVERVIEW OF MODERN TELECOMMUNICATION NETWORKS SECURITY CHALLENGES

TIAMIYU A. OSUOLALE

ABSTRACT

Not long ago, digital security was not seeing as everybody's business, very unlike nowadays when everyone believe that it is imperative that computing and networking systems operate securely. And this is of utmost importance as many aspects of our business and private life rely on computing systems and telecommunication networks. Telecommunication networks security promotes trust among stakeholders. This paper presents an overview of challenges facing modern telecommunication networks security and suggest ways forward at facing those challenges.

Keywords: network security; cyber security; e-commerce; security awareness; security training.

Telecommunications is greatly aiding globalization, and globally telecommunications networks are seen as critical infrastructures in the society these modern days. And as dependent on telecommunication networks grows, so also the users' perception of treats. Though according to user acceptance of services, and consequently generated revenue by the operators, the vast majority of mobile users in the world use their mobile phones mostly for voice communications and to some extent, SMS, and while in the least, for data services [1]. A gradual increase in data service access is expected as there are vast increase in data traffic associated with e-commerce, web-applications and online services. Owing to these and the fact that the Internet is being used as a tool for business communication, usage of Internet which relies on telecommunication networks is ever increasing; and this exposes hundreds of millions of people worldwide to treats and risks as Internet is vulnerable to cyber-attacks. This furthermore makes telecommunication networks security (TNS) a top issue to deal with now and in the future.

The telecommunication network security deals with the security of communications within LAN, WAN, WLAN and other networking domains. It focuses on solutions against attacks on telecommunication networks to ensure service availability, integrity and confidentiality.

Distinctively TNS are infrastructure and content based. A network infrastructure security includes physically securing network devices and also preventing unauthorized access to the management software that resides in them. While content security refers to protecting the data being transmitted over the telecommunication network(s) and the data stored on attached network devices.

There are several methods of ensuring that telecommunication networks are secured. Among them are:

communication among hosts in a network may be encrypted to ensure privacy.

via firewall and authentication procedure.

physically monitoring of telecommunication networking devices and deployment of surveillance and early-warning tools in telecommunication networks e.g. honeypots, honeynet, honeytoken, padded cell, IDS, IPS, decoy, etc.

In B2C e-commerce, online businesses attempt to sell products or provide services to end-user online. In business world of today, B2C has grown persistently being the type of e-commerce (transactions via telecommunication networks that cross organization boundaries) that most consumers are likely to encounter. B2C worldwide sales expected to reach $1.2 trillion in 2013 according to eMarketer [2]. Presently Internet is available everywhere, anytime and boundaries are already removed via mobile devices. In other words, the market-place is extended beyond traditional geographic location as it can be created virtually anywhere for shopping to take place. Globally now via telecommunication networks, market-space includes potentially billions of consumers and millions of businesses worldwide. Nevertheless level of trust by consumers greatly affects the usage of telecommunication networks services [3]. Though online credit cards usage reduces cash on hand and cash handling time, costs, likelihood of theft and pilfering; yet consumers want to believe that the online transaction service is highly secured. Their perception of risk greatly influences their willingness to patronize online services. All these and more call for provisioning and maintaining secured telecommunication networks globally.

About 2.7 billion people are using Internet worldwide presently [4], and this aids economic growth of nations; and as usual national economic growth raises consumer expectations and the standard of living. Consumers tend to like mobile gadgets with Internet access as this enable them to be wherever they want while still being able to better utilize more of applications and conveniently using/rendering services on Internet. This has contributed immensely to high rate at which people worldwide subscribe to mobile cellular services. Table 1 shows how mobile-cellular telephone subscriptions has increased greatly over the last decade in countries like China, Kenya, Nigeria and Russia.

Table 1: Mobile-cellular telephone subscriptions from 2002 till 2012 according to ITU

	206,005,000	1,187,122	1,569,050	17,608,756
	269,953,000	1,590,785	3,149,473	36,135,135
	334,824,000	2,546,157	9,147,209	73,722,222
	393,406,000	4,611,970	18,587,000	120,000,000
	461,058,000	7,340,317	32,322,202	150,674,000
	547,306,000	11,349,412	40,395,611	171,200,000
	641,245,000	16,303,573	62,988,492	199,522,340
	747,214,000	19,364,559	74,518,264	230,050,000
	859,003,000	24,968,891	87,297,789	237,689,224
	986,253,000	28,080,771	95,167,308	256,116,581
	1,100,000,000	30,731,754	112,777,785	261,886,329

Latest technology has allowed for high speed Internet access over mobile phones and other mobile gadgets, and this has led to continual increase in the percentage of individuals using Internet globally. Table 2 shows this percentage increase over the last decade for countries like China, Kenya, Nigeria and Russia.

Table 2: Percentage of Individuals using the Internet from 2000 till 2012 according to ITU

	1.78	0.32	0.06	1.98
	2.64	0.62	0.09	2.94
	4.60	1.21	0.32	4.13
	6.20	2.94	0.56	8.30
	7.30	3.02	1.29	12.86
	8.52	3.10	3.55	15.23
	10.52	7.53	5.55	18.02
	16.00	7.95	6.77	24.66
	22.60	8.67	15.86	26.83
	28.90	10.04	20.00	29.00
	34.30	14.00	24.00	43.00
	38.30	28.00	28.43	49.00
	42.30	32.10	32.88	53.27

The rapid increase in the Internet usage is being engineered by telecommunication networks that has removed various barriers which, until recently, has hindered fast and easy access to information or data worldwide. Notwithstanding, the same telecommunication networks are excellent avenue for evil-minded and or very curious individual (hackers, individual or organization or nation that are obsessed with having super-control) to spy, hijack, modify or delete information/data being transferred on telecommunication networks from user to receiver. This poses a very serious threat to our existence as presently we depend on these telecommunication networks to great extent, and in the nearest future, we would to a greater extent. And as a result of these challenges that could cause a serious havoc or even real war among nations, many nations are declaring war on cybercrimes; believing that there is need to have control over cybercriminals who are undermining the global socio-economic and political gains being globally achieved and still being achieved lately via telecommunication networks usage.

Stability in global economy is at stake. For instance, being a nation with 100% geographical coverage with all possible methods of payments has online retail in total retail amounted to approximately 2% in 2012. And the forecast is that this could amount to 6% by 2020. Russian e-commerce could represent a market of up to $150 billion within 15 to 20 years considering the scope of e-commerce extending to cheaper product categories, mass demand for nonmaterial products such as insurance and tour package offers, growing investments in the regions, improvements in delivery across Russia, and lower online prices [7].

B2C E-Commerce is growing fast in and it is expected to grow by more than 30 percent annually between 2010 and 2016 as B2C e-commerce with luxury goods is one of the leading trends. Social commerce is expected to become even more significant in China than in the USA [7].

has experienced a phenomenal growth in the percentage of individuals using Internet from 0.32% in 2002 to 32.88% in 2012, and mobile-cellular telephone subscriptions from 1,569,050 in 2002 to 112,777,785 in 2012 [5,6]. This trend has brought about a monumental development in the major sectors of the economy, e-commerce. But as number of individuals using Internet is getting higher and continues to increase, the B2C e-commerce would be gaining ground. Moreover the federal government of Nigeria has emphasized on

cashless economy which implies that e-commerce grows fast in the nearest future. Internet use by one third of the population of Nigeria is expected for 2013, with wireless broadband spreading in the country by 2015 According to yStats [7]. Nigeria's e-commerce sector is still in its infancy though, yet it is growing rapidly. Recently various e-commerce platforms sprang up in Nigeria some of which are Jumia.com, Konga, Buylocalthings.com, Wakanow.com, and worldmartafrica.com. In December 2011, Nigeria has over 40 million Internet users already, the highest in Africa [8].

In with internet penetration of 16.2 million (about 40 percent of the population); e-commerce and other ICT applications have become enablers for development. A revolution in mobile money transfer has occurred in Kenya. Over 90% of the population has a phone and 96% of mobile phone users has used a handset to make a mobile payment or for m-banking [9]. Presently there are many local payment platforms that have integrated payment methods that work for and in Kenya. Some of these payment platforms are Pesapal, the most popular payment platform in Kenya, Ipay which is well-known among merchants, and Jambo Pay. Kenyans now use their phones to pay not just for electric bills but also taxi fares, get cash or even buy produce and other essentials in rural markets [10]. More and more Kenyans go online, the future of e-commerce in Kenya is very promising but at stake as could-be victims of Internet fraud/cyber-attacks are also many and are increasing in number; and this explained why Kenyan government declared war against cybercrimes [11]. Kenya showed strong growth potential. In 20011, it was the fastest growing Internet market.

Considering the above and the fact that presently about 2.7 billion people are now on the Internet; and out of about seven billion people in the world today, $^{2}/_{3}$ is now with mobile phones [4]. Though the sales volume of online retails in countries like Nigeria and Kenya is yet insignificant compared to that of Russia as at 2012, yet all these nations e-commerce is fast growing. In China, online retail sales accounted for 4.3% of the total retail sales in 2011, and are set to reach 6.3% by 2015 [7]. Being that China has the largest online population in the world (538 million as of June 2012), the market size of the online retail market in China is ever increasing, it is expected to overtake the US online retail to become the largest in the world by 2013 [12]. As Cyber-attacks are increasing with little sign of abatement; and as intruders/attackers will never stop trying to compromise systems to obtain valuable customer and private users' information, the growth of online retails worldwide is under a serious threat that could cripple financial world globally. Another thing that could cause disaster is that people are not so much security-conscious; unlike in pc environment where people do most at time use certain software to analyze and secure their networks, the case is not so in the people's usage of mobile gadgets. End-users or customers are relying most at time solely on the service provider for security when it is obvious that e-payment, like any other means of financial transactions, is vulnerable to criminal activities; and that societal, political and economic impacts of cyber-attacks could be very disastrous.

: When not available locally, the importation of telecom equipment may lead to supply chain contamination should malware be embedded in such equipment; and this could happen despite proper security scrutiny of the telecommunication networks' infrastructure.

: While owing to need for better security maintenance of telecommunication networks infrastructure and the fact that investments are fixed, sunk and irreversible, with a high risk factor; sharing of telecom infrastructure among telecommunication service providers could be a good strategy to combat cyber-crimes. This would allow for better and joint monitoring, better bandwidth usage and reduced costs on operation, research and training that could as well facilitate improved innovation, better and reliable services to consumers. The degree and method of infrastructure sharing can vary depending on stakeholders and competitive climate.

Sharing of telecommunication infrastructure among others could be active sharing (sharing of electronic infrastructure in the cell

site), passive infrastructure sharing (sharing of non-electronic infrastructure), mast sharing (sharing of a mast) or site sharing (sharing of a site).

Nowadays, computing products' live-cycles are very short due to the fact that competition is fierce. Products Manufacturer are endlessly eager releasing their products to the market ignoring or overlooking to some extent interactions problems with other available products in the market; and this may lead to vulnerabilities of products. These vulnerabilities normally give chance to exploitation of the products by hackers/intruders. Also development of many versions of particular products in a short period of time requires training and re-training of the users of the products. This may bring about security challenges as it may be difficult to cope with the rate at which new version is appearing in the market. It may require a steep learning curve as the new version may expose the vulnerabilities of the old version via interoperability and interconnection thereby making it compulsory to switch to new version.

Despite the fact that security awareness and training have serious implications on ICT generally, they are most at time being overlooked. And as such valuable data/information is lost sometimes; and organization and even government are put to shame online; the case of Nigerian government website, www.nigeria.gov.ng, hacked on Thursday, July 18, 2013 [13]. The case of loss of the medical records of tens of thousands of patients by NHS, UK in 2009 [14]. Training and re-training of personnel in the telecommunication sector on TNS challenges every now and then are a necessity; as failure to do so for one reason or the other, could make personnel do sometimes fail to deal adequately with security issues. Training creates awareness that in turn is an avenue to build high level of commitment and dedication required to tackle telecommunication networks security challenges favorably and professionally.

Standardization is hard to achieve in the domain of open source software because the open source software's providers are completely free in their choice of design, implementation or adherence to existing standards. Usually standardization is enforced by market forces and industry regulators, however in the case of open source software both these factors do not exercise enough pressure to drive the process. And as such open source software lacks strict adherence to standardization and this could amount to vulnerabilities since it has to interact with other software.

E-commerce has come to stay, and everybody is willing to participate and enjoy all the goodies it brings. E-commerce is possible only via telecommunication networks which are prone to attacks. The telecommunication networks serve as medium for fastest exchange of valuable information that mischief-makers may always be after, therefore security challenges posed is highly recognized by stakeholders (industry, government, operators and equipment vendors) and it is being accepted that security is a crucial deployment consideration for future telecommunication networks wherever they are in the world.

And the fact that no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures; and to carry all the related responsibilities implies that collaborative effort is what is needed to address the challenges. Moreover recent development, where employee access corporate data right at home or from any geographical point, provided there is a telecommunication network available there, is changing the approaches to modern TNS challenges. It is calling for unified and sophisticated measures in ensuring security over telecommunication networks globally.

Since the importance of TNS is of paramount importance to all, then the need for international collaboration ought to be generally accepted. And this collaboration could be through information exchange about emerging vulnerabilities and active attacks on telecommunication networks. Thus there is need for

multi-lateral co-operations and partnerships to ensure critical telecommunication networks' infrastructure protection; as well as the need on data protection framework and policies to be revisited often.

i. A basic general level of security where emphasis would be laid on combating and protection against cyber-crimes needs to be implemented in telecommunication networks globally, and also it has to be assessed and acknowledged.

ii. All stakeholders, consumer inclusive, must be enlightened, trained and re-trained to increase their level of awareness and to embrace secured networks; and to use more reliable among available security options.

iii. There must be continual improvement on TNS Systems by studying during and after an attack the techniques used by the attackers that attempt to compromise telecommunication networks to keep an eye on new exploitation techniques so as to use such analysis for further tightening of security of telecommunication networks. And this is best achieved via research project on attack analysis and counter-measures based on collaborative approaches of stakeholders globally.

iv. Security must always be inculcated right from initial stage of process during development of protocols/standards for telecommunication networks, as it is in this stage that vulnerabilities are sometimes born.

v. Government should actively disseminate information to consumers regarding the reliability of service providers by reliably collect statistical data on the operation, consumer views and adherence to security rules and other regulations by the service providers.

vi. A global understanding of the risks and a global coordination strategy; as well as global risk management are very necessary to be achieved as counter-measures to future security breaches on telecommunication networks.

vii. A full lifecycle security plan should be implemented by all developers, particularly those in the e-commerce industry for protection against any form of attacks including zero day.

viii. Consumers must be enlightened for transparency and acceptability reasons; and well-trained about the usability of the security mechanisms so as to be able to control the leakage and exploitation of data.

ix. Double standards' policy in TNS from the side of stakeholders, especially government, should be avoided.

x. The primary forms of host-to-host authentication on the telecommunication networks has to be strong considering that presently most of these authentications are name-based or address-based, both of which are extremely weak.

In the area of active mobile broadband penetration, the 2013 ICT Facts and Figure showed that mobile-broadband subscriptions annual growth, since 2007, is 40%; and has climbed from 268 million in 2007 to 2.1 billion in 2013. This reflects that online community is fast growing; but so also level of impacts of TNS breaches on the global economy and people's life generally.

The consumers have to be stopped from erroneously believing in what actually constitute the TNS problems. Like for instance, recent research on network security trends by Nuspire Networks revealed that though network reconnaissance is on the rise, yet the virus that do normally get almost all the attention represent just 0.08% of all investigated security events. Nuspire Networks' research group 'white hat labs' found out that port scanning incidents have risen and that cases of automated credential guessing, vulnerability being faced by business that use web-based applications, are doubled [15]. Also that out of 4.8 mln severe alerts generated during the survey, only 29% were caught by firewall IDS/IPS systems which most providers do rely on for network monitoring.

Obvious that individual/organization/nation that knows one's secret can use same for his/her/its personal gain/interest, and this explained why some nations actively engage in spying deals around the world. So considering the changing dynamics of the threat landscape associated mostly with socially engineered hacks and interest of some nations, telecommunication networks need to be modernized to meet these data security challenges that are persistently advancing. And government

should seek for the TNS experts locally among citizenry, motivate such experts to be patriotic and solely rely on such for national data security policies' implementation. Furthermore TNS deserves be given highest priority when considering telecommunication networks' creation and expansion.

Telecommunication network is now a part of our basic social amenities. This makes it a paramount to aforehand prepare for TNS challenges. There is need for strict adherence to TNS best practices since the number of could-be victims of cyber-attacks would continue to increase globally. Whatever we do, we are bound to face challenges; nevertheless, these challenges whenever they surface should not make us fall back to old era when we relied solely on typewriters and post masters. World and world commerce seem to have outgrown this. Thus our preparedness, awareness and prevention mechanism against present and future security challenges of telecommunication networks is of paramount importance. And each nation should actively and collaboratively participate in this challenge that is directly facing telecommunication networks and thus indirectly facing world economy; otherwise the aftermath could cripple the economy if not given the degree of attention required now and always.

1. Kevin Fitchard. (in press). 2013: The year mobile data revenue will eclipse voice in the US. Retrieved from http://gigaom.com/2013/03/13/2013-the-year-mobile-data-revenue-will-eclipse-voice-in-the-us/.

2. E-marketer. (20103). B2C Ecommerce Climbs Worldwide, as Emerging Markets Drive Sales Higher. Retrieved from http://www.emarketer.com/Article/ B2C-Ecommerce-Climbs-Worldwide-Emerging-Markets-Drive-Sales-Higher/ 1010004.

3. Keneth C. Laudon and Jane P. Laudon. (2007). Managing the Digital Firm. International Journal of Computers, Communications & Control Vol. II, No. 1, pp. 103-105.

4. ITU. (2013). ICT Facts and Figures [PDF file]. Retrieved from ITU website:http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013. pdf.

5. ITU. (2013). Mobile-cellular telephone subscriptions [Excel file]. Retrieved from ITU website: http://www.itu.int/en/ITU-D/Statistics/Documents /statistics /2013/Mobile_cellular_2000-2012.xls.

6. ITU. (2013). Percentage of Individuals using the Internet [Excel file]. Retrieved from ITU website: http://www.itu.int/en/ITU-D/Statistics/Documents /statistics/2013/Individuals_Internet_2000-2012.xls.

7. yStats. (2013). Global B2C E-Commerce and Online Payment Report 2013 [Brochure]. Retrieved from http://www.ystats.com/en/reports/preview.php? reportId=1033&start=0.

8. yStats. (2012). Africa Internet & B2C E-Commerce Report 2012 [Brochure]. Retrieved from http://www.ystats.com/en/reports/preview.php?reportId= 939&start=0.

9. Biztech Africa. (2013). Kenya Internet users surpass 16 million. Retrieved from http://www.biztechafrica.com/article/kenya-internet-users-surpass-16-million /5806/.

10 Dr KF Lai. (2013). Africa finding its own solutions using mobile tech. Retrieved from http://www.bizcommunity.com/Article/111/394/88287.html.

11. CCK Kenya. (2013). Kenya Declares War on Cybercriminals. Retrieved from http://www.cck.go.ke/news/2013/War_on_cybercrime.html.

12. iResearch. (2013). 2012-2013 China Online Shopper Behavior Report. Retrieved from http://www.iresearchchina.com/reports/4830.html.

13. Premium Times Nigeria. (2013). Gay Activist Hacks Nigerian Government's Website Over Country's Anti-Gay Law. Retrieved from http:// premium-timesng.com/news/140270-gay-activist-hacks-nigerian-governments-website-over-countrys-anti-gay-law.html.

14. The Telegraph UK. (2009). Thousands of NHS medical records lost. Retrieved from http://www.telegraph.co.uk/health/health-news/5381605/Thousands-of-NHS-medical-records-lost.html.

15. PRWeb. (2013). Nuspire Networks Study Reveals Rise in IT Network Security Vulnerabilities at Remote Locations. Retrieved from http://www.prweb.com /releases/2013/nuspire/prweb10873482.htm.