Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

DOI: 10.25045/jpis.v06.i2.09

SECURITY TRENDS IN MODERN COMPUTER NETWORKS

The article analyses the trends in the security of computer networks (CNs). The trends in the infrastructure, applications and usage *of CNs are analysed. The effects of these trends on CN security are analysed. This paper finds that the determination of CN security trends can help uncover new security threats and deal with them effectively.*

Keywords: *computer security, computer networks, security trends, threats.*

Introduction

The scale and complexity of the first computer networks (CNs) was limited, but as information and communication technology (ICT) rapidly developed, CNs have been widely applied in various sectors of society, such that society has become gradually dependent on CN. In addition, the complexity and scale of CNs have expanded. Today, the use of ICT-based services and applications is expanding and those services have become more intelligent and mobilised. Service development and convergence are occurring as available CNs become multi-service, multimedia networks rather than database networks; at the same time, new network architectures have developed and network access technologies have advanced. In addition, the convergence of local and global networks and computer and telecommunications networks has occurred. The above-mentioned technologies, services and applications have penetrated various spheres of modern society including human relations, economics, education, health and finance, and have a direct impact on their growth. Therefore, the safety of available CNs and communication infrastructure is a very important issue. As new threats emerge, the security of the society depends on the security of available ICT. In these circumstances, detecting and eliminating new threats in CNs is very important to ensure the safety of the society, and thus security trends must be identified. These trends are closely connected with the development trends of CNs (i.e., the Internet). Security trends in CNs are security-related changes (the emergence of new vulnerabilities, threats, and attacks) due to the development of infrastructure, applications and usage over time. These trends should be comprehended as soon as possible, in real time and for the longer term. The elimination of threats, the fight against cyber-attacks, and the solution of other security issues is very difficult without identification of these trends. The goal of this article is to analyse the trends occurring in modern CNs, and to identify and analyse safety trends on the basis of previous analyses.

Development trends of computer networks

The security trends of any field are identified by the classification and analysis of development trends of that field. Therefore, this section analyses the development trends of CNs. Several development trends of CNs can be distinguished including infrastructure, applications and usage trends.

The development of the Internet can be divided into three phases. The first phase covers the period of 1969–1992. Research networks, in particular, telnet, email and file transfer services were established and used in this phase. At this stage, the number of network and service users and the volume of network traffic were small. In addition, people with computer skills were mostly working in isolated places. For example, in 1969 the ARPANET was developed in the US, where it was required to be connected to the ARPANET IMP (Interface Message Processor) to join any host in the network. In the 1970s, ALOHANET, connecting universities in Hawaii, was established as a satellite network [1]. The second phase covers the 1990s when commercial services and service providers emerged and Web and P2P services began to be used.

Accordingly, the number of networks and users and the volume of network traffic increased rapidly. The main problem was related to transmission capacity. The third phase covers the present time. Today, services are evolving and converging (Internet/telecom/media). The use of networks and services is expanding; their intelligence is growing and mobilised. New network services (cloud computing, payment card industry, internet banking, etc.) have been developed with the increase in computing power. A large volume of content and multimedia services are now available on the Internet. New network technologies (e.g., mobile technologies) have appeared, and new network architectures and network management technologies (e.g., web-based management technology) have formed. As a result, the number of Internet users and the volume of traffic have significantly increased. In these circumstances, traditional IPv4 protocol started to cause scaling and routing problems. Therefore, the IPv6 [2] version of the Internet protocol was applied to ensure effective routing, high quality services, mobility and security. IPv6's capability to provide a large address space led to the formation of the concept "Internet of Things" [3]. By 2020, 50 billion devices will be connected to the Internet by 2020, 6 billion of which are mobile phones, Ericsson Company predicts. Currently, routers, firewalls and other critical devices do not include the security functions of IPv6, and the lack of IPv6 experience means that most providers are slowly transitioning to IPv6 from IPv4 or running them in parallel.

The development of broadband networks and the increased demand for the network-based services and their delivery rate have led to the creation of a new access infrastructure. Broadband mobile GSM networks ensure high-speed transmission. The wireless local area network (WI-FI) [4, 5] and WiMAX [6], and NFC [7] have emerged.

Today, the concept of the cognitive network is often used in the literature [8, 9]. Emergence of cognitive networks could be one of the most important steps taken for the effective and autonomous management of complex networks. This kind of network architecture uses cognitive processes to assess the current reality, predict and plan for the future, and provide appropriate operations. Cognitive networks can think, learn and remember.

CN infrastructure expansion (widespread use of broadband wired and wireless networks), the rise of computing power and the growth of memory technology makes it possible to develop real-time virtual computing and storage infrastructure, and to implement web-based computing or cloud computing. Internet-connected users located anywhere in the world can access computing and memory resources. Data centre virtualisation is not a new concept, and today these centres provide the virtualisation of servers and other resources (e.g., switches, routers and storage facilities) as well. Virtual resources connect certain physical resources, which can be accessed from anywhere in the world, ultimately producing the impression of a unified local resource [10].

The successful development of the Internet within a few decades made it more flexible, large-scale, reliable and safe. After the first traditional Internet services such as file transfer and email services, some development trends occurred in the creation of both traditional services and mobile Internet services and applications. These trends occurred in the creation of websites; for example, today the number of websites is close to a billion [11] and new technologies are applied in their creation. Recently, social networks, cloud computing, P2P and other new services have been created and developed.

The emergence of network services opened up a wide range of options and opportunities to users in terms of socioeconomic interaction. This has led to the extensive use of the Internet in the socioeconomic sphere. Today, the number of Internet users in the world has reached three billion, the volume of daily Internet traffic (including traditional and mobile traffic) is measured in exabytes, the number of daily emails has reached 100 billion, and the number of active users of Google and Facebook is over a billion. More information on the other trends regarding the use of Internet is available at [11]. Of course, these trends have an impact on network security and cause new threats to security.

Security trends in CNs

The security of CNs plays an important role in the development of ICT, including Internet services. CN's security support and the protection of critical information infrastructure are crucial for the security of any organization or country. A secure Internet ensures the emergence and development of new services. Identification of security trends is one of the most important steps to ensure the high-level security of CNs. The annual safety reports of Cisco, popular in the field of cybersecurity [12], Kaspersky Lab [13], Symantec [14], McAfee [15] and others make it possible to analyse current cyber-attack trends. The trends in cyber-attacks include application-level attacks, social engineering, targeted attacks, information leaks and internal users' attacks, encryption, IPv6 attacks, and attacks on the use of cloud computing. The analysis shows that the main trend in the field of CN is that the attacks mainly focus not on the failure of the network infrastructure or nodes, but on the acquisition of information including corporate and personal data. The attacks aimed at privacy and data theft are attributed to the security trends. Today, as individuals and organisations store their important information on the Internet, security requirements are changing. The main approach to security support should ensure the security of data along with system security.

Increasing the automation level of attack tools is one of the security trends. Automated attacks usually consist of four phases, each of which may change. These phases include the identification of potential victims, the failure of a vulnerable system, the spread of the attack and coordinated control of attack tools. In addition, these attack tools are improving, and their developers are using more advanced methods. Available antivirus programs can hardly detect these attacks. Another security trend has emerged from the widespread use of mobile devices. The increase in the number of mobile devices has led to an exponential increase in security risks. The number of portable or individual mobile devices will reach 8.6 billion by 2017 [16]. Each new smartphone, tablet or other mobile device creates new opportunities for cyber-attacks because each mobile device opens up a new potential vulnerable entry point to the network. In addition, there is malicious application software which uses mobile applications. For example, the number of malicious applications designed for iPhones and Android devices and the devices infected by them is growing exponentially.

Another security trend has emerged from the extensive use of social media, which poses a threat to privacy. Widespread use of social media in organisations causes a sharp increase in the number of attacks and creates an additional channel for the implementation of social engineering. Organisations should use cutting-edge technologies to minimise the risks, prevent information leakage, monitor networks and analyse data logs. Today, one of the key security trends is cloud computing security support [17, 18]. Because of the growing popularity of cloud computing, enterprises and organisations use cloud computing to reduce costs and increase efficiency. Well-developed architecture and well-planned security allow organisations to effectively manage the risks of cloud computing. Cloud computing service providers have addressed all of these issues, but the malefactors have shifted to cloud computing because organisations often store their corporate data in the cloud. One of the main goals of attacks in the cloud is to access personal and corporate data.

Conclusion

Today, CNs are used in almost all spheres of social activity, including various sectors of industry, public administration and public institutions. In addition, CNs are developing very rapidly, and are accompanied by various infrastructure, application and usage trends. This in turn directly affects computer security, leading to new security trends. The development rate of the trends in the field of computer security is directly proportional to the development rate of ICT trends, which increases the risk of computer (in particular, critical infrastructure) security violations, and consequently poses serious threats to national, social and economic security. In

these circumstances, the identification and analysis of computer security trends is of great importance. Identifying the emerging trends in a timely manner will enable the establishment of effective mechanisms against threats to the network.

References

1. Abramson N. The Aloha System - Another Alternative for Computer Communications / Proceedings of Fall Joint Computer Conference, AFIPS Conference, 1970, p.37.
2. https://www.tools.ietf.org/html/rfc2460
3. Agrawal S., Vieira D., A survey on Internet of Things // Abakys, Belo Horizonte, 2013, v. 1, n. 2, pp. 78-95.
4. http://www.tra.gov.eg/uploads/technical%20material/Wi-Fi%20report.pdf
5. Mohapatra S.K., Choudhury R.R., Das P., The future directions in evolving wi-fi: technologies, applications and services // International Journal of Next-Generation Networks, 2014, vol.6, no.3, pp.13-22.
6. http://www.media.johnwiley.com.au/product_data/excerpt/0X/04706968/047069680X.pdf
7. http://www4.kfupm.edu.sa/ssc/4845_MohammedUmair_Yaqub.pdf
8. Thomas R.W. Cognitive Networks, Ph.D. Dissertation, Virginia Polytechnic and State University, Blacksburg, VA, June 15, 2007.
9. Mahmoud Q. Cognitive Networks – Towards Self-Aware Networks, John Wiley and Sons, 2007, 368 p.
10. http://www.newsroom.cisco.com/dlls/2008/ts_012808.html
11. http://www.internetlivestats.com/
12. https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf
13. http://www.securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf
14. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf
15. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf
16. http://www.newsroom.cisco.com/documents
17. Behl A., Behl K. An analysis of cloud computing security issues / Information and Communication Technologies (WICT), World Congress, 2012, pp.109-114.
18. Parekh D.H, Sridaran R. An Analysis of Security Challenges in Cloud Computing // International Journal of Advanced Computer Science and Applications, 2013, vol. 4, no.1, pp. 38-46.