AD VALOREM
Journal of Young Researchers

ARTÍCULO DE REFLEXIÓN

Challenges in security and privacy in wireless communications

Alberto de Jesús Romero Torres
University of Bedfordshire Business School

ABSTRACT

This Research Review Paper highlights some of the main concepts of Wireless Communication including Network Security, Privacy, and Transmission Control Protocol/Internet Protocol (TCP/IP). In equal manner, it illustrates the organizational importance to establish more effective policies to counterattack and prevent cyber-attacks and reduce cyber threats. Therefore, avoiding the financial cost occasioned by hackers and the physical harm that could be cause to an individual by the sensitive data shared via technological devices to the internet without permission.

Keywords: wireless communication; local area network; wide area network; transmission control protocol; internet protocol; cyber-attacks.

Desafíos en seguridad y privacidad en las comunicaciones inalámbricas

RESUMEN

Este documento de revisión de investigación destaca algunos de los conceptos principales de la comunicación inalámbrica, incluida la seguridad de la red, la privacidad y el protocolo de control de transmisión / protocolo de internet (TCP / IP). De igual manera, ilustra la importancia organizacional de establecer políticas más efectivas para contraatacar y prevenir ciberataques y reducir las ciber amenazas. Por tanto, evitando el coste económico ocasionado por los piratas informáticos y el daño físico que pudieran ocasionar a un individuo los datos sensibles compartidos a través de dispositivos tecnológicos a Internet sin permiso.

Palabras clave: comunicación inalámbrica; red de área local; red de área amplia; protocolo de control de transmisión; protocolo de internet; ciberataques.

Para citaciones: Romero Torres, A. (2021). Challenges in security and privacy in wireless communications. Revista de jóvenes investigadores Ad Valorem, 4(2), 74-81. https://doi.org/10.32997/RJIA-vol.4-num.2-2021-3701

Autor de correspondencia:
Alberto de Jesús Romero Torres
albertojromerot@gmail.com

Editor: Bernardo Romero Torres.
Universidad de Cartagena-Colombia.

Tipología IBN Publindex:
Artículo de Reflexión

Universidad Editorial Universitaria de Cartagena

1. INTRODUCTION

The following paper aims to evaluate the fundamentals of networking and some of the most common cyberthreats, both in UK and worldwide, to illustrate the current cyber environment and provide the reader with tools to looks forward. The COVID-19 pandemic seems to have accelerate the adoption of the Internet of Things (IoT) devices including smartphones, wearables, and global positioning system (GPS), that enable the share of information between individuals and organizations physically apart from each other. As new devices and internet platform are created, new risks arise, because more personal and organizational data is created and handle through the internet, especially through wireless communication channels.

1.1. Network Security Concepts

Network Security is the systematical procedures to identify and deny unwanted use or harm to a computer network. The process oversees and look for anomalies in the protocols of a network to impede nonapproved transmissions, therefore being able to establish countermeasures in due time. Furthermore, network security is relative to a backup, essential in organizational communications to support its mission and goals with integrity in its data pipeline.

In regard to computer networks, trust is the assurance that end- users will behave in accordance with the business security rules, to preserve the stability, privacy, and integrity of its digital assets. A frequent case is the third-party trusted system, where a relevant authority releases digital certificates. Such systems connect end-users with a web e-commerce server. Originally, he/she does not know whether the server is exposing its identity, until an assessment of digital certificates provided to all parties, from a certified authority has been validated. The finality of this system is to enable the identity of a valid website by its user via an accepted trustworthy third-party each user knows.

The security objectives including confidentiality, integrity and availability, are what an organization strive to accomplish with its strategies. Firstly, confidentiality safeguards data against unauthorized users that does not need connection to a particular resource. Secondly, integrity grants authorized information changes carry out by authorized end-users. Hence, complementing confidentiality. Thirdly, availability offers protection against loss of information and blocked access, while defending the data and ensuring access to it whenever a user requires it.

A typical information technology (IT) infrastructure is made by the 7 following domains:

- User domain refers to anyone including employees, contractors, and third-party users who utilize organizational IT infrastructure under the business acceptable use policy (AUP).
- Workstation domain or endpoint devices that a user utilize includes, but are not limited to a desktop computer, laptop, and a Voice over Internet Protocol (VoIP) telephone.
- Local Area Network (LAN) domain are those physical and logical network technologies that assist workstation connectivity to the organization's IT infrastructure.
- LAN-to-WAN (Wide Area Network) domain is the process of interconnectivity point between an organization's LAN and WAN network infrastructure such as routers, firewalls, switches, proxies, demilitarized zones (DMZs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and the encryption of communication, frequently adopt to audit devices in this domain.
- Remote Access domain indicate the steps to provide authorization and authentications so users can access remotely an organization's IT infrastructure, system, and data. Often is refers to a safe remote communication through an encrypted virtual private network (VPN).
- WAN domain is a service than an organization often outsource to a carrier network company, to get end-to- end connection and bandwidth.
- System/Application domain means the hardware, operating system software, database software, client/server applications, and data that an organization possess in its data center(s).

Transmission Control Protocol/Internet Protocol (TCP/IP) suite is critical to the successful understanding of network security mechanisms. It provides a framework to enhance the performance of a network, therefore it serves to manage traffic, analyze protocols, and ethically perform hacking (penetration testing) to identify week points in a network. Such protocols are usually support by the Open Systems Interconnection (OSI) reference model, which act as a medium to examine protocols and its function through its seven layers (Stewart & Kinsey, 2020).

- Application layer is the interface between the host software, such an operating system, and the network protocol stack.
- Presentation layer is two-way system of the translation of information into formats that both, the host software, and the network could understand
- Session layers administrate the communication channels, or sessions, between endpoints of the network.
- Transport layers manage the transit and configuration of data.
- Network layer handles IP addresses and routing traffic.

- Data Link layer manage media access control (MAC) addresses and provides support to the topology of a network such as the ethernet.
- Physical layers modify data into transmitted bits over the wireless network.

1.2. Network Security Threats

The importance of logical addresses such as IP, which are unique, is in part due to the enablement of communication between two host independently of the physical proximity of the devices. However, wireless communication carries its own risk. Arguably the issue may have been aggravated by the COVID- 19 pandemic, and the lower power that organizations have over the devices that employees utilize for daily tasks.

The most common cyberattacks in the UK in the last 12 months ending in March 2021 includes phishing, affecting 83% of businesses; impersonating organization in emails or phone 27%; and viruses, spyware, or malware (excluding ransomware) 9%. There is an upward trend from 72% to 83%, in the period between 2017 and 2021 respectively, where phishing attacks being this the most common threat over UK businesses. This kind of attacks are considered by most of the business affected as the most disruptive threat. Moreover, 22% of businesses have suffered cyberattacks. Based on this, some of the outcomes that take form on disrupted business are temporary loss access to files or networks (8%), websites, or online services taken down or made slower (6%), and software or systems corrupted or damaged (4%). Nonetheless 89% of business stated that have been able to reestablish operations from its most disruptive attacks within 24 hours (Department for Digital, Culture, Media & Sport, 2021).

Email phishing could be defined as a form of scam via malicious links and attachments elaborated by hackers tends to accomplish it goals through reputable source Some of the countermeasure that end-users could leverage are checking that the display name and the email address actually match, be aware if there is a sense of urgency in the message, whether the email signature is inappropriate, look for grammar errors or a sender asking for sensitive information, and the looks of attachments or links (Mukherjee, 2020).

2. IMPORTANCE GROWING WITH TIME

2.1. Existing & Emerging Technologies

In 2020 the rate of homes in the United Kingdom with access to fixed telephony was 78 %, with a nearly 31.3 million fixed lines registered in 2019. Although a slight downtrend from 2007 of 90 % of fixed lines access and 34.5 million fixed lines registered in 2007 respectively, just 39 billion (in 2019) minutes are the total of

UK's current fixed-line voice volume, or 74% (149 billion) less than in 2007 (O'Dea, 2021; Alsop, 2021a; 2021b).

In contrast the number of publicly known Internet of Things (IoT) platforms globally have increase in 138% (360) in 2019 with a total of 620, from 260 in 2015. Within the incumbents are bib companies such as Amazon and Microsoft. In the UK the penetration of connected devices has increase almost twice as much to 81% in 2020, from 46% in 2000. In addition to this, the average Briton had access to more than nine connected devices (9.16) in 2020, owning mainly smartphones (97%), TV (93%), laptop (80%), headphones (77%), and tablet (73%) (Liu, 2021; Alsop, 2020; Vailshery, 2021; Kunst, 2021) This highlights how vulnerable end-user of wireless communications and IoT are, given how technology rapidly evolve and the more personal data is gathered by the devices' sensors.

2.2. Impact on Victims

The COVID-19 pandemic has impacted the cybersecurity industry with an increase migration of individuals and organizations to the cyberspace. In 2020 Cybersecurity investment outperformed other sub-industries of the IT industry with US$53 billion or 10%. But workforce productivity outpaced security investment during the pandemic growing 33% in 2020 to US$142 billion, or US$45 billion more than 2019 (Canalys, 2021). In the UK alone, during 2021 cyber breaches has accounted for an average cost of £8,460 per attack on data or assets loss. Whereas on medium and large businesses the cost rises to £13,400 (NCSC, 2021b).

To reduce the risks and support the development of a strategy security framework, the UK government have been elaborating systematical recommendations to mitigate risks within the telecoms industry. They are labeled into 5 main categories including Technical Security Requirements (TSRs) to increase the accountability of operators to tackle cyber risk in the highest risk areas; diversification of the IT infrastructure market; better policies regarding the administration of High-Risk Vendors (HRVs); the elaborations of a National Telecom Lab to undertake rigorous tests on the UK's telecoms networks and equipment. Specifically, one of the main aims of the UK government seems to seek to limit the dependency on any private vendor in its society, where HRVs does not hold more than 35% of market share. This cap targets the impossibility of scale of HRV deployment, and further enable the national capability to Remove High Risk vendor equipment from UK networks when necessary (NCSC, 2021a).
A data breach example that could illustrate the vulnerability of end users is the incident on SolarWinds, where malicious individuals obtained access to the secure code of its software through the insertions of a malware into the source code. In this event when a SolarWinds user update the software, hacker got the possibility to surveil customers unknowingly. Such attack seems to have cause

inconvenience to thousands of customers (Peisert et al., 2021). The hack shows the limitations of current security practice such as software's updates and the concern of whether these updates are necessary. However, ignoring updates is a bet not everyone seems willing to make. Whichever the scenario is, the situation portraits the inadequate strategies to software development, maintenance on one side and interference in detection on the other. This implies not only that all parties must have equal responsibility towards the job needed to be done, to get benefits of software and it updates, without any danger. But also, this would imply that there is not a one size fits all methodology, hence the necessity of mixing regulatory, technical, and organizational solutions approaches to move forward (Massacci et al., 2021).

3. CHALLENGES

3.1. Networking cyber-physical systems

With the fast pace that network technology is evolving, processing, and exchanging information has become more of a necessity. This necessity grows in accordance with the concern of end-users to their security and privacy issues such as open channels allowing hackers to eavesdrop and appropriate the data in question; the wireless reproduction could cause signal attenuation, therefore the risk of losing information; the digital migration of networking users could enable attackers to cover under a legitimate image. This implies a necessity to update the technology of wireless network encryption, to reassure users that open and shared wireless network is not vulnerable and could be destroyed by outsiders, hence preserving the confidentiality, safeguarding the data, so authorized individuals can make use of wireless network whenever is needed.

3.2. Connecting physical-world to cyber-world

The integration of the physical information from the physical world to the cyber world has enable to develop more efficient applications to improve users' life and work. For instance, accurately gathering data from a human cardiovascular system with sensors in smart watches. The information could be leveraged to recognize patterns in the user's Heart Rate Variability (HRV) to detect premature beats that indicates heart issues in advance. On the other hand, due to the new kind of connections that comes with technology innovation, the user usually gets exposed to an unprotected pervasive space, leading to security and safety problems. For instance, the interaction of physical world to the cyber-world could be a perfect scenario for a malware to produce a leak of information in a system. However, when the interaction exists in the cyber-physical space (e.g., self-driving-car), such malware could leverage the connection performing actions to interfere the regular physical operation (e.g., stopping a vehicle's braking functions).

3.3. Connecting things to things in physical world

Another emerging technology of the next-generation of wireless networks that have brough new security and privacy threats is the Vehicle Ad-hoc Network (VANET), which provide the communication between moving vehicles. VANET main components are in-vehicle network, inter-vehicle network, and vehicle wireless internet connection, this forms a large-scale interactive network. Via the internal standards a protocol of communication, VANET assist the progress of data exchange between vehicles, road, pedestrian, and internet to construct dynamics mobile communication among users. Security issues in VANET is the sensitive information it manages such as vehicle's location. Therefore, cryptographic measures must be adopted to guarantee the authenticity of information shared. Equally, malicious data must be traceable by a trusted agency to take effective action to guard the safety of the VANET (Zhong et al., 2019).

4. CONCLUSIONS

The global pandemic of COVID-19 has accelerated the rate of adoption of wireless networks in the society by households, organizations, businesses, and workers looking for connectivity solutions. At the same time, the usage of wireless networks has been leveraged by the evolution of technologies such as smart watches, smart phones, cloud servers, and sensors. However, technological innovations come with a shared responsibility of all parties (service providers, authorities, and end users) to guarantee an appropriate administration of the increasingly data handle in the cyberspace. Such cyber threats and cyber-attacks, regardless of the hackers' motives, could harm financially an economy, and worst, physically an individual with irreparable consequences.

5. REFERENCES

Alsop, T. (2020, July 23). Connected device penetration in the United Kingdom (UK) 2000–2020. Statista. Retrieved 4 May 2021, from https://www.statista.com/statistics/274109/connected-device-penetration-in-the-united-kingdom-uk-since-2000/

Alsop, T. (2021a, September 30). Fixed-line voice call volumes: total call minutes in the UK 2004–2020. Statista. Retrieved 10 October 2021, from https://www.statista.com/statistics/215715/fixed-line-voice-call-volumes-in-the-uk/

Alsop, T. (2021b, September 30). Landlines in the United Kingdom (UK) 2007–2020. Statista. Retrieved 10 October 2021, from https://www.statista.com/statistics/270778/fixed-lines-in-the-united-kingdom-uk/

Canalys. (2021). Cybersecurity investment 2020. Retrieved 14 May 2021, from https://www.canalys.com/newsroom/cybersecurity-investment-2020

Department for Digital, Culture, Media & Sport. (2021, May 19). Cyber Security Breaches Survey 2021. GOV.UK. Retrieved 14 June 2021, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Kunst, A. (2021, August 26). Consumer electronics usage in the UK 2021. Statista. Retrieved 10 October 2021, from https://www.statista.com/forecasts/997852/consumer-electronics-usage-in-the-uk

Liu, S. (2021, April 30). Global number of publicly known IoT platforms 2015–2019. Statista. Retrieved 14 May 2021, from https://www.statista.com/statistics/1101483/global-number-iot-platform/

Massacci, F., Jaeger, T., & Peisert, S. (2021). SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil? IEEE Security & Privacy, 19(2), 14–19. https://doi.org/10.1109/msec.2021.3050433

Mukherjee, A. (2020). Network Security Strategies: Protect your network and enterprise against advanced cybersecurity attacks and threats. Packt Publishing.

NCSC. (2021a, January). Security analysis for the UK telecoms sector. UK National Cyber Security Centre. https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector

NCSC. (2021b, March 26). Weekly Threat Report 26th March 2021. UK National Cyber Security Centre. Retrieved 14 May 2021, from https://www.ncsc.gov.uk/report/weekly-threat-report-26th-march-2021

O'Dea, S. (2021, September 30). Mobile telephony adoption in the United Kingdom (UK) 2007–2021. Statista. Retrieved 10 October 2021, from https://www.statista.com/statistics/272221/mobile-telephony-adoption-in-the-united-kingdom-uk/

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the SolarWinds Incident. IEEE Security & Privacy, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

Stewart, M. J., & Kinsey, D. (2020). Network Security, Firewalls, and VPNs (3rd ed.). Jones & Bartlett Publishers.

Vailshery, L. S. (2021, January 22). Average number of connected devices in UK households 2020. Statista. Retrieved 14 May 2021, from https://www.statista.com/statistics/1107269/average-number-connected-devices-uk-house/

Zhong, S., Zhong, H., Huang, X., Yang, P., Shi, J., Xie, L., & Wang, K. (2019). Security and Privacy for Next-Generation Wireless Networks. Springer.