Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 201 (2022) 158–165

Procedia Computer Science

www.elsevier.com/locate/procedia

The 13th International Conference on Ambient Systems, Networks and Technologies (ANT)
March 22 - 25, 2022, Porto, Portugal

The COVID-19 pandemic and remote working did not improve WLAN security

Saku Lindroos[a,*], Antti Hakkala[a], Seppo Virtanen[a]

[a]*Department of Computing, University of Turku, 20014, Turku , Finland*

Abstract

In this article, we present an analysis of the COVID-19 pandemic's effects on Wireless Local Area Network (WLAN) security and abundance in Southwest Finland. We hypothesised that the drastic increase in telecommuting caused by the pandemic would encourage many to update obsolete WLAN devices, improving the state of WLAN security and increasing WLAN deployment in the survey region. To test our hypotheses, data from seven WLAN surveys carried out between February 2020 and October 2021 was analysed. Surprisingly, although the results show a 50.2% increase in WLAN deployment during the second and fourth waves of the pandemic, this had no significant effect on WLAN security in the survey region. The survey data shows little change in the number of unencrypted networks and networks configured with vulnerable encryption protocols. While most of the located networks were encrypted with the secure WPA2 protocol, the number of networks configured with the newest WPA3 has not notably increased.

Keywords: COVID-19; IEEE 802.11; Wardriving; Wireless LAN; Wireless security

1. Introduction

In March of 2020, the World Health Organisation (WHO) declared the coronavirus COVID-19 outbreak as a global pandemic. In many countries, one of the immediate effects of the pandemic has been the closing of businesses and schools in efforts to prevent the infection from spreading. For many, this has meant a move from offices and schools to working and learning remotely over the internet. According to Eurofound's COVID-19 e-survey data [4], 36.5% of the European respondents, and over 60% of the Finnish survey respondents, had started working remotely during the spring of 2020 because of the pandemic. Before the pandemic, only 15.3% of the Finnish and 15.8% of all European survey respondents had telecommuted regularly. According to a Pew Research Centre survey of over 5.800 working

* Corresponding author.
E-mail address: saku.p.lindroos@utu.fi

1877-0509
10.1016/j.procs.2022.03.023

adults in the United States, 71% of the respondents were working remotely during the pandemic, whereas only 20% of the respondents had worked remotely before the pandemic [13].

As the pandemic has forced many to continue their daily routines remotely from home, Wireless Local Area Network (WLAN) connections have become essential for individuals, businesses, and governments to function through the pandemic. Wireless internet connections have made it possible for individuals to continue their essential daily activities throughout the pandemic. Moreover, wireless internet connections have allowed people to remotely carry out tasks that traditionally have required physical contacts, such as grocery shopping and healthcare appointments.

The need for wireless internet connections has become so essential that special programs have been issued to provide free WLAN connections. For instance, in Hawaii, a special "Wi-Fi on wheels" program was established to bring WLAN connections to students by turning vans into moving WLAN hotspots [12]. Similar efforts have been made in other parts of the United States. For example, in Sacramento, California, school busses have been turned into moving hotspots to provide WLAN connections for students [1]. In Canada, the city of Toronto temporarily set up free WLAN connections for 25 large residential apartment buildings in low-income neighbourhoods [17].

In this article, we present unique and high-value data on how the onset of the COVID-19 pandemic has affected the security and abundance of WLAN networks. We hypothesise that the increase in telecommuting creates an incentive to upgrade obsolete WLAN devices, improving the state of WLAN security and increasing WLAN deployment in the surveyed region. To test our hypotheses, data from seven WLAN surveys carried out between February 2020 and October 2021 was analysed to observe how the pandemic has affected WLAN security and abundance. The WLAN surveys were conducted in three separate locations within a typical medium-sized city in Southwest Finland. To the best of our knowledge, no similar research about the effects of the COVID-19 pandemic on the WLAN landscape has been published.

2. Information security during the COVID-19 pandemic

Because the internet has acted as the primary gateway for accessing work and learning-related online services during the pandemic, the importance of cybersecurity has increased dramatically. This new kind of mass dependency on internet connections and online services has presented cybercriminals with a plethora of new opportunities. Under the guise of the pandemic, criminals have increased their efforts in spreading malware and stealing sensitive information through large-scale social engineering campaigns, taking advantage of economic and mental distress. In May 2020, the United Nations' disarmament chief, Izumi Nakamitsu, reported that the COVID-19 pandemic has caused a significant rise in cybercrime, most notably a 600% increase in malicious email campaigns [14]. The International Criminal Police Organization (Interpol) reports that its private sector partners had detected over 907,000 spam messages, 737 malware incidents, and 48,000 malicious URLs related to COVID-19 between January and April 2020 [8].

In June 2020, Interpol reported that its Cybercrime Directorate Global Malicious Domain Taskforce identified and analysed over 200,000 malicious domains, affecting over 80 countries [8]. The newly registered malicious domains hosted data harvesting malware or had been constructed for garnering sensitive information via spam email campaigns. Palo Alto Networks report a 569% growth in malicious domains between February and March 2020. They also report a 788% growth in malicious COVID-19 related domains containing scams and unauthorised cryptocurrency mining [8].

In their 2020 report [18], Trend Micro reports that they detected nearly 9 million COVID-19 related threats between January and June 2020. The threats include malicious emails, URLs, and files related to the pandemic. Emails and links containing malicious files making up 91.5% of all the considered threats. The Trend Micro report also shows a 25% increase in attacks against networked devices, and a 22% increase in attacks against network routers, from the second half of 2019 to the first half of 2020. Furthermore, the report shows a 70% overall increase in inbound attacks from the second half of 2019, brute force login attempts being the most common (88.9%) form of attack. A similar increase in brute force login attempts has been reported by the security company Kaspersky [3]. This kind of increase in brute force login attempts is to be expected as organisations have been forced to deploy remote access services for their employees during the pandemic.

Because of increased remote work and the consequential increase in cyberattacks, having secure end devices and wireless internet connections has become essential. This sudden transition to mass telecommuting has led to a situation where employees must rely on their insecure personal devices and home networks, making them vulnerable to attacks.

In the Eurofound survey, 36% of the respondents tell that their employer had not provided them with equipment for working remotely [4]. A similar survey by Kaspersky Labs shows that only 55% of the respondents had been provided with devices for remote work by their employer [9]. The Kaspersky survey also shows that 73% of respondents had not received any additional IT security awareness training after they had switched to working from home. In their study, Georgiadou et al. [6] found that 53% of the participants had not received any security guidelines from their employers regarding working from home during the pandemic.

In addition to personal computers and smartphones, employees must rely on personal or public WLAN connections whilst working remotely. Typical consumer routers often lack the additional security mechanism of enterprise network devices such as packet filtering or intrusion detection and prevention systems. Another issue in home routers is that they are left unattended once deployed. It is a common practice that Internet service providers provide their customers with a pre-configured router. As a consequence, the end-users do not change the pre-configured default passwords and settings or update the router firmware, leaving the device vulnerable to attacks.

A survey of 2.205 people in the United Kingdom showed that 51% of the respondents had never changed any of their home routers settings [15]. Furthermore, 69% of the respondents had never changed their WLAN networks default password, 82% had never changed the router's administrator password, and 86% had never updated the router firmware. These issues were highlighted by the 2016 Mirai malware epidemic, which scoured the internet for devices with weak default credentials and configurations, resulting in massive Distributed Denial of Service (DDoS) attacks.

A study by Weidenbach and Dorp [19] concerning security weaknesses of consumer WLAN routers revealed that 36% out of the 127 tested devices had not received security updates in the past 12 months. They also discovered that among the updated systems, several already known vulnerabilities had not been patched by the new updates. Alarmingly, 52% of the tested systems employed either hard-coded or weak default administrator credentials. In their study of over 15.5 million home networks, Kumar et al. [10] showed that 10.8% and 14.6% out of the scanned home routers supported insecure FTP and Telnet protocols, respectively. Of the devices that supported either or both protocols, 12% had weak FTP credentials, and 1.6% had weak Telnet credentials. Luckily only a small portion of the routers had services such as HTTP (3.4%), FTP (0.8%), Telnet (0.7%) and SSH (0.8%) exposed to the internet.

In the worst-case scenario, an employee using a vulnerable end device or WLAN connection may expose the entire organisation to serious security breaches and loss of sensitive information. As the effects of a security breach do not only affect the individual, but the whole larger organisation, a single compromised device can have devastating effects. Moreover, as it is to be expected that some hybrid form of telecommuting and working at the company premises will continue after the pandemic, it is ever more important to provide employees with security awareness training, secure devices, and connections.

3. Methodology

The WLAN survey methodology used in this article is based on a passive wireless network scanning method known as wardriving. The survey system (Fig. 1) is built on common off-the-shelf hardware and freely available software. A comprehensive description of our WLAN survey methodology is presented in our previous work [11] where we discuss in detail the different stages of the WLAN survey process, the required hardware and software and the legality and moral aspects of wardriving. Here we will briefly introduce the principles of wardriving and describe the used WLAN survey methodology.

The term wardriving is derived from the "wardialing" technique introduced in the movie Wargames in 1983 [7]. The lead character in the movie used his computer to detect other network-enabled computer systems by automatically dialling phone numbers in an increasing sequence. In the 1980s, computer networking from remote locations was managed by modems utilising the traditional telephone system. This kind of connectivity made it possible to identify network-enabled computers simply by dialling phone numbers and assessing whether there was another modem responding to the phone call or not. Wardriving takes the method to the modern ages: instead of dialling phone numbers, one can use a WLAN-enabled computer to detect all nearby wireless networks.

To put it simply, wardriving means moving around some chosen geographical region and recording data of the discovered WLAN devices and networks while moving. The gained results are then gathered into databases for statistical purposes. It is also common to visualise the locations of the surveyed networks on a map based on GPS location data. There are two main ways of surveying WLAN networks: passive methods and active methods. With active methods,

the scanning system always interacts with the target networks it is surveying. The active interaction may include techniques like sending probe request frames and gathering data from probe responses from the nearby WLAN routers. This method is analogous to the traditional telephone wardialing where an attempt to discover remote systems is made by progressively dialling sequential telephone numbers and storing information for each number where a modem picks up the call.

In passive wireless network scanning, the scanner does not interact with the surrounding networks. The network scanner simply listens to the wireless traffic and extracts information from the wireless networking frames. For example, WLAN devices broadcast beacon frames at regular intervals to announce their presence to other surrounding devices. These frames carry varying information such as the wireless network Service Set Identifier (SSID), supported encryption protocol, used wireless channel, and the device MAC address. For the wireless network scanner to be able to scan the entire WLAN wireless spectrum, the Wireless Network Interface Controller (WNIC) must be set to monitor mode. While in monitor mode, the WNIC can utilise channel hopping to scan all wireless channels available in the spectrum for WLAN devices and networks. In this process, the frames broadcasted by nearby systems can be harvested for information regarding the network they are connected to. The passive WLAN scanning process is analogous to performing a scan of the FM frequency to find broadcasting radio channels.

The term wardriving may sound intimidating to some and thus, the activity may be interpreted by some as malicious with an aim to intrude wireless networks. It is however, quite the opposite: while wardriving could be a part of an attempt to break the security of WLAN networks, it is not per se a criminal act. In fact, wardriving itself is harmless to the surveyed networks, and security professionals as well as hobbyists commonly use it legitimately as a tool for research and analysis. Obviously, while legal, some moral questions still arise concerning the privacy and consent of WLAN network owners, and these should be taken into consideration in the process.

We divide the WLAN survey process into three stages: planning and preparation, data collection and data analysis. During the planning and preparation stage, the survey location, mode of transportation, hardware and software are chosen and prepared. Furthermore, as laws and regulations can differ between regions, the legality of surveying WLAN networks is ensured in the planning stage. During the data collection stage, the wardriver surveys the surrounding wireless networks within the predetermined area. After the area has been thoroughly surveyed, the collected data is further processed and analysed. During the data analysis stage, the collected survey data is compiled into databases and refined into statistics. If the wardriving process is accompanied with location (GPS) data collection, the geographical locations of the detected WLANs can be visualized in services like Google Earth or WiGLE.net.

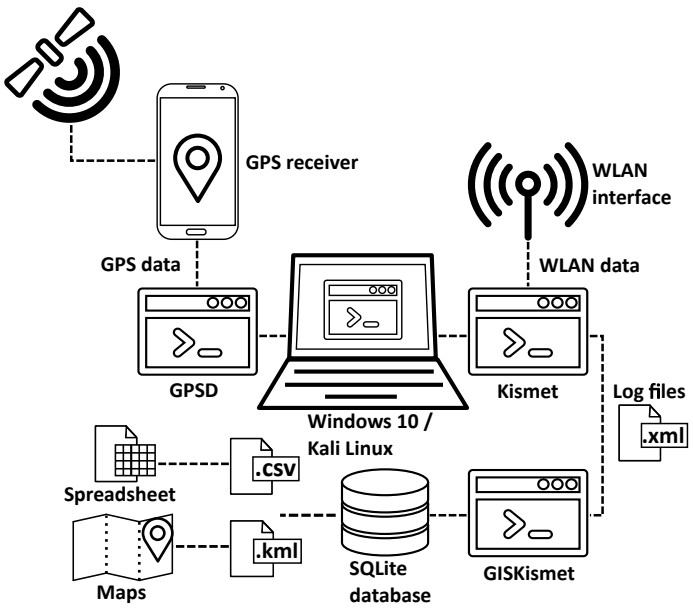

Fig. 1. The used WLAN survey system

3.1. The WLAN survey system

The hardware used in our system is composed of a PC laptop, a USB powered WNIC with dual-band capability, and an Android phone for receiving location data (GPS). In this study, we used the TP-Link AC600 Archer T2UH as the WNIC. The WNIC chipset was Mediatek MT610U.

As the survey platform, we have used the Debian based Kali Linux operating system running as a virtualised guest host on top of the laptop's main Windows 10 operating system. VMware Workstation Player was used as the hypervisor software to virtualise the guest operating system. From the Kali Linux software library, the open-source wireless network detector Kismet was used as the WLAN survey software [16, 2]. To incorporate GPS location data with the survey results, the Global Positioning System Daemon (GPSD) was used for collecting GPS location data during the survey sessions [7].

3.2. Survey data acquisition and analysis

For this article, we have used data from seven WLAN surveys. The surveys were carried out in February 2020, June 2020, October 2020, January 2021, March 2021, June 2021 and October 2021. The February 2020 survey is considered the control sample before the onset of the COVID-19 pandemic. The COVID-19 statistics used in this article are based on data published by the Finnish Institute for Health and Welfare THL [5].

The location for our study was a typical medium-sized city in Southwest Finland. We chose three different areas within the city to carry out the surveys. By surveying three distinct locations within the city, it is possible to form a more comprehensive picture of the city's WLAN landscape. The three survey locations: the industrial district, the city centre, and the suburb were chosen to represent different locations for typical WLAN deployment and usage.

- Industrial district route (2.9 km): along this route, there are very few private homes. The buildings in the area mostly host commercial operators ranging from gyms, technology start-ups and automotive dealerships to metal workshops
- City centre route (3.7 km): the city centre buildings host private homes as well as administrative officials. In this survey area, in addition to private homes, there are service sector businesses such as restaurants, clubs and florists, and also the market square, a police station and the town hall reside on this route.
- Suburban route (2.2 km): in this area, there are only detached houses and small condominiums that are private homes. The area is considerably more scarcely populated than the city centre.

During each survey session, the locations have been surveyed three consecutive times to ensure the best possible results. After each survey session, the collected data has been imported into SQLite databases. Data from the databases has then been parsed into .csv files and turned into spreadsheets for further statistical analysis.

4. Results

Because cryptographic encryption protocols, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), are the most notable security mechanisms introduced in the IEEE 802.11 WLAN standard, the main focus of our research is on the use and deployment of encryption protocols. WEP and the first generation of the WPA protocol, known as WPA-TKIP, have been deprecated from the WLAN standard due to severe vulnerabilities and are no longer suitable for encrypting WLAN communication. WPA2, the second generation of the WPA protocol, was officially ratified to the IEEE 802.11 standard in 2004 and is still the predominant WLAN encryption protocol. While WPA2 is considerably more secure than its predecessors, several vulnerabilities have been found in its implementation over the years. In 2018 the Wi-Fi Alliance announced that the third generation of the WPA protocol, WPA3, would replace the outdated WPA2.

Surprisingly, the survey results show no significant changes in WLAN encryption protocol deployment during the pandemic as can be seen from Fig. 2 and Table 1. The number of insecure WEP and WPA-TKIP encrypted networks did not notably decrease during the pandemic, while the number of WPA2 encrypted networks steadily increased. Also remarkable is that we have been able to locate only a few devices configured with the newest WPA3 encryption

protocol, even though devices supporting WPA3 became available for consumers in late 2019, and the Wi-Fi Alliance certification program has required support for the protocol since July 2020.

Further inspection of the WEP encrypted networks reveals that most of them originate from what we perceive as being legacy devices residing in the industrial district and city centre areas. Some efforts to increase the security of the detected WEP encrypted networks can be seen from the research data as a clear majority of them have masked SSIDs, making the network name invisible to surrounding devices. Similar remarks can be made about the WPA-TKIP encrypted networks. Some have masked SSIDs and roughly half of them seem to originate from PDA devices in the industrial district, while the other half originates from legacy access points in the industrial district and city centre.

A look into the open unencrypted networks shows that a clear majority of them have been set up as guest networks by businesses, schools, and public administration and are therefore intentionally left unencrypted. Nonetheless, the survey data reveals a handful of wireless access points, IoT devices, wireless printers, storage devices, and Google Chromecasts that have been left unconfigured and unencrypted. These kinds of unencrypted devices are a serious threat to the network user's security.

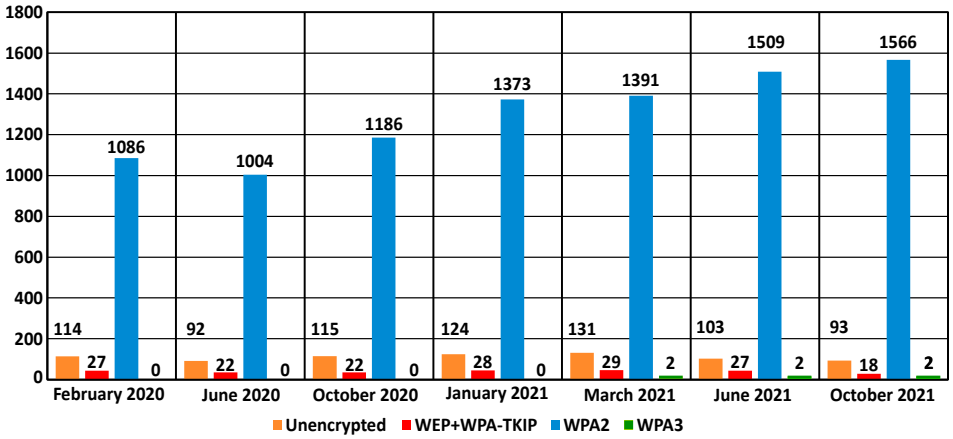

Fig. 2. Encryption protocol usage evolvement during the pandemic. WEP and WPA-TKIP encrypted networks grouped.

Table 1. Encryption protocol deployment during the pandemic

	Open	WEP	WPA-TKIP	WPA2	WPA3	Total
February 2020	114	7	20	1086	0	1227
June 2020	92	10	12	1004	0	1118
October 2020	115	7	15	1186	0	1323
January 2021	124	9	19	1373	0	1525
March 2021	131	10	19	1391	2	1553
June 2021	103	7	20	1509	2	1641
October 2021	93	6	12	1566	2	1679

When comparing the number of detected networks to the number of confirmed COVID-19 infections in Southwest Finland (Fig. 3), we observe the onset of the pandemic has indeed correlated with WLAN deployment. This confirms the latter part of our hypothesis. As the number of confirmed infections increases, there is a steady increase in the number of detected WLAN networks. This is especially clear during the second and fourth waves of the pandemic between June 2020 and October 2021. During this time, the number of detected networks increased by 50.2%, suggesting some correlation between WLAN deployment and COVID-19 infections and restrictions.

A deeper inspection of the June 2021 survey results revealed significant changes in the city centre's WLAN infrastructure. At some time during the spring of 2021, the city administration had updated the WLAN networks it provides for its employees, residents, and schools. This change added roughly 117 new wireless networks to the city centre area and updated 23 previously unencrypted networks to use WPA2 encryption. Without these added networks, the number of detected networks in June 2021 would decrease to the level of January 2021.

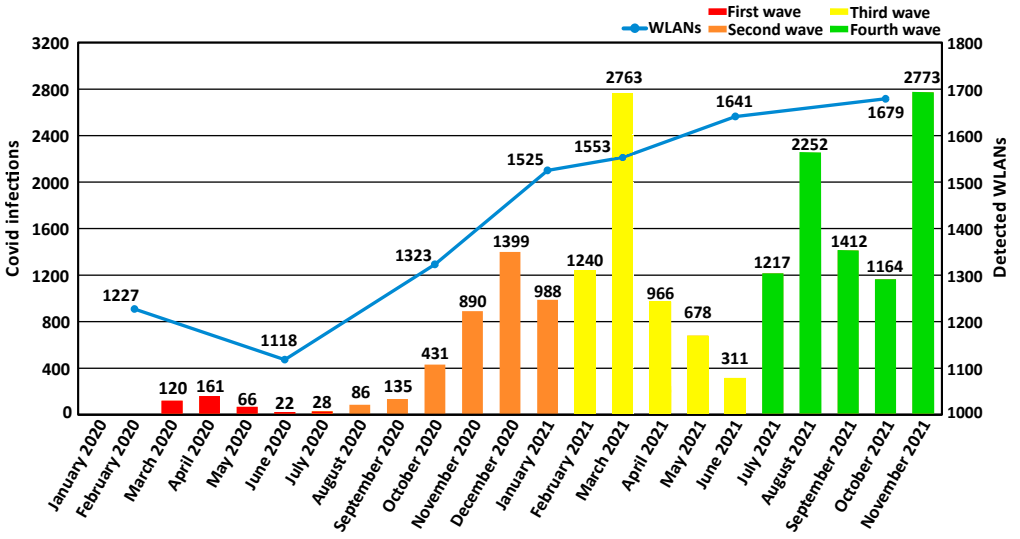

Fig. 3. New COVID-19 infections per month (vertical bars) in Southwest Finland and detected WLAN networks (blue line) in the survey region during the pandemic.

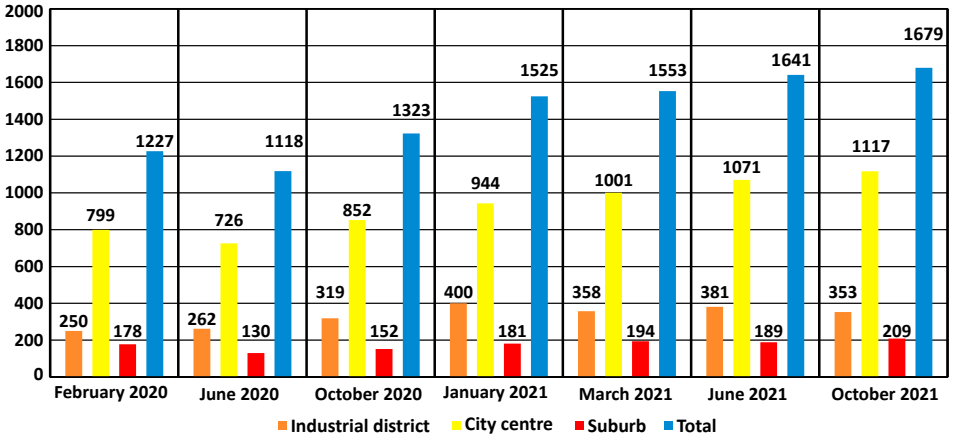

Fig. 4. WLAN network deployment during the pandemic by survey location

The WLAN deployment numbers also interestingly show an 8.8% decrease between February and June 2020, after the first wave of the pandemic had ceded and many of the restrictions had been lifted (Fig. 4). Similarly, in June 2021, deducting the 117 networks added by the city administration from the results would result in a 1.9% decrease in detected networks between March and June 2021. We believe the decreases occurred in part because the June surveys were conducted during the summer holiday season, which may have led some individuals and small businesses to temporarily turn off their wireless network devices. This speculation is supported by the fact that the number of detected networks declined only in the city centre and suburb areas as seen in Fig. 4. We also speculate that the decrease in detected networks in the Industrial district between January 2021 and March 2021 could be a consequence of the increasing restrictions, resulting in smaller businesses shutting down their wireless networks due to increased telecommuting.

5. Conclusions

We presented an analysis of the COVID-19 pandemic's effects on WLAN security and abundance in Southwest Finland. We set the premise for this study by defining two hypotheses: the vast increase in telecommuting due to the

COVID-19 pandemic 1) creates an incentive to upgrade obsolete devices, thereby improving WLAN security, and 2) results in an increase in WLAN deployment as large portions of the population work and study remotely. To the best of our knowledge, no similar research about the COVID-19 pandemic's effects on the WLAN landscape has been published.

Our research data shows that while WLAN deployment increased 50.2% during the second and third waves of the pandemic, there was no advancement in the state of WLAN security. The findings suggest that although new wireless devices and networks were increasingly deployed during the pandemic, it was not done to replace outdated and insecure devices, indicating deficient wireless networking security awareness among the general population. WLAN connections should always be protected with either the WPA2 or the WPA3 encryption protocol. Legacy devices supporting the deprecated WEP and WPA-TKIP protocols should be upgraded. The use of public unencrypted networks should be avoided altogether. In this time where we are increasingly dependent on wireless internet connections, and the number of WLAN capable devices is increasing by the day, raising WLAN security awareness is crucial for cybercrime prevention both during and after the pandemic.

References

[1] Aruba Networks, 2020. Innovative multi-agency Wi-Fi Bus proof of concept delivers connectivity to digital deserts using Aruba SD-Branch Gateways, Wi-Fi and Central. https://www.arubanetworks.com/resources/case-studies/wi-fi-bus/. (Accessed: November 28, 2021).

[2] Cache, J., Wright, J., Liu, V., 2010. Hacking Exposed Wireless, Second Edition: Wireless Security Secrets and Solutions. 2nd ed., McGraw-Hill, New York, USA.

[3] Dmitry, G., 2020. Remote spring: the rise of RDP bruteforce attacks. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/. (Accessed: September 11, 2021).

[4] Eurofound, 2021. Living, working and COVID-19 dataset. https://www.eurofound.europa.eu/data/covid-19. (Accessed: September 1, 2021).

[5] Finnish institute for healt and welfare, 2021. Covid-19 cases in the infectious diseases registry. https://sampo.thl.fi/pivot/prod/fi/epirapo/covid19case/fact_epirapo_covid19case. (Accessed: December 1, 2021).

[6] Georgiadou, A., Mouzakitis, S., Askounis, D., 2021. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal , 1–20.

[7] Hurley, C., Rogers, R., Thornton, F., Connelly, D., Baker, B., 2007. WarDriving and Wireless Penetration Testing. 1st ed., Syngress Publishing Inc, Rockland, USA.

[8] Interpol, 2020. Cybercrime - Covid-19 Impact. Technical Report. Interpol. Lyon, France.

[9] Kaspersky Lab, 2020. How COVID-19 changed the way people work. Technical Report. Kaspersky Lab.

[10] Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R., Durumeric, Z., 2019. All things considered: An analysis of IoT devices on home networks, in: 28th USENIX Security Symposium (USENIX Security 19), USENIX Association, Santa Clara, CA. pp. 1169–1185. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak.

[11] Lindroos, S., Hakkala, A., Virtanen, S., 2021. A systematic methodology for continuous WLAN abundance and security analysis. Computer Networks 197, 108359.

[12] Mizuo, A., 2020. Wifi on wheels delivers internet to westside families, promoting distance learning. https://www.hawaiipublicradio.org/post/wifi-wheels-delivers-internet-westside-families-promoting-distance-learning. (Accessed: November 28, 2021).

[13] Parker, K., Menasce-Horowitz, J., Minkin, R., 2020. How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work. https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/. (Accessed: September 10, 2021).

[14] Pietenpol, L., 2020. Cybersecurity in the time of covid. Quality Progress 53, 7–8.

[15] Powel, M., 2021. Wi-fi router security knowledge gap putting devices and private data at risk in uk homes. https://sampo.thl.fi/pivot/prod/en/epirapo/covid19case/fact_epirapo_covid19case?&row=hcdmunicipality2020-445222&column=dateweek20200101-509030. (Accessed: November 28, 2021).

[16] Sak, B., Jilumudi Raghu, R., 2016. Mastering Kali Linux Wireless Pentesting. 1st ed., Packt Publishing, Birmingham, United Kingdom.

[17] Toronto.ca, 2020. City of Toronto and partners help connect vulnerable populations with internet access during COVID-19 pandemic. https://www.toronto.ca/news/city-of-toronto-and-partners-help-connect-vulnerable-populations-with-internet-access-during-covid-19-pandemic/. (Accessed: November 28, 2021).

[18] Trend Micro Research, 2020. Securing the Pandemic-Disrupted Workplace. Technical Report. Trend Micro Research. Irving, Texas, USA.

[19] Weidenbach, P., Vom Dorp, J., 2020. Home Router Security Report 2020. Technical Report. Fraunhofer Institute for Communication, Information Processing and Ergonomics. Wachtberg, Germany.