PERSONNEL PRIVACY AND ORGANISATIONAL DATA: THE AWARENESS AND POLICY ENFORCEMENT FOR SMARTPHONE SECURITY AMONG THE MALAYSIAN ARMED FORCES PERSONNEL

Suriatie Alias, Mohd Fahmi Mohamad Amran, Syahaneim Marzukhi, Muhammad Fairuz Abd Rauf

Faculty of Defence Science and Technology, National Defence University Malaysia, Kuala Lumpur 57000, Malaysia
fahmiamran@upnm.edu.my

Abstract. The utilisation and people's dependency on smartphones in this digital era are unavoidable. Smartphones play certain functions in every lifestyle and have become 'a must have' gadget to everyone. Some new issues emerge when the users do not consider the security of their multipurpose mobile devices, leaving an opening to digital crime. This includes the use of various communication applications which are prone to security breach. There have been complaints of misuse or improper handling of smartphone usage among Malaysian Armed Forces (MAF) personnel, which also falls under the category of information security. This paper focuses on identifying the perception of smartphone usage and security awareness among the MAF which data from 100 participants has been gathered and analyzed. The MAF personnel are not exceptional to the prevalence of smartphone usage, making them also at risk of being targeted by the enemy or any particular parties with bad agendas towards the organization and the country.

Keywords: Security, Policies, Awareness

1 INTRODUCTION

Smartphones have had a significant effect on society and other facets of life, with people shifting away from traditional mobile phones as smartphones became the norm among people in the community (Sarwar and Soomro, 2013). The expanding usage of smartphones comes with advantages and disadvantages (Parker et al., 2015). With a massive amount of data available in smartphones nowadays, it has become one of the main targets for intruders to get information. Therefore, mobile security is the critical element based on the rapid data growth and smartphone market shares (Becher et al., 2011). Due to its size and functionality, the most significant threats of smartphones are data loss, wireless network attackers, malicious applications, and physical theft (Parker et al., 2015).

1.1 Background of study

Generally, a smartphone is a mobile phone that can do more than make phone calls and submit text messages. Smartphones, like laptops, can enter the Internet and operate software programs. Smartphones enable users to communicate with them using a touch screen. Normally, users look for access to the services unaware of the potential related risk, while they become connected with a constant network. The desire to enjoy the unique features and multiple applications of smartphones might leave users vulnerable, especially when using free Internet networks. Such practices are common even across systems or networks with faulty and unmanaged configurations that will leave users defenceless against unauthorised access, agreeing to the associated risks. Thus, vulnerabilities emerging from users conduct or structure deficiencies can encourage destructive action, permitting enemies to dispatch attacks that can prompt protection ruptures and fraud (Gkioulos et al., 2017). Considering this, users must know about the related risks, and, all the more critically, users must be aware of the appropriate actions and protection to change the system's set-up and configuration for the users' safety.

All levels of MAF personnel are subject to the Laws of Malaysia Law Act 77, the Armed Forces Act 1972. Beside that, the MAF personnel are responsible to maintain the military security without compromise whereas any breaches and disobedient may subject a personnel to disciplinary and legal action in accordance with the provisions of certain Laws of Malaysia that have been outlined. In terms of ensuring the security of all areas of the service, military security refers to the procedures taken to ensure the highest degree of information security, personnel security, and property security at all times. Threats to security aspects can occur in the form of subversive action to personnel, espionage of information, sabotage of property, terrorism, attacks or cyber threats, as well as human weaknesses (Bahagian Staf Perisikan Pertahanan, 2019).

Nowadays, smartphones run indistinguishable procedures and applications similar to a personal computer. Thus, the users change their interest in the smartphone to improve their routine activity and expand their social network. However, some new issues emerge when the users do not consider the security of their multipurpose mobile devices, leaving an opening to digital crime (Rondeau and Hopkins, 2014). This matter is a serious and thoughtful security problem for all users, particularly those who use smartphones insecurely or without adequate security protection (Rondeau and Hopkins, 2014).

Today's swift working culture has demanded quick access to information. While the widespread use of smartphones is unquestionably advantageous in this case, it implicitly compromises some information security principles. According to Ikram (2019), one of the information security models is the CIA Triad, which is Availability of information, Confidentiality of data and privacy, and Integrity of information that requires Authenticity and Accountability. The CIA Triad emphasises fundamental data security objectives and serves as a guide for any organisation to safeguard sensitive data from any unauthorised access and data exfiltration. However, while smartphones only meet the principle of Availability, Confidentiality and Integrity are not guaranteed if no strong control or enforcement is in place in any organization.

No doubt, the employees in Malaysia, in the Private and Government Sector, even the personnel in defense organizations are also benefiting from the convenience of smartphones. Due to the growth of data and information sharing and the ease of use of smartphones, the Ministry of Defence (MINDEF) personnel, including civilian, army, navy and air force personnel, use various techniques and applications to enhance the operational performance and increase information sharing. The practice includes using some of the technology and unknown security control applications, such as WhatsApp and Telegram. However, recent progress has revealed that these type of communication platforms is prone to the security breach. For example, local press has reported that "the security hole in the WhatsApp messaging could enable an attacker to inject malware to gain access to Android or Apple smartphones" (The Star, 2019). Therefore, users who hold an important position should consider this kind of security issue dealing with sensitive data when using their smartphones to perform their tasks.

The possible threats towards the national defense organizations and MAF are always prominent. Latest statement issued by the Chief of Armed Forces that the MAF are constantly strengthening their cybersecurity and defense capabilities to counter any threat, especially from foreign elements, and to avoid any disruption to the MAF and MINDEF's operations. The MAF also released an internal directive emphasizing the importance of enhancing the country's cyber defenses following the cyber threat from Israel on 17th May 21 (The Star, 2021).

These incidents show that the organizations and personnel belonging to MINDEF are significantly prone to security threats. The MAF website frequently accessed by the personnel using their smartphones could lead to a more severe attack such as eavesdropping. Hence, it is essential to educate the MAF personnel regarding security awareness when utilizing their smartphone. Besides that, it is important to enhance the awareness of responsibility when disseminating and sharing restricted organizational information through smartphones in preventing data leakage to unauthorized users.

2 LITERATURE REVIEW

2.1 Introduction

This part will highlight previous studies and articles on smartphone topics. It comprises the influence of smartphones in Malaysia, perception towards smartphone usage, smartphone potential threats and risks and awareness issues.

2.2 Influence of smartphones in Malaysia

Over the years, smartphones are becoming a big and lucrative industry and are rising tremendously in Malaysia (Harun et al., 2015). According to Norhayati-Wolff (2020), in the Asia-Pacific region, the smartphone adoption rate reached 64% in 2019, anticipated to grow to 81% by 2025. While in Malaysia, the number of smartphone users in the country was about 17.2 million in 2018, expected to reach nearly 21 million in 2023. While 85% of mobile users under the age of 20 have a smartphone, only around 30.6% of users 65 years old have a smartphone. The same income difference is also evident: people who receive over five thousand

Malaysian ringgit are most likely to own a smartphone. However, the distance becomes smaller, and about 59% of Malaysian users with income below one thousand Ringgit Malaysia still have a smartphone. Gong (2020) said Malaysia is a mobile-first country, with a mobile broadband penetration rate of 123% in 2019 compared to a fixed broadband penetration rate of 9%. In other words, the average Malaysian has at least one method of connecting to the Internet and prefers to do so through mobile broadband.

2.3 Perception towards smartphone usage

An article written by Rohrig (2015) states that, in 2014, more than one billion smartphones were purchased worldwide. It is also reported that 84% of US citizens would not last a day without mobile phones. In the year 2017, Edwards (2017) said that there were 2.5 billion smartphone users worldwide. Even smartphone users are seen as similar in needs and preferences, but there is a diverse set based on smartphone adoption. Referring to a study conducted by Zhao et al. (2017) towards 106,762 Android users from multiple provinces in China, in one month of usage, they learned that there are 382 different categories of users based on their application usage behaviours. They labelled the most significant cluster as "Screen Checkers", where they wake up the screen but seldom unlock and enter the interface. This finding shows that most people own a smartphone, although with minimum use or interaction.

According to Harun et al. (2015), people seem to rely on smartphones due to the gadget's simplicity, excellent camera features, simple program installation, and, most importantly, the ability to perform most computer functions while on the go. These features define the benefits of smartphones and justify why people are so dependent on smartphones. According to Edwards (2017), around 5 billion people use a mobile device, where half of it or 2.5 billion are using smartphones. The average smartphone users have over 80 apps, and they use around 40 of them every month. The most popular smartphone app categories are social networking, music, multimedia, and games.

Smartphones have also become increasingly relevant to the military environment. Smartphones are employed as a medium for disseminating information and assisting in task execution due to their convenience features, such as executing functions like a mini-computer and being pocket-sized. It is not overemphasized that smartphones are anticipated to be able to restructure an army in the future. Wong (2021) said that the era of the digital revolution has influenced the smartphone is the single breakthrough that will fundamentally transform the modern battlefield. The smartphone has grown so pervasive and popular due to three important and interrelated factors: connectivity, flexibility, and convergence. These three criteria will influence how future armies utilise smartphone technology to achieve decisive advantages in future wars.

2.4 Smartphone's potential threats and risks

Mobile device threats, including smartphones, commonly, hackers are believed as at the heart of many attacks. However, certain threats are completely unintentional and can appear anywhere, whether with personal devices or any organisation. It also happens due to natural

human weaknesses such as a lack of awareness and a complacent attitude. According to Becher et al. (2011), from Q3/2009 to Q3/2010, the number of cell phones running a full-fledged operating system increased by nearly 200%. As a consequence, mobile protection is no longer optional but rather necessary. Table 1 shows various types of malware activities:

Table 1 Various Types of Malware Activities (Source: Jian et al. (2016))

Threat	Areas Being Compromised/Approach
Data Theft	Accounts Contacts Call logs Emails Files and documents International mobile identity number (IMEI) Phone numbers
Surveillance	Audio Camera Phone calls Locations SMS messages
Impersonation	Posting to social media Sending email messages SMS redirection
Financial	Extortion via ransomware Fake antivirus Making expensive calls Sending premium SMS messages Stealing transaction authentication numbers
Botnet Activities	Click fraud Launching DDoS attack Sending premium SMS messages

There are few significant areas in smartphone become targets or prone to any threats. However, Zlatanov (2016) identifies three major areas commonly targeted by attackers: data, identity, and availability.

3 METHODOLOGY

3.1 Introduction

This section aims to define the approaches and methodology used for the research to achieve its objectives. As described previously, this study aims to identify the level of security awareness regarding potential threats and risks among the MAF personnel in using smartphones for their daily routine work.

3.2 Research approach

Research strategies or research approaches can be classified into four categories: case study, quantitative strategy, qualitative strategy, and action research. According to Patten and Newhart (2017), approaches can differ depending on the question asked, the researcher's opportunities and resources, and the existing evidence to address the problem. For this particular study, the researcher will use the quantitative approach. The quantitative method will be based on a survey conducted among a number of military personnel at the respective departments. This survey will provide the primary data that will be analyzed statistically to answer the research objectives.

3.3 Research strategy

The research questions and objectives guide the choice of the research strategy. To answer the research questions, the survey, usually associated with deductive research (Saunders, M., Lewis, P., & Thornhill, 2013) will be conducted. The survey involves collecting knowledge from a group of individuals for reacting to different questions. For this particular survey, there are two types of questions; closed-ended and open- ended questions. Closed-ended questions provide respondents with a list of options, whereas open-ended questions allow them to express their views freely.

In this study, the targeted respondents are military personnel working at various departments and branches under MAF headquarters. A random sampling approach is carried out but with a selection of departments to ensure a set of relevant respondents are chosen. Various levels of rank are involved from lower-level management, middle management and upper management. The selection of respondents is based on a few factors, which are rank, from Senior Non-Commissioned Officer (NCO) to Major, year of service, expertise and experience. This group of ranks is the main element of executing and implementing roles and tasks of an organisation at tactical level, which means they access and hold the organisational important data and information. The main targets are those involved with human resources, operation, training, logistics, administration and finance matters. The detailed demographic factors that have been considered for the respondents are gender, age, year of service, rank, higher education and appointment or job scope.

3.4 Data collection through questionnaire

A questionnaire is developed to gather related data required to achieve the first and second research objectives. According to Taherdoost (2017), the author suggested that the sample size is a significant feature for any empirical research in which the purpose is to draw inferences from a sample about a population. A random sample needs to be sufficient to generalise from a random sample to prevent biases and ensure that any sampling errors are at the very minimum. Therefore, a number of participants will be selected to answer the questionnaire related to smartphone usage, perception of the enforcement of the policy, awareness of smartphone security issues, awareness of existing policy and related instructions regarding information security, including smartphone security in MINDEF and the MAF.

The questionnaire also covers awareness of potential threats and risks of using smartphones in their routine task. In this study, the targeted respondents are military personnel working at various departments, branches and directorates under the Services Headquarters. Stratified random sampling is carried out to ensure a set of quality and reliable respondents are chosen. For the sample size of the respondent, a total of 100 participants will be selected. This sample size is adapted based on the calculation proposed by Taherdoost (2017). The questionnaire is built based on four Independent Variables (IV) that will determine the Dependent Variable (DV), which is awareness of smartphone security issues among the MAF personnel. The theoretical framework is shown in Figure 1.

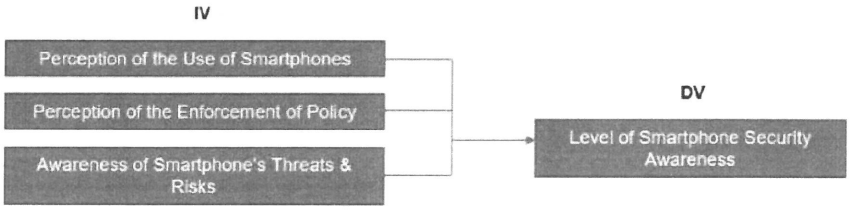

Figure 1 Theoretical framework

The questionnaire comprises seven sections (please refer to Appendix A for the survey questionnaire). It starts with a brief outline of the purpose of the research and getting the participant's consent before proceeding further to answer those questions. The next section is to collect the participant's demographic data. Later on, the questions are divided into that four IV identified earlier that use a five-point Likert Scale technique ranging from Strongly Agree to Strongly Disagree and finished by three open-ended questions. The purpose of the open-ended question is to allow the participant to give comments and suggestions particular to smartphone usage in the MAF.

4 RESULTS

4.1 Analysis

The stability or consistency of test scores is measured by reliability test. The Cronbach's Alpha is the most widely used internal-consistency coefficient for reliability test (Glen, 2016). The reliability test result is 0.902. If the value of Cronbach's Alpha is more than 0.7, the data is reliable. Table 2 shows findings based on the results from questionnaire:

Table 2 Findings based on the results from questionnaire

Item	Description
Perception of the use of smart phone	i. Respondents agree that smartphones are important for their daily life and work. ii. They agree that smartphones have become the main communi¬cation platform in the workplace. iii. They agree that smartphones have become the leading com¬munication platform and working tool in the MAF. iv. The percentage of agree level of smartphone usage is significantly lower for The Senior NCO than the Officer. Therefore, the NCO is also more preferable to choose unsure/neither agree nor disagree than the Officer. v. There are differences in perception of smartphone use between the Officer and Senior NCO group (Mann-Whitney U Test Results)
Perception of the enforcement of policy	i. Respondents agree that the Service (MAF) emphasises the se¬curity of information and personnel data, and the personnel are regularly briefed on security risks and policy. ii. In term of policy enforcement, both groups agree that the en¬forcement is strictly implemented but at only a satisfactory level (79% and 67%). The neutral stance or unsure rate is also high (21% and 33%). iii. Specifically, on incident response policy, only 71% (Officer) and 52% (Senior NCO) agree that a clear policy is there to be followed.
Awareness of smartphone's threats and risks	i. Both groups state that they take necessary steps to protect their personal data (90% Officer, 81% Senior NCO). However, the rate is lower in protecting the organisational data (88% Officer, 76% Senior NCO). ii. Both groups admit that sometimes they have to use the smartphone to execute urgent tasks regardless of data confidentiality, but they also choose natural stance/unsure with the issue (Officer 43% agree/do, 34% disagree/not do, 23% neutral/unsure, Senior NCO 34% agree/do, 33% disagree/not do, 33% neutral/unsure). iii. In terms of accessing social media through smartphones, both groups admit the habit (Officer 92%, Senior NCO 77%). iv. Some respondents admit that they use public Wi-Fi to perform banking transactions (Officer 24%, Senior NCO 33%). While some respondents admit that they use public Wi-Fi because it is convenient (Officer 23%, Senior NCO 33%). v. Both groups state that they are aware of smartphone security risks (Officer 100%, Senior NCO 86%).

4.2 Findings

Based on the findings from the survey, the perception of smartphone usage among MAF personnel can be identified and assessed as the followings:

i. The MAF personnel, regardless of rank, job scope, expertise and experiences, are dependable to smartphones, where they need smartphones for their daily routine and working purposes.

ii. The MAF personnel rely upon the smartphone, and they admit that the gadget has become the main communication platform and working tool in the MAF.

iii. This finding on dependency matter is consistent with previous studies by Ruggiero and Foote (2011), Rohrig (2015) and (Edwards, 2017). People prefer smartphones because of their convenience feature, the gadget's simplicity, excellent camera features, simple program installation, and the ability to perform most computer functions. These features define the benefits of smartphones and justify why people are so dependent on smartphones, as explored by Harun et al. (2015).

iv. The increasing use of smartphones in the workplace is not something new or unusual. Ruggiero and Foote (2011) quoted that mobile phones are being used for a growing variety of tasks and confidential data such as email, schedules, contact details, and passwords storage. Besides, the features of social networking apps allow users to perform commerce and banking transactions.

v. However, based on the survey, there is a difference in terms of perception of smartphone usage and dependency level between the Officer and Senior NCO, whereby Officers are identified as more dependable to smartphones. The situation is relevant because Officers hold greater roles and bear higher responsibilities in any military force. Not to say that Senior NCOs refuse to acknowledge the importance of smartphones, but they prefer to reserve their comment for own reasons.

The survey findings also have answered the question about the awareness level of smartphone's potential threats and risks among MAF personnel. Further assessments are as follows:

i. Based on hypothesis testing, there are no significant differences in the awareness level among the MAF personnel, particularly between Officer and Senior NCO. However, some aspects should be considered, where the MAF personnel keep their credentials and organisational data for easy and quick access when that information is required. Moreover, for them to utilise the smartphone definitely, they will install various applications. This circumstance means that the MAF personnel are prone to smartphone risks such as data leakage, phishing attacks and malicious apps.

ii. In terms of specific measures for smartphone users to protect their privacy and guard any organisational data kept in the smartphone depend on individual basic knowledge and awareness in smartphone usage.

iii. Although the survey identifies that the MAF personnel, as smartphone users, are aware of the gadget's possible threats and risks, they believed the awareness should be improved and enhanced.

iv. It is important to emphasise smartphone awareness in the MAF since the personnel are dependable on the gadget. As mentioned in previous studies, smartphone characteristics and widespread use can lead to certain consequences and risks.

v. As stressed by Al-Hadadi and Al Shidhani (2013), the security of a smartphone

depends on the operating systems that include a variety of software the user can download. Some programs are created by reputable application development companies, while others are created by hobbyists and inexperienced programmers

vi. The MAF, as a military organisation, faces a higher risk than the commercial company or enterprise since smartphones are being utilised. The utilisation of smartphones in the MAF is in line with Zlatanov (2016) statement that the gadget is increasingly used as networking tools for planning and managing professional and personal lives by a growing number of consumers and businesses. These advancements are driving significant changes in how firms organise their information systems, and as a result, they have become a source of new risks. Smartphones collect and compile a rising amount of sensitive data, to which users' privacy and the company's intellectual property must be protected.

vii. P. DeMuro (2018) has identified eight reasons why smartphones are serious threats; tracking function, malicious apps, risk of using public Wifi, need of protection by virus, risks of own camera, microphone eavesdropping, lack of security patches and backdoor threat.

5 SUMMARY

The perception of smartphone usage and awareness of smartphone's potential threats and risks among the MAF personnel have been identified. The findings indicate that the MAF personnel are dependable on smartphones and admit that the devices have become the main communication platform and working tool in the MAF. The use of smartphones and dependency on gadgets among MAF personnel must be tackled positively. It is because of the conveniences and the need to cope with current role and task challenges, which require the personnel to act swiftly. As smartphones become easy targets to cyber-attacks, the smartphone security issue, the awareness of smartphone's potential threats and risks, the awareness towards policies and instructions, and policy enforcement are the key elements to be emphasized by any department heads and commanders. Moreover, MAF personnel as users are exposed to the new form of threat, where radicalism and terrorism use social media to spread ideology.

6 ACKNOWLEDGMENT

The authors greatly acknowledge Ministry of Higher Education Malaysia and National Defence University Malaysia for the financial support. Special thank you to the reviewers for their valuable comments and suggestions.

References

1. Bahagian Staf Perisikan Pertahanan (2019) Perintah Keselamatan Angkatan Tentera Malaysia 2019.

2. Becher, M. et al. (2011) 'Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices', Proceedings - IEEE Symposium on Security and Privacy. IEEE,

(March 2010), pp. 96-111. doi: 10.1109/SP.2011.29.

3. Edwards, B. (2017) 'Do you know what's in your pocket?', Family Practice Management, 20(4), pp. 23-28.

4. Gkioulos, V. et al. (2017) 'Security awareness of the digital natives', Information (Switzerland), 8(2), pp. 1-13. doi: 10.3390/info8020042

5. Gong, R. (2020) Malaysia's Response to COVID-19: Mobile Data and Infrastructure | LSE Southeast Asia Blog. Available at: https://blogs.lse.ac.uk/seac/2020/11/23/malaysias-response-to-covid-19-mobile-data-and-infrastructure/ (Accessed: 28 March 2021).

6. Harun, A. et al. (2015) 'Smartphone dependency and its impact on purchase behavior', Asian Social Science, 11(26), pp. 196-211. doi: 10.5539/ass.v11n26p196.

7. Jian, P. et al. (2016) 'Challenges in Mobile Security', pp. 32-39.

8. Norhayati-Wolff, H. (2020) Smartphone market in Malaysia - statistics and facts | Statista. Available at: https://www.statista.com/topics/6615/smartphones-in-malaysia/ (Accessed: 22 March 2021).

9. Parker, F. et al. (2015) 'Security awareness and adoption of security controls by smartphone users', 2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015. IEEE, pp. 99-104. doi: 10.1109/InfoSec.2015.7435513.

10. Patten, M. L. and Newhart, M. (2017) Understanding Research Methods: An Overview of the Essentials - Mildred L. Patten, Michelle Newhart - Google Books. Available at: https://books.google.com.my/books?hl=en&lr=&id=YAoqDwAAQBAJ&oi=fnd&pg=PP1 &dq=Patten,+M.L.+and+Newhart,+M.+(2017)+%27Understanding+research+methods:+An+overview+of+the+essentials%27,+Taylor+%26+Francis.+&ots=1gAy-PPOlDs&sig=3AFu4GnhcfXmHZS3UE3KrpyvUVs&redir (Accessed: 2 May 2020).

11. Rohrig, B. (2015) 'Smartphones. Smart chemistry', ChemMatters, pp. 10-12. Available at: https://www.acs.org/content/acs/en/education/resources/highschool/chemmatters/past-issues/archive-2014-2015/smartphones.html.

12. Rondeau, L. and Hopkins, D. (2014) *Mobile Device Vulnerabilities & Securities, Mobile Device Vulnerabilities & Securities.* Available at: http://commons.emich.edu/honors.

13. Sarwar, M. and Soomro, T. R. (2013) 'Impact of Smartphone's on Society', European Journal of Scientific Research, 98(2), pp. 216-226.

14. Taherdoost, H. (2017) 'Determining sample size; How to calculate survey sample size', International Journal of Economics and Management Systems, 2(2), pp. 237-239.

15. The Star (2019) *WhatsApp, security and spyware: what happened | The Star.* Available at: https://www.thestar.com.my/tech/tech-news/2019/05/17/whatsapp-security-and-spyware-what-happened (Accessed: 27 August 2020).

16. The Star (2021) *Military constantly monitoring cyber threats | The Star.* Available at:

https://www.thestar.com.my/news/nation/2021/05/18/military-constantly-monitoring-cyber-threats (Accessed: 22 May 2021).

17. Wong, E. (2021) How Smartphones will Reshape the Modern Battlefield - Modern War Institute. Available at: https://mwi.usma.edu/smartphones-will-reshape-modern-battlefield/ (Accessed: 6 June 2021).

18. Zhao, S. et al. (2017) 'Who Are the Smartphone Users?', GetMobile: Mobile Computing and Communications, 21(2), pp. 31-34. doi: 10.1145/3131214.3131224.

19. Zlatanov, N. (2015) Computer Security and Mobile Security Challenges. Conference: Tech Security ConferenceAt: San Fransisco, CA.