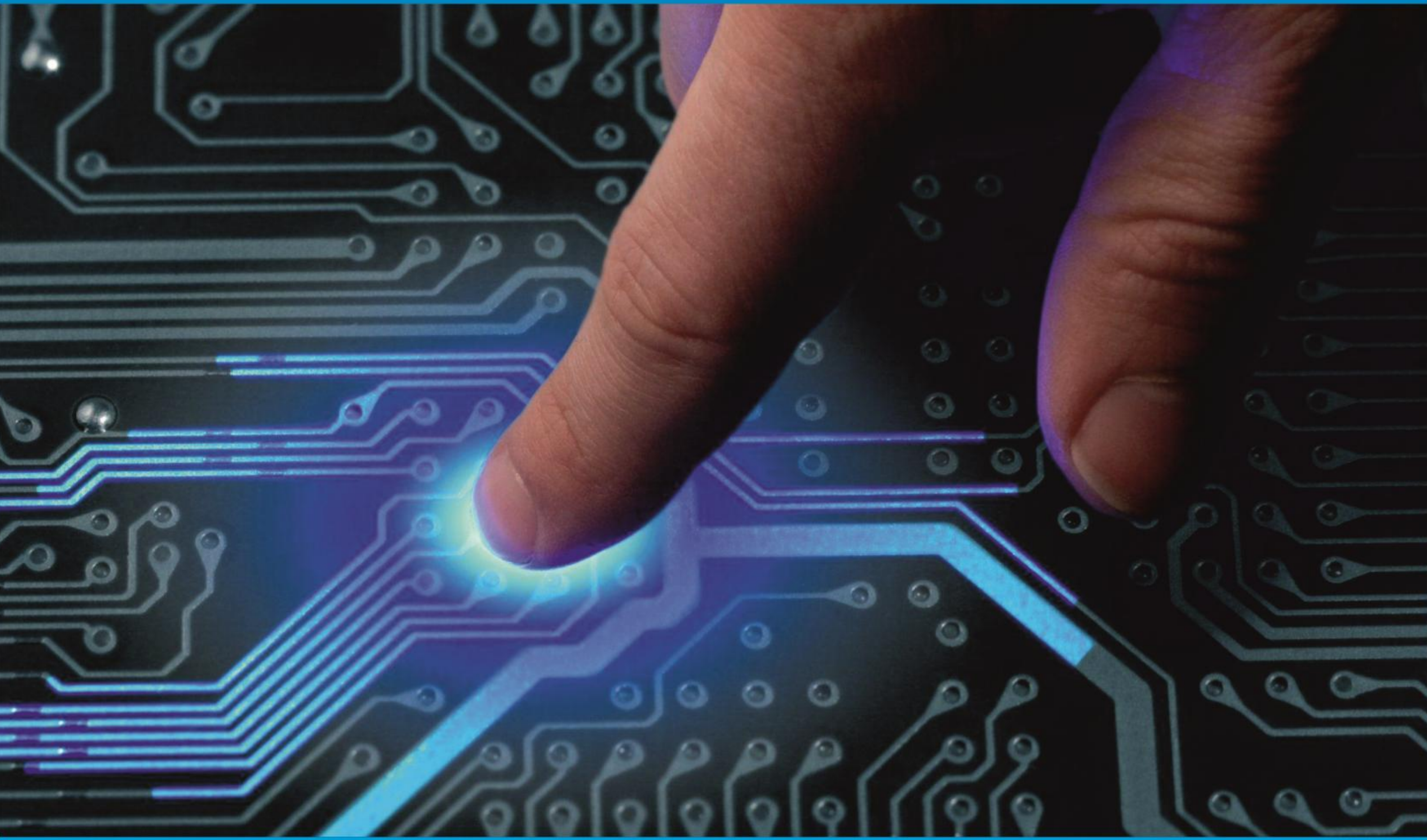
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| DOI: 10.15680/IJIRCCE.2021.0905037 |

Mobile Devices as a Major Cyber Security Risk

Tirth Dodiya[1], Sharad Kumar Singh[2], Samson Sathe[3], Ms.Rajeshwari Gundla[4]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[1]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [2]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [3]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [4]

ABSTRACT: Mobile phones are becoming a vehicle to provide an efficient and convenient way to access, find and share information however, the availability of this information has caused an increase in cyber-attack and currently cyber threats range from Trojans and viruses to botnets and toolkits. In today’s world, 96% of smartphones do not have pre-installed security software. So this lack of security and an opportunity for malicious cyber attackers to hack into the various devices that are popular that is Android, iPhone, and Blackberry. Traditional and old security software found in personal computers (PCs) such as firewalls antivirus and encryption is not currently available in smartphones. Besides, those affected smartphones are even more vulnerable than personal computers because more people are using smartphones to do personal tasks. Nowadays mobile phone users can email, use social networking applications (Facebook and Twitter), buy and download various applications, and shop. Moreover, users can now conduct monetary transactions such as buying goods, redeeming coupons and tickets, banking, and processing point-of-sale payments. Not so many transactions are especially attractive to cyber attackers because they can gain access to bank account information after hacking a user’s smartphone. Mobile phones (smartphone) are small and are portable. The convenience of using smartphones to do personal tasks is the loophole cyber attackers need to gain access to personal data. The paper examines the importance of developing a national security policy created for mobile devices so that it protects sensitive personal data.

KEYWORDS: Smartphones Vulnerabilities, Trojans and Viruses, Cyber-attacks, Security Softwares, Loophole Cyber attackers, Malicious Scripting.

I. INTRODUCTION

Also Now a days smartphones are the preferred device for web browsing, emailing, using social media, and making online purchases. Smartphones are easily carried in people’s pockets, purses, or briefcases. Sadly the popularity of smartphones is a breeding ground for cyber attackers. Operating systems on smartphones are not so strong security software to protect data. In computers (PCs) such as firewalls, antivirus and encryption currently, this is not available in smartphones. In addition to this mobile phone operating systems are not frequently updated like their PC counterparts. The attackers can use this gap in security to their advantage [2]. An example of this gap in security is seen in the 2011 Valentine’s Day attack. The Attackers dispersed a mobile picture-sharing application that covertly sent premium-rate text messages from a user’s mobile phone.

Mobile applications are constantly encountered and very easy to install on almost every mobile operating system. Result of competitive competition among application providers, we all can observe more and more advanced and customized applications appearing on the market resolving complex problems. These applications greatly change a user’s behavior by facilitating their day-to-day transactions or work [3].

II. LITERATURE SURVEY

Many people believe their smartphones try to do numerous activities, like sending emails, storing contact information, passwords, and other sensitive data. In addition to the present, smartphones are the device of choice when it involves social networking; thus, mobile applications for social networking sites (Facebook, Twitter, Google+) are another loophole for cyber attackers to realize personal data from unsuspecting users (Ruggiero, 2011). Social networking sites are host to a surplus of private data. That is why malicious applications that use social networking sites to steal data yield severe consequences. Recently, M-Commerce or “mobile e-commerce” has gained popularity in our society [4]. Many smartphone users can now conduct monetary transactions, like buying goods and applications (apps), redeeming coupons and tickets, banking, and processing point-of-sale payments (Ruggiero, 2011). Again all of those smartphone functions are convenient for the user but advantageous for malicious cyber attackers. Ultimately there's a distinct segment in technology for cybersecurity software that is specifically designed for the mobile OS

The consequences of cyberattacks on a smartphone are often even as detrimental, or maybe more detrimental than an attack on a PC. According to Patrick, a researcher, and professor at the Georgia Tech School of computing, mobile apps believe the browser to work. As a result of this, more Web-based attacks on smartphones will increase throughout the year [5]. Neither tray nor also states that IT professionals, computer scientists, and engineers still got to explore the variations between mobile and traditional browsers to completely understand the way to prevent cyberattacks.

According to many researchers, the foremost influential factors which help the spread of mobile technology among customers are as follows:

(i) Gaining access to information that is up to date: there's no more information asymmetry; instead, we will observe information democratization

(ii) Lower production costs, granted by the technology revolution: thus, products/services offered on the market are easier to deliver to the top consumer and, at an equivalent time, more customized to meet individual requirements

(iii) Fast access to less biased market research: the private character of mobile technology allows real-time information to be gathered about consumers supported their actual behavior

(iv) A shift from accessing only local markets to a worldwide economy and digital channels, yet at an equivalent time, because of the private character of mobile technology, consumers may be accessed in a personalized way

(v) A shift from mass markets to non-public, one-2-one relations

(vi) A shift from “on time” to “right now” mobile technology which allows communication, regardless of what localization and time and, at an equivalent time, with customization of data observed never before

According to the Ericsson Mobility Report, we'll observe growth in mobile subscriptions starting in 2015 and predicted to achieve nearly 9 billion mobile subscriptions in 2025.

The aforementioned report also shows the rapid increase in our consumption of data and points to constant growth within the number of mobile subscriptions and even quicker growth within the number of mobile broadband subscriptions (mobile broadband includes radio access technologies: 3G, 4G, 5G, CDMA20000 EV-DO, TD-SCDMA, and Mobile WiMAX) [6].

According to researchers and agencies, mobile computing is that a phenomenon worth observing since our habits as consumers, a couple of which are listed within the following and are radically changing:

(i) Over 73%, counting on the age bracket, of all emails are opened on mobile devices

(ii) Already in 2017, around 95% of Facebook users accessed the social network via mobile devices

(iii) 80% of users used a mobile device to look the web in 2019

(iv) 40% of online transactions are done using mobile devices

(v) Quite 50% of internet sites now use responsive web design technologies that employment for all devices

(vi) Quite 75% of shoppers use mobile devices alongside physical shopping

(vii) Global mobile data traffic is quite 30 Exabytes per month

(viii) Mobile devices now account for half the online traffic globally, and this grew 68% between Q3 2018 and Q3 2019.

These all data suggest that users are installing mobile apps on their mobile devices, and mobile data consumption is rapidly growing. This trend is visible not only to developers, who are constantly trying to supply a smooth and convenient app experience but also to all or any kinds of hackers, who are interested in obtaining personal information to use during a malicious way against the unaware user [6].

III. MOBILE SECURITY THREATS

Users of mobile devices or so-called mobile users are increasingly subject to malicious activity, mainly concerning pushing malware apps to smartphones, tablets, or other devices employing a mobile OS. These handheld devices, carried in our pockets, are wont to store and protect sensitive information. Even though Google and Apple offer distribution environments that are closed and controlled, users are still exposed to different sorts of attacks. A few of them are given within the following [7].

(i) Phishing in an app: we observed that the method criminals can bypass the app market ASCII text file checks wasn't by including anything malicious within the app itself, but rather by making an app that, in essence, maybe a browser window to a phishing site. Such apps, during this case, are designed in tandem with the phishing site in order that the user features a seamless experience.

(ii) Supply chain compromise: it had been observed that a trepanised version of a legitimate app had been included within the factory firmware from a little mobile manufacturer and shipped to customers on brand new phones. The original app, called Sound Recorder, was found to have been modified to incorporate code that wasn't a part of its stated purpose: it could intercept and send SMS messages secretly. The malicious version of the app could be inserted into the availability chain in several ways to affect various places. It was never made available through any app store, but only during a specific firmware image on a selected model of a cheap Android phone.

(iii) Crypto miner code in games or utilities: we encountered a big jump within the number of apps that, without notification to the user, included crypto-miner code within the app. The code would run whether or not the app itself was running and functioned as a continuing drain on the phone’s (or other device’s) battery.

(iv) Click-fraud advertising embedded in apps: advertisement fraud is, surprisingly, one among the foremost profitable criminal enterprises nowadays, and mobile apps appear to be a key part of this subtle crime. The advertising industry estimates that today the value to advertisers of fraudulently “clicked” ads, consistent with data published by the planet Federation of Advertisers, top US $19 billion annually.

According to Landman, the unprecedented growth within the number of smartphones and mobile workers features a direct impact on the number of attacks deployed on mobile devices. Smartphones today store hefty amounts of knowledge and operate over international cellular networks, WLANs, and Bluetooth PANs. They run various sets of complex operating systems like Symbian, iOS, BlackBerry OS, Android, and Windows Mobile. Most smartphones also support the Java platform for mobile devices, J2ME, with a selection of extensions. All this network connectivity and diverse rich code make these devices more vulnerable than traditional PCs, which usually run standard operating systems that many security products are readily available.

It is also crucial to say top 10 web application security risks consistent with the foremost prominent security community worldwide named OWASP Foundation. Mitigation of those threats would be the primary step within the production of secure code of mobile apps:

(i) Injection

(ii) Broken Authentication

(iii) Sensitive Data Exposure

(iv) XML External Entities (XXE)

(v) Broken Access Control

(vi) Security Misconfiguration

(vii) Cross-Site Scripting XSS

(viii) Insecure Deserialization

(ix) Using Components with Known Vulnerabilities

(x) Insufficient Logging & Monitoring

Conventional viruses haven't been the main threat to smartphones that they need to PCs. More often, the threat is just rogue code or malfunctioning applications that aren't addressed by antivirus vendors focused on the more virulent and simply detectable PC viruses. Threats also exist from lost or stolen mobile devices or accidental/malicious misuse by end-users. Administrators often cannot remotely audit the content of smartphones as mandated within the world organization for Standardization (ISO) 27001 security requirements. They frequently don't know what information has been stored on a phone and should not be ready to remotely delete data or “kill” the device [7-8].

The worldwide information security market is forecast to succeed in $170.4 billion in 2022; the foremost frequent mobile threats include the subsequent

(i) Data leakage: 71% of breaches were motivated by financial aspect and 25% by espionage

(ii) Malware or malicious software: among most malicious email attachments are .doc and .dot which make 37%, and therefore the second highest is .exe

(iii) Phishing and social engineering: 62% of business experienced this sort of attack in 2018

(iv) Direct hacker attack: data breaches exposed 4.1 billion records within the half of 2019

(v) Intercepting communication: hackers globally attack every 39 seconds which makes, on average, 2244 times per day

(vi) Stolen and lost phones: by 2020, the estimated number of passwords employed by users will grow to 3000 billion

(vii) User behavior: 64% of USA citizens haven't checked to ascertain if they were suffering from a data breach [9].

IV. MALWARE AND ITS DETECTION IN MOBILE DEVICE

Smartphones are quickly approaching PC capabilities, and therefore the same incentives exist for hackers: fraud, stealing personal and business information, and extortion—hackers are poised for the attack, with many various avenues available to spread malware. The following brief review of smartphone malware shows that the malicious capabilities of hackers are clearly demonstrated; these are just a few of the malware threats listed within the report by MobileIron [10].

Learning-based approaches using hand-designed features are applied extensively to both dynamic and static malware detection. A variety of comparable approaches to static malware detection have used manually derived features, like API calls, intents, permissions, and commands, with different classifiers like support vector machine (SVM), Naive Bayes, and k-Nearest Neighbour. Malware detection approaches have also been proposed that use static features derived exclusively from the permissions requested by the appliance. In contrast with approaches using high-level hand-designed features, n-grams based malware detection uses sequences of low-level opcodes as features. The n-grams features are often wont to train a classifier to differentiate between malware and benign software. Perhaps surprisingly, even a 1-gram based feature, which is just a histogram of the number of times each opcode is employed, can distinguish malware from benign software. The length of the n-gram used and the number of n-gram sequences used in classification can both have an effect on the accuracy of the classifier. However, increasing either parameter can massively increase the computational resources needed, which is an obstacle of ordinary n-gram based malware detection approaches. The N-grams method also requires feature selection to scale back the length of the feature-vector, which might rather be many elements long within the case of long n-grams. In this work, we propose a method that allows very long grams features to be used, and allows an n-grams classifier to be trained in a much more efficient manner, based on neural networks [11].

(i) Android GM Bot—spyware, usually from third-party app stores, which tries to trick users into abandoning their bank credentials

(ii) Ace Deceiver iOS malware—malware that works to steal a user's Apple ID

(iii) Marcher Android malware—malware that pretends to be a bank website within the hope that users will hand over their login credentials

(iv) Backdoor families—distributed via Google Play Store as trepanised apps hidden within different types of applications [12].

(v) Mobile miners—distributed via spam e-mail or SMS, an application that uses processing powers of mobile devices

(vi) Fake applications—a malware category of apps that mimics popular and useful applications, once installed asks the user for mobile verification or redirects to a link with instructions

Last but not least, applications and therefore the given OS should be maintained so far to maximize their protection, and running an antimalware app is additionally recommended [13].

V. PHISHING AND SOCIAL ENGINEERING

The main platform for phishing attacks is spam emails, which are sent calls in mass quantities by cybercriminals. Recently, we have witnessed a new form of phishing, which is using SMS text messaging (so-called “smashing”) to send a fraudulent link to a mobile device. Social media also are employed by hackers to require advantage of mobile users.

This type of attack is aimed toward users directly, most often exploiting human psychology instead of using technical hacking techniques. This aims to:

(i) Make money from a little percentage of recipients who answer the message

(ii) Run phishing scams—to obtain passwords, credit card numbers, bank account details, and more

(iii) Spread malicious code onto recipients’ devices

Protection against this sort of attack is sense-based and concerns mainly not responding to dubious messages, keeping applications up so far, etc [14-15].

VI. DIRECT HACKER ATTACK AND INTERCEPTING COMMUNICATION

Contemporary users have access to stylish mobile devices which are a part of their everyday lives, and this directly results in a rise in the number of users. This rapid climb in users entices hackers to either intercept communication or directly attack mobile devices.

According to Bishop, there are three prime targets for hackers

(i) Data—mobile devices store data and should contain sensitive data of all kinds

(ii) Identity—mobile devices are customizable, so it's easy to associate a tool with a selected person, so stolen identity could also be wont to commit other offenses [6].

(iii) Availability—limiting access to a tool or maybe depriving the owner of its use

Intercepting communication concerns a situation during which 2 mobile devices are communicating, usually via a public LAN—the users believe they're in direct communication. This interception of communication is named a man-in-the-middle attack (MITM); the perpetrator redirects the info route, either eavesdropping or impersonating one among the parties, to steal personal data. To prevent this type of attack, users should

(i) Avoid public Wi-Fi or no password-protected connections

(ii) Pay attention to notifications in their browser

(iii) Conduct sensitive transactions via secure connections

Taking into consideration the above rules, the user of a mobile device significantly reduces the likelihood of the interception of communication and therefore the loss of sensitive data [16].

VII. METHODOLOGY

This is conceptual research, thus the main scope of this research is to illustrate the importance of security software for smartphone operating systems. Case studies in scholarly journals and reports were utilized in the development of this paper. Most sources contain qualitative information, describing predictions of varied cyber-attacks on mobile devices which will occur by the top of 2012. Quantitative methods were also used to assess the statistical increase in cyber-attacks [17].

VIII. REALISTIC TESTING

To assess the potential of our proposed classification technique in realistic environments, we apply our trained network to a completely new dataset. This allows us to demonstrate the real-world potential of our classification technique when applied to an unknown and realistic dataset at a bigger scale. The network used in this experiment was trained on the V. Large dataset, introduced in Section 4. Our new dataset consists of 96,412 benign apps and 24,103 malware apps. The benign apps were randomly selected from the Google Play store and were collected during July and August 2016 [18]. To represent a distinct set of malicious apps, we used another dataset containing known malware apps, including those from the Android Malware Genome Project, but removing the ones overlapping with the training set of the network. Approximately 1 TB of APKs was used in this experiment. The APKs were converted to opcode sequences using a cloud architecture consisting of 29 machines running in parallel, in a process that took around 11 hours. Classification of the opcode sequences was performed using an NVidia GTX 1080 GPU and took an hour to complete. Note that for this experiment we assume that all APKs in the Google Play dataset are benign and all the APKs in the malicious dataset are malicious. Of course, this may be a naive assumption, as malicious apps can exist on Google Play. The cross validation testing was performed on a new dataset. In each cross-validation, fold, approximately 24,000 malware applications and 24,000 benign applications were used. Therefore, to present all applications to the network fourfold cross-validation was used. The results of this experiment are reported in Malware classification results of our system tested on an independent dataset of benign and malware Android applications. We can see from the results in Table 3 that although the f score is lower than previous experiments, our system has the potential to work in realistic environments. This is because our new testing dataset is much larger than the one used for training the network and contains greater variability of applications. The results of this experiment show that the network has learned features with the ability to generalize to real data. In future work, we hope to take advantage of our new dataset to explore more complex network architectures that can be learned given more training data [18-19].

IX. MALWARE ATTACKS ON SMARTPHONE OS

Along with this malware that targets mobile phone operating systems is constantly evolving. An example of this is often seen with “Zeus-in-the-mobile” (Gitmo), a selected sort of malware common to the android operating system.
Gitmo targeted android users’ bank apps; it attempted to Bypass the banking two-factor authentication, steal credentials and gain access to users’ bank Accounts, and ultimately money. So this is just one form of cyber-attacks that professionals are trying to prevent from occurring. Lastly, it's believed that mobile devices are going to be the new vector for targeting networks and important Systems [20]. From the report, Smartphones are an excellent way to spread malware because phones are great storage Devices. A hypothetical example of a cyber-attack against a company’s network is seen when Malware is implanted during a smartphone. For example, an ingenious cyber attacker can write code to remotely control wireless connectivity technology and plant malware on the mobile. If the same phone is connected to a corporate network i.e. the user is charging the phone on the Company’s computer the malware can now attack the company’s network. It professionals Want to stop attacks like that from occurring because the economic consequences of such an event would be catastrophic. Ultimately, a national security standard must be created for mobile devices to guard personal [20-21].

X. THE ANDROID SECURITY MODEL

Android may be a multi-process system where each application (and parts of the system) runs its small-and-medium-sized process. The standard Linux facilities enforce security between applications and therefore the system at the method level; those applications are assigned by users and group IDs. Applications are restricted in what they will perform by a permission mechanism, called permission labels, that uses access control to regulate what applications are often performed. This permission mechanism is fine-grained therein it even controls what operations a specific process can perform. The permission labels are a part of a security policy that wants to restrict access to every component within an application. Android uses security policies to work out whether to grant or deny permissions to applications installed on Android OS [22].

Those security policies suffer from shortcomings therein they can't specify to which application rights or permissions are given because they believe users and therefore the OS to form that guess. They are therefore taking the danger of permitting applications with malicious intentions to access confidential data on the phone. Ong tang, McLaughlin, Enck, and McDaniel (2009) best described this security shortcoming by their hypothetical example of “PayPal service built on Android. Applications like browsers, email clients, software marketplaces, music players, etc. use the PayPal service to purchase goods [23]. In this case, PayPal service is an application that gains permissions that must be allowed to the other applications that use its interfaces” (On tang, McLaughlin, Enck, & McDaniel, 2009). In this hypothetical scenario, it's unknown whether the PayPal application is legitimate or not because there are no thanks to determining whether this is often the particular PayPal service application or another malicious program. Again, Android lacks security measures to work out and enforce how, when, where, and to whom permissions are granted [24].

XI. CONCLUSION & SUGGESTIONS

There are some possible solutions to the cyber security problems with smartphones. Once our society acknowledges that cyber security threats are detrimental not only to one smartphone user but to society as a whole; then the inception of a solution can begin. The value of data is steadily increasing even more than the actual money. It is imperative to establish a culture of cybersecurity because this issue is multifaceted and technology is constantly evolving.

REFERENCES

[1]. Drew, Jeff. "Managing cybersecurity risks." *Journal of Accountancy* 214.2 (2012): 44.
[2]. Harris, Mark A., Karen Patten, and Elizabeth Regan. "The need for BYOD mobile device security awareness and training." (2013).
[3].Wroclaw University of Economics, Komandorska 118/120, Wroclaw, Poland
[4].https://www.Slideshare.net/Dawsoncross-validation/mobile-devices-the-case-for-cyber-security-hardened-systems-and-methods-to-address-security-related-issue 4
[5]. Florida Institute of Technology, USA, 5 Alabama A&M University, USA and Colorado Technical University, USA
[6].https://www.academia.Edu/2431028/Cyber_Security_and_Mobile_Threats_The_Need_for_Antivirus_Applications_for_Smart_Phones
[7]. Gdansk University of Technology, Narutowicza 11/12, Gdansk, Poland
[8]. https://www.researchgate.net/publication/234806389_Managing_smart_phone_security_risks
[9]. Patten, Karen P., and Mark Harris. "The need to address mobile device security in the higher education IT curriculum." *Journal of Information Systems Education* 24.1 (2013): 41.
[10]. Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. Purdue University, 48, 2007-2
[11]. Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011, October). Crowdroid: behavior-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 15-26).
[12]. Shabtai, Asaf, et al. "Andromaly”: a behavioral malware detection framework for android devices." *Journal of Intelligent Information Systems* 38.1 (2012): 161-190.
[13]. Zarni Aung, Win Zaw. "Permission-based android malware detection." *International Journal of Scientific & Technology Research* 2.3 (2013): 228-234.

[14]. Koyun, Arif, and Ehssan Al Janabi. "Social engineering attacks." *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* 4.6 (2017): 7533-7538.
[15]. Hong, Jason. "The state of phishing attacks." *Communications of the ACM* 55.1 (2012): 74-81.
[16]. Kárpáti, Péter, Guttorm Sindre, and Andreas L. Opdahl. "Towards a Hacker Attack Representation Method." *ICSOFT (2)*. 2010.
[17]. Milligan, Patricia Mayer, and Donna Hutcheson. "Business risks and security assessment for mobile devices." *Information Systems Control Journal* 1 (2008): 24.
[18]. Spremić, Mario, and Alen Šimunic. "Cybersecurity challenges in the digital economy." *Proceedings of the World Congress on Engineering*. Vol. 1. 2018.
[19]. Harris, Mark A., and Karen P. Patten. "Mobile device security considerations for small-and-medium-sized enterprise business mobility." *Information Management & Computer Security* (2014).
[20]. Mylonas, Alexios, et al. "On the feasibility of malware attacks in smartphone platforms." *International conference on e-business and telecommunications*. Springer, Berlin, Heidelberg, 2011.
[21]. Mylonas, Alexios, et al. "Smartphone security evaluation the malware attack case." *Proceedings of the international conference on security and cryptography*. IEEE, 2011.
[22]. Mayrhofer, René, et al."The android platform security model." *ar Xivpreprint arXiv:1904.05572* (2019).
[23]. Tesfay, Welderufael Berhane, Todd Booth, and Karl Andersson. "Reputation-based security model for android applications." *2012 IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications*. IEEE, 2012.
[24]. Shin, Wook, et al. "Towards a formal analysis of the permission-based security model for android." *2009 Fifth International Conference on Wireless and Mobile Communications*. IEEE, 2009.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details