JCARM
Journal of Contemporary Academic Research and Methodologies

An Online Peer Reviewed / Refereed Journal
Volume 1 | Issue 2 | March 2026
Website: www.journal.jcarm.in

Research

Personal Mobile Device Management (PMDM): The Security Perspective

Kayang Justin Kanung*, Omini Emmanuel E, Akima Ogar A, Obu, Olumba O

Department of Computer Science, University of Calabar, Nigeria.

Correspondence should be addressed to: kayangjkanung@gmail.com

Abstract: Mobile devices are becoming more sophisticated and powerful day by day, since the devices can do so much and are available at a much lower cost. They seem to be everywhere. However, because of their capabilities, they require much better management practices than users are used to. Mobile device users have had several complaints about their devices. This could have been a result of poor management or the lack of technical know-how on the use of mobile devices beyond making or receiving calls and texting. Some users imagine how mobile phones suddenly malfunction, how information on their devices is revealed to unknown people and others how they cannot make use of their phones shortly after purchase. These problems could be classified as hardware, software and user-based problems. Ruggiero and Foote (2011) observed that; Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker. The security of mobile devices has not just become important but necessary as mobile device users are vulnerable to wireless technology, device loss and ignorance of high cybercriminals. This paper seeks to address these problems through a user-friendly questionnaire to be served to sampled mobile device users, so that they can provide an understanding of the risk associated with mobile devices, provide users with knowledge of the threats associated with mobile devices, and provide users with a list of safeguards and best practices on mobile device security.

Keywords: Mobile device security, Personal Mobile Device Management, Data leakage, Malware, User awareness.

1.0 Introduction

Mobile communication technology can be disabled by a few occurrences. It may be harmed by human, procedural, and software errors; by electromagnetic problems; and by

https://doi.org/10.5281/zenodo.19591711

"dirty data". It may be threatened by natural hazards, civil unrest, strife, or even terrorism. Criminal acts perpetrated against mobile devices include theft of hardware (i.e. the device itself), software (system or application), time and services, and information, as well as acts of malice and destruction. Mobile devices may also be harmed by viruses. Furthermore, mobile devices can be used as instruments of crime (Mehrnezhad, 2017). Criminals may include employees, outside users, hackers, crackers, and professional criminals.

Mobile devices are perceived differently based on their uses and applications. Aaron (2012) found that while mobile phone users note some drawbacks, they are generally optimistic about the benefits of connectivity and see value in owning a phone.

Billieux (2012) is of the view that smartphones or devices do not only enable users to take care of all their handheld computing and communication needs, whether through texts, calls, emails or social networking sites (SNSs), but they also allow owners to engage in a number of online activities, such as surfing the internet, playing games, listening to music and videos, reading e-books, managing their day-to-day banking, online shopping and navigation. Hence, Plant (2001) stated that it is no wonder smartphones and mobile devices have become such an integral part of modern society, with people constantly immersed in their virtual world.

From the foregoing, one could generally agree that a mobile device is a handheld device that allows a user to make and receive telephone calls while moving around a wide geographical area. It also offers additional features such as text messaging, email, e-commerce, internet access, and more.

Notwithstanding, Berend et al. (2017) view mobile security as the protection of mobile devices, e.g. smartphones, tablets, laptops, and other portable computing devices, as well as the networks they connect to, from threats and vulnerabilities associated with wireless technology. Mobile security could also be referred to as wireless security.

Whereas, in the view of Edim and Kayang (2017), there is an increasing awareness of the advantages associated with the use of cell phones and Personal Data Assistants (PDAs) in the management of disasters and general life operations. Hence, securing these mobile devices has become increasingly important as the number of devices in operation and the uses to which they are put have expanded dramatically. In a related view, Woongryul et al. (2011) stated that smartphones can be connected to various subjects, including the internet, PCs, and other mobile devices, using a wireless network. This feature makes smartphones useful and the most popular mobile device. However, this

feature also means that malicious attackers or software can invade smartphones in various ways. The following Figure 1 shows the general environment of smartphones.

A mobile device attack is an exploit targeting handheld communication devices such as smartphones and tablets. The above suggests some security issues that stem from users, while others originate from manufacturers. Security issues go right to the heart of the workability of mobile devices and communication systems. Brain and Stacey (2011) opined that the following are threats to mobile devices as communication tools:

1. Error and accident.
2. Natural and Other Hazards.
3. Crimes against mobile devices as communication tools
4. Crime against the use of mobile devices as communication tools.
5. Worms and viruses.
6. Mobile device and computing criminals.

According to Bryant et al. (2008), threats from smartphones or mobile devices shape attacks by exploiting vulnerabilities. In this paper, we divide threats into two groups: threats caused by attackers and threats caused by user unawareness or intention.

1. Error and Accident.

We often know that mobile devices have errors caused by human indifference or poor management. Generally, errors and accidents from mobile devices may be classified as human, procedural, software, electromechanical problems, and dirty data.

Human errors are the unintended consequences of technology on mobile device users. These can occur in various ways.

✔ When users are not good at assessing their own information needs, they may end up buying devices that are either not sophisticated enough or far more complex than they need.

Human emotions affect performance, leading to emotional disturbance due to the inability to use a mobile device more effectively.

✔ Procedural error: when a spectacular failure occurs because the mobile device user did not follow the procedure when system and application designers shut down for more user-friendly updates, technical improvements, or the addition of more features to the application or software, and the delay ironically causes users not to follow the new procedures.

✔ Software errors occur when a fault arises in a programme or software, causing it to function improperly.

✔ Electromechanical error: when a power failure (battery low) occurs, causing mobile devices to shut down, or when power surges resulting from charging devices damage the device.

✔ Dirty data: data that is incomplete, outdated, or otherwise inaccurate. Though an opportunity to correct them may exist, it does not always prevent complications for users.

2. Natural and Other Hazards

Whatever is harmful to man and property can also be harmful to mobile devices and communication systems. These include fire, floods, etc. As much as they inflict damage on humans, they can disable mobile devices and electronic systems. This may also include riots and unrest.

3. Crime Against Devices and Communication:

An information technology crime can be of two types: it can be an illegal act perpetrated against mobile devices or telecommunication devices, or it can involve the use of mobile devices as communication tools to conduct an illegal act.

The crime against information technology may include hardware and device software, which encompasses system or application software. Cables (USB cords, chargers, etc.) are also included. Other illegal acts involve destruction. An example of theft is removing a phone from someone's car. Such devices may contain data that is highly private, and hence the loss can be devastating, as such information may not be recoverable if users do not have backup copies saved in safer locations away from the device. An example of software theft is copying programmes and applications without the user's knowledge. Some mobile users unknowingly receive counterfeit or stolen software programmes from vendors.

4. Crime Using Mobile Devices and Communication:

Using mobile devices as communication tools to perpetrate mischief involves utilising social media platforms and emails to distribute fake and false information. Theft of information includes the infiltration of security administration files, stealing confidential personal records, and selling information.

The crime of destruction pertains to criminals who are more interested in abusing or vandalising mobile devices and telecommunication systems than in profiting from them.

5. Worms and Viruses:

These are high-tech forms of maliciousness. A worm is a programme that copies and replicates itself repeatedly into memory or onto a disk drive until no more space is left, causing the device to begin to malfunction. Meanwhile, a virus is a “deviant” programme that attaches itself to mobile devices and destroys or corrupts data. Mariantonietta (2012)

Malware is any kind of hostile, intrusive, or annoying software or program code (e.g. Trojan, rootkit, backdoor) designed to use a device without the owner’s consent. Malware is often distributed as spam within a malicious attachment or a link on an infected website. Malware is categorised by its characteristics, such as the delivery vector used for its payload.

6. Mobile Device Criminals:

According to Larry (2016), most information technology crimes are committed by individuals, including hackers, crackers, and professional criminals. This occurs through the authorisation of access to confidential information, files, electronic data interchange, and so on.

The smartphone is infected with malware specifically designed to steal credit card numbers and online banking credentials, subverting online banking or e-commerce transactions.

This may be by simply using a keylogger to collect credit card numbers or by more sophisticated means, such as intercepting SMS authentication codes to attack online banking applications. Another strategy is for an attacker to send an app to an app store, impersonating a real banking app. If users download and use the app, the attacker can mount a man-in-the-middle attack on banking transactions.

Phishing is a method used to obtain sensitive information such as usernames, passwords, and credit card numbers, and sometimes even money, by pretending to be a reliable source in electronic communications.

2.0 SECURITY.

Mobile device attacks are conducted through almost all wireless network interfaces, especially the unsecured ones. These attacks may eventually provide access to the mobile device's functionality. Mulliner (2006) recalled that these devices have become commonplace in the past few years, integrating multiple wireless networking technologies to support added functionality and services. Unfortunately, the development of both devices

and services has been driven by market demand, focusing on new features and neglecting security. Therefore, smartphones now face new security problems not found elsewhere.

Urban et al. (2012) opined that mobile phones are rich sources of personal information about individuals. Both private and public sector actors seek to collect this information. Many mobile apps collect user identification, location, and other data. Meanwhile, Zhang (2009) regarded mobile device security as an emerging area of technology that calls for greater attention due to the limited focus it has received thus far.

Security is a system of safeguards for protecting information technology against disasters, system failures, and unauthorised access that can result in damage or loss of critical personal information.

Woongryul (2011) sees security mechanisms as 'the solutions that include various antivirus software and intrusion detection systems that run on the smartphone, and smartphone users can obtain these applications from the online market'. He opined that these applications can prevent attacks from outside, such as malware, but they cannot prevent attacks from within, caused by implementation errors or user unawareness. To ensure smartphones remain safe, it is important to use other security methods, such as changing the platform and regularly updating software. The diagram below illustrates the attack flow of mobile devices.

Fig. 1: Attack Flow of Mobile Devices

2.1 Security Components

Four major security components are considered for mobile devices:

1. Identification and Access
2. Encryption
3. Protection of Software and Data
4. Disaster Recovery Planning

(1.) Identification and Access

The legitimate right of ownership of a mobile device must be verified before access is granted. This security system may employ a mix of techniques to authenticate users, determined by (1) what you have: a key, password, or PIN code; (2) what you know: knowledge of specific words, codes, or symbols required to access a mobile device, which should certainly not be known by criminals; and (3) who you are: your physical traits as a means of identification, which can be faked. Hence, biometrics aim to utilise these traits in the security of mobile devices. Here, biometrics is the science of measuring individual body characteristics, e.g. fingerprints (computerised "finger imaging"), voices, entire faces, etc.

(2.) Encryption

Putting images into secret codes: Encryption or enciphering is the alteration of data so that it is not usable unless the changes are reversed. This is primarily done for privacy.

(3.) Protection of Software and Data

Efforts to protect data and programmes running on the mobile device include ensuring that the user has proper education, making backups of data, and protecting against viruses, among other measures. This can be achieved by controlling access to the device and restricting its use to those who have legitimate rights only.

(4.) Disaster Recovery Plans

A disaster recovery plan is a method of restoring information processing operations that have been disrupted by destruction or accidents. This involves arrangements for alternative locations, either online or on other components. The disaster recovery plan includes methods for backing up and storing programmes and data in another location, ways of alerting necessary legitimate users of the system, and possibly training them.

2.2 TOP FIVE (5) MOBILE SECURITY CONCERNS:

1. Device loss: if a user leaves his or her mobile device in a taxi, cab, supermarket, or restaurant, sensitive data such as bank account numbers can be put at risk. This has led to high-profile data breaches.

2. Application Security: Many mobile applications request broad permissions to access various types of device data. Many free apps ask for access to contacts, browsing history, and location.

Another concern is malicious or Trojan-infected applications that are designed to look like they perform normally but secretly upload sensitive data to a remote server.

3. Data leakage: Nearly all the concerns identified in the mobile security survey, from data loss and theft to malicious applications and mobile malware, are sources of data leakage. New mobile apps can tap into a variety of sources if the user accepts the risk. Cybercriminals can target both devices and back-end systems.

4. Malware attacks: 81 per cent of mobile malware can be classified as Trojans, followed by monitoring tools at 10.1 per cent and malicious applications at 5.1 per cent.

5. Device theft: Mobile device theft is a widespread problem for owners of highly coveted devices such as high-end Android devices. The danger of personal data, such as account credentials and access to emails, falling into the hands of tech-savvy thieves makes the issue a major threat to IT security professionals who took the survey.

2.3 PUTTING YOUR PRIVACY AT RISK

Mobile devices have become essential companions, but they can reveal important data about you without your knowledge and often without your permission.

Mobile phones make for versatile pocket assistants. This is because they are equipped with sensors that detect light, humidity, pressure, temperature, and other factors.

Busse and Fuchs (2013) opined that information sharing/transmission over electronic lines is vulnerable to passive wiretapping, which threatens secrecy, and to active wiretapping, which threatens authenticity. Passive wiretapping means intercepting messages, typically without being detected. Although it is normally used to show message contents, on computer networks, it can also be used to check traffic flow through the network to determine who is communicating with whom.

Protection against the disclosure of message content is provided by enciphering transformations and cryptographic techniques. Active wiretapping (tampering) refers to deliberate modifications made to the message stream. This can involve making arbitrary changes to the message or replacing data in a message with data from earlier messages (for example, crediting an account with N10,000 using N5,000). It can also involve injecting false messages or replaying earlier messages.

Phones' access to various personal information can make them effective spying tools. Mobile phones have opened new opportunities for invasion of privacy. Certain Google apps from Android devices and the app store can access the microphone, track location, take photos, and collect data. All this can be done without users' knowledge.

2.4 PASSWORD YOUR DEVICE

Personal information contained in personal devices is at risk. Devices can be lost or stolen, and when this occurs, it can be very devastating.

Users often have several apps running on their devices, which they frequently log into, including critical accounts such as emails, texts, banking, social media, and payment apps linked to users' credit cards. Developers of these mobile apps understand that users are likely to use these programmes because they are easy to access and convenient to use. The programmes will automatically keep users logged in for days, weeks, or even months until they manually revoke access.

If users' devices are not password-protected and are stolen or lost, their accounts are 100% accessible to whoever has control over the device. This is concerning, yet most device users do not use password protection (McAfee, 2013).

Mobile phone users seem unconcerned about keeping data on their devices safe. A limited number of individuals have utilised data backup features on their phones; additionally, approximately 15% store passwords or confidential PINs directly on their devices. This implies that if the phone falls into the hands of the wrong person, users risk exposing all sorts of personal information, such as bank details and online logins, to whoever finds the device.

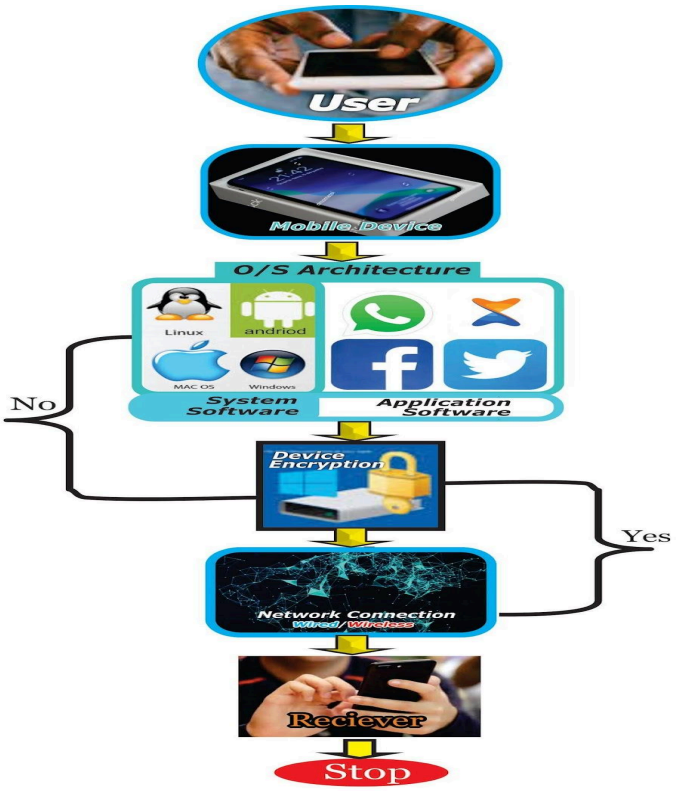
A password or PIN alone cannot protect data because users often share personal information with others.

3.0 Methodology

A survey was conducted using a questionnaire with a sampled population of 150 individuals aged between 24 and 60, both male and female, with a diploma as the minimum academic qualification.

Participants were asked whether mobile device users know the reasons why their devices fail or sometimes malfunction. Do users make use of encryption, passwords, or PIN codes and data privacy settings? Additionally, do they know about mobile malware threats, whether they protect their smartphones and themselves against online threats, how ready they are to adopt mobile security services, and what their feelings are regarding the

communication service provider's (CSP) role in protecting them online? The questionnaires were all answered and returned. All but one participant responded to each question, either agreeing, disagreeing, or remaining undecided; only one was unresponsive once. Furthermore, the questions were targeted at mobile device management and malware protection; data was collected and analysed based on the number of mobile devices that people have used, how they have been protecting them, and how they connect to the Internet. The results are analysed using simple percentages and presented in pie charts. This is done by calculating the separate sectorial angles as given in the data analysis. The activity of the mobile device and the user is illustrated in the diagram below.



Mobile Device Architecture

Fig. 2: Activity of the Mobile Device User

4.0 Analyses

One hundred and fifty people were sampled who use different phones and various operating systems, e.g. iOS, Windows, Android, etc., because these platforms provide access to the internet, which poses a risk to privacy.

Questions regarding awareness of the reasons why devices fail, or malfunction, data is lost, privacy details or information are leaked, and accessing unsecured sites or accepting spoofing and pop-ups while browsing the internet were major concerns.

Some respondents were undecided because they were unfamiliar with the issues. This suggests that, prior to making decisions about the device, some users may not have had adequate awareness of these matters.

The three major questions raised and their various responses are given as follows.

1. Knowledge of device failure or malfunction.

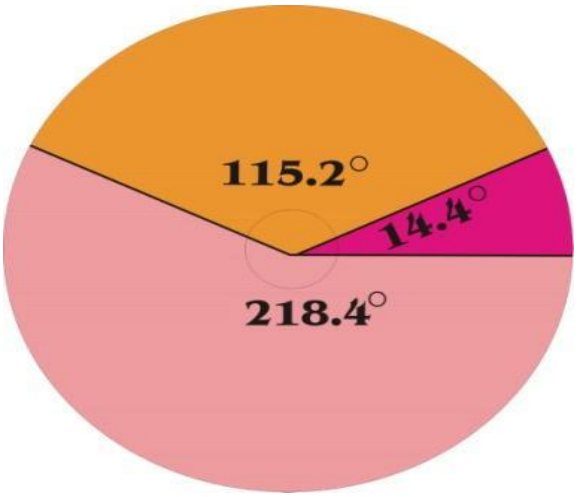
Do mobile device users know the reasons why their devices fail or sometimes malfunction?

Out of the sampled population, 48 people (32%) agreed that they had knowledge of device failure or malfunction, while 91 people (61%) disagreed that they had no knowledge of the reasons their phones often fail or malfunction. Seven people were undecided, and four people did not respond. The percentages are represented in the table below:

s/no	Group	Response	Percentage %
1	Agreed	48	32%
2	Disagreed	91	61%
3	Undecided	11	7 %

Table 1

The sectorial angle for the pie chart is given as follows:



48/150 * 360 = 115.2 Agreed

91/150 * 360 = 218.4 Disagreed

11/150 * 360 = 14.4 Undecided

Fig. 3: Pie chart showing knowledge of device failure or malfunction.

2. Knowledge of protecting devices against data leakage

Do users utilise encryption and data privacy settings?

Fifty-one people, making up 34%, agreed to make use of security and privacy settings, while 90 people, representing 60%, disagreed, and 9 individuals were undecided. Device security settings protect users' data and privacy through access controls, passwords, lock screen codes, and encryption settings, particularly when a device is lost.

s/no	**Group**	**Response**	**Percentage** %
1	**Agreed**	51	34%
2	**Disagreed**	**90**	60%
3	**Undecided**	**9**	6%

Table 2.

The sectorial angle for the pie chart is given as follows:

51/150 * 360 = 122.4 Agreed

90/150 * 360 = 216 Disagreed

9/150 * 360 = 21.6 Undecided

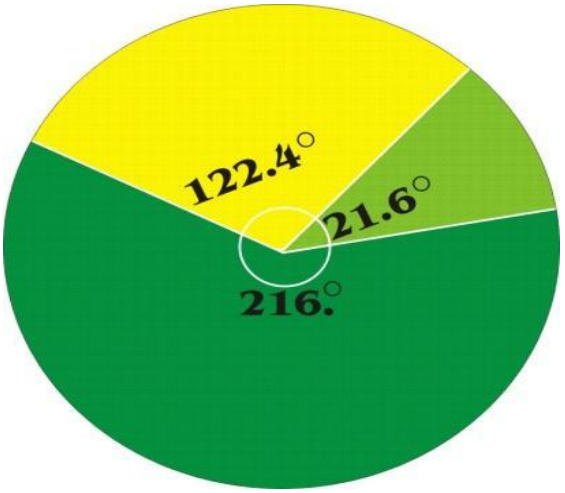


Fig. 4: Pie Chart Showing Knowledge of Protecting Devices from Data Leakage.

3. Knowledge of whether mobile device users protect their devices from viruses and malware.

Considering the evolving ways in which cybercriminals can put users' personal information at risk on mobile devices, a user may want to protect the device, as device security settings alone will not safeguard against malware.

In this case, the question of whether users protect their devices from viruses and malware will arise.

At this point, 68 people, representing 45%, agreed that they often ask for antivirus software from software vendors and often seek it online when the system demands antivirus updates. Meanwhile, 76 people disagreed, representing 51%, as they may not have seen a reason to have one or any impending danger. Additionally, 6 people were undecided, representing 4%.

s/no	Group	Response	Percentage %
1	Agreed	68	45%
2	Disagreed	76	51%
3	Undecided	6	4%.

Table 3.

The sectorial angle for the pie chart is given as follows:

68/150 * 360 = 163.2 Agreed

76/150 * 360 = 182.4 Disagreed

6/150 * 360 = 4.4 Undecided

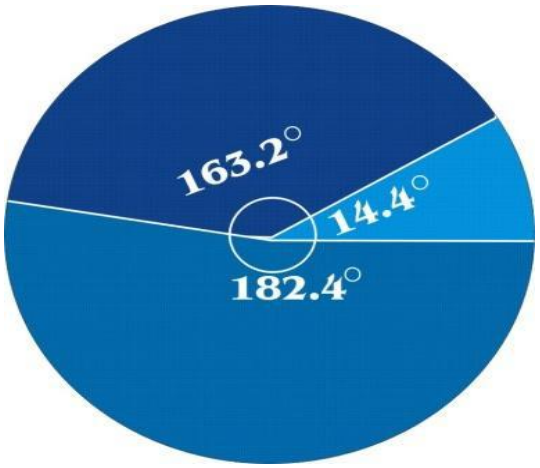


Fig. 5: Pie Chart Showing Knowledge of Whether Mobile Device Users Protect Their Devices from Viruses and Malware.

4.0 Highlights of Findings

In this research, it was found that most mobile device users store data and information on their mobile devices (sensitive personal information such as text messages, contact lists, bank account and BVN numbers, and passwords or PIN codes to accounts; voicemail is also stored on phones) in order to maintain privacy. However, they unfortunately do not consider securing such information, as they lack the understanding that information could be leaked when unauthorised users gain access to their devices, either online or physically.

Hackers use hyped content to attract, manipulate, or persuade people into revealing confidential information through deception, such as phishing, for the purpose of information gathering, fraud, or access rights.

Most users with smart mobile devices frequently engage in activities that generate sensitive information, such as browsing websites, using social networks, and accessing location services.

Although users view mobile device information as private, most still readily accept various online data requests from pop-ups.

Ninety-one per cent of mobile device users disagreed with not having knowledge about their device's failure or malfunction. Similarly, ninety per cent also disagreed that they lack knowledge of how data is leaked from their devices and do not know how to protect against data leakage by either encrypting or using the device's privacy settings. They bypass security measures such as screen locking, PIN coding, and encryption settings

in case the device is lost. Finally, seventy-six per cent stated that they do not have knowledge of protecting devices from viruses and malware, even though they have experienced a malware attack in the past.

Palen et al. (2000) stated that as the Internet continues to go mobile, devices such as smartphones and tablets have become prime targets for malware attacks. The threat is real. But how much do users know about the risk of mobile malware? Do they protect their mobile devices from online threats? If they don't, they certainly could become victims of malware.

5.0 Summary and Conclusion

Yair and Adi (2014) stated that in network-based attacks, there are implementation-based vulnerabilities and design-based vulnerabilities; however, focusing more on design issues, they opined that these issues are much more interesting and significantly harder to fix. These are divided into two types: general "protocol" vulnerabilities and design issues affecting mobile operating systems. It is, however, important to note that mobile devices are more susceptible due to a lack of adequate security solutions and excessive use of untrusted networks, which could lead to device mismanagement or misuse.

Bryant et al. (2008) pointed out that mobile malware is a real and major threat affecting consumers, businesses, and governments. The mobile industry is familiar with online threats, but are users as informed? They are often nonchalant and careless about the security of their devices. Poynter (2015) found three cardinal principles in the security of mobile devices, which include the following: Confidentiality, which determines who is allowed to access what; Integrity, which shows who is allowed to change or use a certain resource; and Availability, which describes the requirement that a resource be usable by its legitimate owner. He advised mobile device users to take care of these aspects. In a related view, Larry (2016) stated that critical elements of a successful mobile security plan include password protection, which has become a key tool in today's world, providing an innovative and efficient way to accomplish tasks within a given timeframe. However, it has also created security risks that need attention. Experts must find a way to collaborate with users to discover the best possible methods to secure mobile devices and mitigate risk. He further opined that secrecy or privacy helps to prevent the unauthorised disclosure of data, and finally, authenticity or integrity helps to prevent the unauthorised modification of data.

Encryption protects against message modification and the injection of false messages by making it infeasible for an opponent to create a ciphertext that deciphers into meaningful plaintext. Note, however, that while it can be used to detect message modification, it cannot prevent it. Raggo (2017) concluded that the following could help in protecting mobile devices:

- Use strong passwords for your devices; avoid simple ones like 1234, 1111, or ABCD. Never use the "remember me" function on your apps or the web browser, and take care to log out of your account. Consider not sharing your PIN and password, as it will save users from heartache.
- Device handling: prevent loss or theft.
- Mobile operating system issues: precautions against viruses or malicious code ought to be executed as needed.
- Sensitive data stored on mobile devices; a clear management policy that balances the risks of data leakage with convenience.
- Other technical measures, security procedures, and measures to protect mobile business applications and data.

Generally, a stolen or lost mobile device with unprotected storage allows an attacker to access the data on it. If the device is infected with malware, it may lead to hidden use of premium services or the leaking of sensitive information. Here are some basic tips for mobile device security.

References

1. Mariantonietta La Polla, Fabio Martinelli & Daniele Sgandurra (2012). Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials.
2. Mehrnezhad M. (2017). Stealing plus via mobile sensors: Actual risk versus user perception. International Journal of Information Security.
3. Berend D, Jungk B & Bhasin S. (2017). There goes your PIN: Exploiting Smartphone & sensor fusion and single and cross-user settings. Cryptology e-prints Archive.
4. Edim, Azom Emmanuel & Kayang, Justin Kanung (2017). A Mobile Application for Critical Environmental Situation Management. International Journal of Engineering Research and Allied Sciences (IJERAS) ISSN :
5. Woongryul Jeon, Jeeyeon Kim, Youngsook Lee, & Dongho Won. (2010). National Research Foundation of Korea (NRF); School of Information and Communication Engineering, Sungkyunkwan University, Korea.

6. Brain K. William & Stacy W. Sawyer (2011). Using Information Technology – A practical guide to computers and communication. McGraw-Hill, New York.

7. Larry G. Wlosinski (2016). Mobile Device Security: Threats, Governance, and Safeguards. CIO Council: Government Mobile and Wireless Security Baseline

8. Urban J. M., Hoofnagle C. J. and Su Li. (2012): Mobile Phones and Privacy. Berkeley Consumer Privacy Survey BCLT Research Paper.

9. Lei Zhang (2009). Mobile Security Threats and Issues -- A Broad Overview of Mobile Device Security. Tianjin University, Tianjin, China.

10. Paul Ruggiero & Jon Foote (2011). Cyber Threats to Mobile Phones, United States Computer Emergency Readiness Team, US-CERT. Carnegie Mellon University, US.

11. Yair Amit & Adi Sharabani (2014). Mobile Security Attacks: A Glimpse From the Trenches.RSA Conference 2014, Asia Pacific and Japan.

12. Bryant, P., Furnell, S., & Phippen, A. (2008). Improving protection and security awareness amongst home users. Advances in Networks, Computing and Communications.

13. Paul van Kessel & Jay Layman (2012). Mobile device security: Understanding vulnerabilities and managing risks. Insights on governance, risk and compliance. Ernst & Young EYGM Limited America.

14. Palen Leysia, Marilyn Salzman & Ed Youngs (2000). Going Wireless: Behavior & Practice of New Mobile Phone Users: University of Colorado, Boulder.

15. Busse, B., & Fuchs, M. (2013). Prevalence of Cell Phone Sharing. Survey Methods: Insights from the Field.

16. Poynter, R. 2015. The Utilization of Mobile Technology and Approaches in Commercial Market Research.

17. Mulliner Collin Richard (2017). Security of Smart Phones Master's Degree Thesis in Computer Science; University Of California, Santa Barbara.

18. Aaron Smith (2012). The Best (and Worst) of Mobile Connectivity; Pew Research Center's Internet & American Life Project. Washington, D.C. http://pewinternet.org/Reports/2012/Best-Worst-Mobile.

19. Billieux, J. (2012). Problematic use of the mobile phone: a literature review and a pathways model. Current Psychiatry Reviews, 8 (4), 299