Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism

Sujithra. M
Assistant Professor,
Dept of Computer Technology & Applications,
Coimbatore Institute of Technology,
Coimbatore, India.

Padmavathi .G, PhD.
Professor & Head,
Department of Computer Science,
Avinashilingam Institute for Home Science
and Higher Education for Women , Cbe, India

ABSTRACT

Mobile communication has become a serious business tool nowadays. Mobile devices are the major platform for the users to transfer and exchange diverse data for communication. These devices are variably used for applications like banking, personal digital assistance, remote working, m-commerce, internet access, entertainment and medical usage. However people are still hesitant to use mobile devices because of its security issue. It is necessary to provide a reliable and easy to use method for securing these mobile devices against unauthorized access and diverse attacks. It is preferred to apply biometrics for the security of mobile devices and improve reliability over wireless services. This paper deals with various threats and vulnerabilities that affect the mobile devices and also it discusses how biometrics can be a solution to the mobile devices ensuring security.

General Terms

Mobile Device Security

Keywords

Mobile devices, Security, Threats, Vulnerabilities, Biometrics.

1. INTRODUCTION

Mobile devices are the fastest growing consumer technology, with worldwide unit sales expected to increase from 300 million in 2010, to 650 million in 2012 [1]. Mobile applications are always booming over period of time. In June 2011, for the first time ever, people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes) [2]. While once limited to simple voice communication, the mobile device now enables also sending text messages, access email, browse the web, and even perform financial transactions. Even more significant, applications are turning the mobile device into a general-purpose computing platform. Apple i-phone SDK was introduced in 2008, within a short span of three years Apple boasts over 425,000 applications for i-OS devices. Similarly explosive growth of Android Market also now contains over 200,000 applications after only a short period of time [3]. As mobile devices grow in popularity, it will be the incentives for attackers. In addition to financial information, mobile devices store tremendous amounts of personal and commercial data that may attract both targeted and mass-scale attacks. Security is a vital challenge for IT departments as mobile devices, primarily smart phones and tablets, become key productivity tools in the workplace. Protecting mobile devices is critical because they are part of a company's network. Maintaining the reliability and security of data and devices at the frontlines can be very challenging. These environments are diverse, complex, and often beyond direct, onsite IT control. IT must be able to proactively manage all the devices, applications, data, and communications critical to the success of mobile workers. In this paper, S**ection II** describes about the various security challenges in the mobile devices, **Section III** describes the different mobile device threats and vulnerabilities, **Section IV** discuss the various traits used in defending against these threats and vulnerabilities.

2. MOBILE DEVICE SECURITY CHALLENGES

The growth in the wireless technology and the improvement of mobile device usage is increased in the mobile market. The growth in the creation and maintenance of secure identities for mobile devices has created challenges for individuals, society and businesses particularly in mobile added value services like mobile banking, mobile check-in, mobile ticket, etc. and government security services. The below are the few prominent challenges with the mobile devices because of the threats and vulnerabilities.

- ***Poor Authorization and Authentication***:

  Poor authorization and authentication schemes relying on device identifiers such as IMEI(International Mobile Equipment Identity), IMSI(International Mobile Subscriber Identity), UUID(universally unique identifier) values for security are the perfect recipe for a failure and can lead to broken authentication and privilege access issues.

- ***Insecure Data Storage***:

  Applies to scenarios when sensitive data stored on device or cloud synced data is left unprotected. It is generally a result of non– encryption of sensitive data, caching of information not intended for long term storage, global file permissions and not leveraging platform best practices, leading to exposure of sensitive information, privacy violations and non-compliance.

- ***Security Decisions via Un-trusted Inputs***:

  If applications make security decisions via user input, then it can be leveraged by malware or client side injection attacks for various nefarious purposes such as consuming paid resources, data and privilege escalation. For e.g. abuse of URL schemes in iOS and abuse of intents in android mobile devices.

- ***Sensitive Information Disclosure:***

  Sensitive information such as login credentials, shared secret keys, access token , sensitive business logic and the like when hardcoded into the application code, presents the possibility of these information being disclosed to a attacker by reverse engineering, which is fairly trivial. Once such information is in an adversary's hands, rest can be easily assumed. Code obfuscation makes it difficult to comprehend code.

- ***Broken Cryptography:***

  This risk emanates from insecure development practices such as use of custom instead of standard cryptographic algorithms, assumption that encoding and obfuscation are equivalent to encryption and cryptographic keys being hardcoded into the application code itself. It can lead to failure of cryptographic implementation resulting into loss of confidentiality of data, privilege escalation and so on.

- ***Insufficient Transport Layer Protection***:

  Complete lack of encryption for transmitted data is often observed in mobile applications. Even if strong encryption is in place, ignoring certificate validation errors or falling back to plain text communication after failures can put security in jeopardy and have severe impacts such as lack of confidentiality of data, data tampering, and can facilitate man-in-the middle attacks.

- ***Server Side Controls***:

  Failure to implement proper security controls such as patches and updates, secure configurations, changing default accounts or disabling unnecessary running services, in the backend services can result in compromise and confidentiality and data integrity risks.

- ***Client Side Injection:***

  Apart from the known injection attacks such as html injection, and SQL injection applicable to mobile web and hybrid application, mobile application are witnessing newer attacks such as abusing phone dialer, SMS and in application payments.

- ***Improper Session Handling*** *:*

  Session with long expiry time, or use of device identifiers as session id pose security risks such as privilege escalation , unauthorized access and so on.

- ***Side Channel Data Leakage***:

  Caused due to programmatic flaws or not disabling insecure OS features in applications. It can result in sensitive data ending up at places like web caches, global OS logs, screenshots (iOS back- grounding issue), temp directories and up for grabs for malware or an attacker who manages to get the mobile device. These challenges are mainly caused by various threats and vulnerabilities in the mobile devices.[10]. In the following section, various types of threats, vulnerabilities and the issues related with these are discussed.

3. MOBILE THREATS AND VULNERABILITIES

Security support is mandatory for any database system. For mobile database systems, security support is even more important to protect the users and devices as well as the database. In mobile communication, since wireless medium is available to all, the attackers can easily access the network and the database becomes more vulnerable for the user and the data in the mobile device.

3.1 Mobile threats

Mobile threat is defined as any malware that targets smart phones and PDA. Various security threats that can affect mobile devices are categorized as follows in Figure 1.

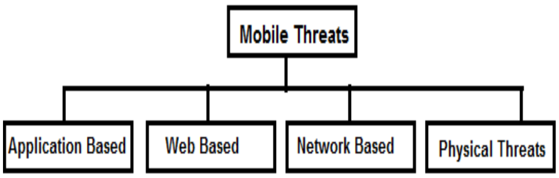

Fig.1 : Various Mobile Threats

- Application-based threats
- Web-based threats
- Network-based threats
- Physical threats

Application Based Threats

Downloadable applications introduces many security threats on mobile devices, including both software specifically designed to be malicious as well as software that can be exploited for malicious purposes.

- ***Malware***
  Software is designed to engage in malicious behavior on a device. Malware can also be used to steal personal information from a mobile device that could result in theft or financial fraud.
- ***Spyware***
  Designed to collect or use data without a user's knowledge or approval. Data commonly targeted by spyware includes phone call history, text messages, location, browser history, contact list, email, and camera pictures.
- ***Privacy threats***
  Caused by the applications that is not necessarily malicious, but gathers or uses more sensitive information than is necessary to perform their function or than a user is comfortable with.
- ***Vulnerable applications***
  Contain software vulnerabilities that can be exploited for malicious purposes. Such vulnerabilities can often allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, and automatically download additional applications.

Web-based Threats

Since mobile devices are often connected to the Internet and used to access web-based services, web-based threats pose issues for mobile devices.

- ***Phishing Scams***
  Use web pages or other user interfaces designed to trick a user into providing information such as account login information to a malicious for the user.
- ***Party Posing as a Legitimate service***
  Attackers often use email, text messages, Face book, and Twitter to send links to phishing sites.
- ***Drive by Downloads***
  Automatically begins downloading an application when a user visits a web page.
- ***Browser Exploits***
  Browser Exploits are designed to take advantage of vulnerabilities in a web browser or software that can be launched via a web browser such as a Flash player, PDF reader, or image viewer.

Network-Based Threats

Mobile devices typically support cellular networks as well as local wireless networks. There are a number of threats that can affect these networks:

- ***Network Exploits***
  Takes advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, WI-Fi) or cellular (e.g., SMS, MMS) networks.
- ***Wi-Fi Sniffing***
  Compromise data being sent to or from a device by taking advantage of the fact that many applications and web pages do not use proper security measures, sending their data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network.
- **Mobile Network Services**
  Cellular services like SMS, MMS and voice calls can be used as attack vectors for mobile devices. The cellular services provide opportunities for phishing attacks. Phishing is an attack strategy in which the attacker gains sensitive information from the user by presenting itself as a trustworthy entity. Two basic phishing attacks over mobile networks exist: Smishing and Vishing. Smishing attacks are executed using SMS messages. Vishing attacks are carried out using voice calls. Figure 2 represents the diverse usage of applications in mobile devices and their security level.

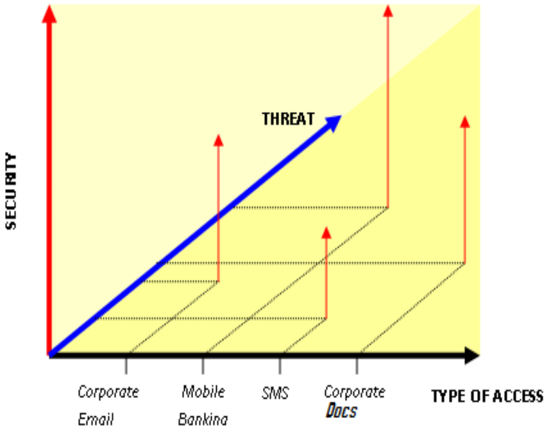

Fig.2 Mobile Device Applications and their security level

Physical Threats

Since mobile devices are portable and designed for use throughout the daily lives, their physical security is an important consideration.

- ***Lost or Stolen Devices***
  The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain. [4].
- ***Computing Resources***
  The increase in computing resources is setting the contemporary mobile devices into focus for malicious attacks with aim to covertly exploit the raw computing power in combination with broadband network access.
- ***Internet Access***
  Mobile devices can access the Internet using Wi-Fi networks or 3G/4G services provided by mobile network operators. Although such high speed Internet connections ensure comfortable browsing, they also expose the mobile devices to the same threats as PCs. Since mobile devices are usually constantly switched on, they can maintain a continuous connection to the Internet. However, prolonged connection to the Internet also increases the chances of a successful malicious attack.
- ***Bluetooth***
  Bluetooth attacks are a method used for device-to device malware spreading. Once the two devices are in range, the compromised device pairs with its target by using default Bluetooth passwords. When the connection is established, the compromised device sends malicious content. Consolidating all the above issues the following Table 1 compares the various mobile threats.

Table 1 Comparison of mobile device threats.

Threats	***Mobile units***	***Over the air***	***Wired hosts***
Physical Threats	theft, damage	physical disasters	physical disasters
Web-Based	problematic operation	interruptions, bad quality	-
Network – Based	denial of service, interference, covert channels, used by third parties	eavesdropping, denial of service, routing alterations	denial of service, faults in hardware and software
Application-Based	-	Overloading	Improper handling

Thus it is clearly discussed about the various threats, their issues with the mobile devices in this section. The next section discusses about the various vulnerabilities

3.2 Mobile Vulnerabilities

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface. [12].Various vulnerabilities that can affect mobile devices are categorized as follows in Figure 3.

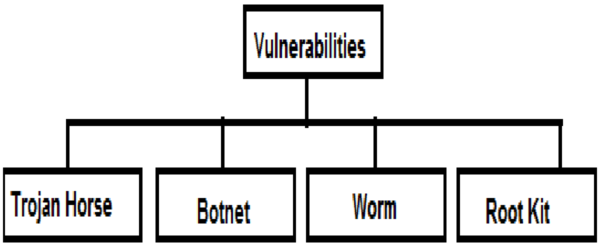

Fig 3 Mobile Device Vulnerabilities

Table 2 Comparison of various vulnerabilities

Types	**Host**	**Mobile units**	**Over the air**
Physical	Different locations	small size and weight, portability, exposure in hostile places	random happenings that easy affect wireless communications
Natural	Unknown boundaries, many points to attack	exposure in outdoor environmental conditions	affected from weather situations, hand-offs between cells
H/ W and S/W	heterogeneity, shared use of resources	not enough hardware controls and resources	-
Communication	controls and resources communication infrastructure	Broadcasting	-
Human	away from technical support and management, lack of attention	unlimited capability for physical access	-

- ***Trojan Horse***
  Trojan can be used to gather private information or to install other malicious applications like worms or botnets. In addition, Trojans can be used to commit phishing activities. For example, a false banking application could collect sensitive data from the user. Such applications can easily spread through unsupervised application stores or through social networks.

- ***Botnet***
  Botnet is a set of compromised devices which can be controlled and coordinated remotely. This attack strategy is used to utilize the computing power of compromised devices in order to commit various activities ranging from sending spam mail to committing Dos attacks.

- ***Worm***
  Worm is a self-replicating malicious application designed to spread autonomously to uninfected systems. A more recent example of a worm type malware for mobile devices is Ikee.B which is used to steal financially sensitive data from jail broken iPhones.[9]

- ***Rootkit***
  Rootkit is a malicious application which gained rights to run in a privileged mode. Such malicious applications usually mask their presence from the user by modifying standard operating system functionalities. Table 2 compares the various Mobile device Vulnerabilities.

4. DEFENCIVE MECHANISMS AND VULNERABILITIES

All security access methods are based on three fundamental pieces of information: who you are, what you have, and what you know [5], which also corresponds to biometric authentication, token-based authentication and knowledge-based authentication respectively. For proving who they are, users can provide their biometrics ID for identification. For proving what they have, users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards, or one-time login cards such as the Secure ID card [6]. For proving what they know, users can provide a password or pass phrase, or a personal identification number (PIN). Figure 4 shows different user authentication mechanisms.

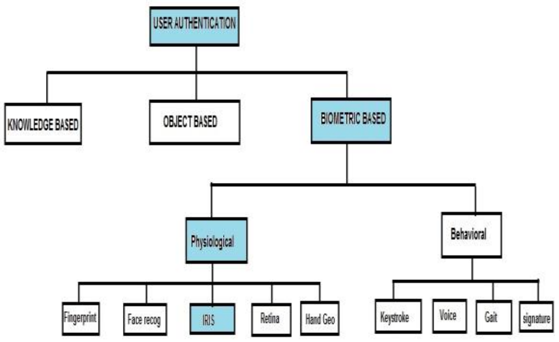

Fig 4 – User Authentication Mechanism

However, this type of technique provides the highest level of security. High cost of hardware, processing and memory requirements are the major arguments to circumvent these technologies in mobile and handheld devices at present. We have studied and analyzed the cost effective user authentication schemes those are mainly based on what you are, biometric authentication schemes are especially relevant to mobile and handheld devices that interact via a touch screen, keyboard, voice recorder and stylus. Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Some of these measures are taken by the user to their mobile devices which prevent the attacks from the various threats and risks caused by the external factors.[7]

- While choosing the mobile devices itself consider their security features such as file encryption, find and wipe the device, delete malicious applications and authentication features.

- Before start using the device configures the device to be more secure as many smart phones have a password feature that locks the device until the correct PIN or password is entered. Enable this feature, and choose a reasonably complex password.

- Do not follow links sent in suspicious email or text messages. Such links may lead to malicious websites.

Table 3 Comparison of Various Authentication Types

User Authentication		Tele-login	One time password	Smart card	Biometric
Security	Prevention of impersonation by an attacker	Good Difficult to falsify calling number	Good Difficult to guess	Good Difficult to duplicate	Excellent Difficult to forge
	Prevention of theft	Good Cell phone theft is easily noticed, cell phone can be disabled remotely	Poor Theft unnoticed	Poor Difficult to notify theft	Excellent No theft
Usability	Ease of operation	Excellent Easy authentication by telephone	Poor Difficult to use by elderly	Excellent Easy	Excellent Easy
	Use of special hardware	Good A cellphone is all that is needed	Poor Requires special token, different for each service	Fair Requires smart card for each service	Excellent No need for extra Hardware
Economy	Initial cost (to strengthen authentication)	Excellent Registration of cellphone telephone number is all that is needed	Fair Requires token	Fair Requires smart card reader	Poor Requires expensive specialized hardware, difficult to install in ordinary user terminals
	Running cost (to strengthen authentication)	Fair Charge for call	Poor Expense of token maintenance and management	Fair Expense of card maintenance and management	Poor Requires maintenance and management of expensive special hardware

- Be choosy when selecting and installing applications. Carefully consider what information one want store on the device. Remember that with enough time, sophistication, and access to the device, any attacker could obtain the stored information from the mobile device.

- Be especially careful when using services that track your location. Do not "root" or "jailbreak" the device which is sometimes used to get access to device features that are locked by default, can contain malicious code or unintentional security vulnerabilities. Altering the firmware could also prevent the device from receiving future operating system updates, which often contain valuable security updates and other feature upgrades.[8]

Biometric authentication such as fingerprints, voice recognition, iris scans, and facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process hardware, processing and memory requirements are the major arguments to circumvent these technologies in mobile and handheld devices at present, these type of techniques provides the highest level of security. Hence it is preferable to adopt Biometrics for Mobile devices. [11]

5. CONCLUSION

Since lot of sensitive personal and corporate information, such as login credentials, credit card details, account details, private contact entries, invoices, purchase orders among others, are being stored or transmitted through these mobile applications. The growth in the creation and maintenance of secure identities for mobile devices has created challenges for individuals, society and businesses particularly in mobile added value services (mobile banking, mobile check-in, mobile ticket, etc.) and government security services. Although many obstacles remain, the growth in wireless technology, and the improvement of mobile devices will stimulate growth in the mobile biometrics market. In a world challenged to find new ways to authenticate identity and privileges when processing people and information, all with increased levels of security, the future of biometric recognition technology on portable computing devices looks bright. By using the recent technologies in the mobile devices the biometric features of the individuals are easily captured and measured. These systems are proved highly confidential portable mobile based security systems which is much essential. Comparing various biometric traits such as fingerprint, face, gait, iris, signature and voice. Iris is considered as the most efficient biometric trait due to its reliability and accuracy. Since most of the Mobile devices are attached with the camera it is easy to use Iris Biometric trait even though it is less popular, it guarantees high security.

6. REFERENCES

[1] Roberta Cozza, "Forecast: Mobile Communications Devices by Open Operating System, Worldwide, 2008-2015," Gartner, April 5, 2011

[2] Flurry (June 2011), Mobile Application Put the Web in Their Rear-view Mirror: http://blog.flurry.com/bid/63907/Mobile- Application-Put-the- Web-in-Their-Rear-view-Mirror

[3] Erica Ogg, "HP: Number of mobile application doesn't matter," CNET News, June 29, 2011

[4] Mavridis I., Pangalos G "Security Issues in a Mobile Computing Paradigm"2012

[5] Lookout Mobile Threat Report, August 2011

[6] http://en.wikipedia.org/wiki/Vulnerability_(computing)

[7] Anurag Kumar Jain,Devendra Shanbhag "Addressing Security and Risks in Mobile Applications".2012

[8] Brostoff, S. and Sasse, M. A. Are Pass faces more usable than passwords: a field trial investigation, in People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000

[9] http://www.rsasecurity.com/products/securid/Last accessed in January 2008.

[10] Daniel, K. Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX UNIX Security Workshop, pp.5-14, August 1990.

[11] Wiedenbeck, S.,Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Effects of tolerance and image choice, in Symposium on Usable Privacy and Security (SOUPS), at Carnegie-Mellon Univ., Pittsburgh, 6-8 July 2005.

[12] Paul Ruggiero and Jon Foote "Cyber Threats to Mobile ", Produced for US-CERT, a government organization, Carnegie Mellon University-US, 2011