ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Pilot Study on the Security Issues of Smartphone Systems

Sayantan Majumdar [1], Abhisek Maiti [2], Sudipto Bhattacharjee [3], Asoke Nath [4]

[1,2,3] PG Scholar, Department of Computer Science, St. Xavier's College Kolkata, India

[4] Assistant Professor, Department of Computer Science, St. Xavier's College Kolkata, India

ABSTRACT: The mobile phones are now almost essential for most of us especially for school, college university students. This is because the mobile devices enable an user to access a large variety of ubiquitous services. In recent years, the availability of these ubiquitous and mobile services has significantly increased due to the different form of connectivities provided by mobile devices, such as GSM, GPRS, Bluetooth and Wi-Fi. Generally, smartphone users can program any application which is customized for their needs. However, to provide these customized services, smartphone needs more private information and this can cause security vulnerabilities, thereby representing an ideal target for black hats. As the number of vulnerabilities and, hence, of attacks increase, there has been a corresponding rise of security solutions proposed by researchers. This research which includes the security issues in smartphone systems are being new and still unexplored in depth. In the present paper the authors aim to provide a structured and comprehensive overview of the research on security threats and some solutions for smartphone devices.

KEYWORDS: Smartphone, Mobile security, Black hats, Ubiquitous services

I. INTRODUCTION

Access to information and communication on the move is not only possible today, it is critical to maintain a competitive edge. Emerging wireless technologies make it possible to access the web, email, business applications and to synchronize calendars, contacts and other applications, in real-time, anytime, anywhere.

Today's mobile phones combine these wireless technologies with dedicated operating systems and advanced multimedia functionalities, thus the term smartphone. Smartphones are equipped with full fledged, purpose-built operating systems, designed for optimizing resources. The dominating operating systems are Android, iOS and Windows.

Smartphones facilitate the flow of information over heterogeneous networks, through untrusted domains. This flow of information represents risks for the owner of the smartphone and for the owner of the information. Given their growing popularity, smartphones need to be acknowledged when considering an information system, and more particularly when considering the security of any information system.

II. WIRELESS NETWORKING

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home, most of whom are connected through their smartphones. Some of the basic technologies of wireless network systems are as follows:

A. **Wireless Local Area Network:** A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

B. **Access Point:** A wireless access point (AP) is a hardware device that allows wireless communication devices, such as PDAs and mobile computers, to connect to a wireless network. Usually, an AP connects to a wired network, and provides a bridge for data communication between wireless and wired devices.

C. **Service Set Identifier (SSID):** A Service Set Identifier (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point. With proper configuration, only clients with

DOI: 10.15680/IJIRCCE.2015. 0311032

correct SSID can communicate with the access points. In effect, SSID acts as a single shared password between access points and clients.

D. **Open System Authentication:** It is the default authentication protocol for the 802.11 standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure data. Upon successful authentication, both stations are considered mutually authenticated. It can be used with WEP (Wired Equivalent Privacy) protocol to provide better communication security, however it is important to note that the authentication management frames are still sent in clear text during authentication process. WEP is used only for encrypting data once the client is authenticated and associated. Any client can send its station ID in an attempt to associate with the AP. In effect, no authentication is actually done.

E. **Shared Key Authentication:** This is a standard challenge and response mechanism that makes use of WEP and a shared secret key to provide authentication. Upon encrypting the challenge text with WEP using the shared secret key, the authenticating client will return the encrypted challenge text to the access point for verification. Authentication succeeds if the access point decrypts the same challenge text.

F. **Ad-Hoc Mode:** Ad-hoc mode is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for their communication. However, this topology cannot scale for larger networks and lack of some security features like MAC filtering and access control.

G. **Infrastructure Mode:** This is another networking topology in the 802.11 standard, in addition to ad-hoc mode. It consists of a number of wireless stations and access points. The access points usually connect to a larger wired network. This network topology can scale to form large-scale networks with arbitrary coverage and complexity.

H. **Wired Equivalent Privacy Protocol:** WEP l is a basic security feature in the IEEE 802.11 standard, intended to provide confidentiality over a wireless network by encrypting information sent over the network.

I. **Wi-Fi Protected Access(WPA) & WPA2:** WPA is a wireless security protocol designed to address and fix the known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 802.1x authentication has been introduced in this protocol to improve user authentication.

WPA2, based on IEEE 802.11i, is a new wireless security protocol in which only authorised users can access a wireless device, with features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection and data integrity.

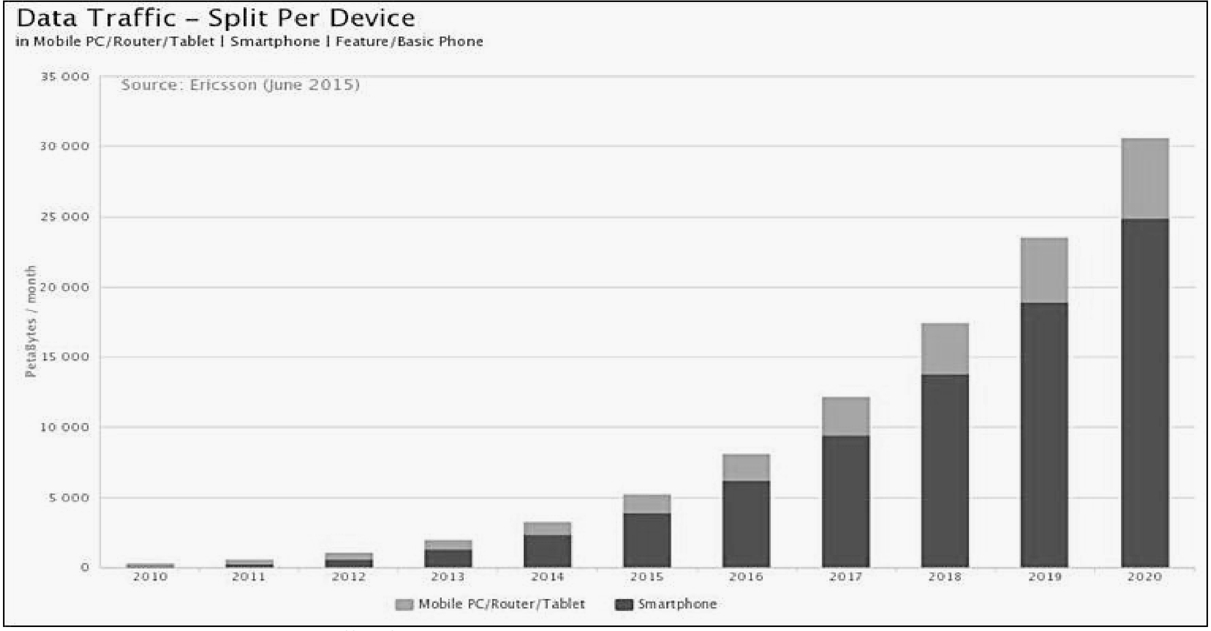

Fig.1. Data Traffic of Smartphones and Tablets based on June 2015 Ericsson mobility report

DOI: 10.15680/IJIRCCE.2015. 0311032

III. SECURITY RISKS

Smartphones, be it through their inherent characteristics, their use (or misuse) or the technologies associated with their use, bring forward risks.

A. **Security risks related to the inherent characteristics of smartphones:**

- As described above, smartphones come equipped with dedicated operating systems. This in itself will induce new risks such as the emergence of security holes and bugs, mainly due to the complex architecture of these operating systems.
  For example, .in August 2013, it was revealed that bugs in some implementations of the Java class SecureRandom sometimes generated collisions in the key value,thereby allowing a solution of the private key, which in turn allowed stealing bitcoins from the containing wallet on Android app implementations, which use Java and rely on ECDSA to authenticate transactions. Bugs have also been documented on Windows and iOS based smartphones .
  It is possible to exploit these bugs to jam devices and provoke a reset. This would erase the data stored on the device. System-based vulnerabilities will be making their way in smartphones, just as they do on computers as smartphone operating systems will grow in sophistication.
- Another issue linked to the inherent nature of smartphones revolves around access control and data security. As there is no form of encryption used to protect the data inside some older devices, the information remains at hand for anyone that can gain physical access to the device. Although all or most newer smartphone models support device encryption, most users are unaware of this feature. This is a kind of risk manufacturers and users of smartphone may have to consider.
  Even if a pin code is protecting access to the telephone features, sometimes the data remains unprotected. Moreover data is (in most of the devices) stored on flash chipsets (or removable memory cards) so, with physical access to the chipset anyone can bypass the access controls and steal data or even destroy the device itself.

B. **Security risks related to the users:**
Data stored on the device can easily become accessible to a third party whether it be by illegitimate connection, loss or theft of the device. Consequences can be serious, ranging from identity theft to leakage of sensitive personal, corporate and client data.

C. **Security risks related to wireless networks:**
Connectivity of smartphones to a variety of different networks presents risks due to the inherent nature of the wireless medium and the always-on connectivity provided by 3G, 4G or WiFi networks.

Low deployment costs make wireless networks attractive to users. However, the easy availability of inexpensive equipment also gives attackers the tools to launch attacks on the network. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

a. **"Parking Lot" Attack**: Access points emit radio signals in a circular pattern, and the signals almost always extend beyond the physical boundaries of the area they intend to cover. Signals can be intercepted outside buildings, or even through the floors in multi-storied buildings. As a result, attackers can implement a "parking lot" attack, where they actually sit in the organization's parking lot and try to access internal hosts via the wireless network. If a network is compromised, attacker has achieved a high level of penetration into the network. They are now through the firewall, and have the same level of network access as trusted employees within the corporation. An attacker may also fool legitimate wireless clients into connecting to the attacker's own network by placing a unauthorized access point with a stronger signal in close proximity to wireless clients. The aim is to capture end-user passwords or other sensitive data when users attempt to log on these rogue servers.

b. **Shared Key Authentication Flaw:** Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client. Such an attack is possible because the attacker can capture both the plaintext (the challenge) and the ciphertext (the response). WEP uses the RC4 stream cipher as its encryption algorithm. A stream cipher works by generating a keystream, i.e. a sequence of pseudo-random bits, based on the shared secret key, together with an initialisation vector. The keystream is then XORed against the plaintext to produce the ciphertext. An important property of a stream cipher is that if both the plaintext and the ciphertext are known, the keystream can be recovered by simply XORing the plaintext and the ciphertext together, in this case the challenge and the response. The recovered keystream can then be used by the attacker to encrypt any subsequent challenge text generated by the access point to produce a valid authentication response by XORing the two values together. As a result, the attacker can be authenticated to the access point.

c. **SSID Flaw:** Access points come with default SSIDs. If the default SSID is not changed, it is comparatively attract more attacks from attackers since these units are regarded as poorly configured devices. Besides, SSIDs are embedded in management frames that will be broadcasted in clear text regardless access point is configured to disable SSID broadcasting or enabled encryption. By conducting analysis on the captured network traffic from the air, attacker is able to obtain the network SSID and performs further attacks.

d. **WEP Vulnerabilities:** Data passing through a wireless LAN with WEP disabled (which is the default setting for most products) is susceptible to eavesdropping and data modification attacks. However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed, which seriously undermine its claims to security. In particular, the following attacks on WEP are possible:

- Passive attacks to decrypt traffic based on known plaintext and chosen ciphertext attacks
- Passive attacks to decrypt traffic based on statistical analysis on ciphertexts
- Active attacks to inject new traffic from unauthorised mobile stations
- Active attacks to modify data
- Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker’s machine.

A key-scheduling flaw has been discovered in WEP, so it is now considered as unsecured because a WEP key can be cracked in a few minutes with the aid of automated tools. Therefore, WEP should not be used unless a more secure method is not available.

e. **Attack on TKIP:** The TKIP attack uses a mechanism similar to the WEP attack that tries to decode one byte at a time by using multiple replays and observing the response over the air. Using this mechanism, an attacker can decode small packets like ARP frames in about 15 minutes. If Quality of Service (QoS) is enabled in the network, attacker can further inject up to 15 arbitrary frames for every decrypted packet. Potential attacks include ARP poisoning, DNS manipulation and denial of services. Although this is not a key recovery attack and it does not lead to compromise of TKIP keys or decryption of all subsequent frames, it is still a serious attack and poses risks to all TKIP implementations on both WPA and WPA2 network.

f. **WPA2 Vulnerability:** In July 2010, a security vendor claimed they discovered vulnerability on WPA2 protocol, named "Hole 196" [1]. By exploiting the vulnerability, an internal authenticated Wi-Fi user can decrypt private data of others and inject malicious traffic into the wireless network. After investigation , such attack cannot actually recover, break or crack any WPA2 encryption keys (AES or TKIP). Attackers can only masquerade as AP and launch a man-in-the-middle(MITM) attack when clients attached to them. Moreover, such attack would not be succeeded in a proper configured environment. If client isolation feature is enabled in access points, wireless clients are not allowed to talk with each other when they are attaching to the same access point. In this connection, attacker is unable to launch an MITM attack to other wireless users.

D. **Security risks related to the applications:**

An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, the attacker has the potential to exploit the application vulnerability to facilitate a cyber crime. These crimes target the confidentiality, integrity, or availability (known as the “CIA triad”) of resources possessed by an application, its creators, and its users. Attackers typically rely on specific tools or methods to perform application vulnerability discovery and compromise. According to Gartner Security, the application layer currently contains 90% of all vulnerabilities.

While there are many different tools and techniques for exploiting application vulnerabilities, there are a handful that are much more common than others. These include:

- Cross Site Scripting
- SQL Injection
- LDAP Injection
- Cross Site Request Forgery
- Insecure Cryptographic Storage
- Vulnerabilities of Obsolete Software

According to the European Union Agency for Network and Information Security, the top ten security risks for smartphone users include the following:

No.	Title	Risk	Description
1	Data leakage resulting from device loss or theft	High	The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.
2	Unintentional disclosure of data	High	The smartphone user unintentionally discloses data on the smartphone.
3	Attacks on decommissioned smartphones	High	The smartphone is decommissioned improperly allowing an attacker access to the data on the device.
4	Phishing attacks	Medium	An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.
5	Spyware attacks	Medium	The smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.
6	Network Spoofing Attacks	Medium	An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.
7	Surveillance attacks	Medium	An attacker keeps a specific user under surveillance through the target user’s smartphone.
8	Diallerware attacks	Medium	An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.
9	Financial	Medium	The smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or

	malware attacks	🟧	ecommerce transactions.
10	Network congestion	Low	Network resource overload due to smartphone usage leading to network unavailability for the end-user.

Recently, a major vulnerability was found in the Swiftkey keyboard [2] that comes pre-installed with Samsung smartphone devices. About 600 million devices were at the risk of being hacked. First discovered by the security company NowSecure, the vulnerability would have allowed the black hats to:

- access sensors and resources like GPS, camera and microphone
- secretly install malicious apps without the user knowing
- tamper with how other apps work or how the phone works
- eavesdrop on incoming/outgoing messages or voice calls
- attempt to access sensitive personal data like pictures and text messages

Another such major vulnerability was recently discovered in the Google Chrome browser for Android. It has been showcased at PacSec conference in Tokyo. Because of this vulnerability, the JavaScript V8 engine can be targeted. This vulnerability allows attackers to gain full control of the device. Currently this vulnerability affects all the android devices having Chrome browser. Full details of the exploit was not disclosed for security reasons [6].

Use of obsolete software is also a big problem. For an example, although the patch for the Master-Key vulnerability has been released in Android, still 900 million devices are affected by this vulnerability. Many people still use flash in their mobile devices in spite of Google and Adobe stopped supporting flash on Android for being extremely vulnerable [7].

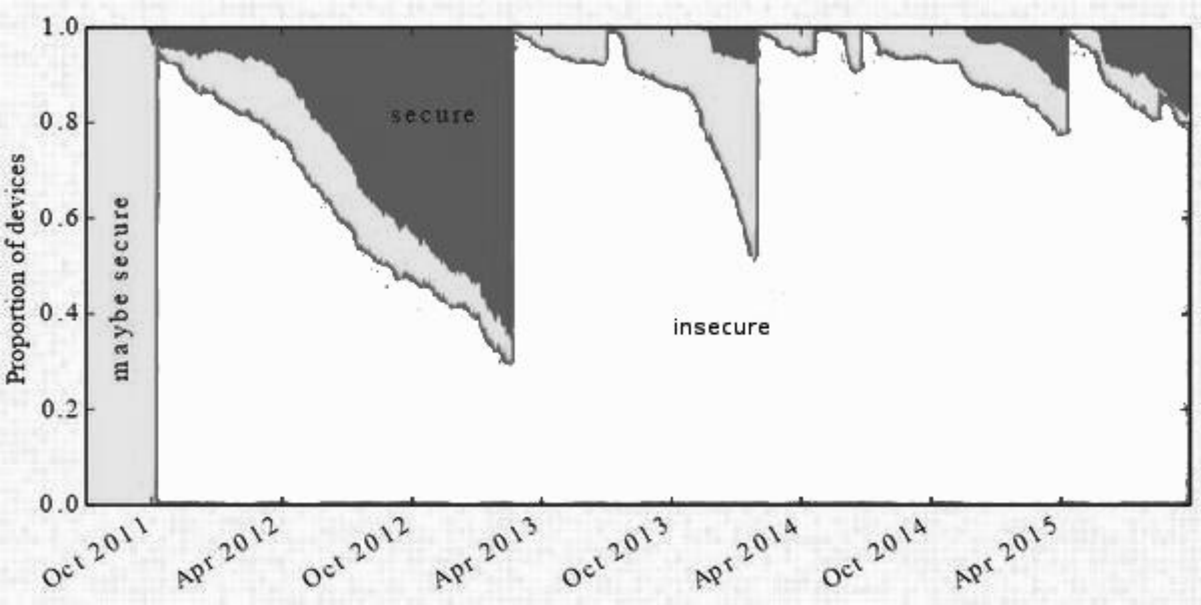

Fig.2. Proportion of Devices Running Vulnerable Versions of Android [10]

IV. MITIGATION

A. Security Solutions for Wireless Networks:

- One approach to reducing the risk of "parking lot" attacks on your WLAN is to reduce exposure by using shielding products, such as specialized paint, to attenuate RF signals. There are several varieties of paint and window film available, with attenuation ranging from 40dB to 80dB for the frequencies that wireless LANs use. One can simply paint the walls and apply film to the windows, and the additional attenuation does a good job of shielding the building.
- Use of latest security protocols for wireless networks is always recommended. For an example, till date WPA2 with CCMP(Counter Mode Cipher Block Chaining Message Authentication Code Protocol) is considered as secured for WiFi networks. Currently IEEE 802.11i standard [5] is followed for wireless networks.

B. User Awareness:

- People are notoriously poor at achieving sufficient entropy to produce satisfactory passwords. According to one study involving half a million users, the average password entropy was estimated at 40.54 bits [9]. A password policy is a guide to choosing satisfactory passwords. Some are controversial. They are usually intended to:
  a. assist users in choosing strong passwords
  b. ensure the passwords are suited to the target population
  c. provide recommendations for users with regard to the handling of their passwords
  d. impose a requirement to change any password which has been lost or compromised, and perhaps that no password be used longer than a limited time.
- People are also poor at choosing right software and verified source of software. Softwares from third party sources should be verified carefully before installation. The permissions granted to a particular app must be checked carefully before installations. There are provision in latest mobile OSs like Android to control these permissions.
- In-app advertisements may cause security risks also. In many cases ads redirect to harmful and malicious websites. Users should be careful about handling the apps.
- Very often software updates contain major security updates. So use of latest software minimizes the security risk.

C. **Best Practices for Security & Privacy in App Development:** The following app development practices should be followed:

- Use of HTTPS and SSL in network transaction modules
- Updating security provider to protect against SSL exploits
- Carefully defining device management policies

V. CONCLUSION

With the rapid proliferation of smartphones equipped with a lot of features, as multiple connections and sensors, the number of mobile malware is increasing. Differently from PC environment, solutions aimed at preventing the infection and the diffusion of malicious code in smartphone have to consider multiple factors: the limited resources available, including the power and the processing unit, the large number of features that can be exploited by the attackers, such as different kinds of connections, services, sensors and the privacy of the user.

Smartphones are complex in design and architecture, and the same goes for the network protocols used by smartphones. This complexity opens the doors to implementation errors and structural weaknesses, making smartphones vulnerable to different types of attacks. Attacks are simple to implement, and the growing interest in the technologies associated with smartphones will lead to the discovery of more weaknesses and multiply the risk of attacks.

To secure a framework incorporating smartphones as part of the information system against attacks, the first step for organizations would be to communicate with the users on smartphone security issues and work on an adequate security policy. Taking measures to secure the interactions between the smartphones and the information system and harden the smartphone can then help mitigate the risks associated with their use.

REFERENCES

1. “Hole-196”: http://www.airtightnetworks.com/WPA2-Hole196
2. ”Samsung is fixing the vulnerability that left 600 million smartphones at risk of hacking”, Business Insider: http://goo.gl/vhsbiS
3. “Device Management Policy”: https://developer.android.com/training/enterprise/device-management-policy.html
4. “Android vulnerabilities”: http://androidvulnerabilities.org/
5. “802.11i standard”: http://csrc.nist.gov/archive/wireless/S10_802.11i%20Overview-jw1.pdf
6. Android "Master Key" vulnerability - more malware exploits code verification bypass: https://goo.gl/apGK4T
7. Chrome on Android Security Vulnerability: http://goo.gl/K13XYr
8. Sayantan Majumdar, Abhisek Maiti, Asoke Nath, “ SECURITY AND PRIVACY ISSUES OF INTERNET OF THINGS: CHALLENGES AND THREATS”, International Journal of Advanced Technology in Engineering and Science (IJATES), Vol. No. 3, Issue 11, November 2015 ISSN 2348-7550
9. Florencio, Dinei; Herley, Cormac (May 8, 2007). "A Large-Scale Study of Web Password Habits", Proceeds of the International World Wide Web Conference Committee.
10. Daniel R. Thomas, Alastair R. Beresford, Andrew Rice, “ Security Metrics for the Android Ecosystem”, University of Cambridge