International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

IoT DEVICES SECURITY RISKS AND VULNERABLITIES: ANDROID DEVICES AS USE CASES

Aamir Parvaiz Wagay[1], Dr. Khalid Mohiuddin[2]

[1]Ph.D. Scholar, Himalayan University, Itanagar, Arunachal Pradesh, (India)

[2]Assistant Professor, King Khalid University, Kingdom of Saudi Arabia(India)

ABSTRACT

The Internet of Things (IoT) remains at the highest of the Gartner Hype Cycle as the most hyped technology, which implies that it’s the most popular topic has gained the foremost attraction of the researchers presently. In recent years, there has been an enormous quantity of analysis that has investigating totally different aspects and considerations of this field. Meanwhile, privacy and security is an indivisible a part of this technology. While not providing enough security, the promising edges of this flourishing technology are abused and otiose.

In this paper, we will give a brief definition of IoT devices security risks, attacks, vulnerabilities and then we will go through more details about the current challenges.

Keywords: *Authentication, Internet of Things, Network, Privacy, Security.*

I. INTRODUCTION

Ubiquitous sensing enabled by Wireless detector Network (WSN) technologies cuts across several areas of recent day living. This offers the flexibility to live, infer and perceive environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of those devices during a communicating-actuating network creates the web of Things (IoT), wherein, sensors and actuators mix seamlessly with the setting around North American country, and also the info is shared across platforms so as to develop a standard operative image (COP). Oxyacetylene by the recent adaptation of a spread of enabling device technologies like RFID tags and readers, close to field communication (NFC) devices and embedded detector and mechanism nodes, the IoT has stepped out of its infancy and is that the next revolutionary technology in remodeling the web into a completely integrated Future net. As we tend to move from WWW (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the necessity for data-on-demand victimization refined intuitive queries will increase considerably. Net of Things (IoT) devices is chop-chop turning into present whereas IoT services are getting pervasive. Their success has not gone unobserved and also the range of threats and attacks against IoT devices and services area unit on the rise still. Cyber-attacks aren't unaccustomed IoT, however as IoT are deeply complex in our lives and societies, it's turning into necessary to intensify and take cyber defense seriously. Hence, there's a true ought to secure IoT, that has consequently resulted in an ought to comprehensively perceive the threats and attacks on IoT infrastructure.

The invention of IoT by exploitation the recreate of informatics address (IPv6), which fits on the far side the restrictions of IPv4, can modification the planet of web by providing the property for a massive range of well connected devices around seventy billion, or perhaps a lot of. Flourishing this technology has been known as because of the Second Economy or the commercial web revolution **[1]**. It will turn out an enormous marketplace for varied services, and also the size of this market is calculable within the trillions of greenbacks. This market may be a promising theme to achieve success, but providing the privacy aspects get into consideration before this Brobdingnagian method starts to be enforced wide.

The IoT's anyplace, anything, anytime nature might simply amendment these benefits into disadvantages if privacy aspects wouldn't be provided enough. For instance, if anyone will have access to any personal services and data, or if the knowledge of a good varies of individuals is reached by the atmosphere mechanically, the IoT wouldn't have a reliable atmosphere **[2]**.

There is not any enough backbone to outline management and data spatial property policies for interaction among many alternative users and devices. Dominant the flow with the standard tools can cause an enormous quantity of traffic that's onerous to ensure the privacy and protection of parts **[3].** Also, solutions for various security necessities have the direct impact on the value and time to plug. Moreover, each answer has its own business necessities which can or might not be as strict **[4]**.

Another vital issue in IoT is that the quality of the user's satisfaction. IoT ought to give a higher service by avoiding the rejecting bound services that will happen by current classic mechanisms accustomed get user's consent. Hence, IoT ought to give totally different ways like implementing consent mechanisms through the devices themselves as privacy proxies and policies for every device, which incorporates conditions and constraints hooked up to the knowledge that describe however it ought to be treated**[3]**.

II. PRIVACY ISSUES

The Android devices have the following privacy issues:

1. Insecure Web Interface

The first purpose considerations security-related problems with the online interfaces designed into IoT devices that permits a user to interact with the device, however at an equivalent time might enable a wrongdoer to realize unauthorized access to the device.

2. Insufficient Authentication/Authorization:

This space deals with ineffective mechanisms being in situ to manifest to the IoT programme and/or poor authorization mechanisms whereby a user will gain higher levels of access then allowed.

3. Insecure Network Services

This point relates to vulnerabilities within the network services that area unit accustomed access the IoT device which may enable a persona non grata to achieve unauthorized access to the device or associated information.

4. Lack of Transport Encryption

This deals with information being changed with the IoT device in an unencrypted format. This might simply result in associate persona non grata sniffing the information and either capturing this data for later use or compromising the device itself.

5. Privacy Concerns

Privacy issues square measure generated by the gathering of non-public knowledge additionally to the shortage of correct protection of that knowledge. Privacy issues square measure simple to get by merely reviewing the information that's being collected because the user sets up and activates the device. Machine-controlled tools may hunt for specific patterns of knowledge which will indicate a set of non-public knowledge or alternative sensitive data.

6. Insecure Cloud Interface

This point considerations security problem associated with the cloud interface accustomed act with the IoT device. Usually this is able to imply poor authentication controls or information traveling in associate degree unencrypted format permitting associate degree wrongdoer access to the device or the underlying information.

7. Insufficient Security Configurability

Insufficient security configurability is present once users of the device have restricted or no ability to change its security controls. Lean security configurability is clear once the net interface of the device has no choices for making granular user permissions or as an example, forcing the utilization of robust passwords. The chance with this is often that the IoT device might be easier to attack permitting unauthorized access to the device or the information.

III. ATTACKS ON ANDROID MOBILE DEVICES

In the following sections, we tend to discuss many types of attacks against smartphones [Android]. We firstly detail the potential methodologies to perform associate attack during a mobile surroundings and, for every quite attack, we offer a true example. Secondly, we tend to show however these methodologies will be exploited to succeed in totally different goals.

Methodologies of the Attacks: The distinct methodologies to perform attacks against smartphones are categorized using the following classes: • wireless; • break-in; • infrastructure-based; • worm-based.

1) Wireless Attacks: There are many alternative types of wireless attacks against smartphones, particularly those targeting personal and sensitive information. The foremost common attack is eavesdropping on wireless transmissions to extract confidential info, like usernames and passwords. Wireless attacks also can abuse the distinctive hardware identification (e.g., wireless computer network mac address) for chase or profiling the owner of the device. Finally, malware typically exploits Bluetooth as a medium to hurry up its propagation. **[5]** Discusses security issues in wireless environments and presents this analysis activity. A comprehensive review of Bluetooth attacks touching smartphones will be found in [6]. Some studies for preventing this category of attacks square measure projected in **[5, 7, 8, and 9].**

Example - Cabir: Cabir is a worm that propagates through Bluetooth. This worm consists of a message containing an application file, caribe.sis, which seems like a Security Manager utility. If installed, the worm uses the device’s native Bluetooth functionality to search for other Bluetooth-discoverable devices. Then, the worm attempts to send infected SIS files to the discovered devices as well.

2) Break-in Attacks: Break-in attacks change the offender to achieve management over the targeted device by exploiting either programming errors, e.g. to cause buffer overflows or format string vulnerabilities. Typically, these attacks area unit used as a stepping stone for playacting any attacks, like overbilling attacks or data/identity thieving. Some studies for preventing this category of attacks area unit planned in **[10, 11].**

Example - Doomboot.A: This Trojan installs corrupted system binaries into the C:\driveof the device. The corrupted binaries contain further Trojans, as CommWarrior, which are also installed on the device.

3) Infrastructure-based Attacks: Since the services provided by the infrastructure ar the idea for essential smartphone functionalities, like placing/receiving calls, SMS and e-mail services, the economic and social impact of those attacks could also be terribly giant, like the one mentioned in **[12]. [13]** Evaluates the protection impact of the SMS interface on the supply of the cell phone network. As an example, if associate aggressor is ready to at the same time send messages through the many obtainable portals into the SMS network, the ensuing combination load will saturate the management channels and, therefore, block legitimate voice and SMS communications. The authors demonstrate that an aggressor that injects text messages from the net will deny voice service in an exceedingly metropolitan space victimization hit-lists containing as few as two, 500 targets with very little over a cable electronic equipment.

a) GPRS: Since the GPRS design is made on the GSM infrastructure; it uses a security design primarily based upon the protection measures already adopted by GSM (fora review of DoS attacks and confidentiality threats in GSM networks, see **[14]**). Attacks against GPRS will target the device, the radio access network, the backbone network, and therefore the interfaces connecting GPRS networks with one another or with the net. The results of those attacks is the compromise of finish users security, over bill users, the revealing or alteration of important info, the services inconvenience, or the network breakdown. we've got additionally to contemplate that GPRS is additional exposed to attackers compared to GSM as a result of it uses the information processing technology, that is very vulnerable.

b) UMTS: The UMTS security design defines a collection of procedures to attain hyperbolic message confidentiality and integrity throughout their communication. At the kernel of its security design lie’s the user authentication mechanism, called Authentication and Key Agreement (AKA). Authentication in UMTS relies on a 128-bit stellate secret key, namely Ki, which is hold on within the user’s tamper-resistant Universal microcircuit Card (UICC) and within the corresponding Home Location Register (HLR) of the user’s Home Network (HN).

4) Worm-Based Attacks: The main features that characterize attacks based upon worms are:

- **Transmission channel.**
- **Spreading parameters.**
- **User mobility models.**

a) Transmission Channel: Smartphones are usually equipped with several connectivity options and, hence, offer many possible routes for infection vectors, such as:

- Downloading infected files while surfing the Internet;
- transferring malicious files between smartphones using the Bluetooth interface;
- synchronizing a smartphone with an infected computer;
- accessing an infected memory card;
- Opening infected files attached to MMS messages.

b) Spreading Parameters: In addition to infecting the device, worms may also attack the communication network itself. During this situation, worms not solely compromise users' ability to use their smartphones however the networks as well.

c) User Mobility Models: Compared with the web, portable networks have terribly completely different characteristics in terms of topologies, services, provisioning and capability, devices and communication patterns. These options conjointly characterize the manner new styles of mobile worms propagate: the foremost vital one is that they are doing not need net property for their propagation and, therefore, will unfold while not being detected by existing security systems. Hence, mobile worms will infect many devices victimization proximity attacks against vulnerable devices that are physically close. To model the propagation of those worms, 2 steps are required:

1) Build a model that precisely describes how devices meet each other;

2) Understand how malicious code exploits both the mobility of the users and the capacities of the networks.

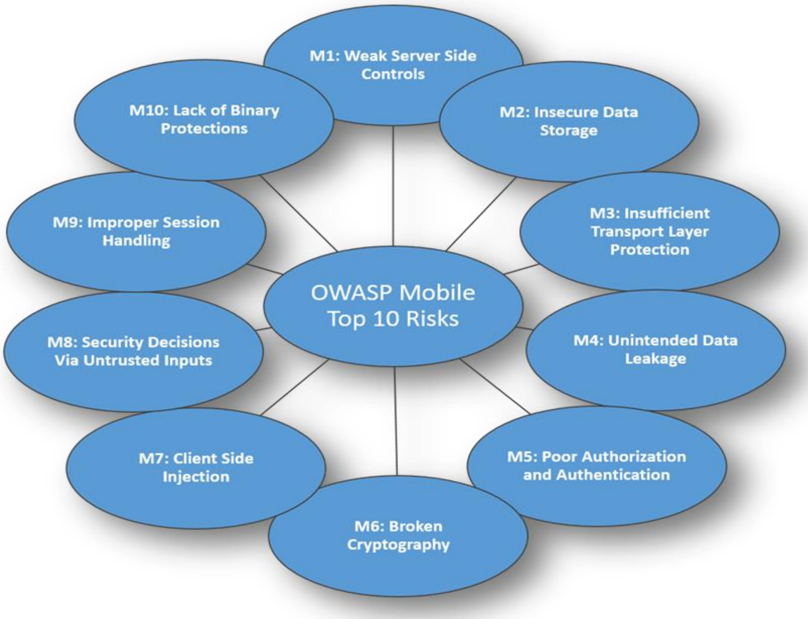
M1: Weak Server Side Controls
M2: Insecure Data Storage
M3: Insufficient Transport Layer Protection
M4: Unintended Data Leakage
M5: Poor Authorization and Authentication
M6: Broken Cryptography
M7: Client Side Injection
M8: Security Decisions Via Untrusted Inputs
M9: Improper Session Handling
M10: Lack of Binary Protections
OWASP Mobile Top 10 Risks

FIG. TOP 10 MOBILE RISKS

IV. ANDROID DEVICES CURRENT SECURITY CHALLENGES:

A decade ago, mobile malware was considered a new and unlikely threat. Many mobile device users even considered themselves immune from such threats. Fast forward to 2017, and more than 1.5 million new incidents of mobile malware have been detected by McAfee Labs in the first quarter of the year alone – for a total of more than 16 million mobile malware incidents.**[15]**

The major challenges to the Android device security are:

1. Persistent, enterprise-class spyware

Employees use their mobile devices in nearly each side of their lives with mobile devices ne'er over arm's-length away. With such shut proximity to company network access, voice activation, and GPS pursuit, state actors are watching ways that to infect mobile devices with spyware. The plan of action has evidenced winning on each iOS and automaton device.

2. Mobile botnets

New malware will quickly flip legions of mobile devices into a botnet that's controlled by hackers while not the information of their owners. The primary mobile botnet targeting android devices, dubbed Northman Horde, was discovered simply over a year past. Northman Horde created a botnet on any nonmoving or non-rooted device that uses proxied informatics addresses to disguise ad clicks, generating revenue for the assaulter. Since then malware researchers have known a few dozen a lot of mobile botnets, together with buzzing dangerous, that infected over ten million android operative systems in mid-2016. User details were sold and a commercial is a broach on while not the user’s information and in doing therefore generates deceitful advertising revenue.

3. Ad and click fraud

Ad and click on fraud in mobile devices may be a growing concern, researchers say. “Compromising that mobile device [through ad and click on malware] would be a pleasant method for a criminal to achieve access to the inner network of a corporation, presumably by causation an SMS phish, obtaining somebody to click on a link wherever they transfer a malicious app, and so currently that they’re on the phone and may management it, they will steal credentials and gain access to the inner network,” Shier says:

The scary part, Padon says, is that “*they start as adware, but they can just as easily decide to spread spyware to the entire botnet. Then you have 10 million devices that record their owners’ every move. It has a devastating potential with just a click on the app,”* he says.

4. IoT

Internet of Things (IoT) malware remains in its infancy, however it hasn’t stopped malware authors from creating the jump, says Irfan Asrar, senior manager in mobile malware analysis at McAfee. “The variety of [IoT malware] families out there's simply ten, and most of them area unit simply variations of a similar code base, however we’re beginning to see within the underground sites that folks area unit vending mobile malware kits and area unit going in the IoT arena,” and plenty of IoT devices area unit for the most part connected to and being designed by smartphones and devices, like mobile entry into a building or through a stop.

“With targeted attack efforts, they are focused on getting to a destination,” Asrar says. “They don’t care what means they use – just the one with least resistance – and right now it’s IoT

Where there are very little measures in place for security, and device manufacturers are just now beginning to follow some standards.”

5. Dead apps

Employees have to be compelled to check the standing of their mobile apps frequently, so update or delete them if they’re now not supported in Google or Apple stores, Asrar says. Security groups for each operative systems are quietly removing associate degree covert range apps from their stores at a growing rate, however they haven’t disclosed a listing of the removed apps or offered any reason for his or her removal, which may vary from malware problems to infringement to the invention that the app was leaky information to a 3rd party.

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.

VI. ACKNOWLEDGEMENT

The authors would love to impart the anonymous reviewers for his or her valuable comments and suggestions that have greatly improved the standard of the paper.

REFERENCES

Journal Papers:

[1] Chris Folk, Dan C. Hurley, Wesley K. Kaplow, James F. X. Payne, "Security Implications of the in AFCEA International Cyber Committee, Feb. 2015, http://www.afcea.org/mission/intel/documents/InternetofThingsFINAL.pdf

[2] Rodrigo Roman, Pablo Najera, Javier Lopez, "Securing the Internet of Things", Computer Society 58, Sep. 2011, https://www.nics.uma.es/sites/default/files/papers/1633.pdf

[3] Blanca Escribano, "Privacy and security in the Internet of Things: challenge or opportunity", Ols http://www.olswang.com/media/48315339/privacy_and_security_in_the_iot.pdf

[4] Ajit Jha, Sunil M C., "Security considerations for Internet of Things", whitepaper, L and T Techno http://www.lnttechservices.com/media/30090/whitepaper_security-considerations-for-internet-of-things.pdf

Books:

[5] A. Makhlouf and N. Boudriga, “Intrusion and anomaly detection in wireless networks,” in Handbook of Research on Wireless Security, Y. Zhan, J. Zheng, and M. Ma, Eds. Information Science Publishing, 2008.

[6] K. Haataja, “Security threats and countermeasures in Bluetooth enabled systems,” Ph.D. dissertation, Department of Computer Science, University of Kuopio, 2009.

[7] Y. L. Ho and S.-H. Heng, “Mobile and ubiquitous malware,” in MoMM ’09: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia. New York, NY, USA: ACM, 2009, pp. 559–563.

[8] A. Bose, X. Hu, K. G. Shin, and T. Park, “Behavioral detection of malware on mobile handsets,” in MobiSys ’08: Proceeding of the 6th international conference on Mobile systems, applications, and services. New York, NY, USA: ACM, 2008, pp. 225–238.

[9] A.-D. Schmidt, F. Peters, F. Lamour, C. Scheel, S. A. C¸amtepe, and S. Albayrak, “Monitoring smartphones for anomaly detection,” Mob. Netw. Appl., vol. 14, no. 1, pp. 92–106, 2009.

[10] L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu, “pBMDS: a behavior-based malware detection system for cellphone devices,” in Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24, 2010. ACM, 2010, pp. 37–48.

[11] M. Becher and F. C. Freiling, “Towards Dynamic Malware Analysis to Increase Mobile Device Security,” in Sicherheit 2008: Sicherheit, Schutz und Zuverl¨assigkeit. Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft f¨ur Informatik e.V. (GI), 2.4. April 2008 im Saarbr¨ucker Schloss, ser. LNI, vol. 128. GI, 2008, pp. 423–433.

[12] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, “On cellular botnets: measuring the impact of malicious devices on a cellular network core,” in CCS ’09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 223–234.

[13] W. Enck, P. Traynor, P. McDaniel, and T. La Porta, “Exploiting open functionality in SMS-capable cellular networks,” in Proceedings of the 12th ACM conference on Computer and communications security, ser. CCS ’05. New York, NY, USA: ACM, 2005, pp. 393–404.

[14] V. Bocan and V. Cretu, “Security and Denial of Service Threats in GSM Networks,” Periodic Politechnica, Transactions on Automatic Control and Computer Science, vol. 49, no. 63, 2004.

[15] Threats to Mobile Security. https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html