Bittium White Paper

Mobile Device Security

Part 1 – Fundamentals

Bittium

Mobile Device Security
Part 1 – Fundamentals

White Paper
Published 2020
Writer: Jouni Hiltunen

Table of Contents

1 Characteristics of Mobile Device Security 4
1.1 Always Available and Connected 4
1.2 Work and Personal Use United 5
1.3 Mobile Device Ecosystem 5

2 Threat Landscape 6
2.1 Malware 6
2.2 Insecure Communications 6
2.3 Ecosystem and Human Complications 7

3 Security Enablers 8
3.1 On-Device Protections 8
3.2 Secure Communications 8
3.3 Security Enhanced Ecosystem and Policies 9

4 Summary 10

1 Characteristics of Mobile Device Security

In this paper we will dive into the fundamentals of mobile device security. With mobile devices we refer to computing devices small enough to hold and operate in the hand such as mobile phones. The mobile devices have shaped our life in many ways: how we communicate, find information, store memories, work and spend our spare time.

As the mobile technologies are playing a significant role in our leisure and work activities, the security technologies have become increasingly important in protecting the private and enterprise confidential information. The security best practices and principles provide a solid ground to protect the information but what are the most relevant aspects that must be taken into account? In this section we look into the characteristics of mobile device security.

But first a quick recap of the fundamental security principles. A serious security study would not be complete without taking into account a CIA (the abbreviation should not be confused to certain intelligence agency) triad that stands for confidentiality, integrity and availability. **Confidentiality** means that your data should not be made available to parties that you have not approved. **Integrity** means that protected data could not be modified without your approval (or at least the modifications will be detected). The last but not least is **Availability** which means that you should be able to use your data when needed.

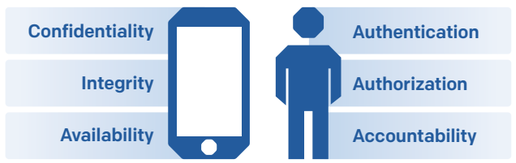
The CIA triad focuses on data protection so we must complete our security evaluation model with an abbreviation that focuses on the user. It is AAA which stands for authentication, authorization and accountability. **Authentication** is the act of proving that you are who you say you are. **Authorization** is the act of giving right to access data based on authentication. **Accountability** is the act of keeping track of things that you have done (in order to figure out what happened in case of a security incident but not to violate your privacy).

1.1 Always Available and Connected

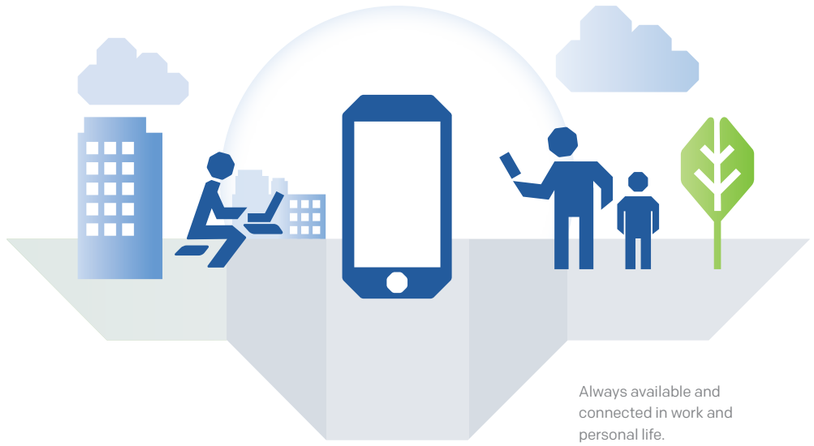
The first and foremost thing about mobile devices is their ubiquitous character. We carry them around in all kinds of places, indoors and outdoors. The environmental conditions that the device must survive will vary a lot and are often quite harsh such as autumn rains, summer dusts and winter colds (at least up here in Finland). So the device must be durable to ensure availability. Fortunately, we don't have to rely on vague marketing terms such as waterproof when evaluating durability but there are standards that define exact levels of protections such as IP Code and MIL-STD. IP Code rates protections against dust and water. For example, IP67 means that the device is dust tight and it can survive in water up to 1 meter depth for 30 minutes. Another common standard is MIL-STD-810G that defines a broad set of environmental (like shock, vibration, temperature, humidity) requirements for mobile devices so that it can survive a drop to the floor, for instance.

We do all the mobile things at home and at work, in private and in public places. This leads to increased probability that the device is lost, stolen or someone gets some other way access to the device. Obviously the device **availability** is threatened again, also in less obvious ways; a smallest of the family may be the biggest threat for device left in the living room table. Traditionally, it is game over security-wise if adversary gets physical access to your device. However, in mobile devices we would prefer that the game goes on while ensuring **confidentiality** and **integrity**.

The mobile devices are always available and connected which separates them from other devices such as laptops. The device will connect to all kinds of networks; private and public Wi-Fi as well as 2G, 3G and 4G cellular networks. Some of the networks you may control and some you may trust but sometimes there are just things you cannot avoid such as lawful interception in some parts of the world that threats the confidentiality of your network communications. In addition, given that some



Fundamental security principles.



Always available and connected in work and personal life.

security incidents are caused by human error and you are always available through your mobile device, you should remain security conscious at every turn, and that's not easy when you are in a laidback mood while chatting with your friends in social media.

1.2 Work and Personal Use United

Using the mobile devices at work has become more common as they have evolved to things that you can actually do all kinds of work; it has the processing power and large enough screen to handle documents, necessary apps to access network services, handle data and communicate with your colleagues, while, as we talked earlier, it is available all the time. But it is tedious to carry around multiple devices each dedicated to personal and work use, and therefore it's common that work and personal things unify in a single device. So confidentiality comes into play; it must be ensured that enterprise data does not leak to your social media and your boss does not invade your privacy.

Even though the enterprise data is safe within the mobile device, IT administrators worry that the network services that provide access to same data is also safe. This means that the devices and users connected to the services must be authenticated and authorized. In practice, this means that the identity of the device should be attested before it is attached to enterprise device fleet (that is approved by the IT administrator) while use of the device is strongly bound to the employee (that is no one else can use it). But to complicate things a bit; the apps within the device can autonomously access the services and forward the data to dubious addresses. Therefore, the IT administrator would also prefer that all the things within the device are trusted (or at least untrusted things cannot mess things up).

1.3 Mobile Device Ecosystem

When buying mobile devices you get a whole ecosystem in the bargain. To put things simply; the device manufacturer takes a bunch of electronics and software and puts them together so that user can do the basic mobile device things and install additional apps. In contrast to PC world, the users cannot just install an operating system of their own. Therefore, you should trust the device manufacturer so that there are no hidden functionalities under the hood that could violate our security evaluation model. The bad news is that, given the mobile device's ubiquitous character, even the simplest information gathering functionality could become a problem in terms of privacy. The good news is that at least the most popular mobile device operating system, Android, is open source. This partly solves this problem but anyways, no software is perfect and some cunning hacker could find a way to use the software for unintended purposes. Therefore, it is preferred that only necessary software is running in the device, including the proprietary firmware installed by the device manufacturer. Also, the software security updates become important when security issues are discovered in software (and if software developers care to provide security updates).

In addition to the operating system and firmware, the user installed apps are also important security-wise. Fortunately, mainstream mobile device security is in pretty good shape in this sense; the things the apps can do are restricted, they are mostly visible to the user and user can influence what the apps are allowed to do in their device. The ecosystem includes also commonly used trusted app stores (that is there is some security based approval process for the apps) that the user can install the apps from, so there are good distribution channels for app security updates.

In terms of operating system and firmware the update situation is not as straightforward. Consumer grade mobile device manufacturers are willing to provide updates for a very limited duration but that is not the bottleneck in all cases. In some countries mobile carriers want to customize the device and in consequence take control of the update availability which could be even more limited than the manufacturer policy.

2 Threat Landscape

At this point of our security analysis it is time to introduce the threat landscape and answer the question: what are we fighting against? Security geeks call this threat modelling and it starts with the simple proposition stating an inventory of the things that we are protecting. Actually, we already discussed it earlier: data (with different sensitivity requirements) stored within the device, network communications and enterprise network services.

2.1 Malware

Based on the latest mobile threat reports, the mobile malware seems to be well off. For example, 6% of customers of a specific vendor reported malware infections and over 1.5 million new mobile malwares were discovered quarterly.[1] The malware could be categorized to opportunistic and targeted types. The opportunistic malware aims to spread widely to gain profit from small streams of income; for example ADB.Miner turns the device into crypto currency mining tool for the malware author.[2] Targeted attacks are focused on specific targets instead and are usually espionage motivated such as in a case of malicious mobile device management system that was able to exfiltrate end-to-end encrypted chats by deploying customized secure chat apps to the victim's device.[3] Such targeted malware, also known as spyware, often come with abundant ways of exploiting the victim such as tracing location, accessing the device's microphones and video cameras as well as gathering information from apps.[4] Unfortunately, unauthorized access to the device's microphones and cameras, and even to sensors[5], endanger also the people nearby through eavesdropping.

2.2 Insecure Communications

Most of the network communications, for instance website or app traffic, goes through the Internet which does not provide any protections related to our security model. Fortunately, public awareness of this issue has grown which has led to extensive use of protections, such as HTTPS, that ensure confidentiality and integrity of the communications.

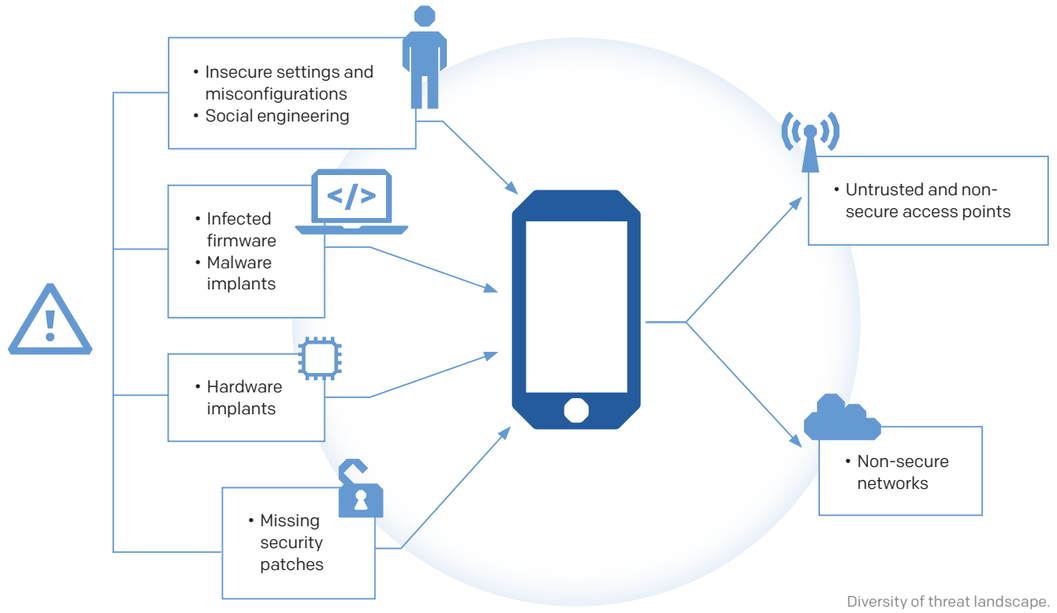
The HTTPS solves also authentication issues but usually only the device is able to authenticate the server and not vice versa. This is because the device comes with preinstalled certificates that enable authenticating the server but obviously it would be difficult to have all the device certificates preinstalled on the server. The preinstalled certificates on the device side are possible because of internet public key infrastructure which has a set of certificate authorities (CAs) that can issue further certificates. Using conveniences of cryptography it is sufficient to preinstall only the CA certificates to the device, which is a manageable amount, to authenticate all server certificates issued by the CAs.

So the internet communication issue boils down to the trust towards the CAs. And you probably guessed it; also the CAs may be breached[6] or have other trustworthiness issues[7]. One could also choose to create a private CA as long as there is a secure way to transfer the certificate of the private CA to the devices. The certificates could also pose a threat to availability by themselves because they have an expiration date. The device should not use an expired certificate so all communication is blocked if the device does not default to an insecure communication.

While well-funded actors have the capability to do attacks on core internet communications, even an average thug can eavesdrop a poorly configured Wi-Fi access point or set up one of their own to do traffic monitoring and tampering. Given that the wireless communications is broadcasted all around, also the vulnerabilities in its security controls are always a big deal[8].

Cellular communications come also with shortcomings of its own although the security has been improving along with new generations of cellular technologies. The main problems are insecure legacy technologies and worldwide interconnectivity requirements leading to complex set of technologies, networks and actors. Caller ID spoofing is one of the main threats that must be taken into account when receiving a cellular call, SMS or MMS[9].

The mobile devices could also provide an access to internal home and enterprise networks and bypass any firewall protecting those networks. One of such malware is Android/TimpDoor malware which is spread via social engineering by tricking the user to download and install a fake app advertised through text messages. It transforms the device to a convenient proxy that the adversary can use as an access point to which ever network the device is connected.



Diversity of threat landscape.

2.3 Ecosystem and Human Complications

One of the biggest threats within the mobile device ecosystem are the devices with outdated firmware. A report from 2017 states that 41% percent of Android devices are missing the latest 2 months security patches[10]. The user installed apps should be also updated as security issues are discovered in them. However, updates could bring in more trouble if the app has been sold to an adversarial party or if related app signing keys or app store accounts have been breached. Not to mention device manufacturers and carriers providing vulnerabilities to the device firmware out of the box[11].

Malicious app updates, such as software implants that are retrofit to a legit app during delivery[12], are one form of supply chain attacks. Supply chain problems have grown in the past years since there is a general trend of supply chains becoming more international. In addition to software implants, also hardware implants are part of the wellfunded threat actors' toolbox that enable eavesdropping calls, for instance[13].

The hardware implants are also a threat after the mobile device has been taken into use. If the adversaries get their hands on the device they could open it and read data directly from the storage chips. If the adversaries get only in the proximity of the device, they could launch so called side-channel attacks to pull out secrets, such as encryption keys, exploiting devices electromagnetic emanations, for instance[14].

In addition to social engineering, the human errors play a significant role in relation to threats. Although the devices are usually configured securely out of the box, there are multiple ways the user can mess with the security settings. For instance, the aforementioned ADB.Miner malware used misconfigured Android devices with open debug interface to spread over the network and a PC based banking trojan named Droidpak installed Android version of itself to devices connected to the infected PC through the debug interface[15]. One of the worst things that could happen is that the user turns off settings that prevent installing apps from untrusted sources and even install untrusted firmware to the device. The user could also ease physical attacks by using a guessable device unlock password.

3 Security Enablers

We have discussed above the characteristics of mobile device security and the threats that mobile devices are facing. All we need for concluding our security evaluation is the definition of techniques that mitigate the threats and enable using the mobile devices in most productive way in all use cases.

There is no silver bullet to mitigate all threats but they must be approached with a set of security controls designed to protect against one or multiple threats. However, all security controls may contain errors and therefore it is desirable that there are multiple layers of defense in the device. This defense in depth approach makes the device more secure as compromising a layer does not compromise the whole system.

3.1 On-Device Protections

In addition to the discussed IP Code and MIL-STD classifications that ensure durability of the mobile device, tampering detection is another mechanics-related protection. It detects attempts to open the device covers as well as other physical tampering events. The device may respond automatically to the tampering events by deleting data from the device and by preventing further usage of the device, for example. Another related layer of protection is data encryption that ensures that data is safe even if tampering mechanisms are circumvented.

To protect against non-intrusive physical attacks, the device should have critical security parameters, such as data encryption keys, stored and handled securely. Secure Element (SE), which is also known as trusted platform module, provides such capability. It could even provide protections against intrusive physical attacks. The SE should be physically separated from the rest of the system (with the exception of necessary communication and power interfaces, of course) in order to minimize attack surface which makes it easier to protect against attacks even if the rest of the system is compromised[16].

To protect against malware and malicious firmware, the infection and spreading paths must be blocked. Mobile device management (MDM) solutions provide a convenient way to allow only trusted applications to be installed to the device. The solution could include also a private enterprise app store which includes only trusted apps and which can force app updates to the devices. Installing malicious firmware to the device can be prevented by forcing secure boot on the device which prevents running any other firmware than the one cryptographically signed by the device manufacturer.

Fortunately, even if the device gets infected by a malicious app, the mainstream mobile device operating systems have built-in protections, such as restricting app capabilities within the device, that limit the damage made by the malware. However, when device is in enterprise use, additional protections are necessary to ensure that malware has no access to enterprise data within the device and to enterprise network services. To provide additional separation of data, apps and virtual private network (VPN), they should be isolated in container workspaces that are each dedicated to enterprise, governmental or personal use.

As an additional defense in depth solution, the device could support privacy mode that disables all audio inputs to ensure confidentiality of meetings and discussions. Device's microphone could be disabled at hardware level which makes it very hard to circumvent this protection. Given that the device is full of legitimate apps that have been given permission to use the microphone, such as VoIP apps and sound recorders, it makes sense to ensure that these apps are not leaking information.

3.2 Secure Communications

In insecure or untrusted networks, such as internet or public Wi-Fi access points, it is important to use end-to-end encryption. As we talked earlier, secure communication protocols are commonly used for this purpose but it comes with certificate management complications. For mobile devices, this problem can be solved with MDM-based certificate management which scales well to large device fleets.

Even if the secure communication standards have become a norm, the reality is that the mobile devices are running various apps that are communicating all around the world through all kinds of network protocols. VPN provides a solution to ensure that all communication is secured no matter which network

Security built in layers.

you are connected to. In untrusted networks it is crucial but it provides also a valuable defense in depth protection which enables uncompromised communication even if waiting Wi-Fi security patches to roll out, for instance. When using VPN, all network traffic goes through the VPN provider's server so the trust to the provider becomes paramount.

In enterprise network the use of VPN is convenient because the client could be authenticated through VPN client certificate. Proper authorization to access internal enterprise network services could be given to the mobile device based on its identity. Since all VPN network traffic goes through the enterprise network, the device will be protected by enterprise network security controls, such as network firewalls and intrusion detection systems, and it enables accountability in terms of network behavior.

To further protect the internal enterprise services, in addition to the VPN client certificates that could be potentially installed in an adversarial device, the device should support remote attestation. It provides a proof that the device is exactly as it left the factory and carries unmodified, official firmware. Although on-device secure boot ensures that only authentic software can be run on the device, the remote attestation provides a defense in depth protection that can be verified remotely. The attestation is based on a unique attestation key written to the device during manufacturing which enables the server to verify that the device is trustworthy. The attestation key is stored securely in the SE. The key is used to create a cryptographic digital signature which provides unforgeable proof of identity that can be verified by the backend service.

One thing to remember when using VPN is that the communication is secured only from device up to the VPN server. The end-to-end security solutions are still required when using internet services. The same applies for voice and messaging communication between mobile devices. A trusted end-to-end secured communication app is required which enables communication confidentiality, integrity and authentication regardless of communication network.

3.3 Security Enhanced Ecosystem and Policies

One of the most important security properties that the ecosystem should provide are timely security updates delivered automatically over the air. Apart from app update issues solved by MDM, the supply chain security is otherwise pretty hard to measure or mitigate. One has to select the manufacturer based on its reputation, reported trust footprint of its manufacturing process and potential geopolitical preferences.

Some devices may also have national or international certifications that enable handling respectively classified data with the device in predefined use cases. This provides additional evidence that the device meets well established set of standards in design and/or implementation. On the other hand, the container based data segregation solutions are necessary if the device is used to handle data with different classification levels or schemes.

Security policies define valid settings and rules for device usage that mitigate human error based threats. Security settings may be forced through MDM but the user should also have clear instructions how to use the mobile device securely, such as entering the device unlock password out of sight.

4 Summary

In this paper we have dived into fundamentals of mobile device security from three different perspectives. To begin with, we identified the demanding use cases and operating environments that characterize the mobile device security. Secondly, we scratched the surface of mobile device threat landscape that the consumer users as well as enterprise and governmental users and service providers are facing. Finally, we listed the security controls and features that enable productive and secure mobile device usage on grounds of the mobile device characteristics and threats. It has become apparent that the security aspects must be taken seriously and addressed in a comprehensive manner.

Fortunately, most of the security controls are transparent to the user but usage policies are also necessary to address the threats that the device has no control of.

Bittium Tough Mobile product family consists of secure smartphone solutions for professionals and security conscious individuals which meet these entire requirements to enable your productive and secure mobile device usage.

> Visit the website for more information:
> **www.bittium.com/secure-communications-connectivity**

References

1 **McAfee Labs Threat Report Dec 2018:**
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

2 **ADB.Miner:**
https://blog.netlab.360.com/adb-miner-more-information-en/

3 **Advanced Mobile Malware Campaign in India uses Malicious MDM:**
https://blog.talosintelligence.com/2018/07/ Mo-bile-Malware-Campaign-uses-Malicious-MDM.html

4 **Pegasus spyware:**
https://en.wikipedia.org/wiki/Pegasus_(spyware)

5 **Gyrophone: Recognizing Speech From Gyroscope Signals:**
https://crypto.stanford.edu/gyrophone/

6 **DigiNotar:**
https://en.wikipedia.org/wiki/DigiNotar

7 **Google Chrome Bans SSL Certificate Authorities:**
https://thehackernews.com/2017/07/chrome-certificate-authority.html

8 **The 'Secure' Wi-Fi Standard Has a Huge, Dangerous Flaw:**
https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/

9 **Caller ID Spoofing – What It Is and What to Do About It:**
https://www.tripwire.com/state-of-security/featured/caller-id-spoofing/

10 **Mobile Threat Intelligence Report 2017 The Year In Review:**
https://www.symantec.com/content/dam/symantec/ docs/reports/mobile-threat-intelligence-report-2017-en.pdf

11 **Vulnerable Out of the Box: An Evaluation of Android Carrier Devices:**
https://www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf

12 **Spy agencies target mobile phones, app stores to implant spyware:**
https://www.cbc.ca/news/canada/spy-agencies-target-mobile-phones-app-stores-to-implant-spyware-1.3076546

13 **NSA ANT catalog:**
https://en.wikipedia.org/wiki/NSA_ANT_catalog

14 **Side-Channel PoC Attack Lifts Private RSA Keys from Mobile Phones:**
https://threatpost.com/side-channel-poc-attack-targets-encryption-software-glitch/136703/

15 **Windows Malware Attempts to Infect Android Devices:**
https://www.symantec.com/connect/blogs/windows-malware-attempts-infect-android-devices

16 **Attack TrustZone with Rowhammer:**
https://www.eshard.com/2017/04/20/download-attack-trustzone-with-rowhammer-presentation-slides/

Bittium

Connectivity
to be trusted.

Bittium / Ritaharjuntie 1, FI-90590 Oulu, Finland / t. +358 40 344 2000 / www.bittium.com