Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

HOW SMARTPHONES AND CO. MAY BE CHEATING ON YOU

An overview of critical attack vectors on smartphones and tablets for enterprise use

Tablets and smartphones have already established themselves in everyday business as practical all-rounders. Devices that were actually designed for personal use are being utilized more frequently for business purposes. Existing guidelines for IT security, however, should be implemented on these devices and adapted to the current threats, so that these beloved helpers remain faithful in the protection of user data. The following presents relevant attack vectors to be taken into consideration for corporate security when assessing risks.

940201305

Introduction

Today, hardly any other commodity is more important than information. This is especially true for companies, because information consists of the data that companies generate, which is a highly sensitive and protection-worthy commodity – an essential asset. The introduction of smartphones and tablets add an additional aspect to the already complex situation of protecting enterprise data. It raises the question of whether and to what extend these tools have to be reviewed in terms of IT security and how existing approaches can be extended to protect the company. A major difference to notebooks, which have been in use for some time, is certainly that smartphones and tablets unite several basic characteristics. From a security perspective these have to be considered all together. In general the following risk factors can be described for the use of smartphones and similar equipment in a company:

- There is a higher risk of loss due to the form factor of typical devices and the ubiquitous use. In addition, the unlocked devices are often operated or accessed in an insecure environment. This increases the risk of a physical intrusion by an attacker.
- Communication is done mainly through public networks, which makes device and software interfaces more easily accessible to attackers.
- There is a high potential for abuse due to an extensive access to corporate information (e.g. corporate passwords, customer data and confidential information) and the protection level is often lower than in notebooks.
- From a security perspective, the greater variety of embedded functions, sensors and interfaces means an increase of exploitable attack surface because of the software complexity associated with it.
- The multitude of software versions and device manufacturers, and their differences that need to be addressed individually, further complicates an effective equipment protection for the companies.
- The user's responsibility to protect the company increases with the option to freely configure and extend the devices' software.
- Smartphones and tablets are perceived as personal, trusted devices, which reduces the acceptance of protective measures if they result in a restriction for the user.

The organizational measures already in place for the desktop area basically remain the same. Though, in the case of smartphones and tablets, they now have to protect the company in a much more dynamic environment with heterogeneous devices, without a protected perimeter and against a larger attack surface.

In the following, general attack vectors for smartphones are studied to understand more precisely what security measures can be used to counter the existing threats. These attack vectors need to be taken into consideration independent of the smartphones operating systems. This essentially also applies to tablets, as they are built identically, except for the phone features.

The attack vectors describe ways and means by which an attacker may achieve his goal. The main issue is to determine how these attack vectors differ when compared to desktop systems. Due to the different preconditions that may be necessary for an attack, the attack vectors will be reviewed separately on the logical and the physical level.

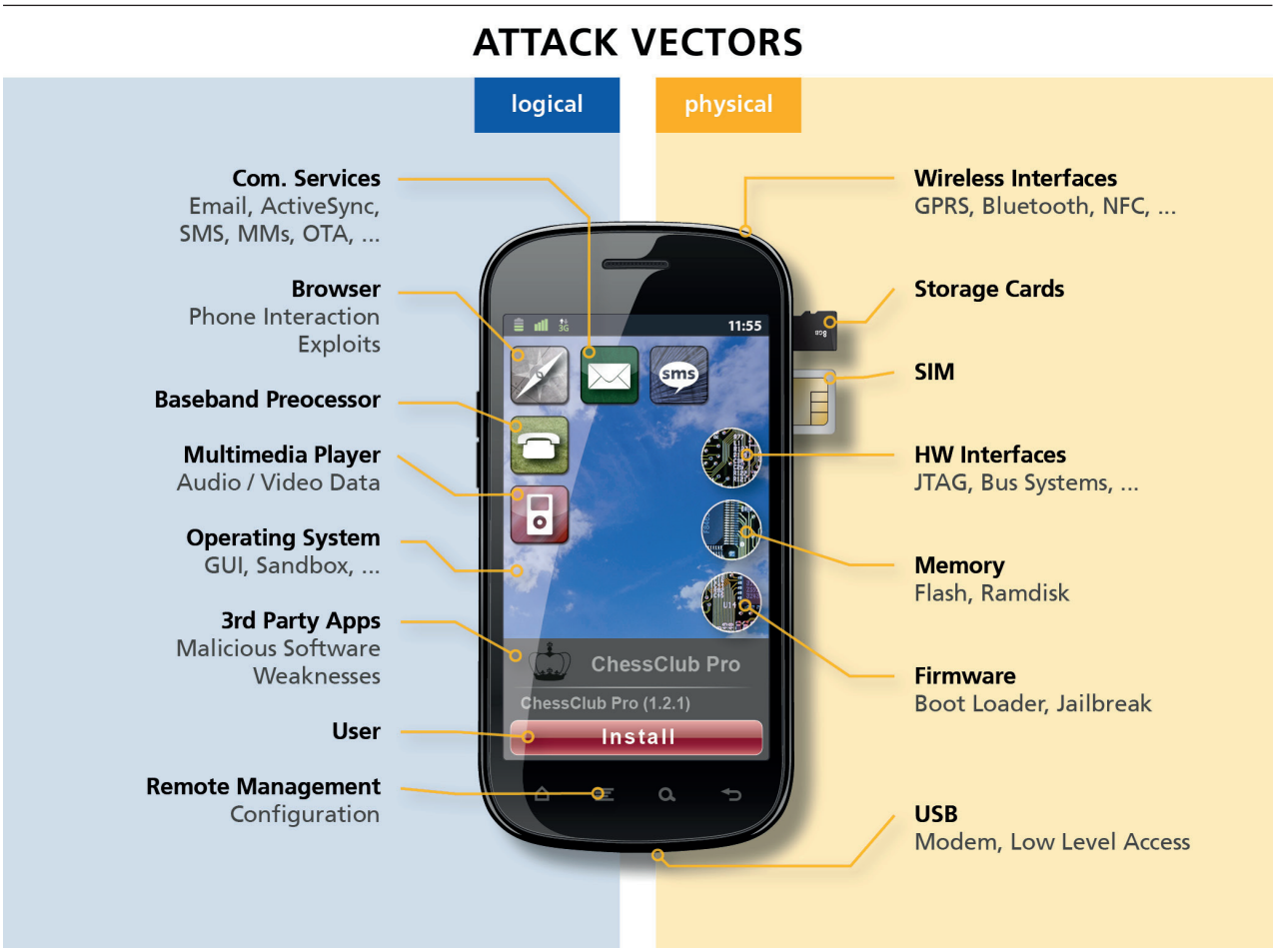
Logical Attack Vectors

Attackers usually always try first, like electric current, to take the path of the least resistance. Especially attacks, in which no physical access to the victim's device is required, represent a great motivation for using logical attack vectors, thus making it possible to attack many potential victims efficiently at the same time. Yet these attack vectors often also offer the possibility to select a specific, individual victim via a digital user identity. This method utilizes potential weaknesses in the various software and service interfaces smartphones and tablets offer on this logical level.

Communication Services

Communication services such as e-mails, SMS, MMS, instant messaging or VoIP services, play a very fundamental role in attacks, since they can be used to transfer malicious software directly to the end device or to direct the user to prepared contents on the Internet.

While servers may be able to filter attacks by e-mail out of the corporate mailbox, it is more difficult for SMS, MMS and instant messages. This data is not checked by the enterprise's security mechanisms and may transport malicious code onto the end device (see for example [3]) or request an installation, undetected by administration. The fake trustworthy sender identities and the targeted addressing of key individuals (so-called spear phishing) are considered to be critical scenarios particularly in the business environment.



Browser

As with desktop computers, the web browser has become one of the most used applications on today's smartphones and tablets. The contents retrieved are often not only of a static nature but data and entries are being processed actively on the end device while browsing. Since the standards used for processing on these end devices are becoming more complex, the risk of potential vulnerabilities, where an attacker can execute malware on the end device, increases as well.

Especially the connection between browser and user identity through the SIM card represents an additional target. Vulnerabilities in the browser may for example use the SIM card user identity to generate from web pages chargeable calls (e.g. demonstrated in [1]) or send out SMS' for services. An attacker may also possibly receive the means to circumvent security procedures to confirm a user's identity or misuse it.

Baseband Processor

The actual phone in the smartphone is realized by a baseband processor. This has recently been identified as another point of attack from two different sides. First from outside over the mobile radio interface for end device attacks and secondly as a stepping stone from the smartphone itself against mobile radio network base stations or its users. In the first case, the attack is usually directed against the availability but may also be targeted at accessing confidential data in the smartphone data storage. In the other case it is directed against the availability of the mobile radio service.

These methods exploit bugs in the baseband processor's proprietary software. In the past such bugs often remained unnoticed during the manufacturers' purely functional tests. The extensive programmability of smartphones and the sharp decline in price for base station technology now give attackers more options to detect and exploit security related vulnerabilities outside of the tested specification. The impact of these attacks has been much discussed lately (see e.g. [2][3][4]).

Apps

Any expansion of a device's functionality involves the risk that the resulting increase in complexity will also result in an impairment of IT security. Especially smartphones and tablets lack transparency in their applications (apps) regarding potentially hidden functions and resulting risks. Through the uncontrolled installation of applications, the ubiquitous (invisible) wireless communication and the direct link to the standardized, real user identities in the smartphone, a high attack potential is being met by only limited user options to detect manipulations before damage occurs.

Inherent in the additionally installed software is the risk that it may contain vulnerabilities that may be used by attackers to gain unauthorized access to the application's data or to other smartphone areas. Currently the poor security properties of a number of apps is not really surprising, especially in view of the pressure on the prices in the app market, the low barriers for inexperienced programmers and the functionality oriented user perception.

This reflects the respective strengths and weaknesses of the competing platforms security models, and the manufacturers' support for the secure application of security concepts and surrounding app ecosystems.

The current ENISA report [5] also confirms the importance of interweaving protection through: review systems, reputation mechanisms, isolating apps from operating system components (sandboxing), the limitation on trusted software sources (walled gardens), and the possibility to remove an application remotely from an end device (the kill switch), if it has been exposed as being harmful.

However, many studies in the Fraunhofer SIT lab often show that in practice the resulting protection is still fragmentary. These risks need to be addressed through continued development. It should also be considered to reduce the functionality at some points to meet higher security requirements, thereby increasing security. Especially these configuration features can usually be found only in devices that have been designed for business use and are not yet available in very many consumer devices.

Many apps are relevant also from a privacy perspective. They often have full access to device identifications, location data, e-mail and phone contacts, the SIM card number and other personal data and can, without informing the user, transmit these to the device manufacturer, the provider or the supplier of analytical services, which is why the Düsseldorfer Kreis Supreme authority of the Federal Commissioner for Data Protection and Freedom of Information in the non-public sector) is requesting the option of privacy-compliant smartphone usage [6].

Multimedia-Player

It is easily overlooked that even a careless use of multimedia data from dubious sources constitutes a risk to corporate data, which security policies need to address. Already in the past attackers were able to exploit vulnerabilities resulting from the complexity of processing compressed multimedia data streams (e.g. MP3, MP4, WMA, TIFF, PDF, etc.).

The „JailbreakMe" iOS exploit demonstrates characteristically the results of vulnerabilities in processing multimedia data. First, it only used the vulnerability in pdf file processing to remove operating system restrictions (jailbreak), after publication, however, it could also be used for undetected attacks on all the data and functions on iOS devices [7].

Remote Maintenance

The remote maintenance of smartphones and tablets as part of mobile device management is an essential security element to review and enforce security policies in a dynamic environment. Especially critical aspects such as a lack of updates, an unsafe device configuration or the use of enterprise services via non-registered devices can be addressed using remote control interfaces.

Nevertheless, such an interface with access to profound operating system functions is associated with certain risks as well. Weaknesses in the interfaces to the remote device management create interesting opportunities for attackers to penetrate the devices or manipulate security settings. Communication links could for example be redirected to the attacker or software may be installed for spying on data and passwords. In particular when using public networks, a significant burden rests on the security of MDM protocols, the server software used and its configuration.

An appropriately tested MDM software solution addresses this risk with safeguards against manipulations and supports enterprise security by enforcing organizational measures with central device administration. Due to operating system differences, the potential of safeguarding options may not always be exhausted and given protection features may not always be implemented for all devices. However, it

should always be kept in mind that a centralized, unified MDM solution for different operating systems is an important control tool.

Users

Ultimately, a user may also serve as a vicarious agent for an attacker. The attacker may target a user's ignorance regarding the proper response to system and warning messages, or uses vulnerabilities in the operating system to deceive the user about the actual consequences. The success of this method is clearly indicated by the distribution of malicious software that is dependent on the confirmation of warning messages (e.g. ZeuS-in-the-Mobile (ZitMo), Cabir). In addition, many users have great confidence into their personal, carried gadgets allowing attackers to abuse this supposed trustworthiness of the devices.

Delegating security decisions to the user is problematic in the case of corporate devices, because many users may not be able to assess the effects of configuration settings correctly (e.g. choices in security dialogues, required password complexity, etc.).

Providing users with the right background for security messages and raising their awareness about the dangers is an important step towards protecting devices in an enterprise. Careful and security-conscious use of the devices can significantly reduce the risk of many attack paths.

Physical Attack Vectors

Due to the high risk of smartphone losses and the widespread local communication interfaces, physical attack vectors, in which smartphones come into the possession of an attacker or it at least is in the vicinity of one, have to be considered as well.

Wireless Interfaces

Processing already occurs when the transmitted data packets are being received, although wireless interfaces (Bluetooth, NFC, WiFi, etc.) initially only allow the transfer of data that has been additionally secured at the higher transmission standard levels on the end device. A common attack vector therefore consists out of creating manipulated data packets that exploit weaknesses in the reception process. If an attacker is successful in injecting a program code in such a manner, he can gain access to user data and passwords. If a weak encryption is applied (e.g. WEP), it is also possible that an attacker can decode the encryption directly and, as a result, read all the transmitted data.

However, from an attacker's point of view, intercepting transmitted, unencrypted data still is often much easier than to break into the device. He could for example take advantage of the fact that only a freely selectable name is displayed to the victim when the latter uses a publicly available wireless access. If an attacker is operating his own hotspot with a corresponding name (e.g. free internet, telecom or hotel), he can imitate a bogus access and is thus able to directly read a victim's data that has been sent or received over this hotspot. Since many applications still use unencrypted connections, an attacker may receive at least the unprotected communication this way (see e.g. [8]). If the same password is used in the insecure application and the corporate environment, the attack can also be extended to company accounts. Therefore, this attack represents not only a threat to insecure enterprise applications.

SmartCards

Data on external storage media is still often unprotected. Unlike notebooks, in which a full encryption with a pre-boot authentication is by now the standard for company notebooks, the same protection is still rare for smartphones. Where protection is present though, it is often vulnerable to brute force attacks due to weak passwords (see for example [9] for attacks on BlackBerry devices with SD card encryption).

Often the touchscreen pad is a cause for the weak passwords. An attacker gaining possession of a smartphone then can often read the data on the smartcard quite simply. If the attacker is furthermore able to place manipulated data on this smartcard and manages quietly to plant it on the victim again, smartphone vulnerabilities may be exploited as well. In addition, attackers may use the smartphone as a host to infect company PCs. The attacker may use smartphones, which are usually considered as trustworthy, to circumvent the recommendation not to use unknown USB sticks or CDs in corporate PCs. During the synchronization with the smartphone the victim's PC may be infiltrated deliberately with infected data and software, which in the next step may attack the corporate network (see e.g. [10]).

SIM Card

Besides smartphones more and more tablets use mobile data networks as well, the access of which is protected by SIM smartcards (Subscriber Identification

Module). Although the SIM card offers high security against attacks, attackers with a physical access can manipulate the communication between the SIM card and the smartphone (SIM toolkit) by exploiting vulnerabilities in the specification. As a result and depending on the corporate application and device usage, IT security relevant information may be read or modified [11].

The attack becomes especially critical when an attacker succeeds in planting such a manipulated device unobtrusively with his victim. The preparation of these attacks is quite complex, whereas the actual manipulation of the device itself can usually be carried out depending on the smartphone model with only a few simple manoeuvers on the device, just as easily as exchanging the battery. The added components in the SIM slot then only get noticed when the SIM or the battery have to be changed, which does not happen that often anymore. Therefore, in security crucial areas a regular inspection of equipment used off-premises may be important.

Hardware Interfaces

Even if software level barriers prevent an unauthorized device usage, attackers may still be able to circumvent such barriers by completely dismantling the device. The access over then attainable memory buses and hardware interfaces (e.g. JTAG) requires a much bigger effort than an access via software interfaces, but it frequently also makes it possible to bypass individual user interface protection mechanisms. Only protection with full encryption counteracts such attacks affectively, though the encryption has to be based on a strong external user secret.

Storage

Specifically the information stored in the memory is at a high risk if an attacker can access it directly. If there is no strong encryption, protection mechanisms may be bypassed by manipulating operating system functions in the flash memory. User data may be read directly from the memory components as well.

Firmware

Firmware integrity protection is often the basis for many of the security functions in smartphones and tablets. If firmware manipulation and restoral of the physical smartphone remain unnoticed by the user (the evil maid attack), the attacker can gain complete remote control over the smartphone and the data. Not only can current data be retrieved over a longer period of time, but functions such as GPS positioning, microphone or camera on the victim's mobile phone can be used by the attacker.

Another critical firmware manipulation is the so-called jailbreak in iOS devices, because it turns off important security functions in the iOS devices. Appropriately, many central MDM solutions offer jailbreak detection in order to exclude such manipulated devices from being used in a company environment. In principle, jailbreak detections on end devices are a race against the jailbreak community, and current detection methods are often easy to circumvent as well. Not only employees can easily and consciously ignore this hurdle, but even for attackers who are planning an evil maid attack this countermeasure represents only a small obstacle.

USB

Many of the accesses enabled by physical smartphone manipulations can be realized by using hardware-related protocols over USB as well, without opening the smartphone. This interface almost always offers the option of exchanging the firmware directly and access the flash memory more or less directly. For example, in iOS devices it is possible to access some content and passwords via USB even though the devices are locked and encrypted [12][13].

Beyond that, many smartphones are furnished with added logical interfaces for modem functions and data access via USB, which may represent an additional entry point for attacks. USBs can frequently be used as a data link and a charger at the same time. Attackers can exploit this in some smartphone models for an unnoticed data access in foreign, manipulated USB charging stations.

Outlook

Many smartphone and operating system suppliers and third party providers are working continuously on further countermeasures against the attack vectors described here. However, it still appears that the consumer requirements are prioritized and functions meeting corporate security requirements are introduced only gradually.

In the future the control concepts for corporate security will be put to an increasingly harder test due to the booming app markets and the resulting desire to use a well-filled smartphone for business purposes. Clearly systems will prevail which make it possible to

enforce interaction control with corporate services on end devices and the corporate side, despite the required extensibility (see e.g. BizzTrust [14]).

Besides improving application control in devices to curtail malicious software in its options, there is also a need for trusted instances that confirm the security features of apps, using specific standards. Consequently, this will already have to begin with the app development, because as a result of the rapid update cycles the practical test procedures will be able to ensure only part of the security features in the long run. Only with these measures companies will be able to channel the bring-your-own-device mentality (BYOD) correctly and securely. The almost explosive proliferation of heterogeneous devices and applications can only be mastered by using comprehensive mobile device management solutions, the use of which can be enforced for all mobile devices with access to corporate resources.

For the operating system suppliers, the device manufacturers, the solution providers and the network operators there is still a need for further action in terms of integrated solutions, to mitigate or even eliminate the existing risks. There is a trend for the forming of consortia in order to meet this challenge. Science as well is obliged at this point to work on the formation of such consortia and to participate in existing consortia to develop short-, medium- and long-term solutions. Generally, close cooperation between industry and research outside of such consortia is useful as well to develop new, initially unconventional seeming methods, which allow a flexible response to the highly dynamic development, thus creating the space to think through more systematic long-term approaches.

Conclusion

Many smartphone and tablet platforms already have more security functionalities implemented than common desktop PCs. Hoever, because of their use characteristic and the number of interfaces, these types of devices offer larger attack areas than the list of attack vectors describes. Moreover, practical tests often show that the basic device settings are not suitable for business and partly do not offer the security they promise.

For corporate use it has to be clarified as a first measure which security requirements can be derived from the business division and which data and services are to be used on the smartphones. Based on this an appropriate security concept will be developed and ultimately the end device setting adapted to the security requirements. Usually it is not sufficient though to adapt these settings once only. Compliance with the regulations has to be controllable and enforceable in an efficient manner. On the corporate side the infrastructure has to be adapted in such a way that only known, controlled devices are connected. Besides, knowledge about potential attacks and its dissemination in the company is very important.

Good technical protection will do a lot for security. However, the user is a factor that must not be neglected in the protection process, both in terms of a security conscious use, but of course also with regard to including requirements concerning productive work. A balance between functionality and security has to be sought. Because if a user is faced with too many obstacles for which he does not understand the reasons, he will look for ways to bypass the obstacles, often with worse consequences for the company's IT security.

From the perspective of business, it is especially important to be aware of the potential risks and dangers. This allows companies to prepare appropriate processes for potential future claims (e.g. loss of device, finding manipulated devices, etc.) in order to be able to react quickly if necessary (commonly known as incident management). This should also include processes for the continuous review of already installed measures with regard to their effectiveness to respond dynamically to changing conditions and findings. It is also helpful to proceed under the „think-like-an-alien" approach, i.e. to check for vulnerabilities where they are not suspected initially. Security properties should always be questioned critically and the assumptions need to be checked whether they are still valid or if they need to be adapted to the current threat through regular review routines.

To assess the secure use in enterprises, device security represents only the first step and should not be considered isolated. Even secure products often have to be adapted individually to the operational environment in order to counter attackers with a more uniform protection that does not show dangerous vulnerabilities at the integration points to the corporate infrastructure and services.

For higher security requirements often a tradeoff between functionality and security is necessary. Nevertheless, a smartphone reduced in its functionality due to protection still allows for a more productive work than forgoing these multifunctional helpers.

Literature

[1] The h Security (2008): iPhone dials by remote control, http://bit.ly/v7TUbs

[2] Weinmann, R.-P. (2011): All Your Baseband Are Belong To Us, http://bit.ly/9Ot4A0

[3] Mulliner, C., Golde, N, Seifert, J.-P. (2011): SMS of Death: from analyzing to attacking mobile phones on a large scale, http://bit.ly/vd9JGh

[4] Grugq (2010): Base Jumping – Attacking the GSM baseband and base station, http://bit.ly/9LaMMd

[5] Dekker, M., Hogben, G. (2011): Appstore security: 5 lines of defence against malware, ENISA Report, http://bit.ly/pj2Tb5

[6] Düsseldorfer Kreis (2011): Beschluss – Datenschutzgerechte Smartphone-Nutzung ermöglichen! http://bit.ly/xFDNY3

[7] Bachfeld, D., Mulliner, C. (2010) Mobile Bedrohungen – Spionageangriffe und Abzocke auf Android und iPhone, http://bit.ly/uwv3cz

[8] Eikenberg, R., Schmidt, J. (2011): Die Hotspot-Falle – Gefahren in öffentlichen Funknetzen, http://bit.ly/uAkLz1

[9] PCWorld (2011): Russian Company Adds BlackBerry Password Cracker, http://bit.ly/SZeCZD

[10] The Register (2010): Vodafone Spain supplies pre-Mariposa'd smartphone (again), http://bit.ly/PJIPwd

[11] heise-Online (2009): BSI-Kongress: Preis für Beitrag zu Handy-Manipulation, http://bit.ly/rYAdh2

[12] Heider, J., Boll, M. (2011): Lost iPhone? Lost Passwords! Practical Consideration of iOS Device Encryption Security, http://bit.ly/hvUnu9

[13] Heider, J., Boll, M. (2011): iOS Keychain Weakness FAQ – Further Information on iOS Password Protection, http://bit.ly/o5nq9I

[14] Fraunhofer-Institut SIT (2011): Fraunhofer SIT: Two Smartphones in One, http://bit.ly/O1VVr7

Author:

Dr. Jens Heider heads the Mobile Security Test Lab at Fraunhofer Institut for Secure Information Technology (SIT) in Darmstadt and has researched mobile systems for vulnerabilities since 2004
E-Mail: jens.heider@sit.fraunhofer.de