prevenity

SECURITY SOLUTIONS

Dangerous smartphones

Artur Maj (artur.maj@prevenity.com)
Marek Janiczek (marek.janiczek@prevenity.com)

Date of publication: 16th of August, 2010

Introduction

Since the inception of cellular telephony, technologies behind mobile telecommunication networks and mobile phones have been continuously developing and improving. From pure voice communication and analog telephony, known as 1st generation (1G) network – up to digital connections and Internet browsing – architecture, technologies and capabilities of telecommunication networks and mobile phones during the last decade have significantly changed. With current smartphones like BlackBerry and iPhone and third generation (3G) mobile networks millions of people around the world have a possibility not only to make calls from almost any place on the world, but have also a true mobility in accessing Internet and information. Slogans like "anywhere, anytime, any device" are no longer exaggerated marketing words as they could have been few years ago, but reality.

But along with all these new opportunities that mobile technologies and in particular state-of-the-art smartphones bring to all of us, new and serious security threats are on their way as well. Not only black hats were able to move most of attacks known in PC world to mobile devices, but also new threats have arisen that were not even known in the traditional Internet environment. At the same time vast majority of mobile devices remains unprotected against worms and viruses, which poses a serious threat not only to privacy of their users, but also to companies permitting the use of smartphones to access internal resources and services.

The purpose of this document is to build awareness of threats related to the usage of modern mobile phones, in particular of smartphones and Personal Digital Assistances (PDAs). The subsequent parts of this publication show examples of threats and potential consequences that individual users or companies may face – from privacy invasions up to serious financial losses. Special attention has been paid to insecurities related to the usage of smartphones for internet/mobile banking purposes, where the consequences of successful attacks can be the most serious and painful, at least from the financial perspective.

Smartphones in today's world

Fifteen years ago, in the middle of 1990's, majority of mobile phones were designed and used mainly to make voice calls and optionally to send short text messages, which were just introduced to the market. Mobile phones were operating mostly on closed operating systems – programming capabilities and availability of Application Programming Interfaces (APIs) were very limited and even cell phone games were at the very beginning of their road (the first game "Snake" for mobile phone was introduced by Nokia in 1997). Central Processing Units (CPUs) were slow, mobile phones' displays were small and primitive, read-only and operating memory was very limited, the same as storage and network connectivity capabilities. Even if we were able to use mobile phone to load and run 3rd party applications, such software could perform little, if at all, harm to the operating system of the mobile phone. In the terms of security, these devices were relatively safe – mostly because of simplicity, and the fact there was very little to break or hack "programmatically".

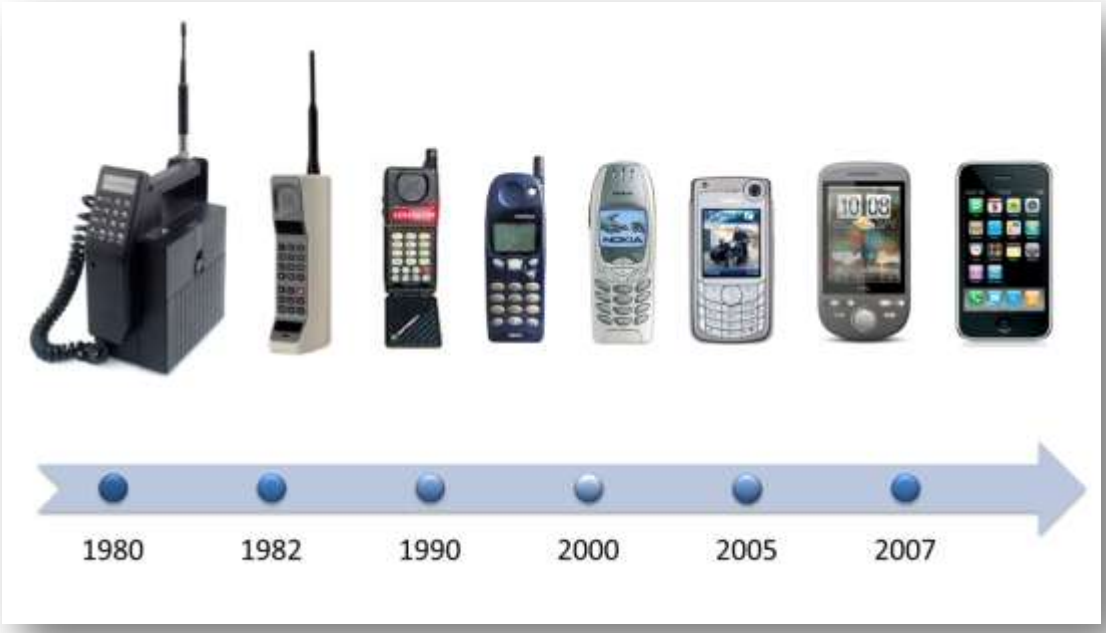

Figure 1: Evolution of mobile phones

In contrast, nowadays we may hardly remember these times. Surrounded by state-of-the-art mobile phones, smartphones and PDAs, it may be tricky to find in the shop mobile phone without built-in camera, or without support for Multimedia Messaging Service (MMS). Operating systems of mobile phones are no longer closed – on the contrary, some of them like Android are open platforms, and we can easily develop, load and run custom mobile applications. We can even change and extend capabilities of operating system if we do not like the ones delivered with the phone by the vendor. Other systems, like Symbian or Windows Mobile gives us a lot of liberty as well, exposing a lot of low-level functions of mobile phone's hardware to 3rd party applications via open APIs. CPUs are much faster – much closer to the PC that we could have bought few years ago. LCD Displays are now colorful and larger; memory and storage are now counted in gigabytes so no longer we need to count every single byte we use in applications. In addition, much more new equipment and functionality were added – GPS microcontrollers, Wi-Fi and Bluetooth network cards, web browsers, email clients and so on. Currently available smartphones no longer remind those old and simple mobile phones used fifteen years ago, but are much similar to powerful PCs with a lot of hardware and software components onboard. The only thing which may seem as not changed since the older times is battery's life. Even this may only "seem" as such, as in reality there was significant progress in this area as well, but longer battery life is now consumed by faster and more demanding CPUs and hardware added to the phones.

In the same way in which these devices have changed over the years, our habits and usage of mobile phones have changed as well. While making calls and sending SMSes still remains as the primary usage of smartphones, the rest is very different comparing to how we used mobile phones fifteen years ago. Ability to browse Internet, take pictures by built-in camera, listen to MP3s, plan time by using built-in calendar or send/receive emails and MMSes – all these features are now being actively used by millions of people around the world.

Not only smartphones are being extensively used for private purposes, but they have been also widely adopted by companies to increase mobility of their employees. Popular usage of mobile phones among corporate as well as small and medium business users include nowadays mobile access to:

- Company's e-mail service (e.g. via RIM Blackberry or MS Mobile Outlook),
- Company's calendar service (e.g. via MS Mobile Outlook and Microsoft Exchange),
- Shared file systems (e.g. Microsoft Sharepoint),
- Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) systems,
- Applications dedicated to mobile phones, for example:
  - Mobile Sales Force Automation (SFA),
  - Mobile Executive Dashboards,
  - SMS alerts and notifications,
- Company's internal network via Virtual Private Network (VPN) connections.

Thousands of various approaches as well as plenty of commercial and free solutions can be found as the result of simple web search for the "mobile solutions" phrase. From push email, through mobile connectors to commercial CRM systems, up to mobile VPN clients based on IPsec and SSL – the diversity and number of mobile solutions is huge.

Beyond typical usage as described above, it is worth to emphasize that cellular phones have been also widely used for e-commerce and e-banking purposes. Examples of such usage include:

- User authentication via software tokens running on smartphones,
- Access to mobile banking applications to make money transfers,
- Electronic transaction authentication via one time passwords sent by bank to the users via SMSes,
- Micropayments via SMS, USSD or interactive voice channel,
- Premium content purchase (so called Premium SMS),
- Alerts and notifications about change of account balance, debit or credit card usage etc.,
- Electronic signatures via online, native or SIM card applications.

The above list is just exemplary – possibilities of practical application of mobile phones and in particular smartphones are almost endless.

To summarize, in today's world not only we can make calls and send SMSes, but we can also access company's resources, make money transfers or access latest sales reports – everything from one small electronic device at our hand.

Mobile malware – myth or reality?

Open mobile operating systems and availability of low-level mobile phone's functions via open APIs provide software developers with almost endless possibilities of developing custom mobile applications. Not only developers are capable of building applications utilizing typical mobile technologies like SMS or USSD, but they can also build custom Graphic User Interfaces (GUIs) and applications that can replace default phone's software components in case it does not meet our needs. Unfortunately, there is also a dark side of it – such openness enables also black hats to leverage these APIs to develop, propagate and hide mobile malware.

How realistic is the threat of mobile malware infection? Is it really a problem for anyone on the planet, or a hypothetical issue that may happen in a more far than near future?

Anyone who thinks that mobile malware is a song of the future will meet a big surprise here. The facts are that mobile malware is not a future but reality. Based on statistics shared by Kaspersky Lab almost a year ago, in September 2009, there were already more than 100 known families and more than 500 modifications of mobile malware. Various statistics shared by other antivirus vendors put this even in a more negative light - the number of mobile malware is continuously growing, and due to growing popularity of smartphones and its increasing share in the mobile phone market this trend is unlikely to get reversed, soon.

Anyone thinking that the concept of mobile malware is new would also meet a surprise. As a matter of fact, first viruses for mobile phones were discovered more than ten years ago.

The below list show a quick overview of the beginnings of mobile malware and examples of propagation methods:

1. SymbOS.Cabir.A – it is believed that it is the first virus that started the era of mobile malware (despite that first malware for mobile phones appeared approximately four years earlier, for example Epoc.Fake.A). Discovered in 2004, it was targeting mobile phones running Symbian OS. It was distributing via Bluetooth to replicate and install on target devices. Cabir is considered as harmless – after replicating it only displays message "Caribe" every time the phone is turn on. The only harm it causes is shortening battery life due to constant searching of devices to infect via Bluetooth.
2. WinCE.Infojack – the first trojan targeting Windows Mobile operating system. It is distributing along with standard mobile applications, which helps to hide trojan's presence and activities. It is able to disable Windows Mobile security mechanisms and to download and install other malicious code, as well as send personal data to the author of malware.
3. SymbOS.Beselo.A – the first worm discovered in 2007 that was distributing via Bluetooth and MMS channels, pretending to be JPG, RM (Real Media) or Mp3 file, while in reality it was a Symbian application. It was also distributing via multimedia memory cards. After infection it was sending its copy to phone numbers taken from user's phone contact list.
4. Trojan.SMS.J2ME.RedBrowser – the first reported trojan horse build based on Java 2 Micro Edition, discovered in 2006. It was designed to continuously send SMSes to purchase premium content. Fortunately enough the user would need to accept sending the messages, therefore financial impact was relatively low. It is worth to emphasize, however, that current malware is able to send SMSes to premium-rate numbers without requesting user's permission.
5. SymbOS.Yxes.A – the first worm that was able to spread via SMSes sent to phone numbers from user's phone contact list. It is interesting that the malware was digitally signed by legitimate Symbian certificate, which means that the software was able to install basically on any Symbian mobile phone without warnings.
6. Worm.MSIL.Cxover – discovered in 2006, it was the first virus infecting both PC and mobile phone. Also it was the first virus for mobile phone developed using .NET Compact Framework. It was propagating via ActiveSync and was deleting all files in device's "My Documents" folder.

It is worth to notice that these are just first viruses identified in corresponding categories – most of them were discovered between the year 2004 and 2007. Since that time hundreds were discovered and reported. Now, we have the year 2010 and every month bring us new mobile malware – potentially more mature, more sophisticated and more dangerous.

Figure 2: SymbOS.Skulls trojan horse

How dangerous the attacks can be?

While the early days of mobile malware were concentrating mainly on enabling self-replication and creating proof-of-concepts, mobile malware authors soon realized that they can gain financial profits from writing such malware. This led to criminalization of mobile malware, and many of modern mobile malware is now capable to cause significant financial losses to the owners of infected mobile phones, for example by making unauthorized calls to premium-rate numbers. One of the examples is SymbOS.Viver.A, which was continuously sending SMSes to several premium-rate numbers, and it was found that the portion of profits was going to the author of this malware.

How serious the losses can be? It depends on the purposes, for which users actually use smartphone devices. Below we take a look at mobile malware from three points of views:

- Private use,
- Business use,
- e-Banking use.

"Private use" shows the threats that users may face when using mobile phone for typical private purposes, like making calls, sending SMSes/MMSes, browsing Internet and occasionally purchasing premium content. "Business use" shows the threats that companies may face as a result of their employees' mobile phones infection. And last but not least – "e-Banking use" shows examples of threats that both users and financial institutions may face when the user's smartphone becomes infected by mobile malware.

The list of the below threats is based on researches that Prevenity team made based on analysis of capabilities of current mobile malware, results of researches coming from other authors (see Bibliography), availability of commercial mobile applications and in certain cases developing proof-of-concepts supporting the below "features". It is worth to notice that the list is probably far from being complete – nevertheless the intention was to show real and practical dangers that may come from the side of mobile malware.

So what possibilities the attacker possesses after successful infection of smartphone, then? Let's see.

Case 1: Private Use

Voice communication

This is the area where privacy of mobile phones' users may probably suffer the most. Current capabilities of majority of modern malware allows to send the attacker the history of all incoming and outgoing calls (phone numbers, time, duration, frequency) but this is just beginning of bad things that may happen to users. To the more serious threats we may include:

- Automatically accepting and hiding incoming calls from the attacker, or secretly calling him back, so the attacker can eavesdrop conversations made near to the phone. What can be eavesdropped? Considering that majority of users carries mobile phones with them most of the time – probably a lot. Notice that to hide such activity calls may not necessarily be performed via GSM, but transmitted also via VoIP and 3G/Internet,
- Forwarding incoming calls to other numbers, for example to implement international "free" calls, premium high-rate calls, or redirect voice communication to the attacker. It is worth to notice that commercially available products implementing such "feature" already exist, example can be found here,
- Distributing SPAM via voice messages – for example, by calling everyone from user's phone contact list and playing uploaded voice message audio file.

Furthermore, certain software like VoxTrack Enterprise is able to automatically record all calls made (incoming and outgoing) to a digital format and send them to the remote server, so they can be searched and listened to later. What stands in a way for the attackers to silently install such software or implement such functionality in mobile malware? From the technical perspective, once the attacker finds a way to install malware on the smartphone, there are no obstacles. Based on the example of VoxTrack, we can be sure that such "feature" can be developed for Nokia phones, future will show if such applications are developed for other platforms.

Messaging (SMS, EMS, MMS, E-mail)

Messaging seems like a very "easy" target for the attacker. Easy, because due to the nature of messages they can be easily intercepted, transformed and sent in an unauthorized manner.

The possible attacks on messaging may include:

- Revealing all messages sent and received, for example by sending them to the attacker via Internet or via SMS/EMS/MMS channels,
- Sending unauthorized messages by the attacker,
- Distributing SPAM and/or phishing messages (text, multimedia, malicious code).

To the more serious attacks that may cause significant impact on user's financials we may include sending SMSes to premium-rate numbers. Such attacks are known from the very beginning of mobile malware, as in case of aforementioned RedBrowser or Viver malware. Notice that such malware is very easy to implement - for example, to develop such functionality the one need to write only couple of lines of code in C#, based on examples that can be found in most of .NET windows mobile programming tutorials.

Personal information and multimedia

Attacks in this category are mostly a threat to privacy of users. Examples include:

- Revealing personal information (contact list, calendar entries, tasks etc.),
- Revealing PINs and passwords (if stored on mobile phone in an unencrypted form),
- Unauthorized sharing of users' multimedia files (photos, videos, software, sound files),
- Making unauthorized pictures and videos via built-in front and rear cameras (though risk may be "low" as the attacker has no control on the position of the cameras),
- Wiping or encrypting user's data (photos, contact list etc.).

It is worth to emphasize here that once attacker is able to remotely control smartphone, he can do anything with what has been stored on mobile phone, including downloading and uploading files from/to the mobile phone. Therefore, as a word of warning and precaution, it is advised for users to not keep any pictures on the phone, which for various reasons they would be afraid of making them public.

Smartphone's location

This is an example of an attack not really known in the Internet world. As smartphones are "by default" mobile devices, which means the user carries them; it is possible to track the user, even in real time – if such functionality is implemented in malware. Such tracking can be easily implemented by periodically reading location of the user based on GPS or aGPS, and sending the location information to the attacker via any channel of communication.

Network connectivity

Last but not least, in this category we may find several attacks known from the PC world, for example:

- Redirecting user's web traffic through attacker's proxy server or unauthorized access points, which the attacker may easily do by remotely changing mobile browser and network configuration, or
- Recording and sharing all web information sent from mobile device (e.g. all information from HTTP GET and POST requests). This may be more tricky, but theoretically possible. Sample method may include modifying web browser (e.g. Firefox for iPhone, or Opera Mini) and replacing executable binaries on the phone, so all information sent to the Internet can be intercepted and spied,

… and attacks specific to mobile phones, like:

- Unauthorized remote use of phone's personal area network capabilities (Bluetooth, Wi-Fi) so the attacker can remotely attack another users and penetrate networks that are in the range of smartphone,
- Creating mobile botnets – attacker may use smartphone to perform distributed denial of service attacks on any target via "regular" (e.g. Internet) or mobile (e.g. SMSes, MMSes etc.) communication channels.

Case 2: Business Use

While the previous case was focused on threats when the smartphone is being used for private purposes, this section show examples of threats that companies may face when employees' smartphones become infected by mobile malware.

Practically speaking, all the threats mentioned in "Private Use" fit into this category, plus the following:

Messaging (Email, SMS, MMS)

Probably not so many companies realizes that when an employee losses mobile phone, the company losses much more than the physical mobile device along with the SIM card. If company's policy allows for using mobile phones, and such usage allows mobile phones to connect to e-mail servers, what an unauthorized person may possess includes:

- E-mail client configuration (IP addresses, port numbers, domain names) and user credentials (login, password) so the attacker can gain access to company's email server and user's emails from unauthorized devices, including "regular" PCs,
- All messages received and sent along with all business secrets they may contain – retrieved either from mobile device's inbox and "sent" folders, or directly from company's email server,
- Ability to send unauthorized messages including SPAM and phishing messages to employees, partners, customers, 3rd parties. Everything on behalf of legitimate user.

The above example touches the fact of losing the device – in practice the threats are almost identical as in the case of infection of smartphone with mobile malware.

Company's resources

Similar threats companies may experience in case of mobile applications used by employees to access company's systems, like CRM, ERP, BI, Sharepoints or other. If only application configuration and credentials can be retrieved by the attacker, he or she may gain unauthorized access to company's resources and services, most likely also from other devices, including "regular" PCs.

Special case may be when mobile databases are being used on smartphones that synchronize with central company's database – if the solution is properly designed and each user has got its own set of credentials (e.g. login/password) for the purpose of connecting with the central database, then the attacker has got limited possibilities of privileges escalation. But what if there is one login/password hardcoded into database configuration, shared among all mobile users? Needless to say, the doors to the company database and other users' data may be widely open.

Another serious threat is the possibility of identity theft. If company uses software tokens running on mobile phones for the purpose of users' authentication, and the attacker is able to gain remote control access to at least one employee's smartphone – the attacker may try to use software token remotely to log-in to any accessible applications the legitimate user has got the access to. Or, he can simply download it to his own device to run it offline – if the token is not logically linked with smartphone.

VPN connection to company's internal network

This is probably the worst case scenario for a company. When mobile VPN solutions are implemented on mobile devices and the attacker is able to read VPN configuration along with user's login and password, the attacker practically gains the ability to penetrate internal network of the company, at least to the extend

in which mobile device is able to see internal network. As in practice there is probably one-for-all VPN solution in the company – the attacker may gain open doors to company's entire internal network.

Social engineering

The ability to fully control one or more employees' mobile phones provides the attacker with almost endless opportunities to perform social engineering attacks and trick company's employees, partners or customers to reveal sensitive information. Such information could have high value on its own, or can be used to escalate attacks on other systems or devices.

Case 3: e-Banking Use

Although this category could be covered within "Private" or "Business" use, we deliberately preferred to treat this individually, as it may cause the most severe and significant financial losses to the owner of mobile phone. The list of the threats may seem short – unfortunately, the impact in case of successful materialization of the threat may be very high.

Mobile Banking applications

Available online, running on SIM Card, or as a native application – once smartphone becomes infected, an attacker can get full access to these applications. Web application and SIM card can be accessed remotely, and native application can be downloaded (if not logically linked to the device). If the only protection is login and password, which – by utilizing keyloggers – the attacker is able to intercept, then both the user and financial institution are in trouble.

Transactions authorization

Sent via SMS or USSD, or generated by application running within smartphone – the concept behind one time passwords requires that the user must supply such information in order to complete transaction. Theoretically such approach seems to be very secure, as in most cases two independent channels are used – PC with the access to the Internet, and mobile phone with the access to telecommunication network. Unfortunately, once malware takes control over the smartphone the attacker is capable to gain full access to authorization codes. If, in addition, he is able to retrieve (e.g. by using keylogger installed on PC) login and password to e-banking application, he can gain full access to user's bank account. Notice that first mobile malware infecting both PC and smartphone was found 4 years before writing this publication (Worm.MSIL.Cxover) so this kind of attack is far away from being theoretical. Prevenity team was also able to build a proof-of-concept of such attack for Windows based PCs and Windows Mobile/CE smartphones.

User authentication

Similarly as described in the example of business use, if in order to access e-banking application user uses software authentication token, then in case of infecting mobile phone by malware the attacker gets full access to the token. What he can do is either access and use such software token remotely or he can download it and use offline. This way or another – the attacker has got the opportunity to use it in an unauthorized manner, in order to log-in into the banking application.

Alerts and notifications (SMS, USSD, Voice messages)

Once smartphones become infected, they can be easily hidden from the user by deleting them before mobile operating system pass them to user's inbox, or can be redirected to attacker's phone.

Micropayments and purchase of premium content

If an attacker has got control over user's smartphone, and in particular possibility to send SMSes or make calls, what stops him to perform micropayments? For example, to pay for tickets or charge another prepaid phone by SMSes? The answer is obvious and leaves no illusions – from the technical point of view, nothing. SMSes to premium-rate numbers, USSD messages to payment service, interactive voice calls – all of them can be triggered remotely on victim's phone.

Mobile e-signatures

Another target of the attack may be mobile electronic signatures applications. Practically speaking, it does not matter whether such applications are installed on SIM card or they are installed as native applications – once the attacker remotely accesses GUI of the phone, he can run any applications he wants, so creating digital signatures in an unauthorized manner can be done as well. If PIN is needed to unlock the application the attacker may try to intercept it earlier as well, by implementing keylogging functionality as mentioned earlier.

Smartphones and authentication

Special emphasis we would like to put to the subject of using smartphones for the authentication purposes. It can be observed that there are a lot of companies, especially financial institutions that have been using mobile phones for the purpose of two-factor authentication, mainly by utilizing:

- One time passwords that are sent from company to the user's mobile phone via SMS or USSD messages,
- Software tokens running on mobile operating systems.

While leveraging smartphones to implement two-factor authentication may seem as "strong authentication", in case of infection of the smartphone by mobile malware such statement may no longer be true. Why is that? Two concepts of possible attacks are described below.

Messages redirection

This attack is targeted mainly toward mechanisms of authenticating electronic transaction via one time passwords delivered by SMS text messages. For example, bank, in order to complete electronic transaction, may require user to supply one time password that is sent to the user via separate communication channel, for example SMS or USSD. If user supplies this password to banking application it – at least in theory – guarantees that the transaction comes from a valid user, as he entered password that only he was supposed to receive and know. This seems to provide high level of security, because in practice two communication channels and two different devices are used – PC/Internet to access e-banking application, and mobile phone with SMS/USSD capabilities to receive one time passwords.

But what happens if the attacker is able to infect both PC and smartphone and redirect (forward) all SMS messages coming to user's mobile phone to mobile phone possessed by the attacker?

The answer is simple – all messages, including one time passwords will go to the attacker's phone. Thus, the attacker will be able to perform and confirm transactions in an unauthorized manner. Furthermore, depends on the mobile operating systems used and capabilities of mobile malware, the user may not even be aware of the messages being received and sent by smartphone. Not a single light will flash, not a single ringtone will ring and not a single vibration will happen. No signs will occur that would tell the user that something wrong is happening in the background.

Figure 3: Messages redirection attack

It must be also noticed that if the user uses only smartphone to access e-banking application and receive one time passwords, then PC infection is not needed in order to perform successful attack.

Remote GUI control

This is relatively a very simple attack to gain unauthorized access to software tokens as well as native and SIM card applications running on the smartphone. To perform this attack, the attacker needs to infect mobile phone with a malware capable of establishing remote desktop session with a phone, so the attacker can control GUI remotely. It must be noticed that such remote desktop software for majority of mobile operating systems is commercially available, so it may be only the matter of remotely installing, running and accessing it. Examples of such software include MyMobiler for Windows Mobile, Veency for iPhone, PDA Controller for Symbian, LogMeIn Rescue for BlackBerry, or Android VNC Server.

From this moment the attacker may easily run any software installed on the smartphone. The potential difficulties may occur when attacker is requested to enter information that is known only to the user (e.g. PIN, password) – but depends on availability of low-level APIs on particular smartphones, even such can be intercepted earlier by implementing key logging functionality similar to the one known from PC world, except that in the world of smartphones it will be rather "click" logging.

Figure 4: Remote GUI control

It must be noticed that the above methods of attacks are just examples, and in practice other methods may be used as well. Regardless of the method, however, companies need to be aware that using smartphone to assure strong authentication may not guarantee high level of security. In order to guarantee such, the one would need first to assure the device cannot be infected by malware so authentication information cannot be used in an unauthorized manner. Given complexity of current mobile operating systems, vulnerabilities in underlying technologies that are periodically discovered and published, and multiple possibilities of infection of mobile devices, this may be an impossible task to achieve in practice.

How smartphone can turn into zombi?

How smartphone can become infected by mobile malware? Analysis of behavior of mobile malware shows that multiple methods exist, and in addition there is a range of not yet used methods, but possible to be leveraged. Sample infection methods are presented below:

- Vulnerable and unpatched mobile operating system and/or mobile applications that would allow an attacker to remotely exploit known or just discovered (zero-day) vulnerability to run malicious code,
- Flawed mobile web browser, which – when tricking the user to visit malicious website – could cause that web browser will install and run attacker's executable code,
- Phishing (emails, WAP Push, SMS/MMS, Service Indication messages) – such attacks are mostly aimed to trick users to install the attachment or click on the URL link, which may contain malicious code,
- Synchronization with infected PC – in this case malware consists of the malicious code for both PC and smartphones. In the first step PC needs to be infected, which will wait for synchronization with a smartphone. Once the smartphone is connected to the PC, it will be automatically infected. This method is being used for example by Cxover worm,
- Vulnerabilities in underlying wireless technologies (Bluetooth, Wi-Fi, GSM, NFC etc.) or the way the technologies are being handled by mobile operating system. Possible infection methods may also leverage potential vulnerabilities in processing SMS, EMS or MMS messages or exploit buffer overflow in one of Bluetooth protocol messages,
- Infected memory card inserted into the smartphone – a physical form of infection, where the malware is trying to propagate by automatic infection of memory cards,
- Infected mobile software – mostly by trojan horses that hide its presence within useful software. This method of infection may include propagation via peer-to-peer networks on regular PC environment, for example among games or ringtones,
- Social engineering – may be very effective especially in case of attacks coming from other infected smartphones of trusted persons.

How to prevent infection?

First of all, it must be emphasized that there are no silver bullets or solutions that will provide 100% protection against successful attacks. Even if security software vendors claim something opposite, we need to be aware that these are only marketing slogans. Every security specialist is aware that achieving 100% security is, like implementation of *perpetuum mobile*, virtually impossible. Besides, security covers not only technologies, but also processes and people. Each of them may turn to be the weakest link and either via technologies' weaknesses, social engineering or flawed processes, mobile malware may always have chance for successful infection. Hence users and organizations may only minimize the risk of successful break-in, but cannot eliminate the risk completely.

Below list provide few recommendations on what users can do to minimize the risk of successful infection:

1. Smartphones should be treated as computers, which means that the same care and security precautions used in case of PCs should be used in case of smartphones. For example, if we do not open e-mail attachments received from unknown sources on PC, we should not open such on smartphone, either.
2. Smartphones should be purchased from trusted and legal sources. "Occasions", especially with regard to the used smartphones should be treated with care. Does the one know what has actually happened to the phone before purchasing from a "strange" source?
3. If smartphone's operating system and mobile applications used by the user offer functionality of automatic update, such features should be definitely enabled. If not, then it is recommended for users to periodically check if such updates (especially security patches) are available and install them manually.
4. Unsolicited EMS, MMS and e-mail messages coming from unknown sources should not be opened. In case of USSD and SMSes the situation is different as majority of operating systems opens and displays them automatically. If we cannot change such default behavior, then this is the risk that we need to learn to live with.
5. Security software – if available for smartphone's operating system – should be used. Antivirus, antispam, antimalware and personal firewall software may help with protecting smartphone against a large number of known attacks. Very often such software offers also possibility of remotely wiping device's memory and storage, in case the device is lost or stolen.
6. If the phone is occasionally connected with the PC (to copy photos, videos, music or synchronize calendar, tasks etc.) then protecting PC against security threats is absolutely crucial as well. Otherwise there is a risk that the smartphone – sooner or later – may become infected from PC, as in case of Cxover worm.
7. Any wireless features of the phone – when not actively used – should be disabled. This is especially important in case of Bluetooth, Wi-Fi, Near Field Communication (NFC), Infrared or any other wireless connectivity. If user is not using smartphone to connect to the Internet – disabling the access to the Internet should be considered as well.

8. Care should be made when following URLs – especially shortcuts or tiny versions of URLs, when receiving such from untrusted sources.
9. Users should be careful when installing 3rd parties software. Needless to say, only digitally signed (with a valid certificate) software should be installed. This is especially true with untrusted mobile applications downloaded from the Internet, WAP portals or from peer-to-peer networks – such software may contain trojan horses or other malware. Notice that black hats may deliberately distribute ringtones and set of mobile apps in peer-to-peer networks for the purpose of malware distribution.
10. Encryption software may be considered but it is worth to emphasize that it will help mostly in cases where the devices is lost or stolen. In case of malware, encryption may not help much if malware is capable of intercepting PINs and cryptographic keys.
11. If mobile operator allows setting up upper financial limits for monthly bills, then such should be set so users will not be surprised to see $10,000 bill for unauthorized SMSes sent to premium-rate numbers. Furthermore, if users have no needs to send or call premium-rate numbers, we recommend blocking such possibility entirely.

In case of organizations and companies that use smartphones to increase mobility of their employees security policies should be updated and risks assessment should be made to consider treats related to the usage of smartphones. Clear procedures should be established especially on what to do when employee's mobile phone is lost or stolen. Software that would allow central management of employee's mobile devices should be considered to use – in particular for the purpose of installation of security updates, updating antiviruses' signatures, tracking inventory of software installed on phones, enforcing security policies and performing data backup. Security awareness should be built among users, so they should be aware how to avoid malware infections. If smartphones are used for authentication purposes, then such approach should be revised - as it has been already shown, once the phones are infected by malware, users' identities and credentials may be stolen.

In case of e-banking situation is different, as the risk of frauds is real, financial impact is potentially high, and there are no easy solutions that could eliminate the risks of performing unauthorized financial transactions – at least unless the way in which smartphones are used in e-banking is changed. Therefore we recommend financial institutions to start evaluating alternative and more secure methods of user and transaction authentication than relying on possible to infect mobile phones. Hence, when the banks are no longer able to accept the risk, they will be ready to switch to more secure methods of users' and transactions' authentication.

Summary

Permanent development of mobile technologies and in particular smartphones every day provides thousands of people around the world with new opportunities. From searching the Internet up to purchasing goods from almost any place on the world – smartphone's users can perform all of these activities in a truly mobile manner.

But new technology and new mobile devices brought new threats as well. Not only users may have valid reasons to worry about invasion of privacy in case of mobile malware infection, but such malware may expose users and companies to serious financial threats. What bill from mobile operator the user will see if malware was able to secretly send 10,000 SMSes to premium-rate numbers, each costs $5? Will the operator warn the user earlier? Whom operator will speak to if malware secretly forwards all calls to the attacker? How much money attackers will be able to transfer from users' bank accounts after intercepting both users' credentials and SMSes with one-time passwords? Will company's system let the user login, once he is able to use software token stolen from the smartphone? And last but not least – will the user trust the call coming from bank, while in reality the call is from the attacker and it is only displayed as such?

These questions and earlier examples show that mobile malware can be really dangerous. Although writing effective mobile malware does not belong to category of trivial tasks, the risk is real and no more theoretical – malware, commercially available software, or low level APIs that could enable attackers to implement all attacks described in this publication already exists. The same as security mechanisms of mobile operating systems, which – sometimes with a little help of social engineering – can unfortunately be circumvented as well.

Links and bibliography

1. "Mobile Application Security", 2010, by Himanshu Dwivedi, Chris Clark, David Thiel.
2. Mobile Malware Attacks and Defense, 2009, by Ken Dunham, Saeed Abu-Nimeh, Michael Becher, Seth Fogie, Brian Hernacki, Jose Andre Morales, Craig Wright.
3. Malware Goes Mobile, 2006, by Mikko Hypponen.
4. Kaspersky Lab, 2009, "Mobile Malware Evolution: An Overview, Part 3".
5. McAffee, Mobile Malware: Threats and Prevention, by Zhu Cheng.

Authors

Artur Maj

Co-founder, and Information Security Professional at Prevenity. He began professional career as a Security Engineer/Consultant in European Network Security Institute, most of his time spending on penetration testing, security monitoring and providing consulting services. From 2003 to 2007 he worked for Oracle Corporation, most of the time at the position of Principal Software Engineer in the Oracle EMEA Mobile & Wireless Center of Excellence, ultimately becoming the Technical Director and Business Development Manager of the Center. Besides security aspects, he was dealing with mobile and embedded technologies, service delivery platforms for mobile telecommunication operators and sensor-based solutions. From 2007 to 2009 he was working for Hewlett Packard, managing the team of 30+ specialists providing ITIL based services for HP's global customers. Author of many publications on security, especially on protecting information systems, published in Poland and internationally, for example at SecurityFocus.com. Author, co-author and trainer of multiple security trainings and workshops. Member of ISACA, ISSA and OWASP. Holder of MSc degree from Rzeszow University of Technology, CISSP and CISM certifications.

Marek Janiczek

Co-founder, and Information Security Professional at Prevenity. Prior to Prevenity, he worked as a Security Consultant for European Network Security Institute and Hewlett Packard. He was performing computer networks, systems and web applications security audits and tests, developing information security policies as well as analyzing and evaluating IT projects from the security point of view. He was also participating in complex implementation and integration projects, with high priority on security and availability. Author of many articles related to information security. Author, co-author and trainer of multiple security trainings. Member of ISACA, ISSA and OWASP. He holds MSc degree from Rzeszow University of Technology, CISSP, CISA, CISM, ISO 27001 Lead Auditor certifications.

About Prevenity

Prevenity is a company that provides highly specialized solutions and services in the area of information security:

- *Comprehensive, modern and effective solutions to ensure information security*
- *Implementation and consultancy services in the area of information security*
- *Professional training services in the field of information security*

The foundation of the company is multi-year, hands-on experience of its team members, gained during projects delivered for large Customers operating on Polish and international markets, and proven by internationally recognized certifications (CISSP, CISA, CISM, ISO 27001 LA, ITIL and other).

As a part of services and solutions portfolio in the mobile, wireless and embedded area we offer:

- *Security reviews, audits and penetration tests of mobile, wireless and embedded solutions*
- *Consulting services aimed to support customers with designing and developing highly secure mobile solutions*
- *Implementation and integration services aimed to apply adequate and effective security products and solutions*

Should you have any inquires about security of mobile, wireless and embedded solutions, please feel free to contact us.

More information about education, solutions and services portfolio can be found at www.prevenity.com.