SUBJECT FACILATOR; SANGRAM ROUTRAY (SOF)

CENTURION UNIVERSITY OF TECHNOLOGY & MANAGEMENT

Email - sangram.routray@cutm.ac.in

Physical Security

Mobile phones will get lost or stolen, period. Whether it is a personal handset or one issued by an employer, the fact that a mobile phone will eventually land in someone else's hands is a security issue.

The best-case scenario for a lost/stolen mobile device is a $200 or $300 loss of hardware, but the worst-case scenario is a goldmine of information sitting on the phone (usually in an e-mail inbox) falling into the wrong hands.

Furthermore, the fact a mobile device will be lost or stolen is simply one use case—what about the other use case where a user allows another person to borrow their mobile device for a quick phone call?

This quick handover equates to an anonymous third party being granted temporary access to a device that holds very sensitive data about the owner (or their employer). How long would it take to download malware on the phone?

Probably less time than to make a fake phone call. In the desktop and laptop world, physical security has always meant no security. The statement is even true to this day, where the latest versions of Microsoft's desktop operating system still seem vulnerable to the very old NT boot disk password-change attack, which requires physical access to change the admin
password.

Unix environments have had this issue as well, where a user can simply
boot into single-user mode and change the root password (which also requires physical access to the machine).

The fact that physical access to a device no longer means breaking into data centers or bypassing building security barriers is tough for the IT world because historically it's just a matter of time before someone is able to break through any physical security measures to access data on a disk (it should be noted that on some mobile devices it is the expandable memory slot, such as the Micro SD, that holds all the sensitive data).

The best solution for this problem is to design systems assuming physical access will be granted to entrusted parties, and not to assume that any physical security layer will stand the test of time. Unlike many other computing environments—from dedicated servers to cloud
Computing—physical security will be the number-one issue facing mobile devices.

Secure Data Storage (on Disk)

Securing data on disk relates closely to the previous issue, which is the physical loss of a mobile device.

As with laptops, the loss of a mobile device will be a non-issue if the data stored on that device is inaccessible to unauthorized parties.

In addition to sensitive documents, information on many mobile applications is stored locally, including password files and authentication tokens, which all need to be protected as
well.

The ability to store sensitive information locally in a secure manner, and also to keep it accessible to the applications that need it to function properly, is an important requirement for secure mobile computing.

Challenges of smart phone mobile security

Threats

A smart phone user is exposed to various threats when they use their phone. In just the last two-quarters of 2012, the number of unique mobile threats grew by 261%, according to ABI Research.These threats can disrupt the operation of the Smartphone, and transmit or modify user data. So applications must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc.).

There are three prime targets for attackers:

- Data: smart phones are devices for data management, and may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);
- Identity: smart phones are highly customizable, so the device or its contents can easily be associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract and an attacker may want to steal the identity of the owner of a Smartphone to commit other offenses;
- Availability: attacking a smart phone can limit access to it and deprive the owner of its use.

There are a number of threats to mobile devices, including annoyance, stealing money, invading privacy, propagation, and malicious tools.

- Botnets: attackers infect multiple machines with malware that victims generally acquire via e-mail attachments or from compromised applications or websites. The malware then gives hackers remote control of "zombie" devices, which can then be instructed to perform harmful acts.
- Malicious applications: hackers upload malicious programs or games to third-party smart phone application marketplaces. The programs steal personal information and open backdoor communication channels to install additional applications and cause other problems.
- Malicious links on social networks: an effective way to spread malware where hackers can place Trojans, spyware, and backdoors.
- Spyware: hackers use this to hijack phones, allowing them to hear calls, see text messages and e-mails as well as track someone's location through GPS updates.

The source of these attacks are the same actors found in the non-mobile computing space.

- Professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;
- Thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;

- Black hat hackers who specifically attack availability.Their goal is to develop viruses, and cause damage to the device. In some cases, hackers have an interest in stealing data on devices.
- Grey hat hackers who reveal vulnerabilities. Their goal is to expose vulnerabilities of the device. Grey hat hackers do not intend on damaging the device or stealing data

Consequences

When a smart phone is infected by an attacker, the attacker can attempt several things:

- The attacker can manipulate the smart phone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email
- The attacker can easily force the smart phone to make phone calls. For example, one can use the API (library that contains the basic functions not present in the smart phone) Phone Make Call by Microsoft, which collects telephone numbers from any source such as yellow pages, and then call them. But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smart phone. It is also very dangerous because the smart phone could call emergency services and thus disrupt those services;
- A compromised smart phone can record conversations between the user and others and send them to a third party.This can cause user privacy and industrial security problems;
- An attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smart phones can be used to place orders, view bank accounts or are used as an identity card;
- The attacker can reduce the utility of the smart phone, by discharging the battery. For example, they can launch an application that will run continuously on the smart phone processor, requiring a lot of energy and draining the battery. One factor that distinguishes mobile computing from traditional desktop PCs is their limited performance. Frank Stajano and Ross Anderson first described this form of attack, calling it an attack of "battery exhaustion" or "sleep deprivation torture";
- The attacker can prevent the operation and/or be starting of the smart phone by making it unusable.This attack can either delete the boot scripts, resulting in a phone without a functioning OS, or modify certain files to make it unusable (e.g. a script that launches at startup that forces the smart phone to restart) or even embed a startup application that would empty the battery;
- The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user.

Attacks based on communication

Attack based on SMS and MMS

Some attacks derive from flaws in the management of SMS and MMS.

Some mobile phone models have problems in managing binary SMS messages. It is possible, by sending an ill-formed block, to cause the phone to restart, leading to the denial of service attacks. If a user with a Siemens S55 received a text message

containing a Chinese character, it would lead to a denial of service. In another case, while the standard requires that the maximum size of a Nokia Mail address is 32 characters, some Nokia phones did not verify this standard, so if a user enters an email address over 32 characters, that leads to complete dysfunction of the e-mail handler and puts it out of commission. This attack is called "curse of silence". A study on the safety of the SMS infrastructure revealed that SMS messages sent from the Internet can be used to perform a distributed denial of service (DDoS) attack against the mobile telecommunications infrastructure of a big city. The attack exploits the delays in the delivery of messages to overload the network.

Another potential attack could begin with a phone that sends an MMS to other phones, with an attachment. This attachment is infected with a virus. Upon receipt of the MMS, the user can choose to open the attachment. If it is opened, the phone is infected, and the virus sends an MMS with an infected attachment to all the contacts in the address book. There is a real-world example of this attack: the virus Commwarrior uses the address book and sends MMS messages including an infected file to recipients. A user installs the software, as received via MMS message. Then, the virus began to send messages to recipients taken from the address book.

Attacks based on communication networks

Attacks based on the GSM networks

The attacker may try to break the encryption of the mobile network.
The GSM network encryption algorithms belong to the family of algorithms called A5.

Due to the policy of security through obscurity it has not been possible to openly test the robustness of these algorithms.

There were originally two variants of the algorithm: A5/1 and A5/2 (stream ciphers), where the former was designed to be relatively strong, and the latter was designed to be weak on purpose to allow easy cryptanalysis and eavesdropping.

ETSI forced some countries (typically outside Europe) to use A5/2. Since the encryption algorithm was made public, it was proved it was possible to break the encryption: A5/2 could be broken on the fly, and A5/1 in about 6 hours

In July 2007, the 3GPP approved a change request to prohibit the implementation of A5/2 in any new mobile phones, which means that it has been decommissioned and is no longer implemented in mobile phones.

Stronger public algorithms have been added to the GSM standard, the A5/3 and A5/4 (Block ciphers), otherwise known as KASUMI or UEA1-published by the ETSI.

If the network does not support A5/1, or any other A5 algorithm implemented by the phone, then the base station can specify A5/0 which is the null-algorithm, whereby the radio traffic is sent unencrypted.

Even in case mobile phones are able to use 3G or 4G which have much stronger encryption than 2G GSM, the base station can downgrade the radio communication to 2G GSM and specify A5/0 (no encryption)

This is the basis for eavesdropping attacks on mobile radio networks using a fake base station commonly called an IMSI catcher.

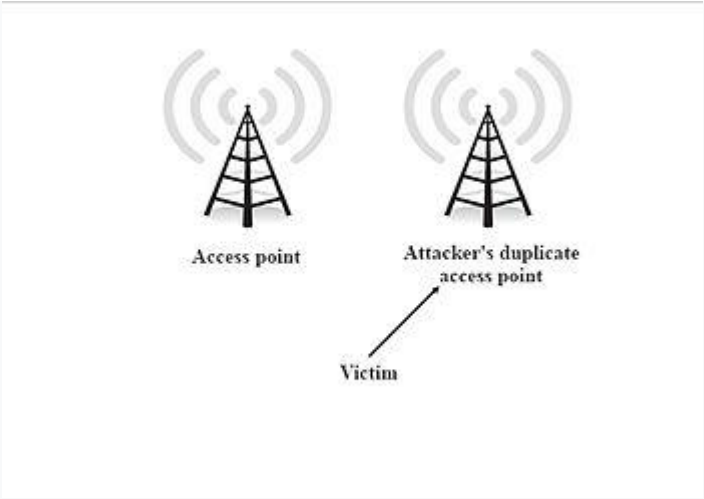
In addition, tracing of mobile terminals is difficult since each time the mobile terminal is accessing or being accessed by the network, a new temporary identity (TMSI) is allocated to the mobile terminal.

The TMSI is used as the identity of the mobile terminal the next time it accesses the network. The TMSI is sent to the mobile terminal in encrypted messages.

Once the encryption algorithm of GSM is broken, the attacker can intercept all unencrypted communications made by the victim's smart phone.

Attacks based on Wi-Fi

See also: Wi-Fi § Network security



Access Point spoofing

An attacker can try to eavesdrop on Wi-Fi communications to derive information (e.g. username, password).

This type of attack is not unique to smart phones, but they are very vulnerable to these attacks because very often the Wi-Fi is the only means of communication they have to access the internet.

The security of wireless networks (WLAN) is thus an important subject. Initially, wireless networks were secured by WEP keys.

The weakness of WEP is a short encryption key which is the same for all connected clients. In addition, several reductions in the search space of the keys have been found by researchers.

Now, most wireless networks are protected by the WPA security protocol. WPA is based on the "Temporal Key Integrity Protocol (TKIP)" which was designed to allow migration from WEP to WPA on the equipment already deployed.

The major improvements in security are the dynamic encryption keys. For small networks, the WPA is a "pre-shared key" which is based on a shared key.

Encryption can be vulnerable if the length of the shared key is short. With limited opportunities for input (i.e. only the numeric keypad), mobile phone users might define short encryption keys that contain only numbers.

This increases the likelihood that an attacker succeeds with a brute-force attack. The successor to WPA, called WPA2, is supposed to be safe enough to withstand a brute force attack.

As with GSM, if the attacker succeeds in breaking the identification key, it will be possible to attack not only the phone but also the entire network it is connected to.Many smart phones for wireless LANs remember they are already connected, and this mechanism prevents the user from having to re-identify with each connection.

However, an attacker could create a WIFI access point twin with the same parameters and characteristics as the real network.

Using the fact that some smart phones remember the networks, they could confuse the two networks and connect to the network of the attacker who can intercept data if it does not transmit its data in encrypted form.

lasco is a worm that initially infects a remote device using the SIS file format.

SIS file format (Software Installation Script) is a script file that can be executed by the system without user interaction.

The smart phone thus believes the file to come from a trusted source and downloads it, infecting the machine.

Principle of Bluetooth-based attacks
Main article: Bluetooth § Security

See also: Bluesnarfing and Blue bugging

Security issues related to Bluetooth on mobile devices have been studied and have shown numerous problems on different phones.

One easy to exploit vulnerability: unregistered services do not require authentication, and vulnerable applications have a virtual serial port used to control the phone.

An attacker only needed to connect to the port to take full control of the device. Another example: a phone must be within reach and Bluetooth in discovery mode.

The attacker sends a file via Bluetooth. If the recipient accepts, a virus is transmitted.

For example: Cabir is a worm that spreads via Bluetooth connection.[1] The worm searches for nearby phones with Bluetooth in discoverable mode and sends itself to the target device.

The user must accept the incoming file and install the program. After installing, the worm infects the machine.