telenor group

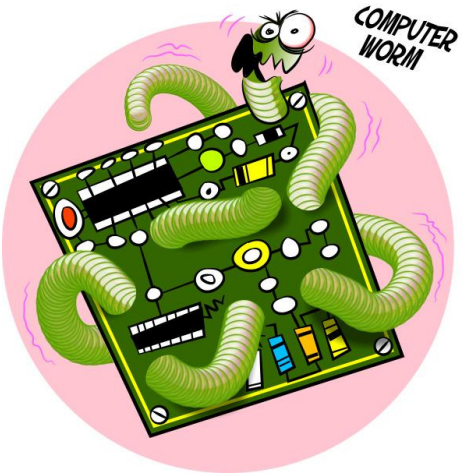
Mobile phone security

Prof. Do van Thanh

Introduction

- Why do we need mobile phone security?
- Is the mobile phone a secure device?
- The answer is: Yes, but only until recently
- Indeed malware starts to appear in the same pace as the popularity of the mobile phone increases
- On the other hand the awareness of the danger is still quite limited making the situation worse
- The goal of this talk is
  - To clarify the risks that the mobile phones are exposed to
  - To present the countermeasures

Malware on Mobile phones



Mobile phones considered as secured until lately:

- Nov 2009 Ikee, the first **worm** targeting jailbroken iPhone was discovered.
  - Not really malicious: all it did was replace the wall paper of the phone to a picture of the singer and internet meme Rick Astley
- A few weeks later, a truly malicious worm appeared which was designed to steal the user's online banking credentials
  - Targeting only jailbroken iPhones
- March 2010 3000 Vodafone's HTC Magic devices found to have the **Mariposa Botnet malware** installed via the phone's memory card
- June 2010 **Brute-force attack** on 100.000 iPad users who had their email addresses stolen via a vulnerability in a feature on AT&T Website.

telenor group

Malware on Mobile phones

- July 2010 Netquin, a mobile security company, claims 100 000 Symbian devices impacted by a Botnet virus that sent messages containing URLs linked to mailicious sites to all the contacts of the address book
- July 2010 LookOut Mobile Security's Apps Genome research finds that 14 percent and 8 percent of free apps available on iPhone and Android can access people's contact data.
- August 2010 on iPhone **malicious code can be hidden in fonts** that automatically load when the user opens a PDF file, allowing hackers to take control of the device
- Aug 2010 Kaspersky identified the first **Trojan horse** targeting Android devices that sends SMS to premium-rate numbers
- Multiple Android malware were discovered but relatively confined
  - Downloaded from 3rd party appstores and not Google's.

telenor group

Malware on Mobile phones

- Spring 2011 DroidDream appeared:
  - The **DroidDream Trojan** gained root access to Google Android mobile devices in order to access unique identification information for the phone.
  - Once compromised, a DroidDream-infected phone could also download additional malicious programs without the user's knowledge as well as open the phone up to control by hackers.
  - DroidDream affected mobile devices running v2.2 (FroYo) and earlier versions of the Android OS operating system
  - Entered phones through the download and installation of one of 50+ third-party applications that were available on Google's official Android Market.

telenor group

Malware on Mobile phones

- Google removed the apps from its marketplace
- Had to utilize its "kill switch" to remotely wipe Android devices that had been infected by DroidDream.
- DroidDream got its name from the fact that
  - it was set up to run between the hours of 11pm and 8am
  - when users were most likely to be sleeping and their phones less likely to be in use.
- Additional variants of DroidDream have since appeared
  - DroidDream Light in June 2011
  - A variant of DroidDream Light that appeared a month later.

Why targeting mobile phones?

- Smartphones and tablets are quickly becoming the **primary computing devices** for many users.
- The landscape for security tools **is not as mature** or sophisticated as it is for PCs
- Many users **aren't even aware of the security risks** with mobile devices--making them fairly easy targets in many cases.
- **Quite lucrative** - Open up money-making options that simply do not exist on the desktop.
  - Examples: malware applications that send text messages to premium numbers opened up by the attacker – raking in a small profit from each infected device.

telenor group

Mobile phone's risks
Risks as a phone

- **Abuse of subscription (Diallerware attacks)**: make call, send message to premium numbers or SMS services
  - From the phone itself
  - From other phones by cloning subscription (More difficult with new SIM authentication algorithm)
  - Read SMS
  - Check call details
- **Monitoring of phone conversations**
  - The mobile phone is bugged/tapped

telenor group

Mobile phone's risks
Risks as a phone

- **Disclosure of voicemail**:
  - Many users may not set or change the default PIN (1234 or 0000) – The trick is to call the voicemail number and enter the PIN to retrieve the voicemails.
- **Impersonation**: cloning or using phone number to make calls.
- **Monitoring of conversations in the vinicity**: the mobile phone being turned to a microphone
  - Activating camera to take pictures
  - Report position of the owner

Mobile phone's risks
Risks as a phone

- **Surveillance attacks:**
  - Smartphones can be used to keep a targeted individual under surveillance
  - Smartphones contain multiple sensors such as a microphone, camera, accelerometer and GPS.
  - Combined with the possibility of installing third-party software and the fact that a smartphone is closely associated with an individual, makes it a useful spying tool.

telenor group

Mobile phone's risks
Risks as a mobile device

- **Risk of being stolen or lost**
  - Being both valuable and mobile the mobile phone is likely to be stolen or lost anytime and anywhere
  - Is exposed to attacks anytime anywhere by anyone
    - Its subscription could be abused i.e. make phone calls, send messages, etc.
    - Its contents i.e. messages, pictures, contact list, etc could be extracted

telenor group

Mobile phone's risks
Risks as a storage device

- Smartphones contain often valuable information such as:
  - Credit card data
  - Bank account numbers
  - Passwords
  - Contact data
  - Corporate emails
  - Documents
  - Sensitive data
- **Data leakage resulting from device loss or theft**
  - If data on the smartphone memory or its removable media is not sufficiently protected (by encryption) then an attacker can access that data.

telenor group

Mobile phone's risks
Risks as a storage device

- **Attacks on decommissioned smartphones**
  - According to market analysts, by 2012 over 100 million mobile phones will be recycled for reuse each year.
    - As previously mentioned, smartphones contain large amounts of sensitive information which may be valuable to an attacker.
    - In a recent study, mobile phones were bought second-hand on eBay
      - Out of the 26 business smartphones
      - 4 contained information from which the owner could be identified
      - While 7 contained enough data to identify the owner's employer.
      - The research team managed to trace one smartphone to a senior sales director of a corporation, recovering call history, address book entries, diary, emails, etc.
    - They are an increasingly attractive target for 'smartphone dumpster divers'

telenor group

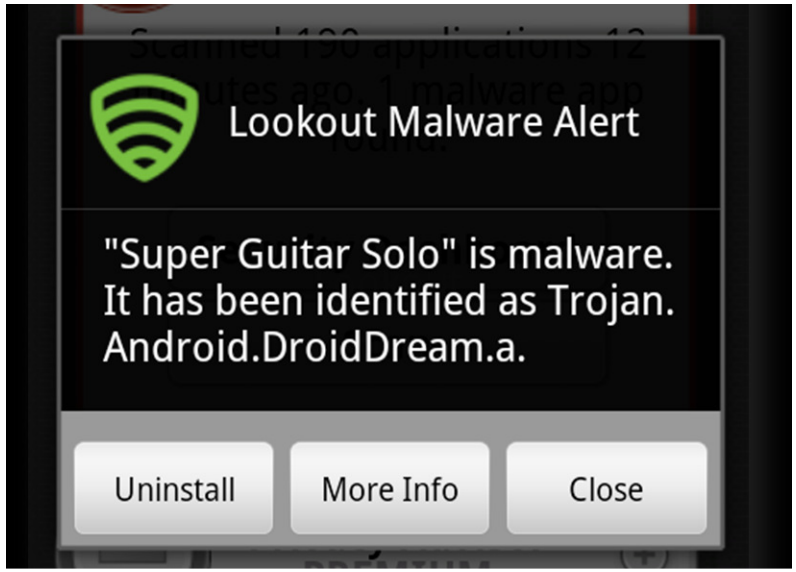
Mobile phone's risks
Risks as a computer

- **Mobile phone hacking by cybercriminals**
  - Malware:
    - Short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software.
    - 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software
    - Include viruses, worms, spyware, keyloggers
    - Can be installed through a message or an email
  - Unlike the draconian rules for the Apple App Store, and the tightly-controlled user experience of iOS,
    - Android is an open source platform with much more lenient access to the Android Market.
    - That freedom can also be exploited, though, to slip malicious apps into the mainstream.

telenor group

Mobile phone's risks
Risks as a computer

- **Unintentional disclosure of data**
  - Most apps have privacy settings for controlling how and when location data is transmitted
  - But many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this.
  - Unintentional disclosure of location data may help attackers to track and trace users and so allow, for example, stalking, robbery or the hijacking of trucks containing valuable goods.



telenor group

Mobile phone's risks
Risks as a computer

- **Spyware attacks**
  - Malicious software that
    - Covertly collects information about users and their activities
    - To use it for marketing purposes, such as profiling or targeted advertisements.
    - Often apparently bona fide software,
    - Installed with the user's consent
    - Which requests and abuses privileges over and above those required for the stated purpose of the app.

telenor group

Mobile phone's risks
Risks as a computer

- **Financial malware attacks**
  - The smartphone is infected with malware specifically designed for stealing
    - credit card numbers
    - online banking credentials
    - subverting online banking or ecommerce transactions.
  - May be simply a key-logger collecting credit card numbers
  - Or more sophisticated and intercept SMS authentication codes to attack online banking applications.
  - Another strategy is for an attacker to submit an app to an app-store, impersonating a real banking app.
    - If users download and use the app, the attacker can mount a man-in-the-middle attack on banking transactions.

telenor group

Mobile phone's risks
Risks as a networked device

- **Phishing attacks**
  - Connected to the Internet the smartphone is exposed to attacks in the same way any PCs.
  - Phishing: Act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication
  - Actually platform independent, because the attacker does not need to attack the user's device in any way

telenor group

Mobile phone's risks
Risks as a networked device

- The risk of phishing is important for smartphone users because:
  - Smartphones have a smaller screen, which means that attackers can more easily disguise trust cues that users rely on to decide on submitting credentials; e.g. cues that show whether the website uses SSL.
  - App-stores provide a new way of phishing by allowing attackers to place fake apps in the app-store, disguising them as legitimate apps (such as in the 09Droid case)
  - Smartphones provide additional channels that can be used for phishing, e.g. SMS (SMiShing). Users may be less cautious about SMS phishing messages.
  - Smartphones are a new type of device and users may not be aware of the fact that phishing is a risk on smartphones as well.

Mobile phone's risks
Risks as a networked device

- **Network Spoofing Attacks**
  - **Rogue WiFi hotspots and Bluetooth devices** can be used to intercept and tamper with the network communication to the smartphone.
  - Rogue Internet gateway names may be configured on the smartphone by a malicious SMS configuration message. In this attack, a spoofed service configuration **SMS is used to change the default access point** used by the phone
  - A more complicated spoofing attack relies **on mounting a rogue GSM base station**. The hardware required to set up such a base station has become relatively inexpensive. This attack is not feasible on 3G networks because of network integrity keys.

telenor group

Mobile phone's risks
Risks as a networked device

- **Network Spoofing Attacks**
  - A rogue WiFi hotspot or other spoofed network nodes can be used as a means to carry out several other attacks, e.g. phishing, SSL downgrade attacks, eavesdropping, etc (making it less likely using 3G networks)
  - Theoretically speaking, such attacks should be detectable by the user.
  - However, in practice most users **do not pay attention to trust cues such as SSL certificates or whether a site uses SSL4**.
  - For smartphone users the risk is even higher because **security indicators (such as a 'trusted SSL connection' indicator) are harder to find or missing on smartphones**.

telenor group

Mobile phone's risks
Risks as a networked device

- **Network congestion**
  - As a network device smartphones can be used to provoke network congestion in two ways:
    - **Signalling overload**: always-on smartphone apps are constantly polling the network for updated information.
      - For every bit of data sent, a large number of signalling messages are sent (e.g. keep-alive messages). A typical smartphone generates 8 times more signalling traffic than a laptop with a USB dongle
    - **Data capacity overload:** Cisco estimates that mobile data traffic will double every year through 2014, increasing 39 times between 2009 and 2014 (33).
      - Mobile data traffic will grow at a compound annual growth rate of 108 percent between 2009 and 2014, reaching 3.6 million terabytes per month by 2014
  - An attack mobilizing a large number of mobile phone can make the mobile network collapse.

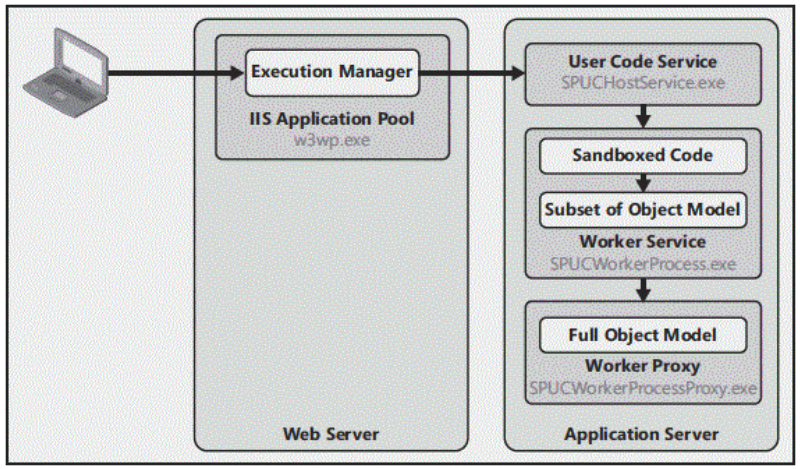
telenor group

Mobile phone's risks
Risks as a networked device

- **Distributed malware attack**
  - Although not yet targeted
  - Smartphones could be used to launch distributed attacks, just as traditional PCs are now used as parts of larger botnets.
  - Smartphone botnets could be used for familiar crimes such as **spam, click fraud and DDoS**.
  - Since smartphones interface with cellular networks, they could also be used for new distributed attack scenarios e.g.
    - **SMS spam** and **DDoS on telephony networks**.
    - Mobile phone coverage is becoming increasingly vital, especially in the event of an emergency, so smartphones open up new possibilities for DDoS attacks with potentially serious impacts.

telenor group

Security measures
Sandboxing and capabilities



- **Sandboxing** is a security mechanism for separating running applications by default.
- Some smartphone vendors use sandboxes for third-party software.
- This is an opportunity from a security point of view because, if correctly implemented, an application in a sandbox cannot access or manipulate the data or functions of other applications for malicious purposes.
- Moreover smartphone operating systems are often based on a **capability-based access control model**.
  - In this model, individual processes are granted separate privileges (called capabilities) which are limited by default, following the principle of least privilege.

telenor group

Security measures
Controlled software distribution

- ‘drive-by download’ attacks
- App-store owners have the opportunity to adopt the ‘walled garden’ approach:
  - To perform a security review of apps before admitting them to the app-store
  - And to remove apps from circulation which are subsequently shown to have security flaws.
  - This makes it more difficult for cyber attackers to spread malware
- Questions have been raised: Can the app-store owner be the independent and expert judge as to decide the admission or removal of an app.
  - If not properly implemented, this may actually be detrimental to security by fostering a misplaced sense of trust in app security

telenor group

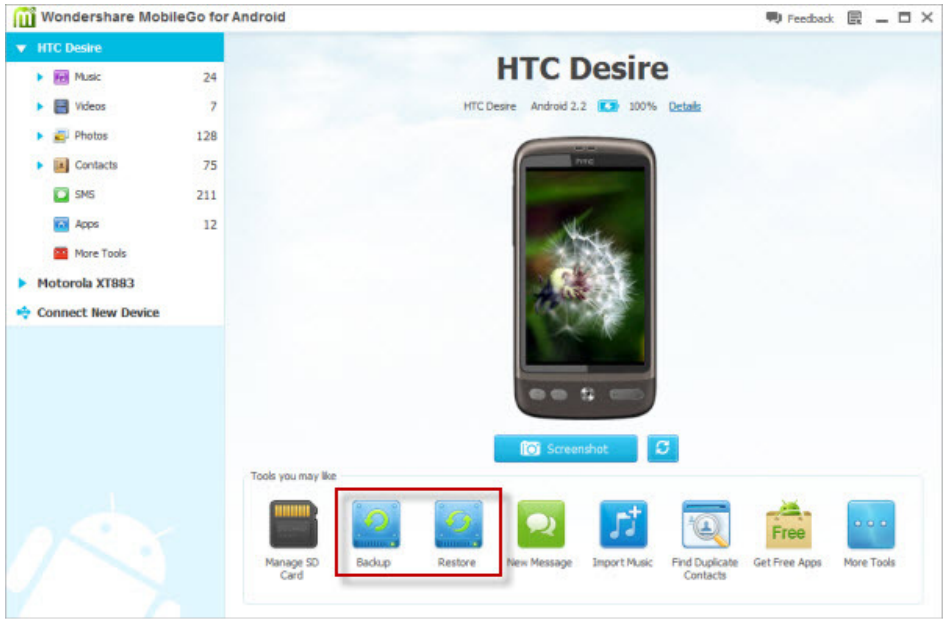
Security measures
Remote application removal

- Some smartphone platforms have a **built-in remote application removal function** which allows the removal of malware from devices after installation
- Sometimes referred to as a '**remote kill-switch**'
- Remote application removal has, however, raised some objections, mainly related to privacy and unfair censorship
  - In general, the public perception appears to be *very sensitive* towards any mechanism seen to invade the user's device even if used exclusively for his or her benefit.
- The judgment about whether a particular app is malicious may *not be clear-cut*
  - there is the potential for 'false positives' that result in the removal of apps that were not acting maliciously
- If not securely implemented, it could be abused by attackers, and be used in a denial of service attack or commercial sabotage.

telenor group

Security measures
Better backup and recovery

- Some smartphones ship with convenient **backup and recovery functions** to address the risk to data availability of failure, loss, or theft
- Can even be located remotely via the network
  - allowing the user to recover a lost device more easily.
- Additionally, some smartphones can be disabled and wiped remotely (and data may be easily recovered by the owner)



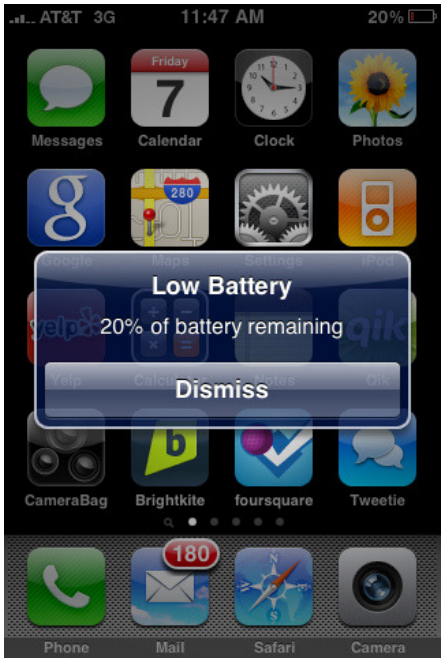
Security measures
Extra authentication and non-repudiation options

Smartphones can be used to improve the process of online authentication and provide a mechanism for non-repudiation

- The SIM card used in smartphones is a smartcard
  - With the appropriate software, licences and certificates in place, can be used for PKI-based authentication and digital signatures such as BankID
- May also take advantage of the current GSM authentication using the secret key stored in the SIM
  - SIM strong authentication
  - 3GPP standard Generic Bootstrapping Architecture (GBA)
- May also be used to create one-time-password codes without using SMS or network connections

Signs the mobile phone may be tapped

- Battery drain
- Display turned on without intervention
- Mobile phone got warm
- Mobile phone became slow
- High phone bills
- High datatraffic
- Unknown call numbers and SMS logs
- Incoming calls went directly to voicemail
- Error messages
- Strange text message
- Other knows your plan even you keep secret



telenor group

Advices to secure your mobile phone

- **Watch** your mobile phone
- **Lock** mobile with password/PIN
- **Update** phone regularly – carry backup
- Avoid jailbreaking/rooting
- **Be critical** when downloading and installing apps
- Be critical which Web sites you visit
- Do not open attachment from unknown senders
- Be critical what information you store on your phone – Is it critical if somebody got it
- Install **antivirus software**
- Use an **on-device personal firewall**
- Install **Remote device lock & wipe**

Advices for enterprises

- Employ **on-device anti-malware** to protect against malicious applications, spyware, infected SD cards and malware-based attacks against the mobile device
- Use **SSL VPN clients** to protect data in transit and ensure appropriate network authentication and access rights
- Centralize locate and **remote lock, wipe, backup and restore facilities** for lost and stolen devices
- Strongly **enforce security policies**, such as mandating the use of strong PINs/passcodes
- Leverage tools to help **monitor device activity** for data leakage and inappropriate use
- **Centralize mobile device administration** to enforce and report on security policies

telenor group

To conclude

- The situation is not that bad
- No need to panic!
- Just need to be aware about the threats
- And to take the right precautions

THANK YOU!