CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

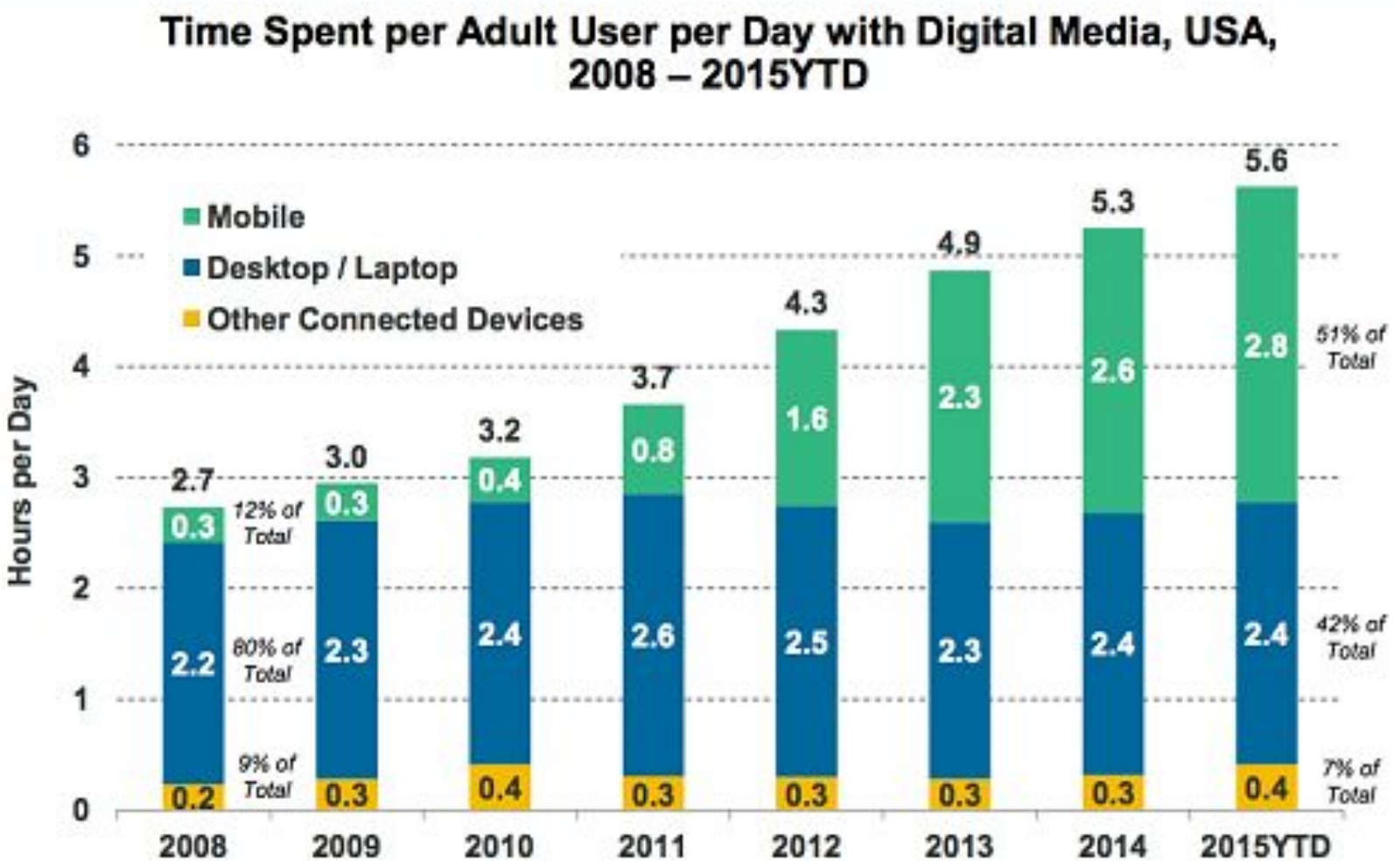
Lecture 10: Bring Your Own Device (BYOD) Security

Overview

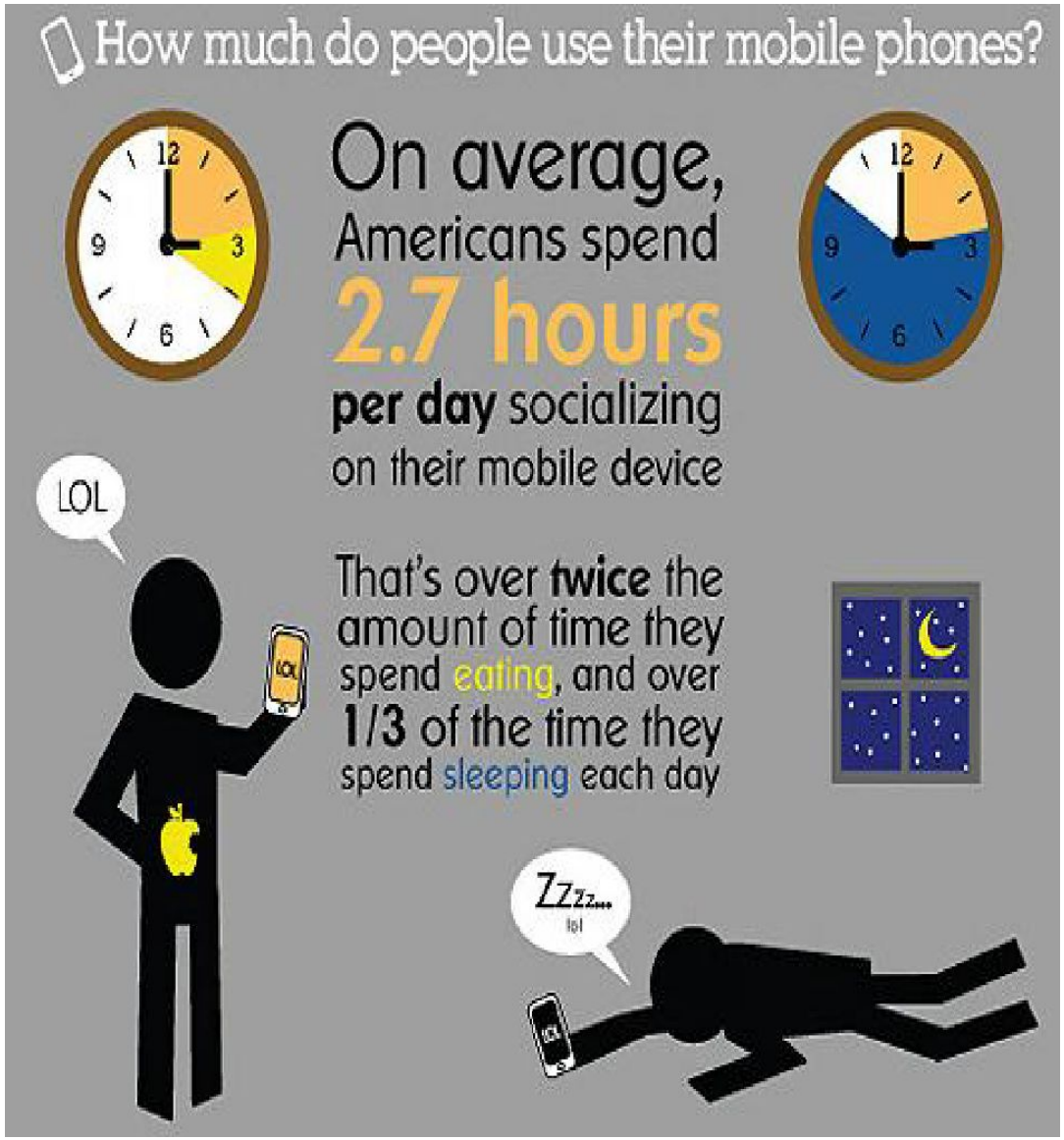
- Different Types of Mobile Devices
- Issues with mobile devices
  - Malware
  - Stolen/Lost
- Techniques for protecting your mobile device

Mobile Internet Usage is Growing

- 71% of Irish people own a smart phone



Mobile Internet Usage is Growing



Smart Phone Operating Systems

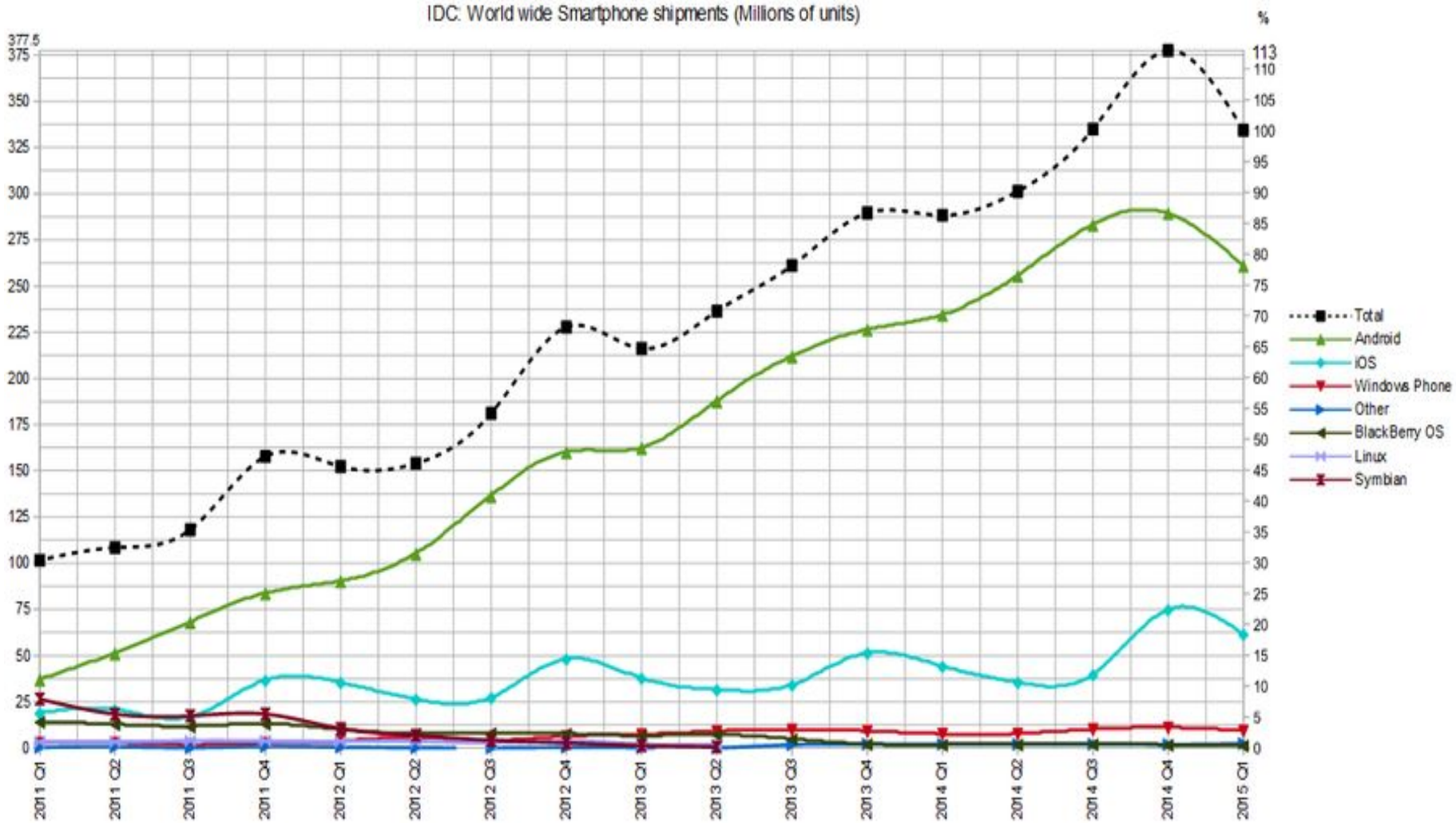
Top Five Smart Phone Operating Systems 2013

Ranking	Manufacturer	Resource: Gartner
1	Android	78.4%
2	iOS	15.6%
3	Blackberry	1.9%
4	Windows Phone/Mobile	3.2%
5	Other	0.9%

Operating System	1Q17 Units	1Q17 Market Share (%)	1Q16 Units	1Q16 Market Share (%)
Android	327,163.6	86.1	292,746.9	84.1
iOS	51,992.5	13.7	51,629.5	14.8
Other OS	821.2	0.2	3,847.8	1.1
Total	**379,977.3**	**100.0**	**348,224.2**	**100.0**

Source: Gartner (May 2017)

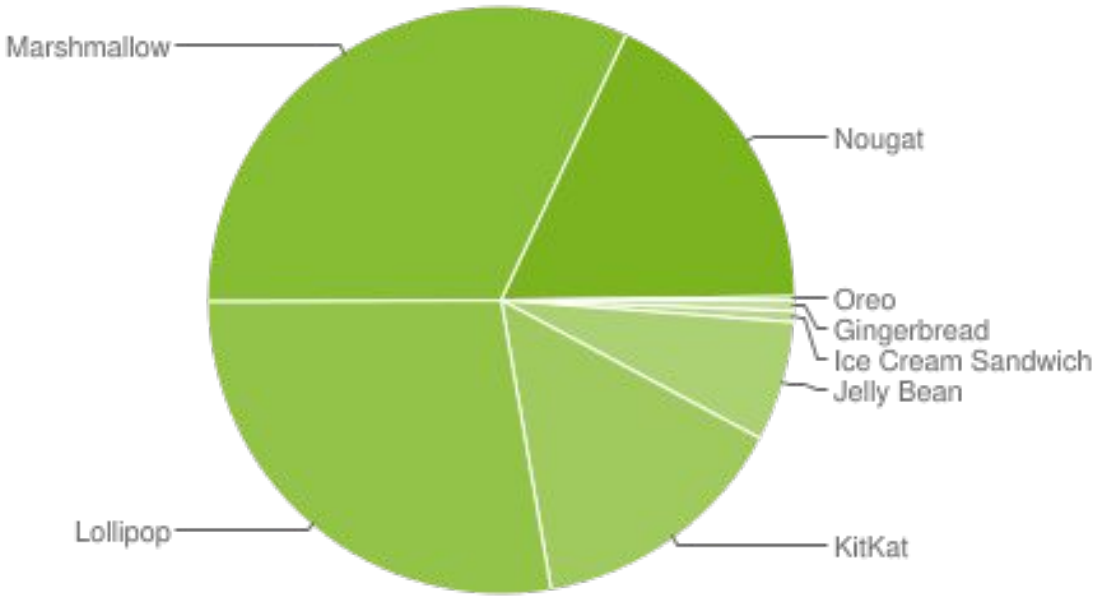
Smart Phone Operating Systems



Mobile Operating Systems - Android

- Different releases

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.6%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.6%
4.1.x	Jelly Bean	16	2.3%
4.2.x		17	3.3%
4.3		18	1.0%
4.4	KitKat	19	14.5%
5.0	Lollipop	21	6.7%
5.1		22	21.0%
6.0	Marshmallow	23	32.0%
7.0	Nougat	24	15.8%
7.1		25	2.0%
8.0	Oreo	26	0.2%



Issues with Android

- No Updates
  - Out of all the Android phones and tablets, just under **0.2% are running the latest version (Oreo 2017)** of Google's operating system.
  - More than 60% of users running a version of the OS which came out 2014 and 2015.
  - When you purchase an android mobile, it has an old version of the operating system which you are not prompted to upgrade.
  - The upgrades are normally left to the manufacturers of the devices and they **do not upgrade until a new version of the phone is available**.
  - No updates leaves these devices open to all sorts of malware.

Issues with Android

- Downloading Applications
  - Numerous places to get your android app
  - Android Marketplace (Google Play Store) has now implemented an additional layer of security called **Bouncer** which they say has seen a **drop in malicious apps by 40%.** This layer can be circumvented as shown by researchers recently.
  - Google Play Store has also introduced an App call **Google Play Protector** that runs a check on app download to identify malware. It also scans your phone for malicious apps.

Issues with Android

- Application Permissions
  - Every app declares its permissions when you install it.
  - **If it doesn't request permissions** — you can't actually control these permissions.
  - The app tells you what it requires, and you can take it or leave it.
  - Android apps must declare permissions for nearly everything, from Internet access and writing to the SD card to monitoring your location and sending SMS messages.
  - For many users, permissions have unfortunately become like a EULA – something to quickly tap through when installing apps.

Issues with Android

- Application Permissions
  - This isn't helped by the way permissions are presented, placing everything from accessing the Internet to sending premium-rate SMS messages in the same list.
  - **Whenever you see an app that requires manual updates, it's because the app requires additional permissions**. Usually, the app's developers added a new feature that requires a new permission.
  - Most users will tap through the message without examining the new permission.
  - If you wish to view your apps permissions then use something like Avast! Mobile Security.

Mobile Operating Systems - iPhone

- iOS
  - Releases
    - 1st gen: 2007
    - 3G
    - 3GS
    - 4
    - 4S
    - 5
    - 6
    - 7
    - 8
    - 9
    - 10
    - 11 (Latest: Oct. 2017)

Issues with Apple iOS

- Jailbreaking
  - iPhones are easily jailbroken which **leaves them open to malware** due to the fact that apps from other places can be downloaded to the phone.
- Privacy
  - Your iPhone keeps track of where you go – and saves **every detail** of it to a secret file on the device which is then copied to the owner's computer when the two are synchronised.
  - The file contains the latitude and longitude of the phone's recorded coordinates along with a timestamp, meaning that anyone who stole the phone or the computer could discover details about the owner's movements using a simple program.

Mobile Malware - Botnets

- **Foncy**: (Jan 2012)
  - IRC bot for Android that worked together with an SMS Trojan
  - The dropper also contained a root exploit.
  - After launching the exploit on an infected system, it would increase privileges up to root level, and then launch the IRC bot, which would then install and launch the SMS Trojan.
  - The SMS Trojan, once it had performed its function, would stop running, while the IRC bot would continue to run, waiting for commands.
  - As a result, the IRC bot was capable of controlling the smartphone post-infection.
  - The Foncy IRC bot comprised of a fully-fledged botnet and could have been used to execute just about any actions at the command of the botnet owner.

Mobile Malware - Botnets

- **MDK Botnet** (Jan 2013)
  - 11,000 malicious apps discovered.
  - Over 1 million users infected.
  - Uses an Advanced Encryption Standard (AES) algorithm to encrypt data, like servers and commands, in a file.
  - Once installed, the Trojan enables the attacker to remotely control users' devices, consequently allowing the attacker to harvest user data, download additional APKs, and generate nuisance adware.
  - The Trojan has been repackaged into legitimate apps, including popular games such as Temple Run and Fishing Joy, to lull users into installing the malware.
  - The Trojan also uses dynamic loading, data encryption, and code obfuscation to evade detection.

Mobile Malware – mTans

- **CitMo Trojan**
  - Changed the landing page of a Russian bank's online banking system.
  - Users were asked to download and install a program allegedly required to enter the system.
  - Users could opt to receive a link to the program by text message, either by providing their phone number in advance, or by scanning a QR code.
  - The link in this example led to the AberSafe application, which was actually Trojan-Spy.AndroidOS.Citmo, and was in the Google Play app store within two weeks.

Mobile Malware – mTans

- **CitMo Trojan**
  - After launching the malicious program, potential victims would be asked to enter their telephone numbers.
  - The numbers would be recorded in an auth.txt file and sent to a remote server run by the malicious users.
  - After a while, the users would receive a text message with a five-figure code meant to be entered in the application.
  - This code was written into an authcode.txt file and used with the telephone number as data ID which the malware would then send to the remote server.
  - It forwards data to the remote, as well as data on numbers associated with incoming texts that did not need to be hidden.

Mobile Malware –SMS Trojans

- How do SMS Trojans work?
  - SMS Trojans **cannot propagate by themselves** so attackers need to hide the malicious code inside other applications such as video games or known applications.
  - Once the users are tricked into downloading and installing the infected app, their mobile phones are infected.
  - When the user executes the infected app, an SMS is sent to a premium-rate number, activating a subscription for which the user will be charged.
  - The subscribed user receives SMS messages with content such as jokes or any other kind of data that can be sent through SMS. Every such message they receive will cost them a few dollars.

Mobile Malware –SMS Trojans

- Boxer Trojan (2011/2012)
  - *Android/TrojanSMS.Boxer.AA*, a malicious program for Google's Android mobile Operating System.
  - Targets 63 different countries
  - reads the **MCC (Mobile Country Code)** and **MNC (Mobile Network Code)** codes from the infected device.
  - Once Boxer knows the country and mobile carrier to which the infected phone belongs, it will try to match it with the information stored inside the program and send an SMS to the 'appropriate' premium-rate service number to which to subscribe the victim.
  - In December 2011, 22 malicious apps were discovered in the Android Market that were able to reach users in all of these countries.

Mobile Malware – App Stores

- **Dougalek** (Primarily Japan 2012)
  - Dougalek is a mobile malware that runs on Android devices.
  - It downloads and plays movie clips from a predetermined remote website while stealing information in the background.
  - The mobile malware requests the following permissions:
    - INTERNET - Allows applications to open network sockets.
    - READ_CONTACTS - Allows an application to read the user's contacts data.
    - READ_PHONE_STATE - Allows read only access to phone state.
  - Upon execution, Dougalek collects information from the compromised Android device and sends the stolen information to a remote server.

Mobile Malware – App Stores

- **Find and Call iPhone App**
  - Made by a Russian firm, claims to be an app that lets you make phone calls by simply typing in or clicking a contact's email address or social-network handle.
  - Once this application was downloaded and launched, the user would see a request to register the program, which required entering an email and phone number.
  - If, after doing so, the user tried to find friends in his contacts using this app, then all of his contacts would be uploaded to a remote server — without the user suspecting a thing.
  - Each number stolen from contacts would then receive a spam text message with a link suggesting the recipient download the Find and Call app.

Mobile Malware – Cyber Espionage

- **FinSpy**
  - Developed by the British firm Gamma International.
  - Features include:
    - logging incoming and outgoing calls;
    - concealed calls to eavesdrop on the target's surroundings;
    - stealing information from smartphones (call logs, text and media messages, contacts, etc.);
    - coordinate tracking;
    - Internet and text message communication with the command centre.

Mobile Malware - Cyber Espionage

- **Red October**
  - Uses a number of security vulnerabilities in MS Excel, Word, PDF documents types and web-based Java exploits to infect PCs, smartphones, and computer networking equipment.
  - The attacks are on-going and targeted at high-level institutions in what are known as spear-phishing attacks.
  - Infections were discovered in more than 300 countries between 2011 and 2012.
  - It can steal data, acquire network configuration information from Cisco-branded equipment, and grab files from removable disk drives including deleted data.
  - It can also steal e-mail messages and attachments, record all keystrokes of an infected machine, take screenshots, and grab browsing history and replicate itself across the network.

Securing your Mobile

1) Use Password Protected Access Controls
2) Control Wireless Network & Service Connectivity
3) Control Application Access & Permissions
4) Keep your OS and Firmware Current
5) Backup your Data
6) Wipe Data Automatically if Lost or Stolen
7) Never Store Personal Financial Data on your Device
8) Beware of Free Apps
9) Try Mobile Anti-virus Software or Scanning Tools
10) Use Mobile Device Management Software

Securing your Mobile

- **Use Password Protected Access Controls**
  - All mobile devices come with the ability to set a lock requiring a passcode or pattern for access.
  - It may take you a couple extra seconds to unlock your smartphone before using it, but it could take a thief a very long time to figure out your PIN.
  - Phones that aren't locked lay bare a treasure trove of personal information – email, contacts, addresses and access to social networks and apps that may contain financial data.
  - Try to pick an association that only you would know, and that won't be personally identifiable with you.

Securing your Mobile

- **Use Password Protected Access Controls**
  - Grid-based **pattern locks** work fine, but they leave smudge marks on the touchscreen that may be easier to guess than passwords.
  - Some devices are rolling out **facial recognition** as an access mechanism, but this technology isn't perfected yet.
  - Newer phones now offer full **device encryption** for the file system itself.
  - Apple's is built in, but Android requires users to enter yet another passcode which, if forgotten, can accidentally wipe all your data.

Securing your Mobile

- **Use Password Protected Access Controls**
  - Many tablets also provide locking mechanisms for USB file sharing (such as syncing files with a PC), so set those PINs as well so a stranger can't just walk up and plug in.
  - And remember that encrypted data on your mobile device may no longer be encrypted when transferred to your PC.
  - Refer to your user manual, or start by looking in the general settings to locate screen and key lock functions.

Securing your Mobile

- **Control Wireless Network & Service Connectivity**
  - Your mobile device is primarily a communications tool.
  - It connects you to all of the information you can ask for.
  - But did you know that your smartphone's default settings may be connecting to nearby Wi-Fi networks automatically? Especially if you've asked it to download new email as it arrives.
  - Some of these networks, like in airports or neighbourhood coffee shops, may be completely open and insecure.
  - **Turn Wi-Fi off completely** and turn it on only when you need it, which will also save your battery power.

Securing your Mobile

- **Control Wireless Network & Service Connectivity**
  - It's safest to set your phone to automatically connect only to your trusted networks, and to ask you before connecting to any other network it finds.
  - If your phone has **Bluetooth support, it's also best to select this feature manually as well**. Nearby attackers could potentially exploit Bluetooth to access data on your phone.
  - Bluetooth settings work like Wi-Fi on most phones – it can be either on or off, so we recommend making your smartphone discoverable to other Bluetooth only when necessary.

Securing your Mobile

- **Control Application Access & Permissions**
  - Apps are wonderful things, but many of them store sensitive data that must be protected.
  - Android users can take advantage of their mobile phones' multitasking capability by employing a special access control app. Most will start up when your smartphone boots and run in the background.
  - These apps further restrict a thief or hacker's access to your device.

Securing your Mobile

- **Control Application Access & Permissions**
  - More important than controlling app access is policing app permissions.
  - Most of today's apps require a network connection to operate.
  - They may store data in the cloud, constantly track your location, or push updates to your smartphone.
  - Get to know the permission settings of each app or service and what data or systems they access.

Securing your Mobile

- **Control Application Access & Permissions**
  - You may be permitting services to access your phone without prior approval, or your apps may be pushing alerts and updates when you aren't specifically requesting them.
  - You can restrict all notifications at once by looking under your device's settings.
  - On many devices you can turn off location based services entirely as well, so your phone isn't constantly broadcasting your GPS location, no matter which apps request it.

Securing your Mobile

- **Keep Your OS & Firmware Current**
  - Your device has an operating system that runs all of its apps and services, as well as firmware which runs the device hardware itself.
  - It's definitely important that you routinely accept the major updates from Apple, Google, or whoever the manufacturer is.
  - Equipment does "age out", rendering older devices unable to run the latest OS version.
  - Unfortunately, there is a huge population of Android users currently using out-dated firmware and OS versions that can't be updated due to hardware incompatibility.
  - Take advantage of the chance to upgrade your device whenever you can.

Securing your Mobile

- **Back Up Your Data**
  - It's amazing that this far into the personal computing age, most users still don't copy their critical info to ease data recovery in case of theft or loss.
  - Start to think of your phone like you do your PC or laptop.
  - Maybe you back up your computer data locally, or use a company approved cloud-based backup service? That's great.
  - Why wouldn't you want to protect your phone as well? Take the time to sync all of your apps and data – not just your email and calendar – just in case your phone becomes lost, stolen or corrupted.

Securing your Mobile

- **Wipe Data Automatically if Lost or Stolen**
  - It's a good idea to enrol your smartphone in a **"find my phone" service** that will help you locate your device should it be lost or stolen.
  - These services typically have the ability to wipe your phone, which means remotely erase all data and completely disable the device should it fall into the wrong hands.
  - On some devices you can add extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of times because brute forcing will get the password in the end.
  - Finally, this may be obvious, but many people don't even think about removing sensitive data before selling their smartphone or sending it in for repairs.

Securing your Mobile

- **Never Store Personal Financial Data on Your Device**
  - Never store personally identifiable information such as such as PPS number, credit card numbers, or bank account numbers on your smartphone, especially in text messages.
  - If you currently use any online banking or online payments software, it shouldn't require this information to authenticate your identity.
  - The best rule of thumb is to access sensitive and confidential data directly on the server, and only ever from an approved and authorized mobile device.

Securing your Mobile

- **Beware of Free Apps**
  - There are lots of great free apps out there, many are well reviewed and are being enjoyed securely by millions of mobile users right now.
  - The problem is, more and more free and innocent apps are trying to make money from their offerings, so sometimes they track your personal information with limited disclosure or authorization, then sell your profile to advertising companies.
  - The app developers in question may not even be aware of their privacy violations – leaking your location, gender, age and other personal data to embedded mobile ad networks while in the pursuit of revenue.
  - **Sometimes free simply means too good to be true.**

Securing your Mobile

- **Try Mobile Antivirus Software or Scanning Tools**
  - Without active virus scanning and updated malware definitions on your mobile device, it could already be infected with spyware and you may not even know it.
  - Good news is the well-known PC antivirus vendors are now offering similar services to mobile users that scan and protect your smartphone just as they did your desktop.
  - They can point out problems in your settings and instruct you how to correct them.
  - Some even offer additional mobile security services such as download protection, SMS/call-screening services, parental controls, and anti-phishing features.

Securing your Mobile

- **Try Mobile Antivirus Software or Scanning Tools**
  - Today's antivirus packages do require quite a bit of memory to run, and its best to plug them to power during the lengthy scanning process.
  - But they are definitely worth a look, especially if you are engaging in high-risk activities like mobile banking or mobile payment services.
  - Stick to the best-known commercial vendors and you'll minimize your risk.

Securing your Mobile

- **Use MDM Software, if Recommended by IT**
  - Mobile Device Management, or MDM is being increasingly employed by IT departments to secure, manage and support all mobile devices that are authorised to access enterprise networks.
  - These services control and protect sensitive and confidential business data by distributing mobile application or configuration settings to company-owned equipment as well as employee-owned.
  - Enrol your mobile device in a managed environment, if your organisation offers one. The goal of MDM is to optimize the functionality and security of your mobile computing experience, not to impede the way you like to work.

Securing your Mobile

- **Use MDM Software, if Recommended by IT**
  - SIM card locks and credential storage functions protect the phone by requiring a passcode to use network dependent services, and operate similar to screen/key access PINs.
  - SIM locks prevent anyone from making unauthorised calls with your smartphone, or from removing your SIM and using it in another phone.
  - Secure credential storage protects authentication certificates such as the one required to access your organisation's Virtual Private Network (VPN), keeping login info out of sight of prying eyes.

Additional Guidelines

BYOD Hardening:

- iOS⟶ https://security.utexas.edu/handheld-hardening-checklists/ios
- Android ⟶ https://security.utexas.edu/handheld-hardening-checklists/android

(This is examinable!)

Institiúid Teicneolaíochta Chorcaí
Cork Institute of Technology