1. List three major security issues associated with Android Smartphone

Issue 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.
- 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.
- 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.

2. List security issues associated with Apple IOS

Issue with 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.

4. List five mobile malwares.

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.
- **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.

- **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.
- 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 – Botnets

- Foncy
- MDK Botnet

Mobile Malware – SMS Trojan

-Boxter Trojan

- CitMo Trojan

Mobile Malware – AppStores

- Dougalek
- Find and Call iPhone App

Mobile Malware -Cyber Espionage

- FinSpy
- Red October

3. List ten steps you can take to secure you mobile phone.

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

What types of data should never be stored on a mobile phone.

- **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.