The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at [http://www.hackerhighschool.org/licensing.html](http://www.hackerhighschool.org/licensing.html).

The Hacker Highschool Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.
Table of Contents

Introduction.................................................................................................................................................. 5
Your Phone Everywhere.......................................................................................................................... 6
What is Mobile Phone Hacking? ............................................................................................................ 7
  Phreaking................................................................................................................................................ 7
  Jailbreaking......................................................................................................................................... 8
Mobile Phone Operating Systems........................................................................................................ 9
  Android.................................................................................................................................................. 9
iOS.......................................................................................................................................................... 10
  BlackBerry.......................................................................................................................................... 10
  Windows Phone................................................................................................................................. 11
  Symbian.............................................................................................................................................. 11
Mobile Phone Threats.............................................................................................................................. 11
  Social Engineering.............................................................................................................................. 11
  Malware.............................................................................................................................................. 11
  Phone Theft....................................................................................................................................... 12
  Bluejacking and Bluesnarfing........................................................................................................... 13
How To Secure Your Phone or Mobile Devices.................................................................................. 14
  Exercises........................................................................................................................................... 14
Further Reading....................................................................................................................................... 15
Contributors

Marta Barceló, ISECOM
Pete Herzog, ISECOM
Bob Monroe, ISECOM
Pablo Ramos
Simone Onofri
Darren Meehan
Pablo Ramos
Greg Playle
Nick Sullivan
Introduction

When you enter a room, you’ll probably see someone with a mobile phone in their hands. It could be a smartphone or a dumb-phone - as we can call the old devices - but think about all the information it involves. We see a lot of different Operating Systems for mobile devices and you truly have to understand all the risks or functions you can find on them. When you carry your mobile device, all your data is with it. Probably you’ll find your contacts, emails, and social network accounts. So, what can you do with your mobile device? And this question is what we will try to answer in this module.

We'll talk about all the things you can do with your mobile, including some hacking, information gathering or protecting them against possible threats. We will also have to discuss how to interact with them in order to be aware of all we can do with mobile devices.

We will discuss commands and basic tools for you to interact with mobile devices. At the end of this lesson, you should be familiar with the following.

- General specifications about Android, iOS, BlackBerry, Windows Phone and Symbian
- Communications protocols and networks
- Threats and security tools
Your Phone Everywhere

If we could describe the most simple scenario for what mobile phones are for, we can talk about our need to be in touch with our family, friends and so on. So actually, having a mobile phone means that you're connected to a network where others can contact you. From a certain point of view, it would be like being on the Internet, but that didn't happen until smartphones came out.

When you are connected to a wireless phone network, the device – also known as a terminal - uses radio frequencies to communicate with the base stations. These base stations belong to the different cells and all the cells make you available for when someone calls you. If you have your wireless phone next to you, try to check your signal and figure out your phone generation. Mobile phone generations are not only for adding photocamera, gyroscope and so on; there are also some network types and phone generations. Each generation differs for standards used, frequencies, interoperability, services and speed (speed is theoretical and depends on terminal used, distances between base station and terminal and network status):

- **0G**: analog networks, considered pre-cellular using macro-cells, between '40s and '80s on 450 Mhz, principally mounted on cars and trucks. You can see big phones on cars from some films.

- **1G**: analog networks from the end of '80s on different frequencies depending on country. Some standards are NMT (Nordic Mobile Telephone) in Northern Europe and Russia, TACS (Total Access Communications System) and ETACS (Extended TACS) in Europe and South Africa, AMPS (Advanced Mobile Phone System) in North America and Australia. A typical threat was phone cloning.

- **2G**: digital networks from the first '90s typically on 900, 1800 and 1900 Mhz. Principal standard is GSM (Global System for Mobile Communications) with different channel access methods: CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access). Differences between 1G – considering digital networking – are authentication and cryptography, the possibility of data services such as SMS (Short Message Service) also known as Text Messages and interoperability. Some evolution of this generation are:
  - **2.5G**: for GPRS (General Packet Radio Service) which introduces Packet Switching. It is now possible to use IP (Internet Protocol) up to 114 kbps.
  - **2.75G**: for EDGE (Enchanted Data rates for GSM Evolution) which adds speed up to 200 kbps and Evolved EDGE up to 1 Mbps.

- **3G**: digital networks from late 2000s. Main standard is UMTS (Universal Mobile Telecommunications System) with new frequencies used, and not only did customers need to buy a new phone, carriers needed to upgrade base-stations. UMTS is based on W-CDMA (Wideband CDMA), CDMA 2000 and TD-SCDMA (Time Division Synchronous CDMA). With more bandwidth, up to 384 kbps, it is possible to offer video-calls and high-speed connections. 3G has also an evolution:
  - **3.5G**: for HSPA (High-Speed Packet Access) on Downlink (HSDPA) up to 14.4 Mbps or Uplink (HSUPA) up to 5.76 Mbps, and HSPA+ (HSPA Evolution) up to 50 Mbps.

- **4G**: From 2011. An all-IP network using either WirelessMAN-Advanced release 2 (Based on the WiMAX IEEE 802.16m standard) and LTE-Advance (based on cellular's LTE standard), instead of CDMA systems. It uses a scalable channel bandwidth of 5-20 MHz, optionally up to 40 MHz. Peak data rates are approximately 100Mbits/s.
Another interesting fact about 4G is that the ITU-R (International Telecommunications Union-Radio communications sector) set up requirements for the 4G designation called IMT-Advanced (International Mobile Telecommunications - Advanced). They admitted that currently the phones being called 4G do not meet the minimum requirements, but have allowed the use of the 4G label because they are considered the forerunners to reaching the regulations and provide significant improvements from 3G. The first LTE-Advanced networks are due to come out in 2013.

![Figure 1: Smart phones](image_url)

**Exercises**

17.1 For each of your mobile devices, find out how many different interfaces it has that can be used to introduce data or applications. Common examples include WiFi, 3G or 4G, Bluetooth, synchronization services. Does the device use SIM cards, microSD or SD cards, a USB or proprietary data interface? Keep this information handy.

17.2 For each of your mobile devices, find out whether it has any of these “features”: GPS; accelerometers or other geolocation or geotagging capabilities; Bluetooth (and the version); cameras (how many, facing where, and controlled how)?

17.3 For each feature on each device, think about how you could abuse that feature. For example: can you track someone using their smartphone GPS? Could this be used to monitor their driving routes? Search for software on the Internet that has the capability of exploiting the features on each of your devices. Find out whether it can be installed or whether you must first “jailbreak” or “root” the device.

17.4 If you have an Android device, search the Internet or the Web for information on CarrierIQ. Find out how to detect whether your device has CarrierIQ installed and check for it. Find out what it could report back to the carrier. Find out how to remove CarrierIQ from your device.

17.5 For each device, is it possible to turn that device into a “hacking tool” to attack other devices? Does such software exist on the Internet? What happens to your mobile device when you use such software – does it need jailbroken or rooted? Does the operating system get replaced? Does any of this void any of the warranty?

**What is Mobile Phone Hacking?**

**Phreaking**

Even when phones were not mobile, a lot of people tried to understand how they work. If we want to talk about the first phone hacker we will have to mention to **Captain Crunch (John Draper)**. He figured out that a whistle that was, at the time, packaged in boxes of Cap’n Crunch cereal could emit a tone at 2600 hertz, curiously the same frequency that was used by AT&T long lines and made him able to route a new call for free to anywhere he wanted. This has been known and **phreaking** (phone + freak), hacking networks.

**Phracking**

Now a few decades later we can still talk about phone hacking (phracking) but now it involves newer technology. Modern mobile phones, or smartphones, have a lot of functionality such as Internet access, high resolution cameras and tons of applications we can download from different repositories. This means to hacking devices, not network itself.

All of these caught the attention of attackers to get information from users, or deceive them in order to install malicious applications and (usually) steal their money. We will explain how to understand these risks and stay secure while we use our mobile phones.

Jailbreaking

You may have heard the term "jailbreaking" when it comes to Androids and iPhones/iPads, but what does this really mean? No, there's no cell phone prisons out there, with smartphones that have done stupid things and are stuck wearing stripped cases. When you get your new smartphone, you only have limited access options to what you can do with it. It seems like a lot, and for most people, they can do everything they want. You can browse the internet, play games, text until your thumbs evolve into points, and most importantly, call your mother and tell her you're alright. But there are some people out there who want everything.

Imagine bringing home a new laptop. Excitedly you tear into the box, plug it in, and hit that power button. At blazing fast speed Windows loads up, you enter your information, log in, and you are ready to do everything you couldn't do on the slower laptop you got last year. So, you go to install your own software onto it, but you can't. You can only install certain programs that Windows wants you to install. Well, that's what happens when you buy your smart phone. You can only do the things your provider wants you to. For the people who want it all, they can jailbreak their phone.

Jailbreaking, also called rooting, involves using a program to give yourself root access on your mobile device. The two main ones out there right now are CTmod or Odin, and depending on which program you use, there is a different procedure. Basically what it involves is using your computer to remove the old operating system from your phone, and replace it with a new one that was written by a 13 year old and is exactly the same as the old one, with one major difference. The user now has root access and can install apps that their provider doesn't want them to. Apps that let them do things like tether their unlimited internet from their phone onto their wifi only iPad or laptop when they're traveling.

There is, however, danger in jailbreaking or rooting a phone. If any one of the steps are done incorrectly, or the wrong operating system is picked for the phone being rooted, this can lead to what is referred to as "bricking" the phone. When a phone is bricked, the phone will no longer load up, and if there wasn't a backup done on the phone before attempting to root it, that phone is now a $400 paper weight, because jailbreaking a phone nullifies the warranty.

The other drawback is, normally when your provider sends an update to your device, you click ok, the update installs, and you go about your business. When your phone is rooted, you have to wait for someone to figure out what the update does exactly (which usually happens the same day the update is released), then you have to go through the whole jailbreaking process all over again to install the new and updated operating system. For more information on jailbreaking, bricking, and about mobile devices in general, there is an extensive forum pertaining to mobile devices and about every phone out there at www.androidforums.com.
Mobile Phone Operating Systems

Android

Android, Google’s operating system for mobile devices, has a user base growing at an astonishing rate, currently at over 900,000 phone activations a day. It is based on the Linux kernel and includes libraries developed in different programming languages. Its user applications – known as apps, run inside the Dalvik Virtual Machine. Applications or games can be installed through Google Play or through other methods of open distribution.

Figure 2: Android

Android apps are written in Java using the Android SDK. As Android gained popularity, as with any platform, it was targeted more and more by different threats, including botnets and SMS trojans.

Figure 3: Market share

Something often discussed with regards to Android is how its updates are handled. While it’s Google that releases the updates, carriers and OEMs are the ones who provide the updates to users. This can cause some serious delays. These delays do more than leave users without the newest features – they leave many users without the protection of the
latest bug fixes. At times, the majority of Android users may be running outdated apps for months. Some users may even buy their phones with outdated software, new in the box. This fragmentation in Android’s versions causes a lot of devices to be vulnerable even to known threats. As you will see in module 17, this can lead to an attacker getting private user information using an exploit targeted against these older versions.

Android has hundreds of thousands of apps, which can cause security issues for users, something we’ll discuss in later sections.

iOS

Apple has its own operating systems for mobile devices, including iPhone, iPad, and iPod. Released in 2007, now it is on version 5.+, and the latest mobile phone form Apple is the iPhone 4S. iOS is developed entirely in Objective-C, C and C++. The official repository is the App Store from Apple. Those users that want to install applications outside the official repository will have to jailbreak their iPhone. This has to be considered a security breach because they will have to use an exploit to be able to install unofficial applications.

Figure 4: iOS

One of the very first jailbreaks for this OS had a huge security breach, for those users that jailbroken their devices: a SSH service was started with a default password (‘airplane’). For this reason an attacker who found a jailbroken devices in his range (through the wireless phone network or someone connected at a coffee shop) could access all the user’s information. One of the malware detected for this platform used this vulnerability to infect many devices in Australia and Europe; this worm was named iKee.

BlackBerry

Research In Motion (RIM) developed this OS for its BlackBerry devices. The first version came out in 1999 and the latest stable release is BlackBerry OS 7.1. During all this time the BlackBerry smartphones have been adopted by companies all over the world. They offer different software for enterprise management of these devices, in order to provide a robust infrastructure and a high security platform to prevent data breaches.
RIM provides their own application store, from which users can download and install applications for their personal or professional use.

**Windows Phone**

Microsoft also has their own mobile platform; at the beginning it was named Windows Mobile but their most recent release is **Windows Phone**

**Symbian**

Symbian was originally based on Psion’s EPOC, has gone through several versions, and runs on **ARM processors**. The company Accenture provides software support and applications for the Symbian OS. Nokia dropped Symbian in 2011 and announced it would migrate to Windows Phone. Apps are written in a Symbian specific C++. A great deal more information is available on Wikipedia.

**Mobile Phone Threats**

As you could imagine there exist a lot of different kind of threats for mobile devices. We have to take into consideration from the risk of losing our own devices with all the data we have in them, to the possibility that malware would steal your private information, including social networks email or banking credentials. In this section we will introduce you to the most important topics regarding the mobile devices that you might encounter in the real world.

**Social Engineering**

This might be the oldest kind of threat you might know about. It’s very important to notice that **Social Engineering** includes a set of techniques that will try to exploit personal characteristics such as curiosity, greed, fear, laziness, or even joy.

Let’s suppose the following scenario: you receive an SMS from an unknown number. It says that you have won a prize and in order to get it the only thing you need to do is to reply to that SMS with your name, email account or any other kind of personal information.

If you were deceived by this message, now the person who sent this SMS to you, knows not only that the wireless phone number is active, he also knows who you are, and any extra data you sent. We know that this might sound silly but it is quite effective. Thousands of users reply to this kind of message and different charges might apply to their mobile account. We’re talking about $1.50 for each message that the user replies to.

**Exercises**

17.6 Search the Web for any kind of threat that has used Social Engineering to fool users into signing in into a premium SMS number.

17.7 Find threats that cause the phones to silently dial premium numbers without telling the owner.

17.8 How may these threats be stopped? What should you do?

**Malware**

You learned in Module 6 about the different types of malware and how to protect your computer from them. You might find this section quite familiar due to the different kinds of threats available for desktop computers that could affect mobile phones.

Just to refresh your memory, **malware** is the acronym for **malicious software**. It is any kind of application that will harm user privacy or take over the device to provide any kind of
benefit to the attacker. We have talked about trojans, worms, viruses, and you might have guessed that with mobile phones, smartphones, and all the capability they have, cybercriminals are developing their malicious applications for these types of devices, including tablets.

Let's include, as malware, SMS trojans, mobile botnets or any other harmful application for your mobile devices. An SMS trojan will use Social Engineering to try to hide the malicious activity from your phone. When you install or execute the malicious application it will send an SMS to a premium number and you will be charged for those SMS in your bill.

You will not notice that this happened if you do not pay attention to the applications you are installing and to your charges. One of the most affected Operating Systems is Android. Many malicious applications have been reported for this platform, and this goes from SMS Trojans like Android/Raden up to mobile botnets like Android/DroidDream.

Malware for mobile devices is not something new; one of the very first malicious applications that infected smartphones is known as Cabir. This malware was able to infect Symbian and Windows Mobile in the 2004.

Exercises
17.9 Search the web for more information about Cabir, Raden and Geinimi and how they work. Answer the following questions:
- How did Cabir spread from one device to another?
- Why did DroidDream receive that name? Hint: it was related to the way it worked.
- Which technique did Raden use to avoid calling the user’s attention when it received a new SMS?
- How did Raden subscribe the user to the Premium number?

17.10 Smishing and SMS Spoofing

Just as fake emails are sent from unknown accounts, try to fool the user and lead them to phishing servers, SMS can be used for this purpose. Another possible type of attack that you could find is when a strange message arrives to your wireless phone announcing that you’ve become the winner of a great prize. You only have to follow the link given in the SMS. But this smishing message could lead to a fake website that hides an exploit or simply try to get your credentials for social networks, like Facebook, Twitter and so on. It is also possible to alter – spoof – the text message sender. Have you ever received a message with “textsender” instead of a number, which is mapped to your address? The sender was forged, but this is not necessarily a bad thing. When in doubt, check for the SMS server. Typically there are dedicated SMS servers for each phone carrier.

Search for the way to use your phone to see SMS servers for messages. Then check the SMS server numbers from your friends. Sometimes the number is from the same carrier. If you received some messages with forged “textual” sender, identify the server number and search on the web to find the service used.

Phone Theft

Phones are smart devices in which you store a lot of personal data: address book, emails, passwords (such as social networking sites), photographs, call logs. What happens if someone steals your phone? A thief that wants your “hardware” usually wipes the phone, memory card and trashes the SIM card, but what if a thief wants your data?
First, regularly back up your data. Protect yourself by using encryptions software to encrypt your personal data; lock the screen with a password or PIN and use remote wiping software in case of emergency. Always use a PIN on your SIM.

Exercises

17.11 Find an easy, convenient way to back up your mobile device’s data to a different storage device. Decide on how often to do this. Discuss your choices with your friends. Why do they, or do they not, back up their data, and how do they do so?

17.12 Search for encryption software you can use on your phone. Does the software encrypt your phone after a period of not using the phone? Does this interfere with any backup system you are using?

17.13 How can you choose a reasonably difficult PIN, password or passphrase for your mobile devices? If you have not done so, change your PIN, password or passphrase to a more difficult-to-guess version.

17.14 Find out if you can use a password on your SIM card. Should you use one? Do your friends know about this capability?

Bluejacking and Bluesnarfing

One of the communication protocols most used by mobile devices is Bluetooth. Using Bluetooth, you can connect your phone to your PC, headsets and so on. But it can also be an access for malware or bad people. Your Bluetooth can be “discoverable” (Bluetooth is on and your phone communicates to other devices it is up and available); “hidden” (Bluetooth is on but communicates only with devices already paired); or “disabled” (Bluetooth is off). Even if you’re “hidden”, someone can access your device using brute-forcing techniques due to the simple structure of the Bluetooth protocol.

Exercises

17.15 Search for how to disable Bluetooth and turn on it only when is strictly necessary.

17.16 Search for how you can discover which devices are paired to your mobile device or laptop. How can you block a device from pairing with your mobile device?

17.17 Find out how far someone can be and still execute Bluetooth attacks. Look for the term Bluesniping. Find out what equipment and software is required.

17.18 Can your mobile device be use for Bluebumping, Bluejacking and Bluesnarfing? What does it take (software or hardware)? Where is this available?

17.19 Other than disabling Bluetooth, is there a way to protect your mobile devices from Bluetooth attacks? How about your friends’ mobile devices?

17.20 In addition to Bluetooth, do your mobile devices use any other wireless technologies, such as WiFi, GPS, or cell phone networks? Find and consider installing software that will limit which apps can access which features and data, and whether those apps may transmit that data.

17.21 Search for attacks against your mobile devices using those additional services, and then search for ways to protect your mobile devices. Should you or should you not implement these protections? What capabilities will you lose? What will you gain?
How To Secure Your Phone or Mobile Devices

In order to keep your phone safe from various threats we will now share with you a few recommendations that will help you to keep the data you store in your device secure.

1. Back up your information regularly. You paid for all those songs, movies, books, etc. How can you keep a restorable copy in case your device gets dropped, stolen or damaged?

2. Lock your device with a PIN, password or passphrase

3. Download applications only from trusted sources. (Which are those sources, for your devices?)

4. Use security software to encrypt your private and/or personal data

5. Use a service for remote wipe if your device gets stolen or lost. Note that you must usually subscribe to this service before losing your device.

6. Install software and applications updates, but from known-good sources.

7. Disable features not currently in use, such as Bluetooth, infrared or wireless.

8. Use caution when opening email or text message attachments or clicking unknown links. Who sent you this? Do you really know them? Why would they send you this message, on this topic, at this time? Are you expecting it?

9. Verify the applications you download before you install them. Check the hash values.

10. Use official application repositories (App Store, Google Play, BlackBerry Store, etc).

11. Note down the IMEI Number on your mobile phone and serial number of your SIM. Keep that information where you can get it quickly if your device is lost or stolen.

Exercises

17.22 List 5 malicious applications that have been reported for each of your mobile devices, and list their main characteristics

17.23 List four Operating Systems for mobile devices and create a table with the main characteristics they have.

17.24 Research about hacking tools published for your mobile devices and how they are used.

17.25 Try to install Android SDK, mount the emulator and install one application on your computer.

17.26 In earlier exercises, you searched for various apps that could be used to collect or steal data or information from your devices. Download and install those applications to the emulator on your computer. Run them and see what you can “steal” from the virtual device.

17.27 Download and install the security software in the emulator. Does it find, alert on or stop the malware applications?
Further Reading

Android - http://www.android.com/
Symbian - http://licensing.symbian.org/
BlackBerry - http://us.blackberry.com/
Today’s teens are in a world with major communication and productivity channels open to them and they don’t have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.