Abstract — Smartphones offer many more functions than traditional mobile phones. In addition to a preinstalled mobile operating system, such as iOS, Android, or Windows Mobile, most smartphones also typically support carrier networks, Wi-Fi connectivity, and Bluetooth so that users can access the Internet to download and run various third party applications. Most smartphones support Multimedia Message Service (MMS) and include embedded sensors such as GPS, gyroscopes, and accelerometers, as well as a high-resolution camera, a microphone, and a speaker. Smartphones’ increasing popularity raises many security concerns. Their central data management makes them easy targets for hackers. Since the first mobile phone viruses emerged in 2004, smartphone users have reported significant malware attacks. In the last seven months of 2011, malware attacks on the Android platform increased 3,325 percent. As the use of smartphones continues its rapid growth, subscribers must be assured that the services they offer are reliable, secure, and trustworthy.

Keywords — Gyroscope, Accelerometer, Embedded sensors.

I. INTRODUCTION

Smartphones provide lots of the capabilities of traditional personal computers (PCs) and, in addition, offer a large selection of connectivity options, Bluetooth, GSM, GPRS, UMTS, and HSPA. This plethora of appealing features has led to a widespread diffusion of smartphones that, as a result, are now an ideal target for attackers. In the beginning, smartphones came packaged with standardized Operating System (OS): less heterogeneity in OS allowed attackers to exploit just a single vulnerability to attack a large number of different kinds of devices by causing major security outbreaks. Recently, the number of OSes for smartphones (Symbian OS, Windows Mobile, Android and iPhone OS) has increased, each mobile OS has now gained a significant market share. Even if global sales of smartphones will pass 420 million devices in 2011, the number of mobile malware is still small compared to that of PC malware. Nonetheless, we can expect malware for smartphones to evolve in the same trend as malware for PCs: hence, in the next incoming years we will face a growing number of malware. Different types of mobile malware, along with some predictions on future threats, and outlines the differences among security solutions for smartphones. firstly, it analyse the different methodologies to perform an attack in a mobile environment then it investigates how these methodologies can be exploited to reach different goals.

II. SMARTPHONE THREATS AND ATTACKS

In a smartphone threat model, a malicious user publishes malware disguised as a normal application through an app store or website. Users will unintentionally download the malware to a smartphone, which carries a large amount of sensitive data. After infiltrating a smartphone, the malware attempts to control its resources, collect data, or redirect the smartphone to a premium account or malicious website. This model divides a smartphone into three layers:

1) The application layer

It includes all of the smartphone’s apps such as social networking software, email, text messaging, and synchronization software.

2) The communication layer

It includes the carrier networks, Wi-Fi connectivity, Bluetooth network, Micro USB ports, and Micro SD slots. Malware can spread through any of these channels.

3) The resource layer

It includes the flash memory, camera, microphone, and sensors within a smartphone. Because smartphones contain sensitive data, malware targets their resources to control them and manipulate data from them.

An attack forms a loop starting with the launch of the malware, moving through the smartphone’s application, communication, and resource layers, on to premium accounts/malicious websites, and back to the malicious user.

Fig. 1 Smartphone Threat Model
III. THREATS AND ATTACKS

All Smartphone threats and attacks include sniffing, spam, attacker spoofing, phishing, pharming, vishing, and data leakage. Sniffing captures and decodes packets as they pass over the airwaves. There are various ways to sniff or tap a smartphone. In 2010, Karsten Nohl showed that A5/1, the Global System for Mobile Communications (GSM) encryption function for call and SMS privacy, could be broken in seconds. Thus, all GSM subscribers are at risk for sniffing attacks. Further, as eavesdropping software continues to be available, smartphone subscribers using 3G or 4G networks are also at risk. Spam can be carried through email or MMS messages. These messages can include URLs that direct users to phishing or pharming websites. MMS spam can also start a denial-of-service (DoS) attack. The number of spam text messages generated in the US increased 45 percent in 2011 to 4.5 billion messages. Another threat involves an attacker spoofing a caller ID and pretending to be a trusted party. Researchers have spoofed MMS messages that appear to come from 611, which carriers use to send alerts or update notifications. Base stations can also be spoofed. A phishing attack can masquerade as a trusted party to steal personal information, such as a username, password or credit card account number. Many phishing attacks have occurred in social networking, email, and MMS messages. For example, a malicious application could include a “Share on Facebook” button that redirects users to a spoofed target application, which could request the user’s secret credentials and steal the data. Pharming attackers can redirect Web traffic on a smartphone to a malicious or bogus website. By collecting the subscriber’s smartphone information, a pharming attack can lead to other attacks. For example, when a user browses a website on a smartphone, the HTTP header usually includes information about the smartphone’s operating system, browser, and version number. With this information, an attacker can learn the smartphone’s security vulnerabilities and start other directed attacks. Vishing is short for “voice phishing.” In a vishing attack, malicious users try to gain access to a smartphone user’s financial and other private information. By spoofing a caller ID, the attacker might look like a trusted party and fool the smartphone user into releasing personal credentials. Data leakage is the unauthorized transmission of or corporate data. Malicious software can steal personal information such as a contact list, location information, or bank information and send this data to a remote website. A smartphone’s data leakage can put its owner at risk of identity theft. Business owners or classified users such as government and military personnel have even more concern about data leakage. ZitMo, a mobile version of Zeus, has been found in Symbian, Black-Berry, and Android devices. An attacker could use ZitMoto steal one-time passwords sent by banks to authenticate mobile transactions. Web browsers are also vulnerable to smartphone attacks. The WebKit engine, which most mobile platforms use, has a vulnerability that lets attackers crash user applications and execute malicious code. CrowdStrike revealed that attackers could use the WebKit vulnerability to install a remote access tool to eavesdrop on smartphone conversations and monitor user locations. The vulnerability has been found in BlackBerry, iOS, and Android devices. For various reasons, smartphones are also vulnerable to DoS attacks:

• Because they are based on radio communication technology, smartphones can incur an attack in which a jamming device is used to disrupt the communication between the smartphone and its base station.
• Flooding attacks can generate hundreds of text messages or incoming calls, thus disabling a smartphone.
• A battery exhaustion attack on a smartphone causes more battery discharge than is typically necessary.
• A malicious user could use a smartphone’s blocking features to start a DoS attack. If a malicious user keep scaling a smartphone from a blocked phone number, the subscriber cannot use any of the smartphone’s functions. Many attacks operate in a stealth mode. Users might not notice these attacks for days or even months. In addition a malicious user could plant malware in a smartphone but not use it until later.

The WebKit engine, which most mobile platforms use, has a vulnerability that lets attackers crash user applications and execute malicious code.

IV. SECURITY SOLUTION FOR DEVICES

In the existing mechanisms that are developed to prevent different type of threats for smartphones. In this present first of all, intrusion detection systems for smartphones then trusted mobile-based solutions.

A. Intrusion Detection System

It is present the state of the art of models and tools that implement Intrusion Detection Systems (IDSes) on smartphones. IDSes can be based upon two complementary approaches:

1) Prevention-based approaches: using cryptographic algorithms, digital signatures, hash functions, important properties such as confidentiality, authentication or integrity can be assured; in this scenario, IDSes have to be running online and in real-time;
2) Detection-based approaches: IDSes serve as a first line of defence by effectively identifying malicious activities.

Furthermore, there are two main types of detection:

i) Anomaly-based (alternative names: anomaly detection, behaviour-based), which compares the “normal” behaviour with the “real” one;

ii) Signature-based (alternative names: signature detection, misuse-based, knowledge based, detection by appearance), based upon patterns of well-known attacks.

B. Mobile Device Forensics

In Mobile device forensics—which covers cell phones, smartphones, tablets, personal digital assistants, and GPS receivers is a subspecialty of computer forensics, necessitated by the near ubiquity of these devices in today’s society. Because mobile devices are increasingly the instrument, target, or record keeper of criminal and other nefarious behaviours,
they are of interest in criminal investigations, civil litigation, and intelligence collection. Some would argue that mobile devices contain more probative information per byte examined than traditional computers. Because most smartphones now come with sophisticated applications, built-in cameras, lots of storage capacity, and high speed network connectivity, a vast amount of computing power is readily available within the user’s grasp. Indeed, smartphones are more properly thought of as portable Internet terminals than merely as phones. Although mobile device forensics involves retrieving and examining data even if it might have been deleted, for both criminal and civil proceedings, the processes and tools are also used in applications outside the courtroom. Data that can be recovered from a mobile device includes call history, sent and received Short Message Service (SMS) and multimedia messages, contacts and phone numbers, emails, photos, videos, geolocation and GPS information, wireless network settings, Web browsing history, voicemail messages, social networking information, application histories and logs, and other data that might be retained within smartphone apps. Numerous commercial and open source products are available for extracting and analysing mobile device data, ranging from camera kits that take screenshots to products that can acquire a file system (logical) or the entire memory (physical) to software that parses databases and hardware to physically examine the device’s chips. Figure shows the most widely used products for logical and physical data extraction and analysis: the Cellebrite Universal Forensics Extraction Device (UFED) device forensics requires a process and tools that can extract information from at least six different mobile operating systems (OSs), including iOS, Android, and Windows Mobile, and thousands of models of phones, tablets, and GPS devices. Even if an examiner can physically acquire the device’s memory, examination of that binary dump might still require good, old fashioned analysis with hex editors, standard computer forensics tools, and regular expressions.

![Fig. 2 Cellebrite UFED](image)

Cellebrite is a privately held company, established in 1999, which manufactures various data extraction, transfer and analysis devices for cellular phones and mobile devices. Its products include specialized hardware and software aimed at acquiring both physical and logical data stored on mobile devices, with the ability to transfer the extracted data to other devices, parse acquired data and analyze content. Cellebrite has two separate business divisions: Cellebrite Wireless Carriers & Retailers and Cellebrite Mobile Forensics. The first division, Cellebrite Wireless Carriers & Retailers, produces hardware and software for phone-to-phone data transfer, backup, mobile applications electronic software distribution, and data analysis tools. Cellebrite Wireless Carriers & Retailers products are used by 150 of the world’s largest mobile operators, including AT&T, Verizon, Sprint, Vodafone, Orange, Telstra, and others; it also claims deployments in more than 100,000 wireless retail points of sale globally, including RadioShack and The Phone House. Cellebrite is the only company that works directly with the handset manufacturers to ensure compatibility before the latest devices are released to the public. Cellebrite’s second division, Cellebrite Mobile Forensics, was established in 2007 and produces software and hardware for mobile forensics purposes used by federal, state, and local law enforcement intelligence agencies; military branches; corporate security and investigations; law firms; and private digital forensic examiners in more than 60 countries. These include West Yorkshire Police, the Indian Army, French National Gendarmerie, Japan National and Regional Police, and more. Building on its expertise in data extraction and mobile synchronization technologies, in 2007 Cellebrite established an independent and separated division targeted at the mobile forensics industry. Cellebrite’s Mobile Forensics Division introduced its first line of mobile forensics products in 2007 under the family brand name ‘Universal Forensic Extraction Device’ (UFED), which had the ability to extract both physical and logical data from mobile devices such as cellular phones and other hand-held mobile devices, including the ability to recover deleted data and decipher encrypted and password protected information. The UFED enables its user to retrieve subject data via logical file system or physical extractions. Physical extraction enables it to recover deleted information, decipher encrypted data, acquire information from password protected mobile applications such as Facebook, Skype, WhatsApp and browser-saved passwords. The UFED’s physical extraction functionality can also overcome devices’ password locks, as well as SIM pin numbers.

The UFED series comes in three distinct flavours:

1. UFED Ultimate (previously known as UFED Physical Pro) incorporates the abilities of all the other UFED versions, allowing for physical, logical, user password and file system extractions, data extraction of existing, hidden and deleted data, decipher lock codes and access and decode internal application data including: International Mobile Subscriber Identity (IMSI) history, past SIM cards used, user lock-code history and more. An add-on device, UFED CHINEX, offers physical extraction and decoding for Chinese mobile phones.

2. UFED Physical Analyser is a software package that comes with the UFED Ultimate. It is meant to decode and parse physical mobile device images. It also allows for direct physical data extraction from various iOS devices, such as:
3. UFED Logical allows for logical data acquisition from smartphones, feature and legacy phones.

In June 2012 Cellebrite introduced a new touch-screen package for its UFED Ultimate and UFED Logical systems: UFED Touch. UFED Touch’s capabilities include decoding, decryption and device password protection defeat, allowing for access to data even when the mobile system that is being investigated has been secured.

V. CONCLUSION

With the rapid proliferation of smartphones equipped with a lot of features, as multiple connections and sensors, the number of mobile malware is increasing. Differently from PC environment, solutions aimed at preventing the infection and the diffusion of malicious code in smartphone have to consider multiple factors: the limited resources available, including the power and the processing unit, the large number of features that can be exploited by the attackers, such as different kinds of connections, services, sensors and the privacy of the user. Finally, we have reviewed current security solutions for smartphones focusing on existing mechanisms based upon intrusion detection and trusted mobile platforms.

REFERENCES

[8] www.cellebrite.com