A Survey on Security for Mobile Devices

Mariantonietta La Polla
Fabio Martinelli
Daniele Sgandurra

Outline

- Introduction
- Mobile Technologies
- Mobile Malware
- Attacks on Mobile Devices
- Security Solutions For Mobile Devices
- Conclusions

Introduction

- This paper aims to provide a structured and comprehensive overview of the research on security solutions for mobile devices over the period 2004-2011.
- Group existing approaches aimed at protecting mobile devices against growing number of attacks into different categories, based upon the detection principles, architectures, collected data and operating systems.

- Increasing number of OSes for smartphones -2010-

Company	Market Share (%)
Symbian	36.6
Android	25.5
iOS	16.7
Research In Motion	14.8
Microsoft Windows Mobile	2.8
Linux	2.1
Other OS	1.5
Total	100.0

- Growing number of mobile malware in the same trend as malware for PCs in the next incoming years.
  - new mobile OS vulnerabilities numbers: from 115 in 2009 to 163 in 2010 (42% more vulnerabilities).

Section II introduces some background notions on mobile technologies.

- wireless telecommunication
- networking standards.

Section III

-describes different types of mobile malware

-outlines the differences among security solutions for smartphones and traditional PCs.

Section IV discusses current threats

-analyzes the different methodologies to perform an attack in a mobile environment

-investigates how they can be exploited to reach different goals.

Section V presents security solutions, focusing on those that exploit intrusion detection systems and trusted platform technologies.

Section VI conclusions.

Mobile Technologies

- Background Notions on wireless telecommunication technologies
  - GSM: *Global System for Mobile communications* is the first and most popular standard in Europe for mobile telecommunication system and is part of 2G wireless telephone technology.
  - GPRS and EDGE: referred as 2.5 generation.
    - *General Packet Radio Service* uses packet switching mechanism to achieve higher data rates and lower access time.
    - *Enhanced Data rates for GSM Evolution* supports higher transmission rate and higher reliability
  - UMTS: *the Universal Mobile Telecommunications System* represents the third-generation (3G) on cellular system
    - Circuit switching connections are supported simultaneously with packet switching connections
    - Users can exploit multiple services and different classes of services, such as conversational, streaming, interactive and background.

Mobile Technologies

- Background Notions on Networking Technologies
  - Bluetooth: Bluetooth is a standard that enables devices to exchange data over a small area through short wavelength radio transmissions.
  - Wireless LAN IEEE 802.11: IEEE 802.11 is a family of standards for WLAN that includes several protocols for communicating at different frequencies (2.4, 3.6 and 5 GHz).

    These standards can be used in two operation mode:
    - in the infrastructure mode, a device, referred as Access Point (AP), plays the role of the referee: an AP regulates the network access and coordinates the devices that are part of the network
    - in the infrastructure-less mode (ad hoc mode), no referee exists and devices monitor the spectrum to gain network access

Outline

- Introduction
- Mobile Technologies
- **Mobile Malware**
- Attacks on Mobile Devices
- Security Solutions For Mobile Devices
- Conclusions

Mobile Malware

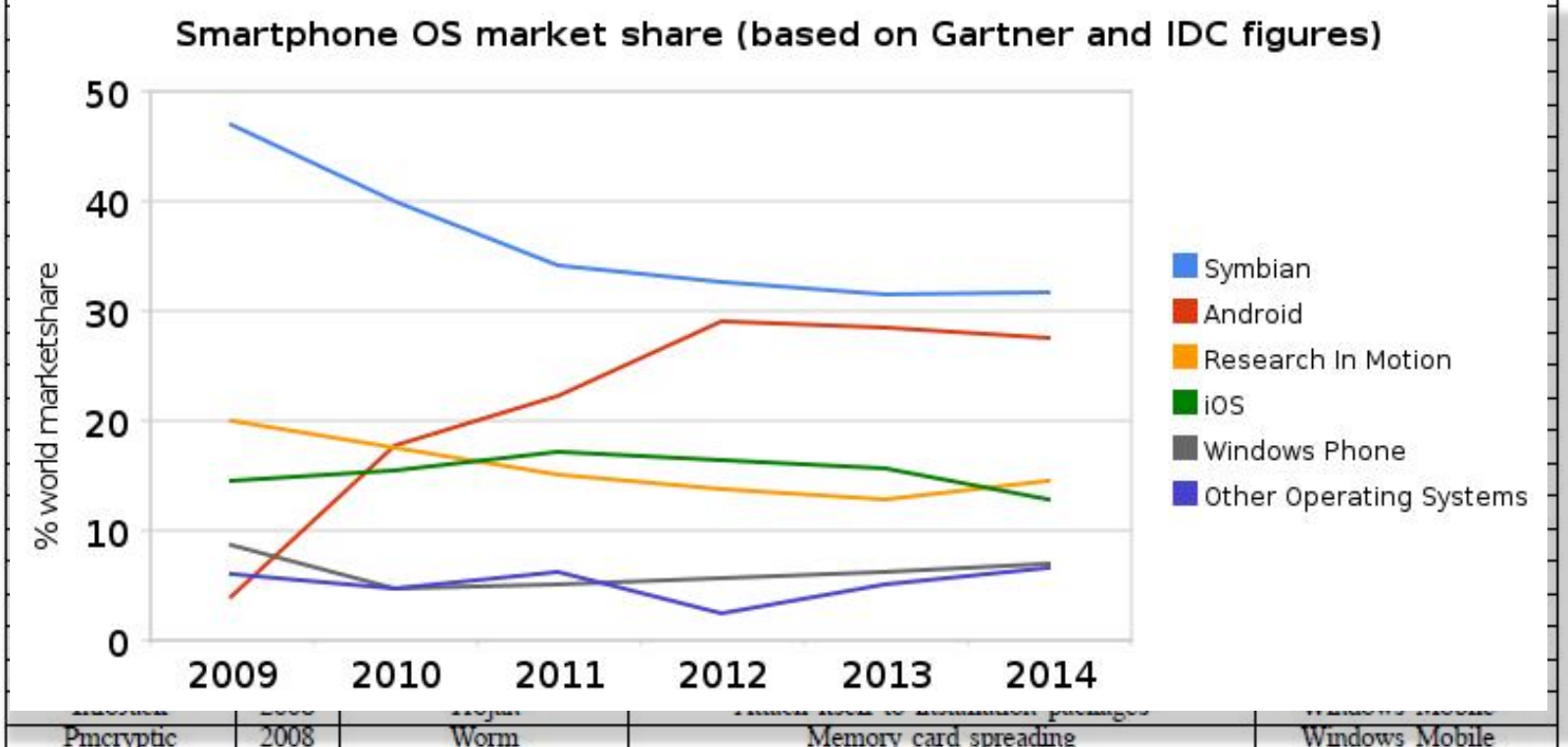
- Malware is any kind of hostile, intrusive, or annoying software or program code (e.g. Trojan, rootkit, backdoor) designed to use a device without the owner's consent.
- Malware can be grouped in the following main categories, according to its features
  - virus
  - worm
  - Trojan
  - rootkits
  - botnet
- Mobile malware can spread through several and distinct vectors, such as SMS links, MMS attachments and infected programs received via Bluetooth.
- Main goals of malware targeted at smartphones include theft of personal data stored in the phone or the user's credit.

Mobile Malware

- Evolution of Mobile Malware
- Predictions and Future Threats
- Mobile Security vs. Personal Computer Security

Mobile Malware Examples

Name	Time	Type	Method of Infection	OS
Liberty Crack	2000	Trojan	Pretend to be a hack	Palm OS
Cabir	2004	Worm	Bluetooth connection and copies itself	Symbian OS
Dust	2004	Virus	File Infector	Windows Mobile
Brador	2004	Trojan	Copy itself in to the startup folder	Windows Mobile
Mosquitos	2004	Trojan	Embedded in a game	Symbian OS
Pmcryptic	2008	Worm	Memory card spreading	Windows Mobile
Yxe	2009	Worm	SMS containing malicious URL	Symbian OS
Yxes	2009	Worm/Botnet	SMS containing malicious URL	Symbian OS
Ikee	2009	Worm	Scanning a IP ranges and SSH	iPhone
FlexiSpy	2009	Spyware	Fake Application	Symbian
Curse of Silence	2009	SMS Exploit	Vulnerabilities in e-mail parsing	Symbian OS
ZeuS MitMo	2010	Worm	Fake SMS	Cross-Plafrom
iSAM	2011	Multifarious malware	Scanning IP and connecting to SSH	iPhone



- Evolution of Mobile Malware

  - Roles in prevention solutions and countermeasures

    - the users, which have to be educated to utilize the device in a secure way
    - the software developer, which can develop security protection targeted at smartphone;
    - the network operator, which can enhance the network infrastructure with mechanisms to avoid intrusions;
    - the phone manufacturers, which should update the devices automatically so that for attackers it would be harder to exploit security holes;
    - new epidemiological models, to forecast if an already detected virus can initiate an epidemic.

- Predictions and Future Threats
  - Security experts foresee massive attacks to come out at any time, McAfee Labs predicts that 2011 will be a turning point for threats to smartphones.
  - In the near future cybercriminals will focus their attention on iPhone and Android platforms.
  - the spreading of mobile virus to desktop platforms

    e.g. USB devices are responsible for the spread of auto-run malware, while the Conficker worm contained a propagation capability that used removable drives to increase spread.
  - The observation of new forms of malware in a testbed environment to predict their behavior

    e.g. MAISim, a framework that uses the technology of mobile agents for simulation of various types of malicious software (viruses, worms, malicious mobile code) for smartphones.

Predictions and Future Threats

- Future threats in a mobile environment may affect different assets, such as:
  - personal data;
  - corporate intellectual property;
  - classified information;
  - financial assets;
  - device and service availability and functionality;
  - personal and political reputation.
- some future risks, threats and countermeasures for smartphones:
  - data leakage resulting from device loss or theft;
  - unintentional disclosure of data;
  - attacks on decommissioned devices;
  - phishing attacks;
  - spyware attacks;
  - network spoofing attacks;
  - surveillance attacks;
  - diallerware attacks;
  - financial malware attacks;
  - network congestion.

- # Mobile Security vs. Personal Computer Security

  - Five key aspects distinguish mobile security from conventional computer security:
    - mobility: each device comes with us anywhere we go and therefore, it can be easily stolen or physically tampered;
    - strong personalization: usually, the owner of device is also its unique user;
    - strong connectivity: a smartphone enables a user to send e-mails, to check her online banking account, to access lot of Internet services; in this way, malware can infect the device, either through SMS or MMS or by exploiting the Internet connection;
    - technology convergence: a single device combines different technologies: this may enable an attacker to exploit different routes to perform her attacks;
    - reduced capabilities: even if smartphones are like pocket PCs, there are some characteristic features that lack on smartphones, e.g. a fully keyboard.

- # Mobile Security vs. Personal Computer Security

  - The limited resources(CPU and memory) of a smartphone are the most obvious difference with a PC.
    - It is highly important that a security solution does not constantly drain large portions of available CPU time to avoid battery exhaustion.
  - Threats to user privacy in a mobile environment are different from those performed on PCs
    - Sensors (e.g. microphones) are not optional and can be used illicitly to sniff user's private data. The attacks work even when the user is not interacting with the mobile phone.

Outline

- Introduction
- Mobile Technologies
- Mobile Malware
- **Attacks on Mobile Devices**
- Security Solutions For Mobile Devices
- Conclusions

Attacks on Mobile Devices

- Methodologies of the Attacks
  - wireless;
  - break-in;
  - Infrastructure-based;
  - worm-based;
  - botnet;
  - user-based.
- Goals of the Attacks
  - privacy;
  - sniffing;
  - denial of service;
  - overbilling.

- # Methodologies of the Attacks

  - wireless attacks against smartphones, especially those targeting personal and sensitive data
    - eavesdropping on wireless transmissions to extract confidential information, such as usernames and passwords
    - abuse the unique hardware identification (e.g.,wireless LAN MAC address) for tracking or profiling the owner of the device
    - exploit Bluetooth as a medium to speed up its propagation.
  - Break-in Attacks enable the attacker to gain control over the targeted device for performing further attacks by exploiting either programming errors or format string vulnerabilities

- Methodologies of the Attacks
  - Infrastructure-based Attacks
    - GSM: the security impact of the SMS interface on the availability of the cellular phone

      -e.g. If an attacker is able to simultaneously send messages through available portals into the SMS network, the resulting aggregate load can saturate the control channels and block legitimate voice and SMS communications.

Infrastructure-based Attacks

- GPRS: Attacks against GPRS can target the device, the radio access network, the backbone network, and the interfaces connecting GPRS networks with each other or with the Internet.

  - Five sensitive area in GPRS security

    - the mobile station (MS) and the SIM-card
    - the interface between the MS and the SGSN (Serving GPRS Support Node)
    - the GPRS backbone network
    - the packet network that connects different operators
    - the Internet

Infrastructure-based Attacks

- UMTS: UMTS security architecture defines a set of procedures to achieve increased message confidentiality and integrity during their communication.

  - Some examples of attacks in UMTS security

    - dropping ACK signal
    - modification of unprotected Radio Resource Control (RRC) messages
    - modification of the initial security capabilities of MS
    - modification of periodic authentication messages
    - SQN synchronization
    - EAP-ALA originated DoS

Methodologies of the Attacks

- Worm-Based Attacks

  The main features that characterize attacks based upon worms are:

  - transmission channel

    possible routes for infection vectors:

    - downloading infected files while surfing the Internet;
    - transferring malicious files between smartphones using the Bluetooth interface;
    - synchronizing a smartphone with an infected computer;
    - accessing an infected memory card;
    - opening infected files attached to MMS messages.

  - spreading parameters
  - user mobility models

- # Methodologies of the Attacks

  - ## Worm-Based Attacks

    The main features that characterize attacks based upon worms are:

    - transmission channel
    - spreading parameters: Worms can also attack the communication network itself. Worms that exploit messaging services are potentially more virulent than Bluetooth ones in terms of speed and area of propagation.
    - user mobility models: mobile worms can infect several devices using proximity attacks against vulnerable devices that are physically nearby without connection with internet.

Methodologies of the Attacks

- Botnets Attacks

  Since mobile networks are now well integrated with the Internet, threats on the Internet will migrate over the mobile networks including botnets.

  - Bluetooth Command-and-Control: construct and maintain mobile-based botnets communicating via Bluetooth
  - SMS C&C: Within the testbed mobile botnet, all C&C communications are carried out using SMS messages. A P2P topology is exploited which makes the detection and disruption much harder.
  - Hybrid C&C: combine P2P with SMS-HTTP hybrid approach to create a fully functional mobile phone botnet out of Apple's jailbroken iPhone

  command-and-control(C&C) network, used to remotely propagate messages, tasks, updated payload among the bots and the botmasters (and viceversa), can be built out using Bluetooth, SMS messages, the Internet (e.g., HTTP), peer-to-peer (P2P) or any combination of them.

Attacks on Mobile Devices

- Goals of the Attacks
  - Privacy

    Privacy attacks of smartphones concern situations in which integrity and confidentiality are corrupted
    - stealing personal data from a lost smartphone, such as contact list or messages.
    - location awareness
  - Sniffing

    Sniffing attacks on smartphones are based upon the use of sensors, e.g. microphone, camera, GPS receiver. These sensors can seriously compromise users' privacy.
  - Denial of Service;
  - Overbilling.

Attacks on Mobile Devices

- Goals of the Attacks
  - Privacy
  - Sniffing
  - Denial of Service

    DoS attacks against smartphones are mostly due to strong connectivity and reduced capabilities: due to the limited hardware, attacking a smartphone can be accomplished with a small effort.

    e.g. battery exhaustion attacks; water torture attack(PHY layer)
  - Overbilling

    overbilling attacks charge additional fees to the victim's account and may transfer these extra fees from the victims to the attackers.

Outline

- Introduction
- Mobile Technologies
- Mobile Malware
- Attacks on Mobile Devices
- **Security Solutions For Mobile Devices**
- Conclusions

Security Solutions For Mobile Devices

- Intrusion Detection Systems
  - two complementary approaches
    - prevention-based approaches

      Assure confidentiality, authentication or integrity using cryptographic algorithms, digital signatures and hash functions
    - detection-based approaches

      effectively identifying malicious activities
  - two main types of detection
    - anomaly detection

      compare the "normal" behavior with the "real" one
    - signature detection

      based upon patterns of well-known attacks
- Trusted mobile-based Solutions

Includes some conventional approaches typically implemented by off-the-shelf smartphone applications to provide basic security

SECURITY AP

Product	Features			
WaveSecure	Lock and Wipe Backup and Restore Localization and SI	J2ME		
Norton Mobile Security Lite	Theft of Private Stuff Unauthorized Access Mobile Viruses Malware and Threats Harmful Downloads	Android	Commercial	[104]
iCareMobile	Parental Control Automatic Pornographic Content Detection	Symbian Android	Free	[105]
BullGuard Mobile Security 10	Antivirus and Anti-spyware Anti-theft Parental Control Firewall Spam-filter Basic Backup	Android BlackBerry Symbian Windows Mobile	Commercial	[106]
Kaspersky Mobile Security 9	Privacy Protection Anti-theft Parental Control Encryption Anti-Spam Anti-Malware Firewall	Android BlackBerry Symbian Windows Mobile	Commercial	[107]
ESET Mobile Security	Antivirus Firewall SMS/MMS Anti-spam Anti-theft	Symbian Windows Mobile	Commercial	[108]
Lookout Mobile Security	Lock Wipe Backup Wipe Privacy of Data	Android iPhone	Free	[109]

CLASSIFICAT

Chronologically list the research security solutions that provides a prototype, according to their detection principles, architecture(distributed or local), reaction (active or passive), collected data (OS event, keystrokes), and OS

Reference	Year	Detection Principles				
[125]	2004	Signatures (Manually)				
[139]	2005	Anomaly Detection				
[117]	2006	Power Consumption				
[57]	2006	Machine Learning				
[59]	2006	Machine Learning				
[120]	2006	Signatures (Automatically)				
[133]	2006	Run-Time Policy Enforcement				
[127]	2007	Run-Time Policy Enforcement				
[156]	2007	Integrity Verification				
[130]	2007	Machine Learning				
[47]	2008	Signatures (Manually)	Distributed	Passive	Applications	Symbian
[157]	2008	Integrity Verification	Local	Passive	OS Events	SELinux
[97]	2008	Power Consumption	Distributed	Passive	Measurements	Windows Mobile
[121]	2008	Signatures (Automatically)	Distributed	Active	Communication Events	Symbian
[137]	2008	Anomaly Detection	Local	Passive	Keystrokes	OS-Independent
[148]	2008	Anomaly Detection	Distributed	Passive	All	Android
[154]	2008	Signatures (Automatically)	Local	Active	OS Event	Windows Mobile
[58]	2009	Machine Learning	Local	Passive	Communication Events	OS-Independent
[46]	2009	Machine Learning	Local	Active	Communication Events	OS-Independent
[48]	2009	Machine Learning	Distributed	Passive	Measurements	OS-Independent
[118]	2009	Power Consumption	Local	Passive	Communication Events	OS-Independent
[123]	2009	Signatures (Automatically)	Local	Active	All	OS-Independent
[39]	2009	Machine Learning	Distributed	Passive	OS Events	OS-Independent
[138]	2009	Machine Learning	Local	Passive	Keystrokes	OS-Independent
[141]	2009	Machine Learning	Local	Passive	Communication Events	OS-Independent
[143]	2009	Machine Learning	Local	Passive	All	Symbian
[147]	2009	Signatures (Manually)	Local	Passive	OS Events	Android
[158]	2009	Integrity Verification	Local	Passive	OS Events	LIMO
[122]	2009	Signatures (Manually)	Distributed	Active	Communication Events	Linux
[94]	2009	Run-Time Policy Enforcement	Local	Active	All	Android
[95]	2009	Run-Time Policy Enforcement	Local	Active	All	Android
[134]	2009	Interception	Local	Passive	OS Events	Windows Mobile
[135]	2009	Signatures (Manually)	Local	Passive	OS Events	Symbian
[136]	2009	Signatures (Manually)	Local	Passive	OS Events	Android
[151]	2010	Run-Time Policy Enforcement	Local	Active	OS Event	Android + SELinux
[153]	2010	Anomaly Detection	Local	Passive	OS Event	Windows Mobile
[124]	2010	Signatures (Automatically)	Local	Passive	Keystrokes	OS-Independent
[49]	2010	Machine Learning	Local	Passive	OS Events	Linux
[113]	2010	Machine Learning	Local	Passive	All	Android
[115]	2011	Machine Learning	Local	Passive	All	Android

Intrusion Detection Systems

partition existing IDS solutions using these features:

- detection principles:
  - anomaly detection:
    - machine learning;
    - power consumption.
  - signature-based:
    - automatically-defined;
    - manually.
- architecture:
  - distributed;
  - local
- reaction:
  - active;
  - passive.
- collected data:
  - system calls;
  - CPU, RAM;
  - keystrokes;
  - SMS, MMS.
- OS:
  - Symbian;
  - Android;
  - Windows Mobile;
  - Apple iOS.

- Intrusion Detection Systems
  - Detection Principles:

    Partition existing IDSes using the following detection principles:

    - anomaly detection
      - An anomaly detection system compares the "expected" behavior of the smartphone with the "real" behavior.
      - Anomaly-based approaches for smartphones are either based upon machine learning techniques or upon monitoring power consumption.
    - signature-based
    - run-time policy enforcement

- Detection Principles:
  - anomaly detection
  - signature-based
    - The signature-based approach checks if each signature derived from an application matches any signature in a malware database.
    - The database of malware signature can be automatically or manually defined.
  - run-time policy enforcement
    - mobile code consumers essentially accept some contractual requirements(a policy) and exploit a supporting mechanism to enforce the policy associated with the code to detect and stop anomalies.

- Intrusion Detection Systems
  - Architecture:
    - local architecture

      both the collecting phase and the analysis phase are locally performed on the device and no interactions with an external server is required. (limited resource)
    - distributed architecture

      a distinct and separated component (i.e., a server) is required to analyze the activities collected and sent by each device.
  - Reaction

    According to whether existing mechanisms for intrusion detection react or not whenever a new threat is found, the solutions can be active reaction or passive reaction.

• Intrusion Detection Systems

- Collected Data:

  All the solutions based upon intrusion detection need to access several features of a smartphone, the problem of privacy of the data accessed should be carefully considered.

  - Operating System Events
    - system calls
    - function calls
    - network operations
  - Measurements
    - CPU activity,
    - memory consumption
    - file I/O activity
    - network I/O activity
  - Keystrokes

    track the keys struck on a keyboard to monitor the actions of the user
  - Communication Events

    Communication events include operations such as sending and receiving of SMS/MMS messages, or file downloads/uploads.

- Operating Systems: Symbian; Android; Windows Mobile; iPhone OS.

Security Solutions For Mobile Devices

- Intrusion Detection Systems
- Trusted mobile-based Solutions
  - Trusted Computing Group (TCG) has published a set of specifications to measure, store, and report hardware and software integrity through a hardware root-of-trust, which is the Trusted Platform Module (TPM) and Core-Root-of-Trust-Measurement (CRTM).
  - Specifications for mobile phone platforms released by the TCG Mobile Phone Working Group, i.e. the Mobile Trusted Module (MTM), provide a root-of-trust for smartphones in the same way as the TPM does for personal computers.

Conclusions

- Solutions aimed at preventing the infection and the diffusion of malicious code in smartphone have to consider multiple factors:
  - limited resources available, including the power and the processing unit
  - 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.
- Work we have done:
  - discussed the current scenario of mobile malware by summarizing its evolution, outlined likely future threats and reported some predictions for the near future.
  - categorized known attacks against smartphones, especially at the application level
  - reviewed current security solutions for smartphones focusing on existing mechanisms based upon intrusion detection and trusted mobile platforms.

Thank you.