Università degli Studi di Perugia

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Specialistica in Informatica

Corso di Sicurezza Informatica

Sicurezza e Smartphone: una Panoramica

Studenti
Riccardo Maria Cefalà
Claudio Tanci

Professore
Stefano Bistarelli

Anno Accademico 2010–2011

1 Introduzione

Gli smartphone sono telefoni mobili con elevate capacità di calcolo. Essi aggiungono alle tipiche funzioni dei telefoni cellulari (Chiamate, SMS) altre funzioni fino a qualche anno fa riscontrabili esclusivamente in dispositivi più complessi come PDA e Personal Computer.

Tali funzioni sono principalmente rivolte alla gestione dei dati personali e più recentemente alla produzione ed al consumo di prodotti multimediali come filmati, giochi, musica.

Si può affermare che la diffusione di tali dispositivi negli ultimi anni è stata la reale novità nel mercato della teconologia di consumo per il trattamento dell'informazione. Secondo previsioni di mercato (Figura 1) il volume di vendite e quindi la diffusione dei "telefoni intelligenti" supererà nei prossimi mesi quella di altri dispositivi (Netbook e PC Portatili)

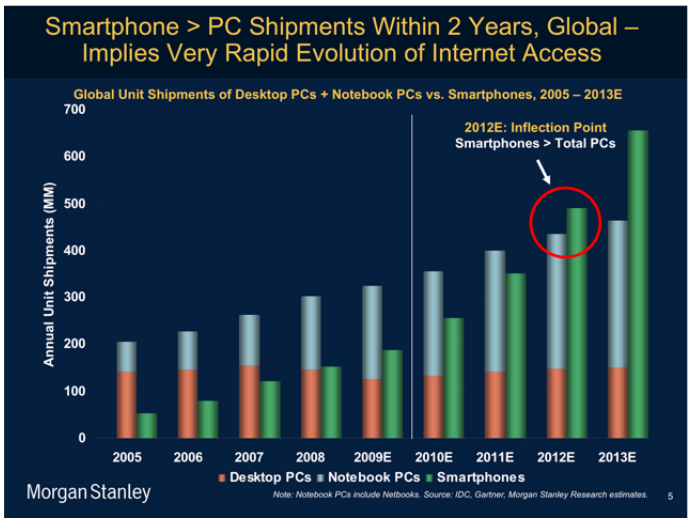

Figura 1: Confronto tra volume di vendite di Smartphones e Computer Portatili negli ultimi anni e previsione per i prossimi mesi.

Si può osservare come questo trend stia cambiando il rapporto con la rete Internet ed in generale con i computer e rappresenti il prosieguo di un'evoluzione con caratteristiche simili a quanto già avvenuto in passato: il passaggio dai sistemi Time Sharing e Batch, tipicamente Mainframe intrinsecamente multi-utente, ai Personal Computer ha portato con se la diminuzione del rapporto utente per computer.

In modo simile, con gli smartphone, ogni utente non è più legato ad un singolo terminale ma tende a possederne tanti (PC di casa, Ufficio, Portatile,

Smartphone, Tablet, ecc.) grazie anche alla possibilità offerte dalle reti Internet cellulari di accedere ai propri dati anche in mobilità. Ciò sta portando ad un ulteriore diminuzione del rapporto utenti per computer.

In questo panorama è facile osservare come alcune delle problematiche tipiche di cui la sicurezza si occupa diventino ancora più critiche e la protezione dei dati personali acquisti un enfasi ancora maggiore.

1.1 Smartphone e Sicurezza

La promessa dei dispositivi mobili è quella di avere sempre a portata di mano tutte le informazioni e i contatti personali che ci interessano attraverso molteplici canali di comunicazione da poter usare in qualsiasi luogo appoggiandosi a reti audio e dati senza fili.

Gli smartphone diventano quindi la porta d'accesso ai propri dati personali sia locali che consegnati a terze parti "in the cloud" ma portano traccia, inevitabilmente, anche di dati non strettamente (o non solamente) riguardanti il proprietario del telefono, ma i suoi amici e colleghi, i loro contatti, messaggi, appuntamenti, appunti condivisi e posizioni. La loro utilità ne fa di per se strumenti "sensibili" la cui sicurezza è importante ora e in misura ancora maggiore in futuro con l'aumento della loro pervasività e delle loro possibili funzioni, per le informazioni che contengono e per la loro funzione di portale di accesso a tutte le informazioni personali e lavorative.

La relativa novità rappresentata da questi dispositivi e i servizi in costante evoluzione che offrono comportano inoltre che lo studio delle problematiche a loro connesse e la valutazione dei mezzi appropriati per la loro risoluzione sia un campo di studio attivo e vivace, non esiste un modello di sicurezza completo e non è detto che un unico modello sia possibile o desiderabile data la flessibilità propria del mezzo e i molteplici scenari configurabili. Studenti, dirigenti di azienda e il Presidente degli Stati Uniti sono tutti utenti di questa stessa classe di dispositivi che esprimono esigenze molto diverse, anche e soprattutto dal punto di vista della sicurezza.

Alcune assunzioni, policy e meccanismi comuni sono comunque emersi nelle piattaforme commerciali proposte da aziende quali Apple, Google, Microsoft e Research in Motion.

Il proprietario dello smartphone viene ad essere naturalmente considerato l'"amministratore" del dispositivo, e spesso alcune policy di sicurezza e relativi meccanismi che le implementano sono pensate per limitare il proprietario stesso.

Una seconda assunzione trasversale riscontrabile nelle offerte dei maggiori player nel mercato è quella che il fornitore della piattaforma in primis, ed eventuali partner strettamente collegati come in alcuni casi gli operatori

telefonici vengano considerati affidabili, e si riservino di conseguenza poteri e facoltà in altri ambiti di esclusiva competenza dell'amministratore, a volte al di là e al di sopra del proprietario del dispositivo.

Assunzioni condivise tra le varie piattaforme portano a meccanismi di sicurezza simili e condivisi, pur con molte differenze e peculiarità, quali un uso consistente di ambienti virtuali per l'astrazione delle risorse e meccanismi di sandboxing delle applicazioni con una pronunciata separazione dei privilegi, una spinta verso lo sviluppo di codice managed, con la compilazione in linguaggi intermedi in ambiente Java e .NET per cercare di limitare alcuni problemi derivanti da errori di programmazione, l'esposizione esplicita delle risorse richieste da parte delle applicazioni e la loro imposizione a run time da parte del sistema, l'uso di protocolli di firma crittografica per garantire l'origine delle applicazioni installate e meccanismi per la loro installazione centralizzata.

In questo lavoro si analizzeranno i concetti di Confidenzialità, Integrità e Disponibilità in relazione alle caratteristiche di questi nuovi dispositivi ed ai sistemi operativi che essi impiegano, tenendo presente il panorama descritto.

1.2 Confidenzialità, Integrità e Disponibilità

L'analisi degli aspetti di sicurezza degli smartphone affrontata in questo lavoro è stata svolta tenendo in considerazione alcuni concetti fondamentali di sicurezza dei sistemi informatici. E' pertanto necessario introdurre brevemente tali concetti:

1.2.1 Confidenzialità

Un sistema che garantisce la confidenzialità è un sistema che assicura che le informazioni o le risorse in esso contenute siano protette dall'accesso non autorizzato. Tale sistema per garantire la confidenzialità deve essere protetto con meccanismi di controllo degli accessi che rendano impossibile per un soggetto non autorizzato la conoscenza delle informazioni o delle risorse o, a volte, della loro stessa esistenza.

1.2.2 Integrità

Garantire l'integrità di un sistema significa assicurare che dati o risorse di tale sistema non vengano modificate in modo non autorizzato o improprio. L'integrità riguarda sia il contenuto stesso delle informazioni, sia la loro origine. Mentre violazioni di confidenzialità compromettono esclusiva-

mente la segretezza di dati o risorse, quelle di integrità ne pregiudicano anche la correttezza e di conseguenza il grado di affidabilità.

1.2.3 Disponibilità

La proprietà di disponibilità di dati o risorse si riferisce alla garanzia della possibilità di utilizzare quei dati o risorse quando desiderato. La disponibilità è un aspetto cruciale dell'affidabilità ed è spesso necessario implementare meccanismi più o meno complessi per salvaguardare tale caratteristica.

1.3 Fattori di rischio

Verrà presentata un'analisi dei fattori di rischio riscontrabili negli smartphone classificandoli in base alle superfici d'attacco tipiche di questi dispositivi:

- Accesso fisico
- Connettività e Reti
- Terze Parti
- Applicazioni

2 Accesso fisico

Per minacce fisiche intendiamo tutti quei potenziali attacchi condotti attraverso un interfacciamento fisico al dispositivo e che dipendono da un accesso diretto.

A differenza di altri dispositivi gli smartphone sono per loro natura più esposti ad accessi diretti non autorizzati. Ciò è dovuto a varie ragioni ma in primis alla scarsa cura degli utenti. Ad esempio il sito CIO.com ha riportato che più di 31000 smartphone sono stati lasciati nei taxi di New York City in soli sei mesi.

Meccanismi di controllo degli accessi diretti non sono certo una novità introdotta dagli smartphone e sono tipicamente svolti da funzioni di bloccaggio/sbloccaggio del dispositivo attraverso l'inserimento di un Personal Identification Number (PIN) o segreti più complessi (ad esempio Windows Phone 7 consente di utilizzare una password ed Android il tocco di una sequenza di aree del display come in figura 2) conosciuti solo dal proprietario, si può quindi considerare una forma semplice di autenticazione.

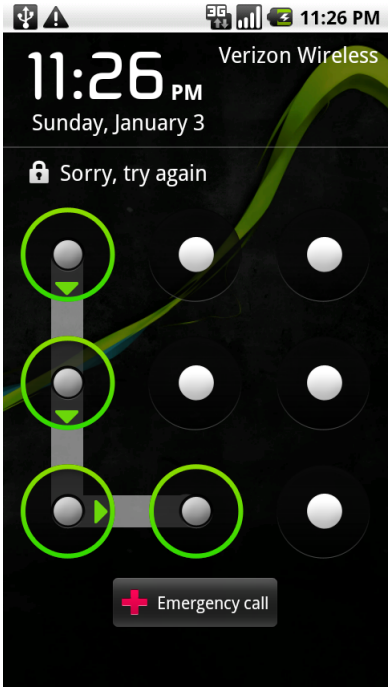

Figura 2: Schermata di sblocco di uno smartphone con Android OS

A questo livello di autenticazione ne è spesso affiancato un secondo gestito dal Subscriber Identity Module (SIM) ed è utilizzato per proteggere l'autenticazione dell'utente (Subscriber) alla rete. Anch'esso consiste in un PIN.

Sebbene un accesso a più basso livello potrebbe rendere queste contromisure inefficaci, la problematica principale è il fatto che solo il 18% degli utenti le utilizza nonostante sui desktop esse rappresentano una misura di sicurezza obbligatoria in molti ambiti dove gli accessi fisici occasionali sono molto probabili.

Molti smartphone moderni consentono l'espandibilità della memoria interna attraverso schede di memoria (tipicamente MicroSD) con capacità nell'ordine della decina di gigabyte. Su questi dispositivi di memoria possono essere conservate molte informazioni, spesso sensibili e con un diversi gradi di coscienza e controllo da parte dell'utente.

Queste schede impiegano spesso filesystem (tipicamente VFAT) che mancano delle caratteristiche di controllo dei permessi dei filesystem più complessi e una volta estratte dal dispositivo possono essere accedute da qualunque altro. Windows Phone adotta un approccio più drastico: formatta la scheda al primo inserimento con un formato proprietario e genera una chiave che associa la scheda permanentemente al telefono. Questo rende i dati su di

essa contenuti illegibili da qualunque altro dispositivo[20].

Oltre a costituire una potenziale minaccia per la confidenzialità, queste memorie lo sono anche per l'integrità. Ad esempio, alcune applicazioni browser mobili offrono la possibilità di conservare i segnalibri e la cronologia delle pagine web visitate sulla memoria esterna. In linea di principio non sarebbe troppo difficile estrarre la scheda e alterare queste informazioni per trarre in inganno l'utente ed indurlo a visitare pagine web contraffatte (Phishing) attraverso mezzi (i suoi segnalibri) che reputa affidabili.

Come per i computer tradizionali due soluzioni potrebbero essere adottabili: l'impiego della crittografia e di Intrusion Detection Systems (IDS) che rispettivamente prevengono e notificano attacchi all'integrità. Tuttavia l'applicabilità di questi strumenti potrebbe essere fortemente limitata a causa della spesso eccessiva necessità di risorse hardware per i dispositivi portatili. Tuttavia, questo aspetto potrebbe cambiare con l'evoluzione degli smartphone.

3 Connettività e Reti

Una delle caratteristiche principali degli smartphone è l'elevata connettività. Essi hanno la capacità di connettersi attraverso varie tipologie di reti con diverse tecnologie, tipicamente wireless.

Ciò espone questi terminali ad ulteriori rischi. E' utile suddividere in classi le reti a cui gli smartphone possono essere connessi: Wireless Wide Area Network (WWAN), Wireless Local Area Network(WLAN), Wireless Private Area Network (WPAN).

3.1 WWAN

Le infrastrutture WWAN comprendono diversi protocolli per reti senza fili su scala geografica o metropolitana tra cui il Global System for Mobile Communications (GSM) con le sue successive evoluzioni General Packet Radio Service (GPRS) e l'Universal Mobile Telecommunications System (UMTS)[1]

Attraverso di esse si può veicolare sia traffico voce che dati e quindi offrire accesso ad Internet su larga scala ed in mobilità. Le reti basate su GSM servono circa 1.5 miliardi di persone, è evidente che una attacco efficace su tale protocollo sarebbe di notevole gravità.

Come già accennato l'autenticazione su una rete GSM si basa sulla scheda SIM. In essa sono contenuti un International Mobile Subscriber Identity

[1]Un'altro protocollo per reti WWAN che sta conoscendo una certa diffusione è il Worldwide Interoperability for Microwave Access (WiMAX).

(IMSI) e una chiave simmetrica a 128-bit che non può essere estratta. Questi dati, in possesso anche dell'operatore vengono usati per superare una challenge.

La confidenzialità delle comunicazioni è affidata alla crittografia. L' algoritmo di criptaggio A5/1, sviluppato nel 1987 ed impiegato nel corso dei venti anni di operatività di GSM è riuscito a rimanere segreto fino al 1999[3]. In seguito sono state individuate delle vulnerabilità che potrebbero consentire di attaccare la segretezza delle comunicazioni. Allo stato attuale la possibilità di portare a termine tali attacchi dipende dalle capacità economiche e tecniche dell'attaccante. Tuttavia successive ricerche hanno reso questa possibilità ancor più concreta diminuendo la complessità computazionale delle procedure d'attacco [4][11]. Vulnerabilità sono state individuate anche nella successiva implementazione dell'algoritmo A5/3 utilizzato in UMTS e GPRS.

Ciò significa che le comunicazioni via GSM non sono intrinsecamente del tutto sicure sebbene la complessità delle tecniche di attacco rende la possibilità di subire un attacco remota.

Poiché, come si è accennato, le reti WWAN consentono l'accesso ad Internet da esse dipende una grande esposizione a quelle problematiche di sicurezza tipiche delle comunicazioni a più alto livello che affliggono terminali più tradizionali come ad esempio IP o DNS Spoofing.

3.2 WLAN

Le tecnologie WLAN sono ormai estremamente diffuse in ambiti sia domestici che enterprise. Le reti WLAN impiegano tipicamente gli standard IEEE 802.11a/b/g/n che consentono il collegamento ad una vasta gamma di dispositivi e l'interoperabilità con LAN Ethernet.

Come per le WWAN le minacce principali derivano dal fatto che il mezzo trasmissivo è condiviso. Per garantire la confidenzialità le reti WLAN possono impiegare algoritmi crittografici. Tuttavia, utilizzando dispositivi mobili come gli smartphone è molto comune entrare in contatto con reti non adeguatamente protette in luoghi pubblici e non.

In questi casi è molto semplice per un attaccante poter osservare tutto il traffico sulla rete tramite programmi di sniffing alla portata di tutti.

I primi algoritmi crittografici usati nelle reti Wi-Fi, Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA) hanno dimostrato di essere vulnerabili ed oggi sono disponibili intere suite di programmi[1] che ne consentono l'aggiramento in tempi nell'ordine delle ore.

La successiva revisione (IEEE 802.11i-2004) WPA2 in congiunzione con meccanismi di autenticazione 802.1X EAP/RADIUS è l'unico meccanismo ritenuto adeguato per garantire autenticazione e confidenzialità su reti WLAN.

Proprio come gli host in una normale LAN, gli smartphone possono essere soggetti a tutti gli attacchi tipici delle reti Ethernet e TCP/IP come DHCP e ARP Spoofing, DoS, Attacchi a livello applicazione. Queste tipologie d'attacco sono mitigate dalla presenza di firewall sugli host.

Sia su iPhone che su Android esistono alcune applicazioni che consentono di filtrare il traffico ma solo a livello TCP/IP, mentre RIM ha un firewall integrato nel sistema operativo dei BlackBerry anch'esso con capacità limitate.

Allo stato attuale l'unica possiblità concreta di avere firewall con tutte le funzionalità è offerta dai telefoni Linux-based con la possibilità di utilizzare il firewall Netfilter integrato nel kernel Linux. Tuttavia questo richiede un accesso con elevati privileggi al dispositivo che è generalmente disabilitato. Per Android esiste anche un applicazione frontend per Netfilter.

3.3 WPAN

Le Personal Area Network sono reti che consentono la connessione dei dispositivi presenti nello spazio di lavoro di un individuo, generalmente unico proprietario, in un raggio che raramente supera la decina di metri. Spesso le tecnologie utilizzate sono di tipo Wireless come Bluetooth (Standardizzato in IEEE 802.15.1) o Infrared Data Association (IrDA) e più recentemente Ultra-wideband (UWB) (IEEE 802.15.3) tra cui il Wireless USB (WUSB). La più diffusa di queste tecnologie è sicuramente Bluetooth che, sebbene considerata sicura in molti ambiti, ha dimostrato di possedere non poche vulnerabilità a Malware e attacchi di confidenzialità [6].

4 Terze Parti

Un'altra caratteristica degli smartphone è la necessità di utilizzare servizi offerti da terze parti per usufruire di servzi che stanno assumendo un ruolo sempre più importante nel trattamento di informazioni riservate o personali. Sebbene questa problematica non coinvolge solo gli utenti di smartphone, su di essi ha effetti molto più profondi. Infatti, molto spesso, per utilizzare tutte le funzionalità che uno smartphone ha da offrire è necessario fare appello alla fiducia che un utente è disposto a concedere: è necessario che l'utente si fidi di tutti gli intermediari che cooperano alla fornitura dei servizi.

Ad esempio, RIM offre servizi per accedere alle proprie informazioni personali come mail, calendario, contatti ecc. con l'ausilio di una infrastruttura di sua proprietà. In particolare la soluzione BlackBerry Enterprise Service mostrata in figura 3 si integra nel sistema aziendale e permette di invia-

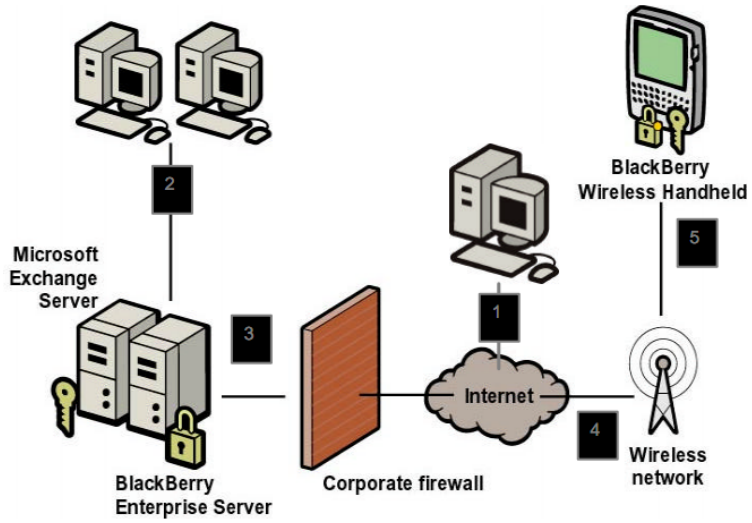

Figura 3: Architettura di BlackBerry Enterprise Service

re e ricevere email attraverso un server interposto tra il server POP/IMAP aziendale e la rete cellulare: la casella mail dell'utente viene monitorata dalla componente BlackBerry Enterprise Server (BES) e i messaggi, criptati con AES o Triple-DES (le cui chiavi non sono sotto il controllo di RIM), vengono inviati ad un server di proprietà di RIM che poi effettuerà la consegna sul dispositivo mobile. Nel caso di utenti privati che non possiedono una infrastruttura IT complessa essi possono utilizzare il servizio BlackBerry Internet Service. A differenza del precedente il BES è tipicamente gestito dalla compagnia telefonica di cui l'utente è cliente. Ciò impone di consegnare le credenziali d'accesso alla propria casella di posta elettronica al gestore della rete cellulare. Ciò pone delle serie questioni di fiducia tra gli utenti e la compagnia telefonica.

Nel 2009 due compagnie statali degli Emirati Arabi Uniti si sono rese protagoniste di una controversia con RIM e gli utenti di BlackBerry (circa 145.000 negli Emirati). A causa delle forti tecniche crittografiche impiegate da RIM, l'Autorità per le Telecomunicazioni degli Emirati Arabi ha minacciato di bandire l'uso di BlackBerry dal proprio territorio di giurisdizione. In seguito le due compagnie statali hanno rilasciato un "update" per i terminali BlackBerry che si è poi rivelata essere uno spyware. L'update, una volta installata avrebbe permesso alle compagnie telefoniche di accedere ai messaggi in chiaro.

Affidarsi a servizi di terze parti per la gestione dei propri dati personali chiama in causa non solo la garanzia di confidenzialità ma anche quella della disponiblità. Poiché l'utilizzo dei servizi è spesso su base gratuita e regolato

Figura 4: Il messaggio con cui il team di GMail comunicò i problemi che si stavano verificando.

da un contratto redatto unilateralmente che l'utente sottoscrive, eventuali disservizi non possono essere esclusi[2] e le responsabilità per i danni derivanti da essi non possono essere ascritte ai fornitori. Ad esempio sono rimasti famoso nell'immaginario collettivo della rete i down-time del 24 Febbraio e 2 Settembre 2009 del servizio di GMail di Google durati qualche ora.

Vi sono altre problematiche come il data lock-in e l'effettiva capacità di garantire confidenzialità, integrità ed adeguati livelli di disponibilità sono molto attuali e riguardano molti aspetti che esulano dallo scopo di questo lavoro.

5 Applicazioni

5.1 Problematiche

La disponibilità di numerosi giochi e applicazioni e la facilità di accesso ad essi è uno dei principali campi di battaglia tra i principali operatori del settore e costituisce uno dei servizi più pubblicizzati e richiesti dal mercato. Non stupisce quindi che l'installazione e l'esecuzione di applicazioni costituisca in varie forme una importante superficie di attacco per i sistemi di comunicazione mobile.

I problemi relativi alla sicurezza derivanti dall'installazione di applicazioni si possono genericamente suddividere in tre categorie: malware, problemi derivanti da bug ed errori di programmazione e problemi derivanti da applicazioni che diffondono involontariamente informazioni potenzialmente riservate per una progettazione poco attenta ai problemi di sicurezza.

[2]Sebbene è comunque interesse del prestatore di servizio mantenere alta la disponibilità per evitare danni d'immagine

5.1.1 Malware

Applicazioni di tipo malware minacciano con dolo di mettere a repentaglio la sicurezza del sistema in vari modi, attaccando la confidenzialità e l'integrità delle comunicazioni o delle informazioni presenti nel dispositivo o la disponibilità di particolari servizi o dell'intera dispositivo con il suo blocco. Dato l'utilizzo di servizi a costo tipici della telefonia e le prospettive di espansione di servizi per il "*mobile payment*" un attacco eseguito con successo può avere anche immediate ripercussioni economiche. Infine un terminale compromesso può essere usato come testa di ponte per la compromissione di altri dispositivi, attraverso la rete o meccanismi di sincronizzazione anche con altre classi di dispositivi o reti di comunicazione.

Le seguenti categorie di attacchi malware possono essere identificate:[17]

Spoofing. Il programma malware fornisce false informazioni all'utente per spingerlo a scelte e decisioni che incidono sulla sicurezza del dispositivo.

Intercettamento o accesso ai dati. Il programma malware riesce ad intercettare ed accedere ai dati presenti nel dispositivo.

Data Theft. Il programma riesce a raccogliere e far filtrare esternamente al dispositivo i dati raccolti.

Backdoor. Il programma offre funzionalità che permettono ad un attaccante di ottenere accesso al dispositivo in un secondo momento.

Abuso dei servizi. Il programma riesce a compiere azioni che comportano un costo finanziario per l'utente.

Disponibilità. La disponibilità o l'integrità del dispositivo o dei dati che risiedono nel dispositivo viene compromessa.

Accesso alla rete. Il programma usa il dispositivo per comunicazioni di rete non autorizzate.

Wormable. Il programma riesce a replicarsi semi-autonomamente su altri dispositivi.

Fino a questo momento gli attacchi a smartphone e dispositivi simili sono stati limitati a confronto con quelli relativi ad altri dispositivi consumer come desktop e portatili. Risorse hardware limitate sono state un limite sia per l'attacco che per la difesa, in particolare il modello d'uso di botnet per spam, denial of service a scopo di estorsione, furto di dati e phishing sembra

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

di scarsa appetibilità data la necessità di avere linee dati veloci e stabili e adeguate risorse hardware, anche se la rete telefonica cellulare sembra essere particolarmente vulnerabile ad attacchi DDOS.[15, 22] Data l'appetibilità di questi dispositivi per attacchi mirati e furto di personalità e l'esplosione che il mercato sta avendo ci si aspetta comunque inevitabilmente un aumento nel numero e nella gravità di attacchi a queste piattaforme.

5.1.2 Bug

Bug nelle applicazioni installate possono mettere a repentaglio la sicurezza del terminale. Un esempio recente è stata la scoperta di una importante vulnerabilità all'attivazione da parte di Google di una interfaccia web al Market per l'installazione di applicazioni Android. E' presto emerso un problema di *cross-site scripting* o *XSS* in cui c'era la possibilità di inserire codice javascript nella descrizione delle applicazioni in modo da innescare l'installazione via browser, anche remota, di applicazioni sul terminale Android di utenti collegati allo store.[13]

Data la mancanza di una conferma obbligatoria sul terminale alla richiesta di installazione quest'ultima può essere forzata dall'attaccate con una semplice procedura POST AJAX all'URI di installazione:

Come si può vedere in fig. 5 nella pagina seguente e in fig. 6 nella pagina successiva per l'esecuzione dell'attacco è sufficiente poi inserire lo script nella form di descrizione dell'applicazione del Market.

5.1.3 *Leaking* di dati

Un tipo più subdolo di bug è quello in cui il problema non è di tipo implementativo, ma deriva da una progettazione non particolarmente attenta alle problematiche di sicurezza. Sicurezza ed usabilità sono spesso in conflitto, non sempre si riesce a comunicare in modo adeguato i rischi di sicurezza e privacy all'utente e le interfacce non sono in molti casi adeguate.[23] Lo sviluppo di applicazioni sicure può essere inoltre costoso in termini di tempo e

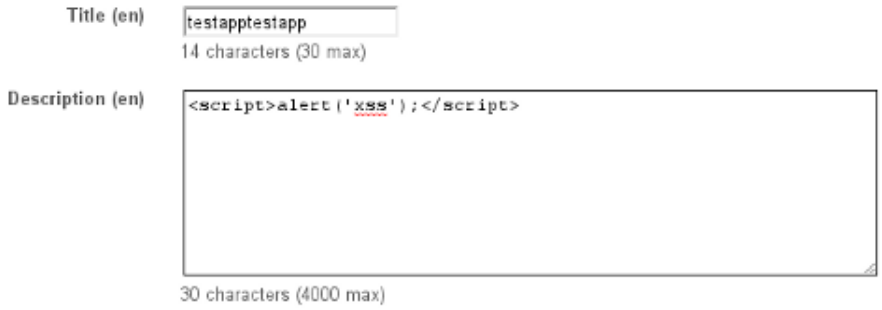

Figura 5: Cross-site scripting, inserimento dello script nella descrizione dell'applicazione

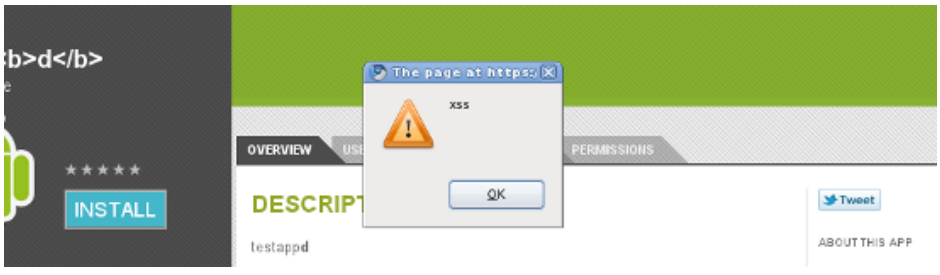

Figura 6: Cross-site scripting, esecuzione

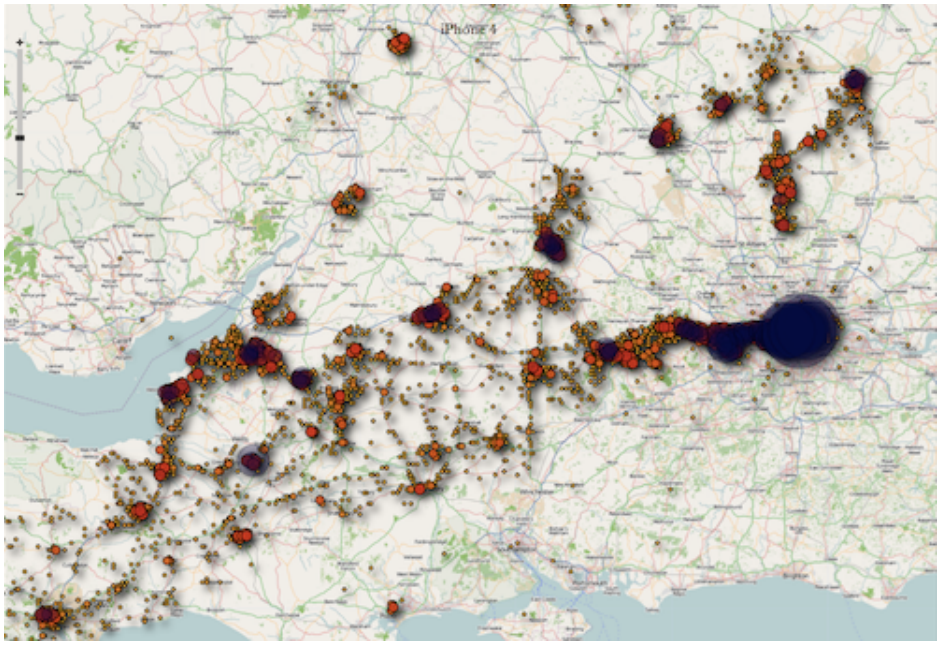

Figura 7: iPhone Tracker mostra i movimenti registrati su iOS 4.0

sforzo e se lo sviluppatore dell'applicazione non presta particolare attenzione alle regole e best practice dell'ambiente per cui programma può involontariamente causare problemi e compromettere la sicurezza del dispositivo e dei dati presenti, ad esempio salvando dati riservati in aree di memoria condivise con altre applicazioni o memorizzando dati non più necessari. Un recente problema di questo tipo è venuto alla luce con la scoperta di un file di log su dispositivi Apple con sistema iOS versione 4.0 contenente una serie di coordinate geografiche e timestamp. I dati, in chiaro e derivanti probabilmente tramite triangolazione con antenne GSM, sono aggiornati con regolarità e documentano, anche se non sempre con esattezza, la posizione del terminale anche quando non sono attivi i servizi di localizzazione.

Anche se non pone un immediato problema di sicurezza (il file non è accessibile da applicazioni di terze parti e i dati non vengono trasferiti) l'esistenza stessa di questi record espone a gravi problemi di confidenzialità e crea nuove ed impreviste superfici di attacco. Come mostrato dal programma iPhone Tracker in fig. 7 si può comunque accedere ai dati connettendo il terminale a un computer.[18]

5.2 Contromisure

Non potendo riporre completa fiducia nelle applicazioni che gli utenti andranno ad installare numerose misure di sicurezza sono prese all'insegna di un generale principio di isolamento delle applicazioni per una difesa in profondità. Alcune misure di mitigazione dei danni possono inoltre essere intraprese una volta accertata una violazione della sicurezza.

5.2.1 Macchine virtuali

L'uso di macchine virtuali oltre a garantire un certo grado di portabilità si presta facilmente ad essere sfruttato per la costruzione di sandbox naturali per le applicazioni. Nei sistemi Android ad esempio ogni applicazione viene eseguita in una separata macchina virtuale Java, limitando fortemente possibili canali di comunicazione tra le applicazioni al di fuori del modello di sicurezza scelto e rendendo possibili controlli a tempo di esecuzione sull'uso non autorizzato delle risorse hardware del terminale.

Quando l'uso di macchine virtuali si accompagna ad ambienti di sviluppo quali Java e .NET si gode inoltre di protezione verso alcune classi tipiche di bug (es. buffer overflow) che possono influenzare in modo negativo la sicurezza.

5.2.2 Permessi

I permessi che regolano l'accesso al file system nei sistemi operativi multiutente possono essere riadattati come misura di non interferenza e isolamento tra le applicazioni nell'accesso alle risorse su file. Mentre nei sistemi operativi tradizionali *User Id* e *Group Id* sono associati agli utenti del sistema nei sistemi mobile che ne fanno uso vengono generati in modo specifico per ogni applicazione al momento della sua installazione [7, 21]

5.2.3 Capabilities

Mentre i permessi regolano l'accesso alle risorse nel file system i meccanismi di capabilities regolano l'accesso da parte delle applicazioni a specifiche API (Application Programming Interface) del sistema operativo che permettono alle applicazioni l'uso di determinati sottosistemi come l'accesso alla rete, la possibilità di effettuare telefonate o l'accesso ai contatti presenti nel telefono. Le capabilities necessarie all'applicazione vengono definite da parte dello sviluppatore e possono essere esplicitate all'utente in fase di installazione per la sua approvazione (fig. 8 nella pagina successiva).[7, 12]

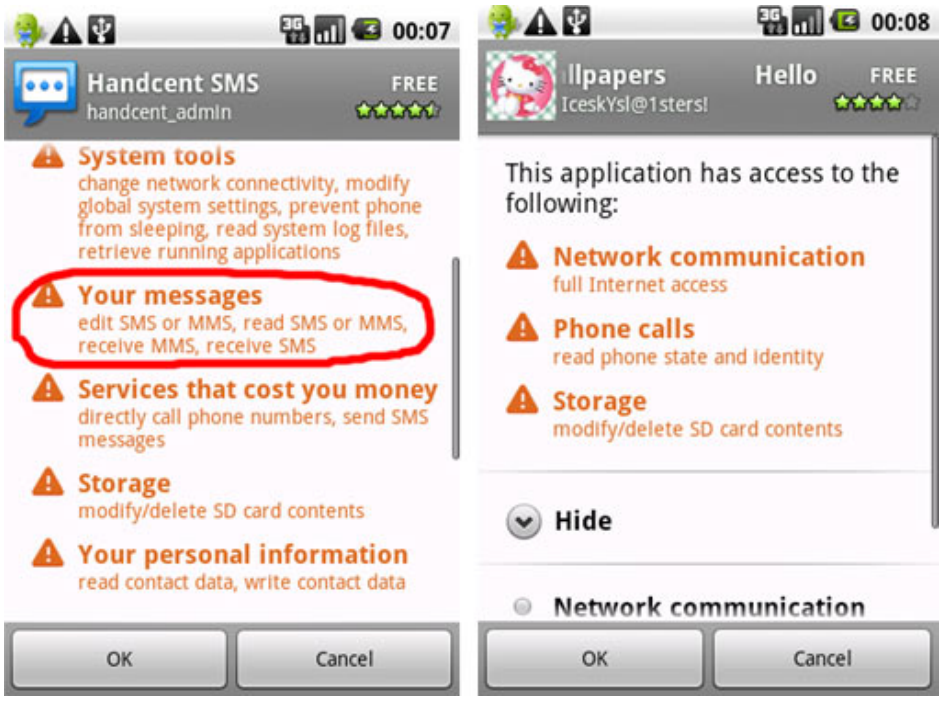

Figura 8: Android, valutazione delle capabilities richieste a momento di installazione

Nonostante l'utente finale sia il soggetto che ha potenzialmente le migliori informazioni per fare una scelta informata numerosi studi hanno evidenziato difficoltà nella valutazione dei potenziali rischi e conseguenze.[9, 5]

5.2.4 Canali di comunicazione

Per quanto arduo sia valutare ed implementare meccanismi di sicurezza al livello della singola applicazione il compito si rivela molto più difficile quando si prende in considerazione i possibili comportamenti emergenti derivanti dalle interazioni tra diverse applicazioni. Allo scopo di limitare possibili effetti indesiderati molti sistemi cercano di limitare i canali di comunicazione tra le applicazioni a meccanismi ben definiti e controllati dal sistema operativo (come il richiamo di activities esterne nei sistemi Android) o di eliminarli tout-court come nel caso di sistemi Windows Phone 7 dove non è previsto a questo scopo l'uso di aree condivise di memoria (in Windows Phone 7, quando presenti, le memorie di tipo esterno, come già specificato in 2, vengono integrate nel file system interno e legate tramite crittografia allo specifico dispositivo) e la condivisione di dati viene implementata solamente tramite l'accesso a servizi cloud.[20, 21]

5.2.5 Installazione centralizzata

L'origine delle applicazioni può essere un indicatore sull'affidabilità delle stesse. Store centralizzati per la ricerca e installazione delle applicazioni sono presenti in molti sistemi per questo motivo oltre che per scopi commerciali e di controllo della piattaforma . L'accesso da parte degli sviluppatori viene controllato con policies diverse da piattaforma a piattaforma, tipicamente il fornitore del servizio si riserva una valutazione sui contenuti dell'applicazione oltre che sulla sua legalità, facendosi in qualche modo garante per le applicazioni distribuite.

In alcuni sistemi (iOS) non è possibile per l'utente finale installare applicazioni al di fuori dello store centralizzato, nei sistemi come Android dove invece è possibile per l'utente installare applicazioni anche da terze parti, vi è una maggiore attenzione all'affidabilità e la reputazione del singolo sviluppatore.

5.2.6 Firma digitale

Misure come l'installazione centralizzata e l'esplicitazione delle capabilities sono di scarso conforto se l'applicazione può venire modificata da terzi prima della sua installazione sul dispositivo dell'utente. Molti sistemi richiedo quindi forme di firma digitale dei pacchetti di installazione a garanzia della loro origine e della loro integrità durante i processi di distribuzione e installazione. Alla firma digitale da parte dello sviluppatore viene affiancata una firma da parte del distributore nei sistemi che prevedono la distribuzione centralizzata delle applicazioni.

5.2.7 Analisi remota

Classici meccanismi di difesa tipici dei personal computer come i programmi antivirus richiedono risorse e potenza non sempre presenti in misura adeguata nei terminali mobili e un controllo a real time del dispositivo implica un consumo di batteria che limita fortemente il loro utilizzo attuale. Si è proposto di spostare la complessità del riconoscimento di malware dal terminale verso servizi esterni allo scopo di migliorarne prestazioni e scalabilità. [16, 19]

L'uso di macchine virtuali permetterebbe l'esecuzione di un numero molto elevato di repliche di dispositivi su server consentendo l'uso di tecniche di individuazione di malware a livello centralizzato.[14]

5.2.8 Black list e kill switch

Una volta accertata una violazione di sicurezza del sistema derivante da applicazioni alcune misure di sicurezza possono essere usate a posteriori per interrompere la violazione e limitarne per quanto possibile ulteriori effetti dannosi. Sistemi che dispongono di un controllo centralizzato delle applicazioni installate prevedono procedure di "kill switch", disinstallazione forzata da remoto delle applicazioni, con successiva rimozione dallo store delle applicazioni e riconoscimento futuro tramite una black list di applicazioni dannose riconosciute.

Procedure di wipe (cancellazione) e brick (disattivazione) remote dei dispositivi sono supportate in modo ufficiale in ambiente Black Berry per clienti corporate allo scopo di contrastare perdite di dati dovute a smarrimento o furto del dispositivo.

6 Conclusioni

Come abbiamo visto servizi sempre nuovi, l'aumento delle prestazioni, profili e necessità profondamente diverse tra utenti "consumer" e aziendali rendono difficile individuare regole e best practice condivisibili da tutti ed è richiesta la collaborazione tra molti attori diversi, l'utente stesso, i fornitori della piattaforma e quelli di servizi e terze parti, carrier, amministratori di reti e sviluppatori di applicazioni per la sicurezza finale dell'utente.

Gli smartphone, che accoppiano una rapida espansione nel mercato che li proietterà presto ad essere la principale piattaforma per l'accesso a internet alle caratteristiche "personali" dei telefoni cellulari, presentano sfide nuove che richiedono per essere affrontate adattamento e innovazione.

Come si è visto vi è già molta attenzione riguardo alle problematiche elencate e descritte in questo lavoro.

Riferimenti bibliografici

[1] *Aircrack-ng web site*. URL: `http://www.aircrack-ng.org/`.

[2] L Banks. *Mobile devices pose security dilemma for CIOs*. 2010. URL: `http://www.cio.com.au/article/346474/mobile_devices_pose_security_dilemma_cios/`.

[3] M. Briceno, I. Goldberg e D. Wagner. "A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms". In: *Available on-line at http://www. cryptome. org/gsm-a512. htm* (1998).

[4] F. van den Broek. “Eavesdropping on GSM: state-of-affairs”. In: (2011).

[5] L.F. Cranor, S. Garfinkel e Safari Tech Books Online. *Security and usability: Designing secure systems that people can use*. O’Reilly, 2005. ISBN: 0596008279.

[6] J.P. Dunning. “Taming the Blue Beast: A Survey of Bluetooth Based Threats”. In: *Security & Privacy, IEEE* 8.2 (2010), pp. 20–27.

[7] Google. *Android security and permissions*. 2011. URL: `http://code.google.com/android/devel/security.html`.

[8] W. Jansen e K. Scarfone. “Guidelines on cell phone and pda security”. In: *NIST Special Publication* 800 (2008), p. 124.

[9] L. Jedrzejczyk et al. “I Know What You Did Last Summer: risks of location data leakage in mobile and social computing”. In: *Department of Computing Faculty of Mathematics, Computing and Technology The Open University* (2009).

[10] Kari Kostiainen et al. “Old, new, borrowed, blue –: a perspective on the evolution of mobile platform security architectures”. In: *Proceedings of the first ACM conference on Data and application security and privacy*. CODASPY ’11. San Antonio, TX, USA: ACM, 2011, pp. 13–24. ISBN: 978-1-4503-0466-5. DOI: `http://doi.acm.org/10.1145/1943513.1943517`. URL: `http://doi.acm.org/10.1145/1943513.1943517`.

[11] M. Landman. “Managing smart phone security risks”. In: *2010 Information Security Curriculum Development Conference*. ACM. 2010, pp. 145–155.

[12] Lei Liu et al. “Exploitation and threat analysis of open mobile devices”. In: *Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*. ANCS ’09. Princeton, New Jersey: ACM, 2009, pp. 20–29. ISBN: 978-1-60558-630-4. DOI: `http://doi.acm.org/10.1145/1882486.1882493`. URL: `http://doi.acm.org/10.1145/1882486.1882493`.

[13] J. Oberheide. *How I Almost Won Pwn2Own via XSS*. 2011. URL: `http://jon.oberheide.org/blog/2011/03/07/how-i-almost-won-pwn2own-via-xss/`.

[14] J. Oberheide, E. Cooke e F. Jahanian. “Cloudav: N-version antivirus in the network cloud”. In: *Proceedings of the 17th conference on Security symposium*. USENIX Association. 2008, pp. 91–106.

[15] J. Oberheide e F. Jahanian. “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments”. In: *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. ACM. 2010, pp. 43–48.

[16] J. Oberheide et al. “Virtualized in-cloud security services for mobile devices”. In: *Proceedings of the First Workshop on Virtualization in Mobile Computing*. Citeseer. 2008, pp. 31–35.

[17] J. O’Connor. “Attack surface analysis of Blackberry devices”. In: *White Paper: Symantec security response* (2007).

[18] Warden P. e Allan A. *iPhone Tracker*. 2011. URL: http://petewarden.github.com/iPhoneTracker/.

[19] Georgios Portokalidis et al. “Paranoid Android: versatile protection for smartphones”. In: *Proceedings of the 26th Annual Computer Security Applications Conference*. ACSAC ’10. Austin, Texas: ACM, 2010, pp. 347–356. ISBN: 978-1-4503-0133-6. DOI: http://doi.acm.org/10.1145/1920261.1920313. URL: http://doi.acm.org/10.1145/1920261.1920313.

[20] Microsoft Support. *Limitazioni della scheda Secure Digital di Windows Phone 7*. URL: http://support.microsoft.com/kb/2450831.

[21] Microsoft Support. *Windows Phone 7 security model*. 2010. URL: http://download.microsoft.com/download/9/3/5/93565816-AD4E-4448-B49B-457D07ABB991/Windows%20Phone%207%20Security%20Model_FINAL_122010.pdf.

[22] Patrick Traynor et al. “On cellular botnets: measuring the impact of malicious devices on a cellular network core”. In: *Proceedings of the 16th ACM conference on Computer and communications security*. CCS ’09. Chicago, Illinois, USA: ACM, 2009, pp. 223–234. ISBN: 978-1-60558-894-0. DOI: http://doi.acm.org/10.1145/1653662.1653690. URL: http://doi.acm.org/10.1145/1653662.1653690.

[23] A. Whitten e JD Tygar. “Why Johnny can’t encrypt”. In: *USENIX Security*. Vol. 1999. 1999, p. 1.