

Mobile: Security & privacy

Paranoia in movimento

Alfredo Morresi (aka Legolas)

<http://www.rainbowbreeze.it>

23/08/2008 – Pescara



Perche' il mobile e' in ascesa

- Popolo di nomadi con dati distribuiti
- Internet of things, realta' distribuite e interconnesse
- Ubiquita' dei dati e dei servizi
- Fa comodo nell'enterprise che nel consumer
- Medicina, commerciale, agenti, tecnici sono ambiti dove la mobilita' e' cruciale
- fa f1k0 (caso Blackberry)



Layer di attacco - device

Perdita dei device: 250k PDA persi (Gartner, 2001); Chicago, in sei mesi, smarriti 85k telefoni cellulari, 21k Pda e 4k laptop (CheckPoint, 2007). Ognuno con dati relativi a chi li a smarriti, colleghi, clienti, fornitori e partner.

Memory card con molti dati sensibili che si possono sottrarre facilmente

Password memorizzate dato che scriverle e' difficile

Facile accesso fisico al device (sottrazione dati)



Layer di attacco - comunicazione

WiFi: sniffing, fake access point, wifi honeypot

Bluetooth: accesso non autorizzato ai servizi, exploit per prendere dati sensibili, utilizzo non autorizzato del dispositivo, tracking del device

GSM: caso Wind nel 2006



Layer di attacco - servizi

Autorizzazione accesso utente, installazione ed esecuzione applicazioni (virus, malware, programmi non autorizzati)

VoIP abilitato in diversi device "business" senza adeguate protezioni

Configurazioni di default opinabili

Restrizioni in ROM da parte degli operatori



Best practices

La rete aziendale cambia morfologia, diventa mutevole: necessario adattamento!

Implementare un firewall sul device

Confidentiality, integrity, authentication a livello di device, service, application

Controllo di chi accede al device e ai dati in esso contenuti: PIN / Password / fingerprint su standby o temporizzabili



Best practices

Uso della crittografia per i dati nel device e per il traffico da esso generato: VPN, SSL, WiFi

Policy per l'installazione e l'esecuzione dei programmi nel device: privileged, normal, blocked

Gestione di virus, malware, allegati, MMS

Applicazione di mobile security policy aziendali

Secure wiping dei dati dopo diversi accessi negato e hard reset dello stesso



Best practices

Rintracciabilità del device una volta rubato:
GPS, CellID, magari direttamente su ROM
(Mobile Justice, Phone Guardian)

Digital certificate per personal, application e
network authentication



Anti best practices

Livello di complessita' delle BP da adottare:
l'utente medio usa il device solo come un elettrodomestico, un tramite per raggiungere un servizio

Accesso al device veloce e in modalita' disconnessa.

Costo dell'implementazione delle BP

Impossibilita' di implementazioni a livello di SO di alcune BP



Anti best practices

ROM personalizzate dagli operatori in diversi smartphone

Symbian e WM ROM non personalizzabili

Scambio di device aziendali uguali

Privilegi della sessione del device: root! =:-|

**COMPROMESSO TRA CONSUMER ED
ENTERPRISE!**



Sistemi operativi

Attualmente sul mercato:

- Symbian
- Windows Mobile
- Linux (OpenMoko, Android, ecc)
- iPhone



Sistemi Operativi - Symbian

Primo nel Modello a certificati nell'installazione delle applicazioni

Ampia diffusione del S.O. e SDK gratuito generano ampia disponibilita' di programmi a basso livello

Nokia Network Security Management



Sistemi Operativi – Windows Mobile

- Encryption della storage card on-the-fly
- Exchange Server 2007 con Windows Mobile 6 oppure WM5 & Local Authentication Plugins:
- Propagazione delle security policy aziendali (pwd strength, lenght, history, expiration, patterns ecc)
- Wiping dei dati personalizzabile
- Riconoscimento di impronte digitali



Sistemi Operativi - GNU/Linux

Tutto quello che gia' conoscete:

- Kernel path
- Disk encryption
- 1000mila programmi per queste cose

PERO'

ancora nulla out-of-the-box ed enterprise ready (minima diffusione dei device con Linux)



Sistemi Operativi - iPhone

Ken Dulaney (Gartner, 2007): "We're telling IT executives to not support it because Apple has no intentions of supporting (iPhone use in) the enterprise. This is basically a cellular iPod with some other capabilities and it's important that it be recognized as such." - No firewall, no wipe, no Exchange, no Lotus Notes

iPhone Metasploit attack: default root shell

iPhone 3G con modello distributivo del software



Divagazioni: in the beginning was Cabir...

2004: nasce il primo virus per mobile, EPOC.Cabir (Symbian, diffusione via BT). Poi WinCE.Dust (Pocket PC)

2004: Exploit dell'autorun per WM 2003

2006: Crossover, dal PC al device mobile WM

2007: exploit per iPhone

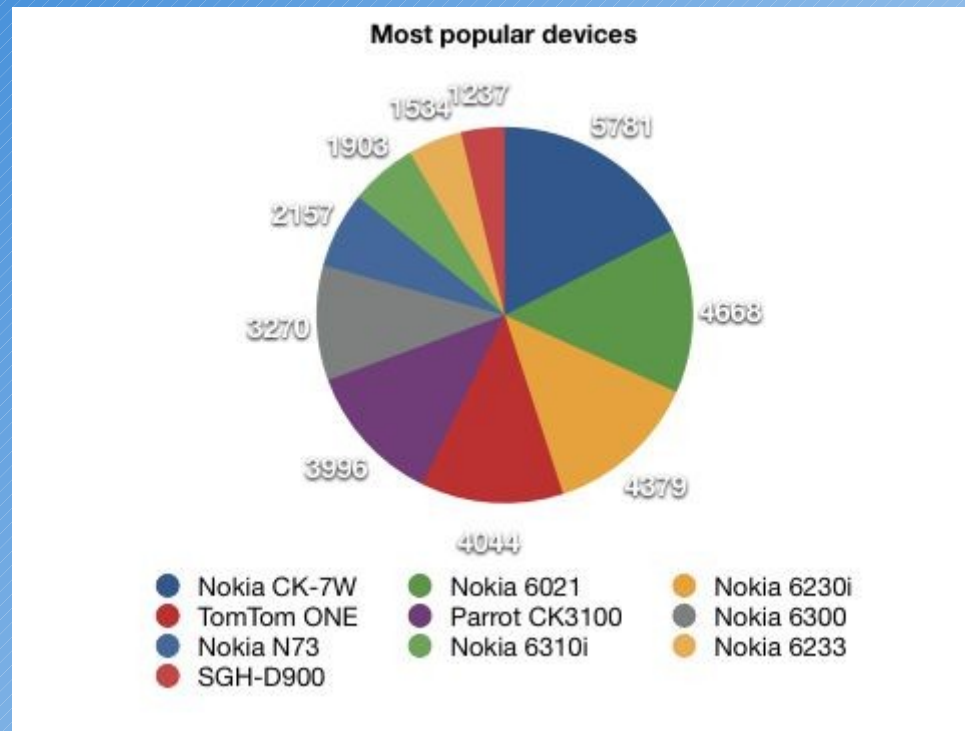
2008: 350 virus per mobile dichiarati (??)



Divagazioni: Bluetooth Tracking

Set 2007: Accese 5 antenne BT da 100 m di range in un'area urbana Olandese

Ago 2008: 219,886 device unici tracciati



Divagazioni: Spying Device

Rimpiazzare la ROM standard con una modificata ad arte

- assolutamente non visibili all'utilizzatore
- controllo SMS, MMS, phonebook, log eventi
- uso del device per remote spy
- tracking del device
- Nokia e pochi altri device

Software tipo backdoor che fa le stesse cose (Mobile Spy)



Momento maieutico

Idee sul mobile hacking



Linkografia

<http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39156887,00.htm>

<http://bluetoothtracking.org/>

<http://www.mobilecomputermag.co.uk/20071126174/anti-virus-firms-offer-protection-for-mobile-devices.html>

<http://blogs.s60.com/mobilesecurity/>

<http://www.networkworld.com/news/2007/061907-apple-iphone-gartner.html>

<http://blog.metasploit.com/2007/09/root-shell-in-my-pocket-and-maybe-yours.html>

<http://www.securityevaluators.com/iphone/bh07.pdf>

...e molti altri...



Questo documento è rilasciato sotto licenza Creative Commons Attribuzione-Non commerciale-Condividi allo stesso modo 2.5 Italia License

