Mobilita', Energy Awareness, Telefoni Programmabili: la Rivoluzione della Sicurezza Informatica

Mauro Migliardi e Alessio Merlo

1 Introduzione

La sicurezza è, da sempre, uno degli aspetti critici e fondamentali nella progettazione e costruzione dei sistemi informatici. Storicamente, il modello di riferimento per i sistemi di sicurezza è stato quello che si riferiva metaforicamente alle fortezze medioevali, ovvero uno in cui un insieme di strutture difensive posizionate staticamente tra le informazioni da proteggere ed il resto del mondo permetteva di controllare chi e come accedesse a quelle stesse informazioni.

Un primo cambiamento epocale per questo modello si è certamente verificato in passato con l'avvento di Internet; tuttavia, oggi la sicurezza informatica si trova ad affrontare una nuova e probabilmente ancora più impegnativa sfida. Alla base di questa nuova sfida si possono identificare tre fattori fondamentali. Il primo è la mobilità dei punti di accesso; ogni modello di difesa perimetrale, siano essi firewall, IDS o quant'altro, è messo completamente in crisi dalla possibilità di trasportare facilmente all'interno di ogni linea di difesa un sistema che può sia facilmente interconnettere le reti interne con quelle pubbliche, sia rappresentare un vettore di "infezione". Un secondo aspetto è dato dalla crescente dipendenza delle pratiche quotidiane di lavoro da strumenti informatici mobili come smartphones e tablet PC; questi dispositivi, infatti, avendo una capacità energetica intrinsecamente limitata, forniscono una sfaccettatura per la loro superficie d'attacco che gli strumenti correnti non sono pronti a difendere adeguatamente. Infine, un ultimo, ma non meno significativo aspetto, è dato dalla natura ibrida, tra telefono e computer, dei nuovi smartphones e dal fatto che essi convivono con una rete nata per dispositivi "stupidi". La diffusione di questi telefoni intelligenti, infatti, mette in contatto l'infrastruttura di rete telefonica con dispositivi anche di notevole capacità computazionale e capaci di essere controllati a distanza da entità malevole fornendo quindi la possibilità di realizzare campagne di attacco nei confronti della rete telefonica impensabili sino a pochi anni fa.

In questo articolo vogliamo analizzare questi recenti aspetti dell'evoluzione informatica nella loro capacità di rivoluzionare i modelli della sicurezza e discutere come la comunità scientifica si stia dedicando ad adeguare le nostre conoscenze ed a produrre strumenti per evitare di essere sorpresi dalla rivoluzione in atto.

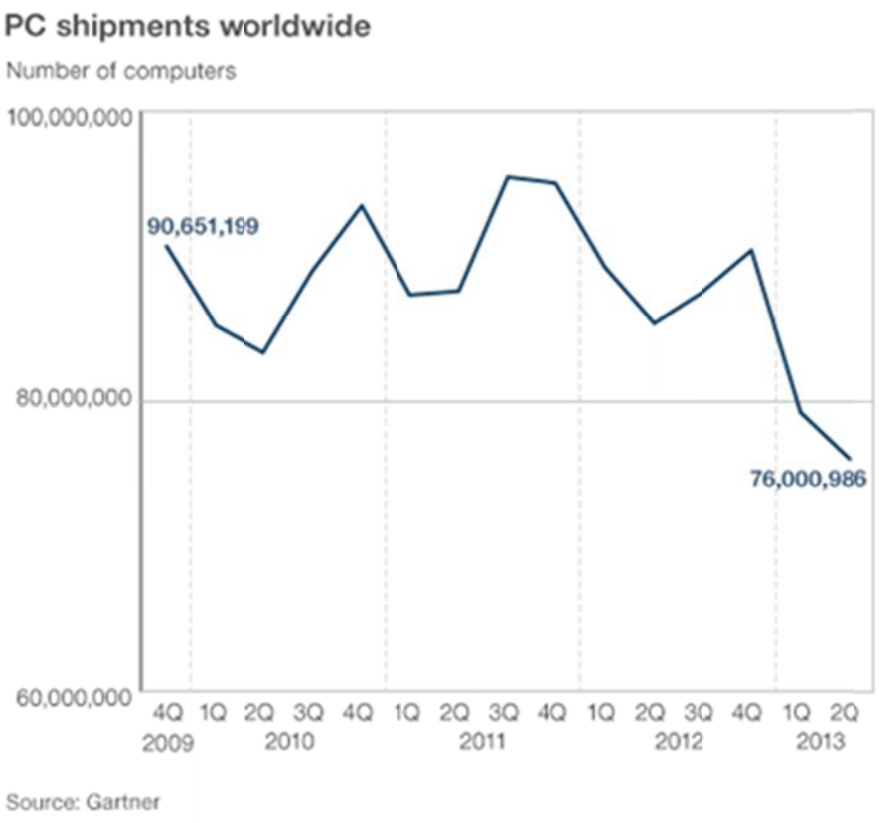

Figura 1 Evoluzione delle vendite di PC negli ultimi 4 anni (fonte Gartner).

2 La crisi del modello a fortezza

Alla base del modello metaforicamente definito "a fortezza" per la sicurezza informatica vi è l'idea di restringere il più possibile i punti di accesso alla dimensione da proteggere (i *cancelli* che permettono l'accesso al cortile) e presidiare queste con adeguate strutture di controllo.

2.1 Identificazione delle difese perimetrali tradizionali

In un sistema informatico questo si traduce in un insieme di difese perimetrali (firewall, IDS, filtri per i contenuti) uniti ad uno stringente controllo degli accessi.

La recente evoluzione dei sistemi di autenticazione con meccanismi biometrici atti a superare la classica “coppia” login e password (si pensi ad esempio all'introduzione di un lettore d’impronte digitali sul nuovo smartphone di Apple, l’iPhone 5s) va oltre lo scopo di quest’articolo, ma vale comunque la pena di citare il fatto che il rafforzamento di questo aspetto, pur essendo fondamentale, non è sufficiente, se utilizzato secondo la classica logica di difesa “perimetrale”, a mettere i sistemi informatici al riparo dalle nuove minacce. Come analizzeremo nel prosieguo dell'articolo, infatti, queste nuove minacce tendono a sgretolare il perimetro rendendolo poroso e permeabile a molteplici vettori di intrusione.

3 La mobilità e le sue implicazioni

Mobilità è una parola chiave del mercato informatico recente. Ormai da alcuni anni le vendite di PC fissi sono in declino (vedi Figura 1) a favore prima di laptop, poi di netbook ed infine di tablet. Questa tendenza del mercato, sebbene non sia assimilabile, come alcuni vogliono portare a credere, con la morte del Personal Computer così come lo conosciamo, implica comunque una significativa espansione del numero di utenti dotati di un dispositivo mobile. Inizialmente, i laptop erano appannaggio dei livelli superiori delle aziende e dei cosiddetti “esterni”, ovvero di quegli impiegati che passavano la maggior parte del loro tempo al di fuori delle pareti aziendali. Il numero limitato di queste figure (all'interno della singola azienda) permetteva l'adozione di soluzioni ad-hoc, di limitato impatto sui sistemi aziendali, quali l'introduzione di Virtual Private Network (VPN) per simulare la presenza del dispositivo mobile all'interno del perimetro aziendale dotandolo di un'interfaccia virtuale che appariva essere parte della Intranet aziendale. Le implicazioni di sicurezza dovute alla presenza di questa VPN rispetto al modello di difesa perimetrale erano piuttosto limitate in quanto si poteva tranquillamente considerarla una porta di accesso secondaria con utenza ben delineata e soggetta e tutti i meccanismi di controllo degli accessi considerati necessari.

3.1 Una nuova tipologia di utenti, di dispositivi, di connettività

Browser	Known unpatched vulnerabilities					
	Secunia					SecurityFocus
	Extremely critical (number / oldest)	Highly critical (number / oldest)	Moderately critical (number / oldest)	Less critical (number / oldest)	Not critical (number / oldest)	Total (number / oldest)
Google Chrome 9	0	0	0	0	0	0
Internet Explorer 6	0	0	4 17 November 2004; 6 years ago	8 27 February 2004; 7 years ago	11 7 November 2003; 7 years ago	473 20 November 2000; 10 years ago
Internet Explorer 7	0	0	1 30 October 2006; 4 years ago	4 6 June 2006; 4 years ago	6 14 June 2007; 3 years ago	26 15 August 2006; 4 years ago
Internet Explorer 8	0	0	0	1 26 February 2007; 4 years ago	4 19 August 2009; 18 months ago	62 14 January 2009; 2 years ago
Mozilla Firefox 3.5	0	0	0	0	0	0
Mozilla Firefox 3.6	0	0	0	0	0	0
SeaMonkey 2	0	0	0	0	0	0
Opera 11	0	0	0	0	0	0
Safari 5	0	0	0	1 8 June 2010; 8 months ago	0	0
Browser	Extremely critical (number / oldest)	Highly critical (number / oldest)	Moderately critical (number / oldest)	Less critical (number / oldest)	Not critical (number / oldest)	Total (number / oldest)
	Secunia					SecurityFocus
	Known unpatched vulnerabilities					

Figura 2 Quadro delle vulnerabilità non risolte nei principali web browsers al Marzo 2011 (fonte: http://en.wikipedia.org/wiki/Comparison_of_web_browser#Vulnerabilities)

La situazione, tuttavia, cambia sostanzialmente nel momento in cui l'evoluzione tecnologica, provocando un significativo calo dei prezzi, ha portato ad avere sempre più utenti dotati di un computer portatile. Dagli “esterni”, utenti tendenzialmente forzati all'uso dei sistemi portatili e, in molti casi, atti a vedere il laptop come un male necessario allo svolgimento del loro lavoro, si passa quindi ad un gran numero di utilizzatori che vedono nel computer portatile una comodità atta a permettergli sia di "portare il lavoro a casa", sia di avere un ambiente integrato di lavoro e di uso domestico.

Questo fatto costringe il reparto IT delle aziende a rinforzare considerevolmente le politiche di utilizzo ammissibile per i dispositivi e porta, nella grande maggioranza dei casi, a non permettere l'installazione di alcun pacchetto software al di fuori di quanto previsto dall'azienda. Nonostante questo, l'utenza continua generalmente a percepire il computer portatile come uno strumento di accesso generico ad Internet non ristretto al solo uso aziendale e le limitazioni imposte centralmente non possono quindi essere considerate sufficienti a garantire l’integrità dello strumento di lavoro. Infatti, anche la sola navigazione su Internet può portare all'inquinamento della stazione di lavoro nel caso in cui si visitino siti malevoli capaci di sfruttare le vulnerabilità dei browser [1] come grimaldello per penetrare il sistema sottostante. L’importanza dei browser nel panorama informatico moderno fa sì che la stragrande maggioranza delle falle presenti venga rapidamente corretta non appena queste sono scoperte (si osservi in Figura 2 una valutazione delle vulnerabilità rimaste non gestite al Marzo 2011), tuttavia, esiste sempre una finestra di pericolo in quanto nuovi punti attaccabili sono scoperti con una frequenza non

nulla come osservabile sulle basi di dati dedicate a tenere traccia di questi eventi (si consideri ad esempio il caso di Mozilla Firefox [2]). Nonostante questo, il pericolo rappresentato da una stazione di lavoro compromessa ma dotata di sola connettività in rete locale (con o senza fili) è controllabile in quanto, nel momento stesso in cui si introduce all'interno dei perimetri di difesa aziendali, ha bisogno di utilizzare l'infrastruttura dell'azienda stessa per contattare qualsiasi altro nodo ed è quindi osservabile, identificabile e, potenzialmente, neutralizzabile dalle difese perimetrali. Si può ovviamente pensare a vettori ad hoc, in grado di distinguere in base alla configurazione di rete la situazione corrente ed adattare in modo automatico il proprio comportamento; tuttavia questo tipo di attacco ha costi sensibili e richiede competenze che lo pongono decisamente al di sopra delle minacce più comuni [3].

Una situazione completamente diversa si pone nel caso di smartphones e tablet PC dotati di connettività 2G/3G/4G. Questi ultimi, infatti, non solo non richiedono l'utilizzo delle risorse di rete aziendali per accedere a risorse esterne, ma possono costituire essi stessi dei punti di ingresso diretto alle aree protette. Infatti, mentre un dispositivo dotato di sola connettività in rete locale (con o senza fili) non è, nella maggior parte dei casi, in grado di connettersi a reti esterne all'azienda per aprire una connessione non controllata tra dentro e fuori, ogni smartphone recente, così come ogni tablet dotato di connettività 2G/3G/4G, dal 2011 in poi nasce con la predisposizione ad agire come router. In questa situazione, il modello a fortezza diventa completamente poroso: ciascun utente dotato di uno smartphone o di un tablet diventa il portatore di un punto di accesso alternativo (collegando appunto la rete locale con la rete cellulare) a quelli più o meno fortemente ed efficacemente sorvegliati dai sistemi di sicurezza aziendali e rende quindi del tutto insufficienti le metodologie di sicurezza tradizionali. In analogia con il modello a fortezza, ove si controllano con attenzione un numero fisso e noto a priori di punti porte di comunicazione tra dentro e fuori (non è un caso che il termine con cui si indicano le porte di una fortezza sia appunto gateway), la presenza di smartphone e tablet che connettono la rete locale alla rete cellulare 2G/3G/4G si configura l'inattesa comparsa di un insieme di stazioni mobili di teletrasporto sparse all'interno dell'area da proteggere: una situazione che vanifica completamente i controlli posti in essere nei punti di scambio predefiniti.

Appare quindi chiaro, a questo punto, come non sia più possibile parlare di difese perimetrali ma diventi invece necessario affrontare il problema della sicurezza in modo più capillare: è necessario controllare ciascun elemento secondo una strategia di "sicurezza del terminale" [4] in quanto ciascun elemento, appunto, diventa un "terminale" attaccabile direttamente o quasi.

Le nuove tecnologie legate "al contesto" forniscono un elemento in più all'arsenale a disposizione della sicurezza aziendale permettendo di introdurre un elemento di discrimine in più nella selezione dei meccanismi di controllo degli accessi [5]; allo stesso tempo, gli elementi di sensorizzazione che permettono di costruire il contesto in cui lavorare e le informazioni stesse che costituiscono il contesto rappresentano un elemento in più da proteggere e richiedono soluzioni ad-hoc [6].

Un primo esempio applicato di sicurezza legata al contesto è rappresentato dal geo-fencing, ovvero dalla creazione di un perimetro virtuale sensibile al transito di determinati dispositivi. Il perimetro può essere determinato in modo semplice dalla distanza radiale da un singolo punto (e.g. calcolando la potenza con cui si riceve il segnale di un "faro"), oppure assumere forme più elaborate sfruttando tecnologie

aggiuntive per il posizionamento (e.g. il GPS) o dispositivi di prossimità (e.g. RFID e NFC). Con la determinazione di un perimetro virtuale, è possibile modificare il comportamento sia dei singoli terminali che dei dispositivi con cui questi interagiscono. Si consideri ad esempio il caso in cui un'azienda abbia istituito un *perimetro* al limite del suo edificio principale: in un settaggio come questo sarebbe possibile sia ai singoli terminali mobili di percepire quando entrano all'interno dell'edificio, sia alle strutture di sicurezza dell'edificio stesso di percepire quali dispositivi mobili entrino o escano. Questo controllo della posizione può essere utilizzata in termini di sicurezza in diversi modi.

Sarebbe possibile, ad esempio, richiedere ai dispositivi in ingresso all'azienda di disabilitare automaticamente la connettività 2G/3G a fronte di una fornitura contestuale di connettività in rete locale senza fili tramite le infrastrutture dell'azienda. In questo modo si verrebbe ad eliminare l'effetto portale incontrollato che pone a rischio elementi interni della rete aziendale.

Un secondo esempio di azioni di sicurezza attivate dall'attraversamento del *perimetro* (da fuori a dentro) è il costringere ogni dispositivo a superare un controllo di integrità prima di essere ammesso all'interno della rete aziendale. Una pratica di questo genere riduce sostanzialmente la pericolosità dei dispositivi stessi in qualità di vettori di programmi malevoli (malware) e agenti aggressivi in generale.

Infine, un ultimo esempio di controllo di sicurezza attivato dall'attraversamento della geo-fence (questa volta da dentro a fuori), è la scansione dei contenuti di ogni dispositivo in uscita per assicurarsi che non vi siano dati incompatibili con il livello di sicurezza del dispositivo e/o dell'utilizzatore del dispositivo.

3.2 La sfida del "Bring Your Own Device"

Se inizialmente il rischio principale di "inquinamento" degli ambienti di lavoro era rappresentato dall'utilizzo degli strumenti aziendali anche per scopi diversi (e.g. navigazione in internet con il laptop aziendale), la massiccia diffusione di dispositivi come smartphones e tablet PC ha portato oggi gli utenti ad essere sempre più dipendenti da essi ed a ribaltare la logica di utilizzo precedente: non si usa più il laptop aziendale per scopi personali, ma si vuole utilizza lo smartphone o il tablet privato anche in ambito lavorativo in quanto il dispositivo è comunque ormai assolutamente capace di fornire i servizi richiesti anche dalle necessità aziendali.

Questa tendenza è etichettata con il termine Bring Your Own Device (BYOD).

I centri IT aziendali tendono a resistere a questa richiesta vedendo con allarme la perdita di controllo del parco dispositivi che essa rappresenta. In effetti, è del tutto palese che il proliferare di soluzioni tecnologiche e configurazioni diverse renda impossibile al momento mantenere un vero controllo e la capacità di standardizzare le procedure di intervento sul parco dispositivi aziendale.

Tale resistenza, comunque, rappresenta una battaglia persa in partenza in quanto gli utenti data la loro ormai conclamata dipendenza dai nuovi dispositivi non sono disponibili a rinunciarvi: il risultato di un irrigidimento da parte dell'azienda è quindi, al più, quello di avere utenti con due o più dispositivi similari, in uso contemporaneo con la tendenza a replicare dati e processi operativi ed una minore capacità di gestione degli stessi dato l'aumento della complessità.

Ingegneria Sociale

Si definisce Ingegneria Sociale la costruzione sistematica e metodica di un profilo del bersaglio dell'attacco a partire dai suoi comportamenti quotidiani, allo scopo di identificare i suoi punti deboli e le modalità più efficaci per carpire informazioni non direttamente disponibili. Si tratta di ingegneria sociale la classica analisi dei rifiuti prodotti dal bersaglio esemplificata in tante pellicole d'azione, ma anche l'analisi del traffico internet di un soggetto volta alla costruzione di attacchi di tipo phishing più evoluti e plausibili.

Il superamento di questo empasse ci sarà solo quando si troveranno modalità per inglobare completamente il BYOD nelle politiche di sicurezza aziendali; tuttavia, anche utilizzando tecniche di sicurezza basate sul contesto delineate in precedenza, implementare una politica sicura di per il BYOD in ambito aziendale rimane una sfida significativa.

Il primo passo è sicuramente rappresentato da una fase di responsabilizzazione degli utenti. Infatti, se il rischio più grande per la sicurezza aziendale è sempre rappresentato dall'utente disattento facile preda dell'ingegneria sociale, il livello di libertà offerto dal BYOD deve essere accompagnato da una parallela crescita della responsabilità dei singoli nella gestione dei loro dispositivi e dei dati.

A tale proposito, le guide pubblicate da diversi istituti dedicati alla sicurezza informatica (e.g. [**Error! Reference source not found.**]) pongono specifico accento sulla necessità di formulare in modo chiaro e completo quali siano gli usi accettabili per i dispositivi coinvolti nel BYOD, quali siano le politiche di uso dei dati aziendali con i dispositivi coinvolti nel BYOD e, non ultimo, quali siano i diritti dell'azienda nei confronti dei dati privati contenuti nel dispositivo stesso. Un esempio classico di problema è quello dato dai sistemi di Mobile Device Management (MDM). Per limitare i rischi di fuga di notizie riservate, in caso di furto di uno dei dispositivi coinvolti nel BYOD, gli stessi sono registrati in un sistema di MDM in grado di tracciarne la posizione e cancellarne il contenuto tramite un comando remoto. Questo rende possibile al reparto IT aziendale riconoscere lo spostamento di un dispositivo e, nel caso questo non coincida con lo spostamento del legittimo proprietario, eliminare i dati contenuti. Tuttavia, è ovvio che questo implica anche la capacità del reparto IT di tracciare gli spostamenti dei dipendenti, con una potenziale grave violazione della loro privacy; allo stesso tempo, rende altresì possibile la cancellazione di tutti i dati privati di un dipendente per mano dell'azienda. Al momento, non esiste una soluzione tecnologica a questo problema e l'unica possibile via rimane quella di definire in modo chiaro quali siano i diritti delle parti coinvolte, quali siano le garanzie fornite da entrambe ad entrambe e quali politiche di comportamento dovranno essere tenute.

4 Dispositivi affamati di energia

Un ulteriore aspetto rivoluzionario con cui si deve confrontare la sicurezza informatica odierna è quello energetico. Una differenza sostanziale tra il personal computer "vecchio modello" e gli attuali smartphone e tablet è, infatti, il consumo energetico. Se nel vecchio modello il consumo energetico è un problema molto poco rilevante nell'ottica della produttività del sistema, con l'avvento di queste nuove tecnologie la questione energetica diventa, di fatto, predominante. Infatti, i tablet e gli smartphone hanno una batteria molto più limitata rispetto ai laptop e ai netbook e la durata della batteria è intrinsecamente legata all'utilizzabilità e quindi alla produttività, del device mobile.

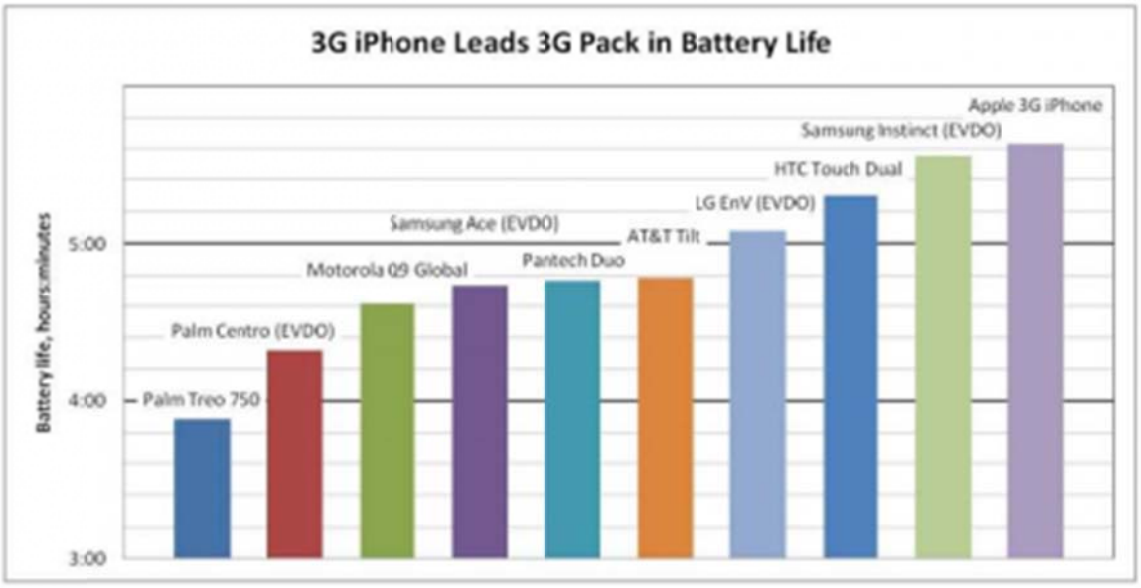

Figura 3 Grafico della durata della batteria in alcuni dispositivi mobili

A titolo di esempio, consideriamo il grafico in Figura 3.

Tale grafico mostra la durata media della batteria di diversi modelli di smartphone di pochi anni fa quando questi utilizzano la rete 3G. Tutti i modelli hanno una durata, in connessione, tra le 3 e le 5 ore prima che la batteria si scarichi totalmente, rendendo il dispositivo mobile inutilizzabile se non si è vicini ad una fonte di corrente elettrica. I nuovi dispositivi tendono ad avere sempre di più un consumo energetico elevato data la dotazione hardware (Multicore e GB di Ram) e di rete (le nuove reti 4G che sostituiranno le 3G e le GPRS), mentre gli avanzamenti in termini di tecnologia delle batterie procedono più a rilento.

Questo fatto porta a continue ricerche da parte dei produttori di dispositivi mobili allo scopo di migliorare l'efficienza energetica sia del dispositivo che della batteria. Ma il problema dell'efficienza energetica non è limitato a questioni di design di architetture e soluzioni software. Al contrario, è un problema che tocca anche la sicurezza informatica. Sempre con riferimento al grafico precedente, i valori ottenuti si basano sull'utilizzo del dispositivo da parte di applicazioni fidate, dove per fidate in un contesto energetico si possono intendere tutte le applicazioni che usano la CPU solo al bisogno per svolgere le proprie funzioni. Dall'altra parte possiamo definire una applicazione come maliziosa se volutamente o forzatamente spinge al consumo energetico speculativo (ad esempio attivando ed usando la CPU a vuoto, senza eseguire computazioni utili). In questa prospettiva, la domanda fondamentale è: che impatto avrebbe un insieme di applicazioni maliziose che non fanno danni ai dati dell'utente né al sistema operativo ma consumano forzatamente la batteria tramite l'uso della CPU o l'attivazione ingiustificata dello schermo o delle periferiche di rete sulla durata della batteria stessa? Inoltre, i sistemi operativi attualmente installati sui dispositivi mobili sono in grado di distinguere tra applicazioni sane e applicazioni che maliziosamente sprecano la carica della batteria fino a rendere il

dispositivo inutilizzabile? In caso contrario, che impatto può avere tutto questo sull'utilizzabilità del dispositivo?

La risposta a queste domande è oggetto di indagine di una nuova branca di ricerca nel settore della sicurezza informatica: la Green Security [8][9]. Presenteremo ora i primi risultati di questo nuovo tipo di studi e la pletora di problematiche non risolte che possono (e devono) essere oggetto di futuri sviluppi e ricerche.

4.1 Vulnerabilità ad attacchi battery drain

Come si può facilmente osservare, la batteria è l'obiettivo primario delle applicazioni maliziose che abbiamo introdotto prima. Tali applicazioni perpetrano nuovi tipi di attacchi, non rivolti (come classicamente accade) a violare la confidenzialità e la privacy dell'utente e dei suoi dati, ma hanno come scopo "abusare" della batteria [10]. Questo nuovo tipo di attacchi, detto appunto *battery-drain* (letteralmente, scarico della batteria), è volto ad accelerare il consumo della carica della batteria portando il dispositivo mobile ad eseguire operazioni non richieste sulle diverse periferiche hardware. Gli attacchi battery-drain possono essere perpetrati dall'interno del dispositivo (le applicazioni maliziose di cui abbiamo accennato in precedenza) o dall'esterno, attraverso tentativi di forzare il consumo energetico sollecitando le interfacce di rete dello smartphone. Lo scopo finale di tali attacchi è realizzare un Denial-of-Device, ovvero, in analogia con gli attacchi Denial-of-Service (DoS), rendere il dispositivo indisponibile al suo legittimo utente fino ad una nuova ricarica della batteria.

Attualmente, gli attacchi *battery-drain* sfruttano la limitata capacità dei sistemi operativi mobili di discriminare tra operazioni legali (richieste dall'utente del dispositivo) da operazioni non legali (forzate da attaccanti esterni) ed apre a nuovi approcci all'analisi delle intrusioni dove anche la componente del consumo energetico diventa una metrica fondamentale per riconoscere gli attacchi alla batteria.

4.2 L'analisi di consumo energetico come identificatore di malware

In quest'ottica, nuove ricerche si stanno concentrando sulla misurazione del consumo energetico legato agli attacchi battery-drain, allo scopo di definire sistemi di sicurezza residenti su dispositivi mobili che siano in grado di riconoscere un attacco in funzione della sua caratteristica "impronta energetica". In particolare, recenti lavori si sono focalizzati sulla misurazione del consumo energetico di attività lecite e illecite su dispositivi Android [11] allo scopo di fare un primo passo verso la catalogazione dei "comportamenti" in funzione del consumo energetico della singola attività. Tale studio ha proposto un nuovo modello per la misurazione del consumo energetico delle attività di un dispositivo ed ha eseguito le prime misurazioni di consumo effettivo su dispositivi reali. Le componenti per tale tipo di misurazioni sono state definite ad hoc e implementate su dispositivi Android, dal momento che questo tipo di misurazione energetica non è prevista in modo analiticamente accurato né su Android né su altri sistemi operativi mobili (come IoS o Windows Phone).

Le componenti di misurazione sono state implementate su diversi dispositivi mobili ed utilizzate per costruire un profilo energetico delle attività legali (applicazioni fidate) e attacchi battery-drain provenienti da applicazioni interne e fonti esterne. A titolo di esempio, nella Figura 4 viene mostrato il

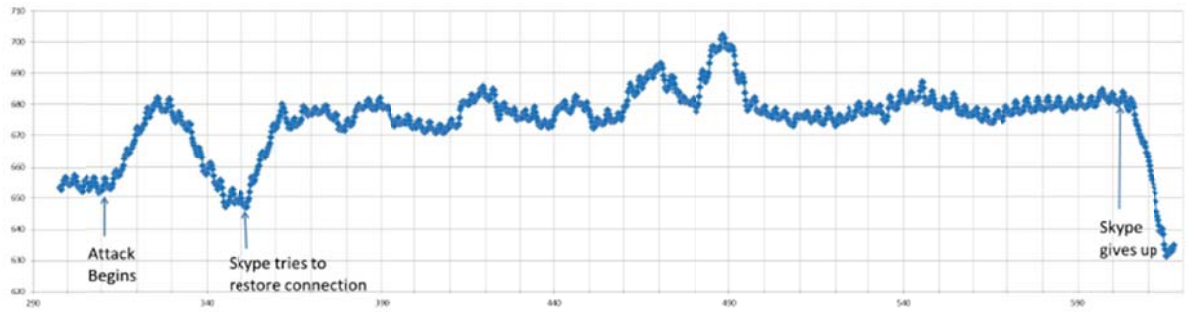

Figura 4 Grafico del consumo energetico di un dispositivo mobile durante un attacco ping flood ed una chiamata skype

risultato di una profilazione energetica di un comportamento di rete legale (chiamata con la applicazione di Skype) e illegale (un attacco battery-drain esterno basato su Ping Flood).

In particolare, il grafico mostra il consumo energetico legato alla periferica WiFi rilevato sulla batteria nel caso in cui un attacco esterno (PingFlood) abbia inizio durante un'attività legale (skype). Senza entrare nei dettagli tecnici, questo grafico è sufficiente a sottolineare come sia possibile catalogare e rilevare gli attacchi (battery-drain, ma non solo) in termini di consumi energetici. Tuttavia, l'analisi del medesimo grafico fornisce una significativa intuizione relativamente ad alcune problematiche correlate a questo nuovo campo di ricerca. Ad esempio, si nota che il consumo energetico di due attività contemporanee non è uguale alla somma algebrica dei consumi delle singole attività: questo richiederà la definizione di opportuni modelli avanzati e non lineari che permettano di isolare le componenti energetiche di attività contemporanee all'interno del dispositivo. Inoltre, il consumo energetico istantaneo di una singola attività può avere una fluttuazione rilevante. Al momento, il problema è affrontato considerando valori medi (in determinati periodi di tempo) del consumo energetico dell'attività (come nel caso del grafico in questione). Tuttavia, occorre anche qui determinare quanto tale variazione si debba all'attività in se, alla latenza del sistema operativo oppure ad imprecisioni dei meccanismi software di misurazione.

Tutto questo mostra che, sebbene l'approccio sia promettente e perseguibile, molto lavoro debba essere fatto sia in termini di modellazione che di misurazione del consumo energetico per poter sviluppare meccanismi *energy-based* di rilevazione e analisi di attacchi.

5 Una rete progettata per dispositivi diversi

Un ultimo aspetto di questa rivoluzione della sicurezza che vogliamo trattare qui è la commistione di diverse generazioni tecnologiche in quella che una delle infrastrutture di telecomunicazione più pervasiva al mondo: la rete cellulare.

Nella rete cellulare sono oggi contemporaneamente presenti la tecnologia di seconda generazione (GSM), la tecnologia di terza generazione (UMTS) e quella di quarta generazione (LTE). Questa rete complessa è nata per gestire dispositivi sostanzialmente stupidi (dumb terminals) ed in grado di fornire

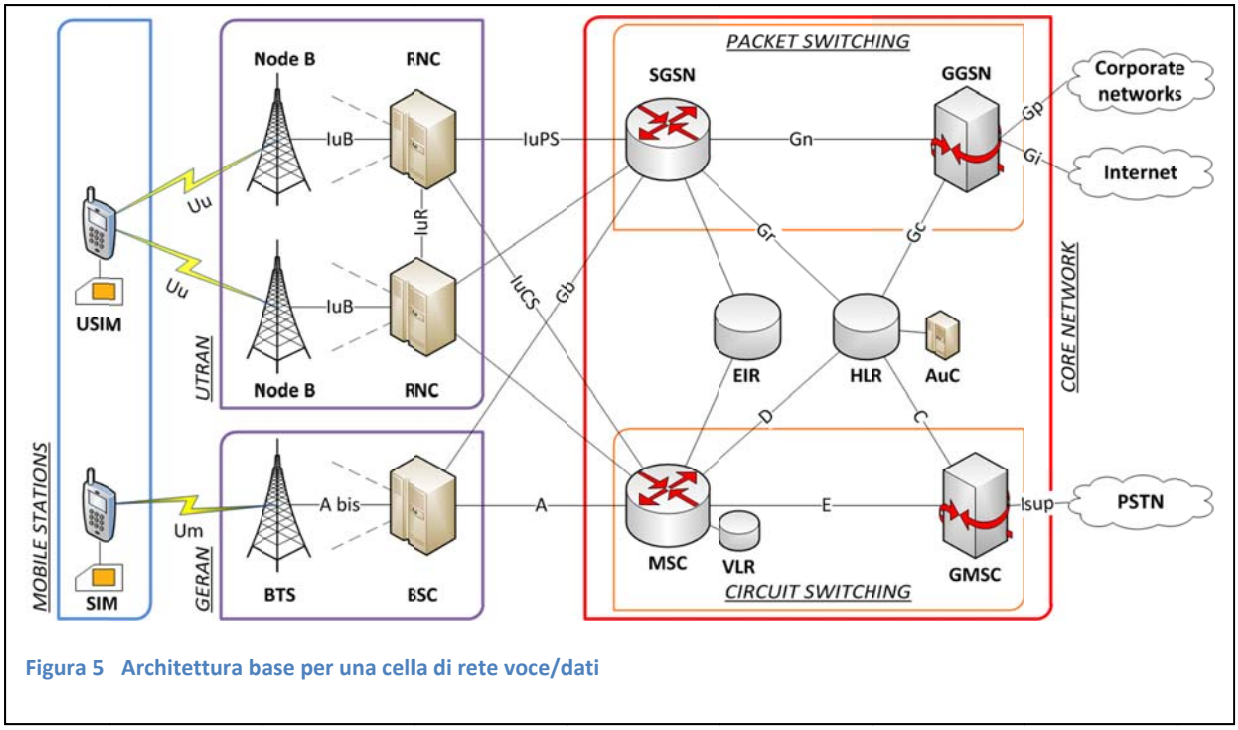

Figura 5 Architettura base per una cella di rete voce/dati

due soli servizi (la voce ed i messaggi di testo), ma si è via via trovata a fornire servizi sempre più evoluti a terminali sempre più intelligenti (smartphones) con bande trasmissive crescenti. Ad oggi, una singola cella 2G/3G si basa sulla struttura mostrata in Figura 5. Come si può notare, mentre le porzioni radio sono separate e distinte, le porzioni di infrastruttura dedicate alla gestione e al trasporto sono in comune. Si consideri inoltre che, mentre i terminali mobili si sono evoluti sino a diventare veri e propri calcolatori con capacità computazionali molto superiori a quelle dei PC degli anni 90 (quando la rete venne progettata), la necessità di mantenere la compatibilità con i terminali più semplici ha fatto in modo che tutte le operazioni di segnalazione e gestione del servizio richiedessero una quantità di risorse molto maggiore da parte della rete di quella richiesta ai terminali.

Questo fatto, rende la rete vulnerabile ad attacchi combinati da parte di terminali completamente programmabili che possono agire in maniera coordinata.

5.1 Un esempio di vulnerabilità

Si consideri, ad esempio, uno dei due elementi condivisi dall'intera architettura di Figura 5, per la precisione lo Home Location Register (HLR). Questo componente dell'architettura si occupa di tenere traccia delle informazioni relative agli utenti della rete. Sia di quelle permanenti, ad esempio le credenziali di accesso, sia di quelle transitorie quali le deviazioni di chiamata, la locazione geografica del terminale o i settaggi GPRS. Dal punto di vista logico, HLR è una struttura distribuita e una rete può avere diversi HLR; tuttavia, un singolo utente è associato in modo univoco con un singolo HLR e le sue informazioni non sono replicate su altri HLR. Ovviamente, questo non implica che HLR non sia intrinsecamente una struttura ridondata e resistente ai guasti, implica solo che è sempre possibile associare un utente con il "suo" HLR di riferimento.

Jamming

Il Radio Jamming è la trasmissione deliberata di segnali radio che interferiscano e rendano inintelleggibile i segnali radio di un canale di comunicazione. Il Jamming è una delle forme più comunemente note di attacco alle infrastrutture di telecomunicazione wireless.

BotNet

Si definisce botnet un insieme di dispositivi informatici connessi in rete ed infettati con un programma di controllo che li rende controllabili da un singolo terminale remoto (il botmaster). Un uso comune delle botnet è lo scatenare un attacco di tipo Distributed Denial of Service particolarmente insidioso in quanto proveniente da un insieme molto numeroso di nodi mai precedentemente associati a comportamenti malevoli.

L'utilizzo di HLR è richiesto da molti dei servizi forniti dalla rete, tuttavia questa base di dati viene interrogata solo in fase di segnalazione e non durante la fase di trasferimento del traffico (sia esso voce o dati, indifferentemente); in particolare, HLR viene interrogato per autenticare inizialmente gli utenti (fase di *attach* alla rete), per instradare le chiamate entranti e per instradare i messaggi SMS.

Per questo motivo HLR non è dimensionato in base all'effettivo traffico di rete, ma piuttosto in base al numero di richieste di servizio effettuate. D'altro canto, essendo coinvolto nella fase iniziale delle chiamate e nella consegna dei messaggi di testo, il suo mancato funzionamento avrebbe effetti disastrosi sulla rete. La combinazione di questi due condizioni lo rende un bersaglio assai interessante per attacchi di tipo Denial of Service.

5.2 Un attacco Denial of Service

In passato, la possibilità di effettuare attacchi DoS alla rete cellulare era fortemente limitata dalla mancanza di dispositivi capaci di utilizzare la rete in modo programmato. E' del tutto evidente che la possibilità di organizzare una folla di migliaia di utenti distribuiti sul territorio in grado di effettuare la stessa operazione sul telefono cellulare nello stesso istante con precisione al millisecondo è nulla. Inoltre, la natura fisica dei terminali "stupidi" disponibili sino a pochi anni fa rendeva altrettanto impossibile una ripetizione rapida delle operazioni al fine di superare il requisito del perfetto sincronismo. Per questo motivo la progettazione della rete cellulare non ha mai posto particolare enfasi sulla sua resistenza ad attacchi di tipo DoS se non nella forma di jamming radio delle singole antenne.

Questi problemi, tuttavia, sono stati superati dalla disponibilità dei moderni smartphones, veri e propri computer il cui comportamento può essere completamente controllato da programmi. Inoltre, mentre in passato l'incapacità dei telefoni cellulari di essere programmati per un comportamento complesso li rendeva impervi ai tentativi di attacco da parte di malware, la completa programmabilità dei moderni telefoni cellulari li ha resi vulnerabili esattamente alla stregua dei comuni PC [12]. La vulnerabilità all'infezione da malware, rende possibile quindi la costruzione da parte di malintenzionati vere e proprie botnet di telefoni cellulari, attivabili con comandi remoti per agire in modo coordinato e ripetitivo anche senza il benché' minimo coinvolgimento dell'utente possessore del telefono stesso.

La botnet è, come ampiamente dimostrato da quanto avviene su internet [13] lo strumento perfetto per perpetrare un attacco di tipo DoS, la possibilità di allestirne una in grado di interagire con la rete cellulare

costituisce quindi lo strumento di scasso che non era stato preso in considerazione in fase di progettazione della rete cellulare stessa.

Recenti studi [14] dimostrano infatti che, tramite una botnet di poco più di undicimila telefoni cellulari sarebbe possibile rendere inutilizzabile la rete su un'area geografica significativa (e.g. una regione Italiana). E' ovvio che la cattura di oltre undicimila telefoni cellulari e la disponibilità di tutti i terminali nello stesso istante e secondo una distribuzione geografica precisa rende questo attacco di non banale realizzazione. Tuttavia, successivi sviluppi di questi stessi studi [15] mostrano che, con l'ausilio di dispositivi dedicati, il numero di risorse richieste può anche essere diminuito drasticamente (sino a raggiungere le millecinquecento unità) rilassando contemporaneamente la dipendenza dal comportamento dell'utente possessore del telefono.

Il rischio di un attacco DoS alla rete cellulare, dunque, non è più oggi solo uno scenario da fantascienza e richiede l'attenzione della comunità scientifica.

6 Conclusioni

In questo breve excursus abbiamo voluto introdurre una serie di nuove problematiche di sicurezza informatica che la recente evoluzione tecnologica, assieme alla commistione tra nuovi paradigmi emergenti ed i limiti intrinseci all'ambiente mobile, ha portato alla luce. Come spiegato nei tre casi esemplari utilizzati, e precisamente mobilità e BYOD, dispositivi energeticamente vincolati e rete cellulare multi-generazionale, il campo della sicurezza informatica si trova oggi costretto ad abbandonare un modello di lavoro stabilizzato. Infatti, il modello a fortezza, quello in cui l'accesso e' limitato a pochi passaggi fortemente sorvegliati, si dimostra incapace di catturare le caratteristiche peculiari che novità ormai capillarmente diffuse - come connettività pervasiva e dispositivi mobili personali - introducono nel panorama IT.

Per superare questo empasse esistono diverse nuove linee di ricerca che vanno dall'applicazione delle metodologie dipendenti dal contesto per il controllo della connettività e del comportamento dei dispositivi, all'applicazione di metodologie legate al consumo energetico per l'identificazione di software malevoli sui dispositivi mobili, sino a studi sulla vulnerabilità della rete cellulare ad attacchi di tipo Denial of Service impensabili sino a pochi anni fa. Queste nuove linee, tuttavia, non possono essere considerate avulse dalla necessità di responsabilizzare gli utenti e di fornire loro politiche di utilizzo chiare e prive di ambiguità, in modo da limitare i rischi non solo dal punto di vista del supporto tecnologico ma anche da quello della componente umana.

7 Bibliografia

1. M. Šilić, J. Krolo, G. Delac. *Security vulnerabilities in modern web browser architecture*, MIPRO, 2010 Proceedings of the 33rd International Convention , vol., no., pp.1240,1245, 24-28 May 2010
2. CVE: *Firefox Vulnerability Statistics*, aggiornato al 14/10/2013 da http://www.cvedetails.com/product/3264/Mozilla-Firefox.html?vendor_id=452

3. C. M. Colombini, A. Colella, M. Mattiucci, A. Castiglione: *Cyber Threats Monitoring: Experimental Analysis of Malware Behavior in Cyberspace*. CD-ARES Workshops 2013: 236-252
4. P. Kuper. *A warning to industry - fix it or lose it*, Security & Privacy, IEEE , vol.4, no.2, pp.56,60, March-April 2006
5. C. Mokdong, C. Jaehyuk, Y. Seokhwan, R. Shi-Kook. *Context-Aware Security Services in DAA Security Model*, Advanced Language Processing and Web Information Technology, 2008. ALPIT '08. International Conference on , vol., no., pp.424,429, 23-25 July 2008. doi: 10.1109/ALPIT.2008.97
6. S. Al-Rabiaah, J. Al-Muhtadi. *ConSec: Context-Aware Security Framework for Smart Spaces*, Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on , vol., no., pp.580,584, 4-6 July 2012. doi: 10.1109/IMIS.2012.41
7. A. Armando, G. Costa, A. Merlo. *Bring Your Own Device, Securely*. In Proceedings of the 28th Annual ACM Symposium on Applied Computing (ACM SAC 2013), pp. 1852-1858.
8. L. Caviglione, A. Merlo, M. Migliardi. What Is Green Security?, Proc. of the 7th International Conference on Information Assurance, Malacca (Malaysia) 5 - 8 December 2011, pgg. 366-371
9. L. Caviglione, A. Merlo, M. Migliardi. *Green Security: risparmio energetico e sicurezza*, Mondo Digitale, N. 44, Dicembre 2012.
10. L. Caviglione, A. Merlo. *The energy impact of security mechanisms in modern mobile devices*, in Network Security, Vol. 2012, N. 2, Elsevier, pp. 11-14.
11. M. Curti, A. Merlo, M. Migliardi, S. Schiappacasse. *Towards Energy-Aware Intrusion Detection Systems on Mobile Devices*, Proc. of the 8th International Workshop on Security and High Performance Computing Systems, 1-5 July 2013, Helsinki. Finland.
12. D. Dagon, T. Martin, T. Starner. *Mobile phones as computing devices: the viruses are coming!* Pervasive Computing, IEEE, vol.3, no.4, pp.11,15, Oct.-Dec. 2004. doi: 10.1109/MPRV.2004.21
13. Z. Lei, Y. Shui, W. Di, P. Watters. *A Survey on Latest Botnet Attack and Defense*, Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on , vol., no., pp.53,60, 16-18 Nov. 2011. doi: 10.1109/TrustCom.2011.11
14. P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, T. La Porta. *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. pp. 223{234. ACM (2009)
15. N. Gobbo, A. Merlo, M. Migliardi. *A Denial of Service Attack to GSM Networks via Attach Procedure*, Proc. of ARES 2013 Workshops, LNCS 8128, pp. 361--376. IFIP International Federation for Information Processing (2013)