Green security

Risparmio energetico e sicurezza

Luca Caviglione, Alessio Merlo, Mauro Migliardi

La diminuzione dei consumi energetici è diventato un elemento centrale di ricerca, soprattutto in ambito industriale. Negli ultimi anni sono nate differenti iniziative, tra le quali il Green Computing e il Green Networking che, rispettivamente, si occupano di analizzare e proporre soluzioni negli ambiti del calcolo e delle telecomunicazioni. Un aspetto critico rimane però quello della sicurezza. A dispetto della sua trasversalità, questo articolo propone di elevarlo a un tema di ricerca autonomo. In particolare, verrà introdotto il concetto di "Green security", con particolare enfasi sui seguenti aspetti: i) comprensione dei requisiti in termini di consumo energetico dell'infrastruttura di sicurezza per contesti di telecomunicazioni; ii) impatto dei meccanismi di sicurezza sui dispositivi mobili e alimentati a batteria; iii) analisi dei nuovi attacchi volti al battery-drain e possibili contromisure; iv) impatto delle soluzioni standard per l'ottimizzazione/riduzione del consumo energetico sul livello di sicurezza globale/locale di una rete di telecomunicazioni; v) eventuali input da considerare in un futuro processo di standardizzazione.

Keywords: Green Security, Energy Awareness, Energy Consumption, Security, Intrusion Detection Systems.

1. Introduzione

La diminuzione dei consumi energetici è ormai un elemento centrale di ricerca, soprattutto in ambito industriale. Infatti, l'impronta energetica dell'umanità sta crescendo in maniera esponenziale. Andando ad analizzare i consumi con una granularità "settoriale", è possibile identificare

nel mondo *dell'Information and Communication Technology* (ICT) un significativo responsabile dell'allarmante andamento dei consumi energetici ed uno dei settori con il maggiore trend di crescita dei consumi stessi. Questo fatto, oltre al problema dell'approvvigionamento energetico, ha serie ripercussioni ambientali dovute all'incremento della produzione di gas ad effetto serra in generale e di CO_2 in particolare. Proprio per questi motivi, l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD - *Organization for Economic Cooperation and Development*) ha prodotto una raccomandazione [1] per promuovere lo sviluppo di iniziative dedicate al *Green Computing* [2] [3]. Parallelamente, anche il settore delle telecomunicazioni sta diventando "esoso" in termini di risorse energetiche. Infatti, studi mirati ad isolare e quantificare i consumi delle reti hanno evidenziato il pesante impatto di quest'ultime nella richiesta globale di energia elettrica. A titolo esemplificativo, l'americana Verizon ha consumato nel 2006 circa 8,9 TWh [16], mentre l'Italiana Telecom consuma, sempre nell'anno 2006, circa 2 TWh [4] [5]. A causa delle specificità delle infrastrutture di telecomunicazioni, la comunità accademica e industriale ha dato vita ad un secondo filone di ricerca molto specifico denominato *Green Networking*; è comunque innegabile che le due iniziative abbiano molti punti in comune, a livello sia di hardware sia di software. Vi è però un altro elemento che accomuna i due mondi: la necessità di garantire livelli di sicurezza che, seppure variabili da situazione a situazione, non possono mai essere completamente azzerati.
Infatti, il moderno utilizzo delle reti, e delle tecnologie ICT in generale, è caratterizzato dalle seguenti assunzioni (spesso implicite):

- Modello di connettività ininterrotta ad Internet (il cosiddetto modello "*always-on*") il quale potenzialmente trasforma ogni host domestico in un bersaglio per intrusioni mirate, per renderlo, ad esempio, parte di una *botnet* [6];
- Diffusione massiccia di connettività wireless (ad esempio IEEE 802.11, UMTS o HSDPA) la quale ha problematiche di sicurezza sensibilmente maggiori a causa del tipo di media, intrinsecamente broadcast, impiegato;
- Proliferazione di "*appliances*", ovvero di dispositivi che utilizzano la connettività Internet per erogare servizi e per lo scambio di dati;
- Spiccata vocazione al social e ai servizi Web.

Per questi motivi, la sicurezza diviene un elemento critico nel moderno panorama dell'ICT e non esiste uno scenario, nella moderna società basata sull'informazione, in cui gli aspetti propri della sicurezza non debbano essere considerati fondamentali. D'altro canto, volendo perseguire gli scopi propri del "*Greening*", l'introduzione di meccanismi di sicurezza può essere vista come controproducente: infatti, essa spesso contribuisce all'aumento dei requisiti computazionali e di scambio dati, risultando quindi in un contributo aggiuntivo al consumo totale di una infrastruttura ICT, in particolar modo in ambito enterprise. Inoltre, la progettazione di soluzioni per garantire un appropriato livello di sicurezza all'interno dei nuovi paradigmi computazionali (questi ultimi, se immaginati ordinati su un asse

temporale, sono ben rappresentati dall'evoluzione da *Web*, al *Grid* fino al *Cloud* [7]) non include lo studio delle caratteristiche energetiche delle stesse, lasciando il problema dei loro requisiti in questo campo completamente irrisolto. Lo stesso accade nel caso della progettazione di nuovi strati (dal livello di rete a quello delle applicazioni) all'interno di sistemi complessi. La mancanza di una conoscenza analitica (e in molti casi persino ad un mero livello quantitativo) di questi aspetti è ancora più grave nel campo, in rapidissima esplosione, dei dispositivi con limitata disponibilità energetica. Questo fatto è reso palese dalla nascita di nuove forme di attacco focalizzate sull'esaurimento delle risorse energetiche (la batteria) di questi dispositivi [8].

Per questi motivi, il presente articolo propone di elevare la relazione tra aspetti energetici e sicurezza a un tema di ricerca autonomo che, in linea con quanto già fatto negli ambiti del computing e del networking, denomineremo "*Green security*". Analogamente con quanto accade per le altre attività "green", presentare la "*Green security*" richiede uno sforzo molto vasto e altamente interdisciplinare. Infatti, tra le molte tematiche che contribuiscono alla definizione di questo nuovo ambito di ricerca citiamo a solo titolo di esempio: problematiche inerenti alla misurazione dei consumi dal punto di vista degli strumenti di misura e loro calibrazione e piazzamento; valutazione dell'overhead introdotto dalle procedure software e dal traffico di segnalazione necessario per lo sviluppo dei sistemi di sicurezza; scelta dei modelli (computazionali, di traffico ed energetici) e dei relativi strumenti matematici e ingegneristici per l'ottimizzazione dei consumi.
Al fine di rendere la trattazione focalizzata ai soli aspetti strettamente correlati al mondo ICT, delimiteremo la discussione ai seguenti punti: nella sezione II affronteremo il tema della comprensione dei requisiti in termini di consumo energetico dell'infrastruttura di sicurezza per contesti di telecomunicazioni; nella sezione III descriveremo l'impatto dei meccanismi di sicurezza su dispositivi mobili e alimentati a batteria; nel paragrafo 4 ci dedicheremo all'analisi dei nuovi attacchi volti al *battery-drain* e delle possibili contromisure; nel paragrafo 5 forniremo una valutazione dell'impatto delle soluzioni standard per l'ottimizzazione/riduzione del consumo energetico sul livello di sicurezza globale/locale di una rete di telecomunicazioni; nel paragrafo 6 indicheremo eventuali input da considerare in un futuro processo di standardizzazione; infine, nel paragrafo 7 trarremo alcune conclusioni.

2. Sicurezza e contesti di telecomunicazioni

Come accennato, la maggior sensibilità su aspetti riguardanti il consumo energetico non può più limitarsi alle tematiche legate al computing, ma deve anche estendersi nell'ambito delle reti di telecomunicazioni. Uno dei motivi fondamentali che hanno spinto alla creazione di un filone di ricerca indipendente è dovuto alla natura sempre più pervasiva d'Internet. Infatti, le moderne applicazioni si basano sull'utilizzo di nodi mobili (tipicamente

alimentati mediante batterie), tecnologie e apparati altamente eterogenei (spesso virtualizzati o utilizzati per la creazione di complesse architetture basate su *overlay*), e suite protocollari pensate per utilizzi diversi da quelli attuali. Parallelamente, Internet sta diventando sempre più un complesso ecosistema di oggetti (denominato *Internet of Things*), e di persone (si pensi alle Social Network, che, di fatto, sono il prototipo di quello che Tim Berners Lee e il suo *World Wide Web Consortium* chiamano *Social Web*). Come conseguenza di questi nuovi paradigmi di utilizzo, oggi le reti veicolano conversazioni (ad esempio mediante il *Voice over IP – VoIP*), controlli e telemetrie di impianti complessi o di applicazioni mission critical, e dati altamente sensibili che possono aver pesanti ripercussioni sulla privacy delle persone se non opportunamente salvaguardati [9]. L'accesso alla rete è ormai una funzionalità presente su diversi tipi di apparati, ad esempio: *set-top-box*, consolle per i videogiochi e TV multimediali. Per questi motivi, la valutazione e l'ottimizzazione complessiva del consumo energetico di questo ecosistema sono operazioni molto complicate. Allo stesso tempo, la natura "network centrica" di molti dei servizi che sono usati quotidianamente impone di dotare Internet, sia a livello applicativo che infrastrutturale, di un adeguato livello di sicurezza.

Purtroppo, garantire un'opportuna efficienza energetica e sviluppare metodologie volte a garantire un adeguato livello di sicurezza in Internet sono due obiettivi che spesso entrano in conflitto. Infatti, l'utilizzo di meccanismi più complessi può richiedere: *i*) una maggiore potenza di calcolo; *ii*) un incremento della dotazione hardware per l'erogazione di servizi "*security oriented*" (ad esempio, al fine di manutenere ed erogare i certificati digitali); *iii*) un aumento nel consumo della banda trasmissiva per servire i flussi di traffico necessari per il trasporto dei dati di segnalazione (ad esempio, per eseguire le procedure di autenticazione).
Al fine di rendere trattabile il problema complessivo, occorre isolare, almeno dal punto di vista concettuale e funzionale, la gestione degli aspetti della sicurezza da quelli più orientati alle telecomunicazioni. Citiamo ad esempio, la gestione del traffico, la pianificazione della rete, e la gestione della Qualità del Servizio (*Quality of Service – QoS*). Viceversa, la *Green security* deve però opportunamente interagire con il *Green Networking* per analizzare l'utilizzo di alcune soluzioni specifiche per la riduzione dei consumi nel suo specifico ambito, e soprattutto, per valutare se le soluzioni introdotte non siano in qualche modo esse stesse dannose per la sicurezza della rete.

3. Impatto dei meccanismi di sicurezza sui dispositivi mobili

Mentre il recente passato vede una certa stagnazione nel panorama di acquisizione di nuovo hardware di tipo desktop e persino laptop [10],quello dei dispositivi mobili (*smartphones* e *tablet* PCs) è certamente in crescita esplosiva. Questa fortissima espansione, unita al fatto che questo tipo di dispositivo sta entrando sempre più nel panorama degli strumenti di lavoro

quotidiano [11] [12], ha iniziato a spostare in questa direzione l'attenzione degli autori e dei diffusori di software malevoli [13]. A fronte di questo aumento di interesse nello sviluppo e diffusione di software malevoli, si è avuta una parallela evoluzione di gran parte delle più note suite per la sicurezza dei sistemi desktop in forme dedicate alle piattaforme mobili (citiamo qui a mero titolo d'esempio AVG, Avast e Kaspersky) allo scopo di sopperire alle vulnerabilità presenti nei sistemi operativi mobili attuali (si veda ad esempio [14], tuttavia, è evidente che gli approcci più moderni utilizzati nei sistemi desktop, cioè l'introduzione nelle attività routinarie del sistema operativo di sezioni di codice dedicate al controllo sia della liceità che dell'identità del richiedente l'azione stessa, non sono direttamente applicabili in ambito mobile. Al contrario, un tale approccio si rivelerebbe estremamente controproducente per due motivi principali: in primo luogo, data la ancor limitata disponibilità di risorse hardware nei sistemi mobili (si pensi, ad esempio, alla memoria) l'introduzione di sezioni di codice aggiuntive porterebbe ad un inaccettabile impoverimento dei livelli prestazionali del sistema stesso; in secondo luogo, ma forse ancora più importante, l'aggiunta di attività di controllo a tutte le azioni di routine del sistema operativo causerebbe un consumo accelerato di quella che è la risorsa più critica di un sistema mobile, cioè la batteria. Questo stesso effetto per cui la cura può essere essa stessa una forma di malattia è ancor più facilmente identificabile se si analizza uno strumento di sicurezza ormai praticamente standard per ogni sistema di tipo desktop o server, cioè il *firewall*. In un sistema collegato alla rete energetica, sia esso di tipo destop o server, il *firewall* analizza ogni singolo pacchetto che giunge all'interfaccia di rete e lo valuta navigando attraverso un grafo di regole che può essere anche assai complesso e che deve tenere in considerazione non solo la morfologia del singolo pacchetto ma anche la storia dei pacchetti ricevuti. Questo tipo di attività, ovviamente, ha un costo computazionale non nullo e, persino sui sistemi non mobili, può arrivare a impegnare una quantità di risorse significativa e degradare le prestazioni del sistema. Si veda, a titolo di esempio, la Figura 1 che mostra la rilevazione della percentuale di CPU utilizzata da un *firewall* a regime.

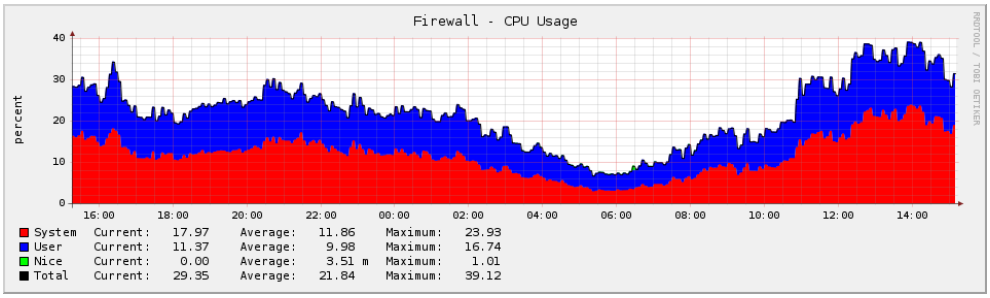

Figura 1
Percentuale di utilizzo di CPU da parte di un firewall durante l'attività giornaliera (immagine tratta da http://netmon.rmutsv.ac.th)

Tuttavia, in un sistema non mobile, il degrado del sistema è percepibile solo per la durata dell'attacco e, se il firewall è configurato correttamente, la difesa impedirà che ci siano effetti negativi persistenti. In un sistema mobile, al contrario, la capacità dell'attacco di penetrare la linea di difesa rappresentata dal *firewall* diventa secondaria: infatti, anche in caso di tenuta del firewall stesso, l'onere computazionale richiesto si traduce in uno scaricamento accelerato della batteria e l'attacco, seppure non efficace in termini tradizionali di penetrazione del sistema, si risolverà comunque in un'efficace messa fuori linea del dispositivo mobile diventando, di fatto, un attacco di tipo "*Denial of Device*" (DoD). Per questi motivi, l'architettura tradizionale del firewall indipendente attestato sul singolo nodo comune in ambito desktop e server non è direttamente trasportabile in ambito mobile ed è necessario valutare nuove metodologie di implementazione che tengano in considerazione gli aspetti energetici dei meccanismi di sicurezza e si appoggino su servizi forniti dalle reti stesse [15] [16].

4. Analisi dei nuovi attacchi volti al *battery-drain*

Nella precedente sezione si è visto quanto una efficiente difesa da attacchi abbia un costo energetico non indifferente dovuto ai sistemi di sicurezza di cui il dispositivo mobile si dota, atti a difendere il dispositivo da *malware* e attacchi tipici di molti sistemi distribuiti.
Oltre agli attacchi classici, l'utilizzo di dispositivi mobili è un vettore per nuove categorie di attacchi, come quelli volti al consumo selvaggio della batteria. L'idea alla base di questi attacchi parte da una considerazione molto semplice: ogni attività eseguita su un dispositivo mobile sottrae energia alla batteria del dispositivo. Inoltre, il funzionamento del dispositivo mobile è strettamente legato alla disponibilità di energia della batteria. Pertanto, la batteria diventa un obiettivo sensibile per la sicurezza del dispositivo, in quanto impedire ad attaccanti di forzare dall'esterno il consumo di batteria significa garantire la disponibilità dei servizi che "girano" sul dispositivo. Al contrario, permettere ad un attaccante esterno di esaurire la batteria (ad esempio forzando il dispositivo a fare calcoli ed elaborazioni inutili, mantenendo attive periferiche non utilizzate o mantenendo attiva la connessione ad Internet) porterebbe ad inficiare pesantemente la disponibilità, e quindi l'utilizzabilità dei dispositivi. Tali attacchi prendono il nome di attacchi "*battery-drain*". Ma sono davvero una reale minaccia? L'utente non specializzato che acquista uno smartphone di ultima generazione si aspetterebbe che i sistemi operativi attualmente utilizzati su smartphone (ad esempio, IOS, Android o Windows Mobile) siano in grado di riconoscere "*battery-drain attack"* e proteggere, di conseguenza la batteria. Tuttavia, recenti studi empirici [8] hanno evidenziato che ciò non avviene. In particolare, tali studi hanno mostrato che qualora un altro dispositivo malizioso (fisso o mobile) nelle vicinanze del dispositivo vittima inondi di traffico un dispositivo vittima tale dispositivo utilizzerà risorse (e quindi batteria) per riceverlo e/o analizzarlo. In particolare, traffico entrante verso il dispositivo porterà ad attivare l'antenna per il trasferimento dei dati e il sistema operativo per instradarlo,

consumando quindi batteria. La Figura 2 mostra un esempio di consumo energetico legato ad un attacco *battery-drain* di tipo *ping-flood* su un dispositivo Android. (Si definisce *ping-flood* un attacco portato generando un numero estremamente grande di pacchetti di tipo *ICMP-ping* e rivolto ad "allagare" le capacità di comunicazione del dispositivo bersaglio).

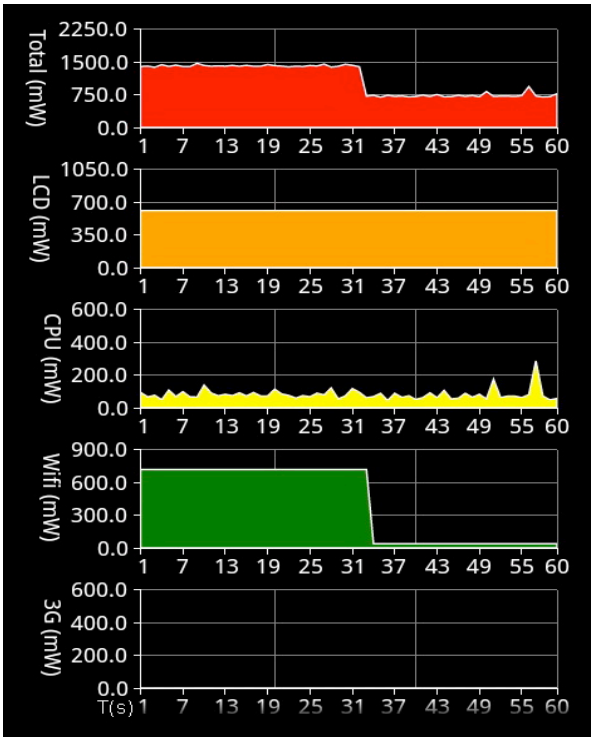

Figura 2
Impatto energetico di un attacco di tipo Ping-flood sollecitato da un dispositivo esterno.

Al momento attuale, nessuno dei sistemi operativi presenti su smartphone sembra nativamente in grado di evitare situazioni di questo tipo. Pertanto, è facile capire come un dispositivo malizioso (o peggio, un insieme di dispositivi maliziosi tra loro collusi) possano impattare sulla batteria di un dispositivo vittima semplicemente generando traffico; infatti, attualmente, risulta essere un problema non semplice poter riconoscere una fonte di traffico malizioso "prima" di aver analizzato il traffico stesso, sprecando quindi risorse e carica della batteria.
Benchè questo tipo di attacchi stiano pian piano prendendo piede, poca ricerca è stata svolta finora a riguardo, in particolar modo tenendo in considerazione l'impatto energetico di tali attacchi. Non è facile al momento valutare quando possa impattare un certo tipo di attacco, in un certo sistema, sulla batteria. Inoltre, come già ribadito, non è facile riconoscere un attacco di tipo "*battery-drain*" in tempo e, tuttavia, il riconoscimento tardivo non risulta di alcuna utilità. A tal proposito, è importante sottolineare

anche come sia un compito non semplice distinguere tra attacchi reali e presunti; questo fatto genera il rischio di avere in fase di analisi sia falsi positivi (ovvero riconoscere un attacco che di fatto non esiste) che falsi negativi (ovvero non riconoscere un tentativo di attacco) e rende poco affidabili le strategie correntemente in uso nei software di sicurezza.
Infine, qualora l'attacco sia chiaramente riconosciuto, un altro problema da affrontare riguarda le strategie da adottare e come intervenire prontamente: non è infatti per nulla immediato stabilire quale sia il modo ottimale per ridurre l'impatto energetico dell'attacco.
Tutti questi aspetti sono oggetto di studio della *Green security* che, tramite la coesione di conoscenze di carattere energetico e di sicurezza, può affrontare il problema di valutare sia il riconoscimento che la valutazione dell'impatto energetico degli attacchi *battery-drain*.

5. Possibili conflitti e soluzioni

Come accennato, il *Green Networking* può fornire soluzioni, sia protocollari che architetturali, applicabili anche nel contesto della *Green security*. Purtroppo, tali metodologie possono esse stesse introdurre nuove problematiche di sicurezza all'interno dell'infrastruttura di telecomunicazioni. Per chiarire meglio il concetto, si pensi al seguente caso paradigmatico. Una delle tecniche sviluppate per la riduzione dei consumi si basa sull'utilizzo di dispositivi che mediano l'accesso alle macchine presenti nelle reti domestiche o negli uffici (cioè, il classico scenario denominato *Small Office Home Office* – SOHO) [17]. In breve, l'utilizzo di un proxy ad-hoc permette di spegnere dinamicamente le macchine di una *Local Area Network* (LAN) nei periodi di *idle* che possono avvenire durante un trasferimento dati (si veda ad esempio, il lavoro [18] per un esempio di sua applicazione al servizio di *file-sharing peer-to-peer BitTorrent*). Senza entrare in eccessivi dettagli, questo meccanismo può introdurre i seguenti problemi: *i*) l'host che implementa tale servizio è tipicamente esposto in rete in maniera pubblica e permanente, diventando così un possibile target per azioni malevole; *ii*) l'aggiunta di software può introdurre possibili bachi non presenti nell'architettura originale; *iii*) apparati di questo tipo, comunemente denominati "*middleboxes*" hanno implicazioni sulla semantica end-to-end tipica del livello di trasporto (cioè, ISO/OSI L4), potendo quindi introdurre eventuali malfunzionamenti utilizzabili per condurre attacchi quali il connection *hijacking*. Riassumendo, *Green Networking* e *Security* devono quindi considerati in maniera sinergica, proprio per evitare questo tipo di casistiche, che potrebbero inficiare anche il risparmio energetico. Ad esempio, l'introduzione di falle nell'assetto globale di sicurezza può causare la "zombificazione" degli host, i quali possono divenire elementi attivi di *botnet* o entità usate per compiere attacchi telematici (citiamo, *Distributed Denial of Service* – DDoS, attacchi basati su *flooding* e *spam*). Ovviamente, questo implica l'utilizzo della loro CPU e della relativa banda trasmissiva, comportando così un costo in termini energetici, ed azzerando pressoché totalmente, i periodi di *idle* delle macchine compromesse.

Altri meccanismi tipici del *Green Networking* sono, oltre il già citato *smart sleeping*, la *dynamic adaptation*, e il cosiddetto *re-engineering* [16]. Il primo consente ai dispositivi, siano essi apparati di rete che nodi periferici, di cambiare la propria configurazione interna (e di conseguenza, il proprio profilo di consumo) mediante l'attivazione/disattivazione in tempo reale di alcune porzioni di hardware o software. Inoltre, è anche possibile cambiare le frequenze di funzionamento della logica cablata (ad esempio, la CPU) utilizzando opportune *Application Programming Interface* (API) o driver specifici. Tale meccanismo può essere preso di ispirazione per lo sviluppo di agenti per la gestione della *network security* in grado di reagire attivando/disattivando porzioni di codice a seconda della gravità della minaccia, o dei requisiti di sicurezza della particolare informazione da trattare. Questa tecnica può anche essere molto promettente nell'ambito dei dispositivi mobili, che essendo alimentati a batterie, hanno requisiti di tipo energetico molto stringenti (si veda ad esempio [8] per una discussione esaustiva sulle implicazioni dei meccanismi di sicurezza in ambito *mobile*). Di contro, la *dynamic adaptation* può introdurre problematiche legate ad attacchi di tipo *DoS*. Ad esempio, un soggetto malevolo potrebbe inibire il traffico di una porzione di rete, forzando così gli apparati a ridurre le proprie capacità funzionali, per poi produrre in traffico a-la *flooding* saturando la capacità di servizio di quest'ultimo in maniera più semplice. Per quanto riguarda il *re-engineering*, tale tecnica si basa sull'abbandono del parco tecnologico e protocollare non considerato "*power-efficient*", sostituendolo con soluzioni nuove. Benché l'abbandono di ogni tipo di *legacy* sia, dal punto di vista ingegneristico, una grossa facilitazione, tale soluzione è difficilmente praticabile, vista la diffusione attuale delle tecnologie di rete, e la mole di investimenti fatti in termini di hardware. Tuttavia, ridisegnare solo alcuni degli aspetti più inefficienti può essere un giusto compromesso. Occorre sempre però valutare questo cosa comporti dal punto di vista della retro-compatibilità, e di eventuali sistemi di conversione/adattamento per far convivere nuove e vecchie tecnologie (anche solo per il periodo necessario alla migrazione verso le soluzioni *energy efficient*). Anche in questo caso, tale scenario può dar luogo a possibili buchi utilizzabili per sferrare attacchi, o sfruttare i meccanismi di transizione per bypassare alcune procedure di sicurezza.

6. Input standardizzazione

Come visto in precedenza (ovvero nei paragrafi 3 e 4) a causa delle risorse limitate, derivanti anche dall'utilizzo di batterie per fornire la necessaria alimentazione, i dispositivi mobili possono essere vittime di un nuovo tipo di attacchi. Per questi motivi, la standardizzazione (ad esempio in ambito IETF e IEEE) dovrebbe tener conto non solo delle implicazioni dal punto di vista della sicurezza (cosa che già avviene negli RFC con la sezione obbligatoria "*Security Considerations*") ma anche dei risvolti di tipo energetico. Un esempio paradigmatico potrebbe essere quello riguardante la creazione di linee guida per stack protocollari dedicati ai dispositivi mobili. Infatti, in virtù dell'elevato grado di sofisticazione degli attuali terminali mobili, è prassi consolidata effettuare *porting* più o meno diretti di,

di intere porzioni di sistemi operativi provenienti dal mondo desktop (si pensi alle porzioni di Linux nei dispositivi Android, e di quelle – basate su BSD e MacOSX dei dispositivi iOS). Come discusso, stimolando le interfacce di livello 2 di tali device, è possibile consumare in maniera anomala le loro risorse energetiche utilizzando banalmente semplici tool (ad esempio, un semplice *flooding* di *ping* può causare un aumento dei consumi [8], [19]). Una possibile contromisura che può essere inserita nell'ambito della standardizzazione è quella di inibire la risposta al *ping* o di prevedere che sia vincolata a non più di x pacchetti. Questo limiterebbe l'impatto di tali attacchi, garantendo però l'utilizzo del protocollo ICMP a fini diagnostici. Un'altra possibile soluzione è quella di prevedere schemi di indirizzamento ad-hoc per questi dispositivi, ad esempio usando sistemi di mediazione alla *Network Address Translation* (NAT), al limite per ridurre gli attacchi dall'esterno. In maniera analoga, nel caso di *deployment* in modalità infrastrutturata, potrebbe essere auspicabile proteggere il *loop wireless* con opportune regole (possibilmente obbligatorie) implementate con un firewall.

7. Conclusioni

I consumi energetici stanno diventando un aspetto estremamente significativo in ambito ICT e questo ha innescato la nascita di filoni di ricerca specifici sulla efficienza energetica dei sistemi di calcolo (*Green Computing*) e della trasmissione dei dati (*Green Networking*). Tuttavia, in una società come la nostra, sempre più dipendente dalla capacità di processare e scambiare in modo rapido e sicuro grandi moli di dati, è impensabile tralasciare gli aspetti relativi alla sicurezza. Inoltre, la rapida diffusione di sistemi mobili alimentati a batteria pone in essere una nuova tipologia di problematiche di sicurezza non presenti nei sistemi collegati alla rete elettrica.

In questo articolo abbiamo quindi introdotto il termine di "*Green security*" per denotare un campo interdisciplinare che si occupa dello studio delle implicazioni energetiche dei meccanismi di sicurezza e delle implicazioni di sicurezza dei meccanismi di risparmio energetico in ambito ICT. In particolare, al fine di mantenere la trattazione focalizzata al solo ambito ICT, abbiamo affrontato il tema della comprensione dei requisiti e delle problematiche in termini di consumo energetico dell'infrastruttura di sicurezza per contesti di telecomunicazioni, abbiamo descritto l'impatto dei meccanismi di sicurezza sui dispositivi mobili e alimentati a batteria, abbiamo analizzato l'evoluzione dei nuovi attacchi volti al *battery-drain* dei dispositivi mobili e delle possibili contromisure. Inoltre, abbiamo fornito una valutazione dell'impatto delle soluzioni standard per l'ottimizzazione/riduzione del consumo energetico sul livello di sicurezza globale/locale di una rete di telecomunicazioni e abbiamo indicato eventuali input da considerare in un futuro processo di standardizzazione.

Il campo della *Green security* è solo ai suoi albori, ma siamo assolutamente persuasi che i temi qui trattati non possono che diventare sempre più centrali in ambito ICT.

Bibliografia

[1] OECD, *Working Party on the Information Economy, Towards Green ICT strategies: Assessing Policies and Programmes on ICTs and the Environment*, giugno 2009, disponibile online at http://www.oecd.org/dataoecd/47/12/42825130.pdf

[2] Van Heddeghem W., Vereecken W., Pickavet M., Demeester P., *Energy in ICT - Trends and research directions*, Proc. of the IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems (ANTS), New Delhi, 14-16 dic. 2009.

[3] N. Hardavellas, M. Ferdman, B. Falsafi, A. Ailamaki, *Toward Dark Silicon in Servers*, IEEE Micro, Vol.: 31, n. 4, pp 6 – 15, 2011

[4] C. Bianco, F. Cucchietti, G. Griffa, *Energy Consumption Trends in the Next Generation Access Network - A Telco Perspective*, Proceedings of the 29th International Telecommunications Energy Conference (INTELEC 2007), Roma, Italia, settembre 2007, pp. 737 – 742.

[5] Bianzino A., Chaudet C., Rossi D., Rougier J., A Survey of *Green Networking* Research, IEEE Communications Surveys & Tutorials, 2010, pp: 1 – 18.

[6] F. Naseem, M. Shafqat, U. Sabir, and A. Shazad, *A Survey of botnet Technology and Detection*, International Journal of Video and Image Processing and Network Security, vol. 10, n. 01.

[7] Mauro Migliardi and Roberto Podestà, *Cloud Computing evoluzionario e rivoluzionario,* Mondo Digitale, n. 33, marzo 2010, pp. 16-26.

[8] L. Caviglione, A. Merlo, *Energy Impact of Security Mechanisms in Modern Mobile Devices*, Network Security, pp. 11 - 14, febbraio 2012, Elsevier.

[9] L. Caviglione, M. Coccoli, *Privacy Problems with Web 2.0, Computer Fraud and Security*, pp. 16 - 19, Ottobre 2011, Elsevier.

[10] Gartner, *Gartner Says Worldwide PC Shipment Growth Was Flat in Second Quarter of 2012*, http://www.gartner.com/it/page.jsp?id=2079015, accessed 13-8-2012.

[11] P. Lewis Dolan, *Doctors quick to adopt tablets into practice*, http://www.ama-assn.org/amednews/2012/06/04/bil20604.htm, accessed 13-8-2012.

[12] S. Bhartiya, *Android Approved By Pentagon For DoD Usage, Major Setback For iPhone*, http://www.muktware.com/news/3145/android-approved-pentagon-dod-usage-major-setback-iphone, accessed 13-08-2012.

[13] G. Lawton, *Is It Finally Time to Worry about Mobile Malware?*, Computer , vol.41, no.5, pp.12-14, maggio 2008

[14] A. Armando, A. Merlo, M. Migliardi, L. Verderame, *Would You Mind Forking This Process? A Denial of Service Attack on Android (and Some Countermeasures)*, in IFIP 27th International Information Security and Privacy Conference (SEC 2012), D. Gritzalis, S. Furnell, and M. Theoharidou (Eds.), IFIP Advances in Information and Communication Technology (AICT), Vol. 376, pp. 13-14, giugno 2012.

[15] Ying Qiu; Jianying Zhou; Feng Bao; , *Design and optimize firewall for mobile networks,* IEEE 60thVehicular Technology Conference, (VTC 2004), vol.5, pp. 3301- 3305, sett. 2004

[16] Ying Qiu; Jianying Zhou; Feng Bao; , *Mobile personal firewall,* 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004), vol.4, n. 5-8, pp. 2866-2870, sett. 2004

[17] A. Bianzino, C. Chaudet, D. Rossi, J. Rougier, *A Survey of Green Networking Research*, IEEE Communications Surveys & Tutorials, pp. 1 - 18, maggio 2010.

[18] G. Anastasi, M. Conti, I. Giannetti, A. Passarella, *Design and Evaluation of a BitTorrent Proxy for Energy Saving*, Proceedings of IEEE Symposium on Computers and Communications (ISCC 2009), pp.116-121, luglio 2009.

[19] L. Caviglione, A. Merlo, *Analysis and Development of Green-aware Security Mechanisms for modern Internet Applications*, Handbook of Green Information and Communication Systems, Wiley, doi: http://dx.doi.org/10.1016/B978-0-12-415844-3.00023-1

Biografia

Luca Caviglione è nato a Genova nel 1978. È ricercatore presso l'Istituto di Studi sui Sistemi Intelligenti per l'Automazione (ISSIA) del Consiglio Nazionale delle Ricerche. I suoi principali interessi di ricerca riguardano le architetture p2p, i sistemi wireless e l'analisi di traffico. È autore o co-autore di circa 80 lavori scientifici e del libro File-sharing Applications Engineering. Inoltre è co-autore di diversi brevetti internazionali sui sistemi p2p, ed è uno dei WG Leader della Task Force Italiana di IPv6.

Alessio Merlo ricevuto il dottorato in Informatica nel 2010 presso l'Università degli Studi di Genova, all'interno del quale si è occupato di problemi di performance e Qualità del Servizio su piattaforme Grid. Attualmente è ricercatore presso l'Università E-Campus e ricercatore associato presso il Dipartimento interscuola di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) dell'Università di Genova. I suoi attuali interessi di ricerca sono attualmente focalizzati sulla sicurezza di sistemi distribuiti (Web, Grid) e di piattaforme mobili (Android).

Mauro Migliardi è nato a Genova nel 1966. Dopo esser stato uno dei principali ricercatori del progetto HARNESS per il meta e Grid computing presso la Emory University di Atlanta, è stato ricercatore universitario presso l'Università di Genova ed è ora Professore associato presso l'Università di Padova. Mauro Migliardi ha pubblicato cira cento articoli scientifici soggetti a peer-review ed ha tra i suoi principali interessi di ricerca le tecnologie e le metodologie per la progettazione e lo sviluppo di sistemi software complessi distribuiti, pervasivi e mobili.