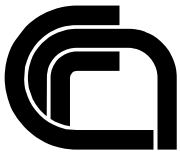


Consiglio Nazionale delle Ricerche

TEC – MOB Analisi preliminari: Information Technology

A. Castrucci, A. Falleni, A. Vaccarelli

IIT B4-06/2006

Nota Interna

Ottobre 2006

Istituto di Informatica e Telematica

DOCUP REGIONE TOSCANA – misura 1.7.1

PROGETTO TEC-MOB

TEC - MOB Analisi preliminari:

Information Technology

Alessandro Castrucci, Alessandro Falleni, Anna Vaccarelli

Istituto di Informatica e Telematica del CNR

INDICE

ABSTRACT

This document describes the TEC-MOB project: “Rete delle alte tecnologie per la mobilità fisica e virtuale nell'area vasta costiera della Toscana”, with particolar attention to security issues. General topics are here discussed, by starting from basic concepts, up to some applicative solutions for helping the phisical and virtual mobility.

Keywords: Mobile Security, Virtual Mobility, Phisical Mobility

PREFAZIONE

Il documento riporta la relazione tecnica del progetto TEC-MOB: “Rete delle alte tecnologie per la mobilità fisica e virtuale nell'area vasta costiera della Toscana”, con particolare attenzione alle problematiche relative alla sicurezza.

Descrizione del contesto: Il progetto fa riferimento al DOCUP Regione Toscana - misura 1.7.1.

Descrizione della misura: Tramite misura 1.7. la Regione Toscana si pone l’obiettivo di far il sistema delle piccole e medie imprese, favorendo il trasferimento dell’innovazione.

Descrizione dell’Azione: Obiettivo dell’azione è favorire la creazione e il consolidamento di reti d’imprese, organismi di ricerca, centri di servizio e istituzioni pubbliche per lo sviluppo di attività di trasferimento tecnologico e di diffusione dell’innovazione nei seguenti ambiti:

- tecnologie relative ai settori tipici dell’economia toscana;
- tecnologie per lo sviluppo dell’innovazione formale;
- tecnologie dell’informazione, della comunicazione e loro applicazione;
- biotecnologie;
- tecnologie per i beni culturali;
- tecnologie per la riduzione della pressione antropica sull’ambiente.

I programmi realizzati dalle reti che vedono coinvolti più soggetti devono essere indirizzati allo sviluppo di un’azione finalizzata a:

- individuazione di progetti/prodotti e risultati della ricerca suscettibili di successive applicazioni e industrializzazioni;
- approfondimento delle opportunità di mercato (posizionamento del prodotto, concorrenza, lancio sui mercati internazionali, ecc.);
- definizione di accordi di valorizzazione;
- realizzazione di un’attività di commercializzazione dei risultati della ricerca toscana;
- sostegno alla creazione di nuove imprese anche come emanazioni di strutture di ricerca;
- sviluppo di un’attività di dimostrazione, disseminazione e di diffusione dei risultati.

Per mobilità fisica si intende tutto ciò che attiene al sistema 2/3/4 ruote, ma anche la mobilità delle persone; per mobilità virtuale ci riferiremo all'uso delle Information e Communication Technologies (ICT) come una alternativa alla mobilità fisica, in quanto utilizzeremo l'ICT per adempiere ad attività che altrimenti sarebbero state necessariamente espletate per mezzo di "trasporto fisico".

Gli argomenti sono trattati comunque in forma generale, partendo dai concetti di base fino a descrivere applicazioni specifiche. Questa caratteristica di generalità conferisce alla relazione tecnica la valenza di documento informativo sulle tecnologie allo stato dell'arte in materia di sicurezza per mobilità virtuale e fisica.

CAPITOLO 1:
LA MOBILITÀ VIRTUALE

Introduzione

Le ultime due decadi del ventesimo secolo hanno visto varie trasformazioni della nostra società. L'industria che ha prosperato fin dal diciassettesimo secolo è entrata nello stadio finale della sua trasformazione: la cosiddetta società post-industriale o dell'informazione. Nella maggior parte dei paesi sviluppati l'attività economica di produzione, mantenimento e consumo dei beni è divenuta strettamente legata ai servizi legati all'informazione. In particolare, le tecnologie di informazione e comunicazione (ICT), hanno giocato un ruolo critico. A causa della loro ampia diffusione e per l'uso intenso che ne facciamo, le ICT hanno cambiato il nostro modo di vivere e di affrontare tutti gli aspetti della vita sociale.

Le ICT, ad ogni modo, non sono l'unico fattore di questa trasformazione: varie altre "vecchie" tecnologie hanno giocato un ruolo significativo. Fin dai primi anni del ventesimo secolo le moderne tecnologie di trasporto sono diventate infatti sempre più sofisticate, più efficaci e utili. Sono vere e proprie arterie del trasporto nella società globale. È allora importante riconoscere che la natura fondamentale della rivoluzione tecnologica negli ultimi decenni risiede nella complessa interazione fra le vecchie e le nuove tecnologie e il loro assimilamento da parte del tessuto sociale: la Mobilità si manifesta proprio come una trasformazione nelle nostre vite sociali dovuta ad una combinazione tra di esse [1].

Una definizione data al termine "Mobilità" è *l'indipendenza dell'uomo dai vincoli geografici*. Makimoto e Manners, ad esempio, ipotizzano che nei prossimi decenni la maggior parte degli oggetti di casa e di ufficio saranno di dimensioni così ridotte da poter essere portate con sé dalle persone, rendendole quindi "*Geograficamente indipendenti*". Coloro che utilizzino tali tecnologie

saranno “libere di vivere dove preferiscano e di viaggiare quanto vogliano”, diventando così dei “*Nomadi Globali*” [3].

La mobilità è anche legata all’interazione che tali persone effettuano, ovvero la maniera in cui interagiscono l’un l’altro nella vita sociale. La diffusione delle ICT porta alla nascita di nuove configurazioni nei rapporti tecnico-sociali, offre nuovi molteplici dimensioni di mobilità alla interazione umana con gli altri nella vita sociale. In letteratura [1] si espande il concetto di mobilità lungo tre dimensioni: mobilità *spaziale, temporale e contestuale*. Tutte e tre i tipi di interazioni sono rese drasticamente mobili con un utilizzo intensivo delle ICT nella vita di ogni giorno.

La mobilità spaziale è legata al trasporto fisico sia delle persone e degli oggetti [4], ma anche dei simboli. Si consideri ad esempio l’apporto dato di media alla mobilità: la rete televisiva satellitare che diffonde immagini provenienti da ogni parte del mondo. La mobilità spaziale è data infine dal rendere mobile lo spazio stesso, svincolarlo da un “dove” e riconfigurarlo in relazione agli interessi delle persone che vi prendono parte: nasce il concetto di *cyberspazio* e di *cyber-comunità*.

La dimensione temporale delle interazioni umane è resa mobile dalle moderne tecnologie. Se da un lato telefoni e fax riducono i tempi di risposta da settimane a pochi secondi, dall’altro lato i computer, Internet e la posta elettronica li riducono fino a nanosecondi. Le ICT permettono una mobilità temporale nel senso che idee e informazioni possono essere istantaneamente trasmesse ed accedute simultaneamente da ogni parte del mondo [6].

L’immanenza e la contestualità delle azioni umane è di fondamentale importanza per capire la natura delle interazioni umane: oltre a il “dove” (spazialità) e a il “quando” (temporalità) si deve considerare anche il “in che modo”, “in che particolare circostanza” e “verso quali attori”. La mobilità contestuale riguarda la flessibilità che i cammini di tali interazioni percorrono attraverso differenti contesti [1].

Da ora in poi, quando si considera il concetto di mobilità dobbiamo avere a che fare con la contestualità così come la spazialità e temporalità delle relazioni nella vita sociale.

Mobilità virtuale e mobilità fisica

Per mobilità virtuale ci si riferisce all’uso delle Information e Communication Technologies (ICT) come una alternativa alla mobilità fisica. Ovvero, si tratta dell’utilizzo di ICT per adempiere ad attività che altrimenti sarebbero state necessariamente espletate per mezzo di “trasporto fisico”.

Il passaggio dalla connettività fissa e corto raggio delle Local Area Network (LAN) a quello delle Wide Area Network (WAN) fino ad arrivare ad Internet con la sua connettività a larga scala,

presenta dei fenomeni che sono direttamente osservabili:

a) Esistono “locazioni virtuali”, ovvero dei confini gestiti separatamente dove girano gli applicativi e dove sono protetti da potenziali attacchi per mezzo di firewall.
b) Le “locazioni fisiche” arrivano ad incidere sulla effettiva connettività. Da una parte all’altra del pianeta la velocità della luce risulta comunque un fenomeno tangibile: un applicativo, per quanto veloce possa trasferirvi informazioni metterà sempre almeno 1/10 di secondo, indipendentemente dalla tecnologia impiegata!
c) Ci sono le “fluttuazioni della banda”, dovute a congestioni nel traffico delle informazioni che risultano non predicibili in maniera certa
d) Si introducono i “malfunzionamenti nella comunicazione” che sono irrisolvibili nella rete (la rete non ha limite superiore ai ritardi nella comunicazione).

Mobilità hardware e mobilità software

Ci sono due visioni sovrapposte della mobilità virtuale: la **mobilità hardware** (*Mobile Computing*) e la **mobilità software** (*Mobile Computation*)[[1]] e i confini tra i due non sono così netti.

La Mobile Computation si ha quando i programmi in esecuzione non devono essere per forza legati ad un singolo nodo della rete, ma il flusso di dati attraversa le barriere tra le diverse locazioni virtuali, le chiamate a funzioni remote vengono risolte in chiamate locali eludendo così il vincolo delle locazioni fisiche, non sono soggette alla fluttuazione della banda poiché possono spostare le computazioni in aree meno congestionate, evitando così i malfunzionamenti predicibili e aggirando quelli in corso.

Il Mobile Computing è un paradigma che si è evoluto indipendentemente dallo Web ed è legato alla possibilità per i diversi nodi di muoversi all’interno di una rete e attraverso reti differenti. Al giorno d’oggi computer portatili e smartphone si muovono abitudinariamente, in futuro avremo intere reti che diventeranno esse stesse mobili. Altri esempi esistenti di questo tipo di mobilità sono ad esempio una Smartcard che entra nel lettore di un computer di rete, un RF-ID attivo che varca il confine di una zona monitorata, un PDA wireless che entra nell’hot spot di un edificio aziendale. Questa visione indipendente della mobilità porta a tutta una nuova serie di problematiche, prima fra tutti è quella dell’attraversamento fisico delle diverse reti. Risulta necessaria una gerarchia di controlli su ogni confine per rafforzare il monitoraggio e per richiedere i diritti per l’attraversamento sia della singola entità (del singolo nodo) che di una intera rete mobile!

La mobilità hardware e quella software non vanno necessariamente affrontate in maniera distinta. Si pensi ad una programmatore che sviluppa codice portabile su diverse macchine di differenti aree virtuali e che lo faccia comodamente dal suo laptop mentre che si sposta da una azienda all’altra: in

questo caso la giusta policy si sicurezza da adottare potrebbe essere quella che associa ad ogni dominio pari garanzie di sicurezza sia per le barriere fisiche (le porte d'ingresso) sia per quelle virtuali (i firewall).

Il rovescio della medaglia per la connettività mobile è l'intermittenza del servizio. Questo può accadere per una varietà di motivi, può affliggere sia la mobilità hardware (ci si muove in una zona assente da copertura di rete) che quella software (lo spostamento avviene "virtualmente" attraverso diversi domini amministrativi), ad ogni modo è una caratteristica essenziale della mobilità stessa.

CAPITOLO 2:
LE TECNOLOGIE DI SUPPORTO ALLA MOBILITÀ

La necessità oggettiva di Network Mobility

Al giorno d'oggi riunire e condividere la business intelligence in tempi rapidi è essenziale per la competitività aziendale. Una rete vasta e che è in continua espansione ha bisogno di una connettività senza i limiti delle Local Area Networks (LANs).

La progettazione di una rete mobile può essere fatta proattivamente o reattivamente. In alcuni casi vengono portate le connessioni wireless alla rete in una maniera controllata e gestita centralmente, mentre in altri casi è chi usufruisce della connessione a scegliere fra i punti di accesso, relegando agli amministratori il compito di gestire la situazione. Qualsiasi sia il caso, non è pensabile un ritardo nello sviluppo di una soluzione mobile: l'imperativo è di incrementare la produttività e l'uniformità dei servizi senza compromettere la sicurezza della rete [7].

L'evoluzione della rete aziendale verso la Mobilità

Fino a poco tempo fa la rete cablata (in particolare la Ethernet) è andata evolvendosi mossa soprattutto dalla necessità di spostare files più velocemente e senza interferenza. La Ethernet è passata infatti da velocità di 10 Mbps (mega bit per secondo) a 100Mbps, poi al Gigabit (1 Giga è pari a 1000 Mega) fino a 10 Gigabit, diventando così una tecnologia assai diffusa per costruire LAN robuste ed efficienti.

L'Ethernet si sta adesso dirigendo verso nuovi domini geografici come le Metropolitan Area Networks (MANs) con connettività di tipo wireless e fa la sua comparsa tutta una nuova classe di applicazioni, come il Voice over Internet Protocol (VoIP). Questa evoluzione sta cambiando la rete aziendale dall'ottica di una condivisione di file e stampanti ad una più comunicativa e, forse più

importante, a una con risorse di tipo “ovunque e a qualunque momento (anytime, anywhere)”.
Ogni innovazione per diventare evoluzione deve essere accompagnata da tecniche e tecnologie di supporto: non appena il raggio delle applicazioni digitali mobili prolifera e si diversifica sta agli amministratori cercare nuove soluzioni di comando e di controllo facendo fronte a problemi di integrazione, gestione e sicurezza che ne conseguono. Ad oggi le reti con e senza fili devono avere a che fare con una classe di applicativi che richiede che coesistano la qualità del servizio, il traffico controllato e limitazioni alla banda occupata.
In un ambiente mobile e caratterizzato da accessi prevalentemente remoti il passo logico successivo è quello di mantenere l’integrità dei programmi, soprattutto se si considera che il confine tra le reti cablate e senza fili sta diventando sempre meno marcato. I punti di accesso wireless fungono da ingressi per gli impiegati, per gli ospiti graditi e non. Essi molto spesso sono realizzati con semplici permessi o con un controllo di accessi che ha limitate capacità di determinazione dei diritti associati all’utente. Possono magari monitorare alcuni dispositivi attivi ma non sono capaci di gestire l’intero carico di traffico né di modellarlo alle esigenze degli altri utenti nella rete: questo è particolarmente importante quando si abbia esigenza di affidare risorse o di allinearle a quelle necessarie a particolari applicativi o utenti.
La diffusione delle tecnologie mobili porta la rete ad estendere i suoi confini: si fornisce connettività mobile con tecnologie wireless locali, con hot spot pubblici ad alta velocità e con l’appoggio della telefonia cellulare digitale. È necessario avere soluzioni che coprano queste differenti infrastrutture mantenendo la continuità della connessione. Non è pensabile che le decisioni sul controllo accessi, sulla modellazione del traffico e sull’ottimizzazione della banda avvengano in maniera centralizzata: tali funzionalità di controllo vanno spostate verso gli estremi della rete. Solo capendo come mantenere centrale il comando spostando il controllo agli estremi si può riuscire ad essere mobili mantenendo integrità delle applicazioni, allocazione della banda e sicurezza nella rete.

Le reti esistenti

Ad oggi la rete di connessione mobile include tecnologie sia cablate (wired) che senza fili (wireless). Le cablate comprendono sia porte LAN dappertutto in un ufficio, un edificio o anche una vasta area, comprendono connettività ti tipo dial-up ma anche reti Virtual Private Network (VPN). Le reti wireless (WLAN) proseguono la loro inarrestabile espansione e si affermano come una essenziale risorsa. Infatti si stima che gli utenti spenderanno nel mercato delle WLAN con un tasso di crescita annuo pari al 12 percento dal 2004 fino agli 1,6 miliardi di dollari del 2009, con il 31 percento del totale speso tra switch e controller wireless [8].

Le reti mobili, sia cablate che senza fili, permettono agli utenti di avere accesso ad una vasta gamma di servizi per ogni tipo di necessità. Le soluzioni portano a notevoli benefici, ma comportano anche problematiche che gli amministratori devono affrontare con una rete unficata e che enfatizzi il rapporto funzionale fra tutti i nodi di cui è composta. Un recente studio [9] ha stimato che alcune delle domande che si pongono gli amministratori sono del tipo: "*I dati che risiedono nella rete e che sono acceduti dagli utenti sono anche protetti dagli hackers o altri potenziali minacce?*", "*Aggiungendo mobilità si può effettuare una differenziazione di privilegi di accesso tra i vari utenti e i diversi tipi di traffico?*","*La qualità del servizio (QoS) può essere controllata e si può ottimizzare la banda di trasmissione?*", "*Se ne può trarre un vantaggio competitivo senza vincolare eccessivamente lo sviluppo di applicativi?*" oppure ancora "*L'infrastruttura di rete mobile sarà abbastanza flessibile da soddisfare le esigenze degli utenti man mano che si espande e che si adatta?*".

A dispetto del rapido aumento della domanda per servizi di rete mobili, c'è ancora qualche riluttanza fra gli amministratori ad installare accessi remoti o wireless alla rete aziendale. Benché noti i potenziali benefici che le WLAN possono fornire, alcuni non giudicano vantaggioso lo sviluppo e la gestione di una rete mobile, o temono delle minacce alla sicurezza o ritengono che non verranno supportate le applicazioni che richiedono QoS e utilizzazione di banda. In effetti, un applicativo mobile di nuova generazione richiede nuovi livelli di controllo e sicurezza così come capacità di adattamento molto più sofisticate.

Implementare la mobilità in una realtà di tipo aziendale porta spesso ad una difficile scelta: da una parte ritardare l'adeguamento all'accesso remoto o wireless alle proprie reti e avere a che fare con i problemi di gestione del traffico dovuti agli accessi "autogestiti" dei dipendenti. Oppure preventivare l'implementazione di un accesso remoto controllato e far fronte a tutti gli adeguamenti relativi a sicurezza, affidabilità e evoluzione della tecnologia. Fortunatamente ci sono nuove tecnologie che risolvono il problema di se e quando implementare la mobilità, permettendo alle azione di introdurre le WLAN in maniera proficua ed efficiente assicurando la protezione dell'informazione.

Per implementare la mobilità è necessario mantenere il controllo a partire dal centro della rete fino ai suoi confini, sia che gli accessi siano wireless o meno. La mobilità deve permettere agli utenti di muoversi di locazione in locazione attraverso sottoreti diverse ma mantenendo la sessione e senza richiedere di nuovo una autenticazione. Per far questo l'infrastruttura deve incorporare soluzioni affidabili, facili da usare, accettabili come costi, sicure e ben integrate.

Le reti cablate

Ethernet è il nome di un protocollo per reti locali, sviluppato a livello sperimentale da Robert Metcalfe e David Boggs, suo assistente, alla Xerox PARC. La data ufficiale è il 1973 quando Metcalfe scrisse un promemoria ai suoi capi della Xerox sulle potenzialità di Ethernet. Nel 1976 Metcalfe e Boggs pubblicano un articolo dal titolo Ethernet: Distributed Packet-Switching For Local Computer Networks.

L'obiettivo originale dell'esperimento era ottenere una trasmissione affidabile a 3Mbps su cavo coassiale in condizioni di traffico contenuto, ma in grado di tollerare bene occasionali picchi di carico. Per regolamentare l'accesso al mezzo trasmissivo era stato adottato un protocollo di tipo CSMA/CD (Carrier Sense Multiple Access / Collision Detect). Il successo dell'esperimento suscitò forte interesse e portò alla formazione di un gruppo di imprese, costituito da Xerox Corporation, Intel Corporation e Digital Equipment Corporation, che nel 1978 portarono alla standardizzazione 802.3 e il 30 settembre 1980 a pubblicare la versione 1.0 dello standard Ethernet.

Intanto Metcalfe lasciò Xerox nel 1979 per promuovere l'uso del PC e delle LAN per cui fondò 3Com. Metcalfe spesso attribuisce il successo di 3Com a Jerry Saltzer. Questi collaborò alla stesura di un articolo importantissimo che suggeriva che l'architettura token ring fosse teoricamente superiore alla Ethernet. Con questo le grosse aziende decisero di non puntare su Ethernet mentre, al contrario, 3Com poté creare un business intorno al sistema riuscendo a guadagnarsi un ottimo vantaggio tecnico e a dominare sul mercato quando Ethernet prese piede.

Successivamente, l'interesse delle imprese del settore aumentò al punto che l'IEEE costituì alcuni gruppi di studio finalizzati a perfezionare e consolidare Ethernet, nonché a creare numerosi altri standard correlati. Uno dei risultati raggiunti fu la pubblicazione, nel 1985, della prima versione dello standard IEEE 802.3, basato sull'originale specifica Ethernet, ma non completamente identificabile con essa. In seguito, lo standard Ethernet come tale non è più stato mantenuto, ma il termine continua ad essere usato quasi come fosse un sinonimo di IEEE 802.3, sebbene i due standard non coincidano affatto.

Al livello fisico del modello ISO/OSI, 802.3 prevede esclusivamente trasmissioni via cavo in banda base, a velocità di 10, 100 e 1000 Mbps, su cavi coassiali, doppini intrecciati (schermati e non) e fibre ottiche.

Le reti wireless

La nascita delle comunicazioni senza fili risale al tardo 1800, quando Marconi stabilì il primo ponte radio tra una stazione a terra e un rimorchiatore. Da allora i sistemi di comunicazione wireless si

sono sviluppati ed evoluti ad un tasso di crescita vertiginoso soprattutto nelle ultime decadi. Il bacino di utenza è passato dalle centinaia di unità dell'inizio secolo fino ai quasi 1,5 miliardi nel 2004.

Le prime comunicazioni consistevano in una *base station* con un trasmettitore ad alta potenza che copriva una vasta area. Ogni stazione poteva servire solo un ristretto numero di utenti ed era inoltre molto costosa. I vari sistemi erano infine isolati l'uno dall'altro e solo alcuni comunicavano con la rete telefonica pubblica (*Public Switched Telephone Network – PSTN*). Oggi la telefonia mobile consiste in un raggruppamento di base station con trasmettitori a bassa potenza. Ogni base station serve un'area geografica denominata cella e lo stesso canale può essere riutilizzato in celle differenti senza causare eccessiva interferenza grazie alla bassa potenza impiegata.

La mobilità è uno degli aspetti chiave nei sistemi di comunicazione senza fili. Esiste la necessità di tracciare gli utenti che si muovono tra celle differenti cambiando il canale radio di comunicazione. Un dispositivo che passa da un canale all'altro si dice che faccia un'operazione di *hand off*. Per permettere tale attraversamento è necessario un meccanismo di segnalazione e di gestione del salto di canale. La chiamata è un altro aspetto chiave nelle reti mobili: utilizza un canale comune per localizzare gli utenti nell'area di servizio e per segnalare messaggi.

Sistemi di comunicazione wireless

La tecnica di accessi multipli è quella che permette agli utenti di condividere un canale di comunicazione massimizzandone la capacità. Esistono tre schemi di accesso multiplo: suddivisione della frequenza (*Frequency Division Multiple Access – FDMA*), del tempo (*Time Division Multiple Access – TDMA*) e del codice (*Code Division Multiple Access – CDMA*).

Senza scendere in dettagli tecnici basti sapere che in caso di FDMA viene assegnata ad ogni trasmissione una banda di frequenza per tutta la durata della chiamata, a sua volta suddivisa in canali. Nel TDMA tutti condividono la stessa banda ma ad ogni chiamata è assegnato uno slot temporale in cui è lecito trasmettere. In caso di CDMA si condividono banda e intervalli temporali, tutte le trasmissioni sono fatte contemporaneamente ma ad ognuna è associato un codice unico: sta al ricevitore il compito di separarle. Sono infine possibili anche combinazioni di questi tre tipi di schema.

Si descrivono alcune implementazioni di sistemi di comunicazione wireless [10].

Advanced Mobile Phone Service (AMPS)

È stata la prima implementazione del sistema di comunicazione mobile cellulare. È un sistema

analogico in cui ogni utente utilizza il canale radio di 30KHz. Ogni base station opera nella banda tra 800 e 900 MHz con trasmissione e ricezione su frequenze differenti (*frequency division duplex – FDD*). Ognuna delle due portanti ha 416 canali divisi in gruppi di sette celle.
Questo sistema analogico evolvette presto in uno digitale Digital AMPS (DAMPS, anche noto come IS-54), operante in modalità TDMA.

Global System for Mobile (GSM) Communication

Introdotto per la prima volta nel 1992 come standard europeo lo standard GSM [11] di comunicazione è stato adottato in tutto il mondo. Le frequenze a cui opera sono alla banda di 800MHz e 1800 MHz in europa mentre negli Stati Uniti si usa la banda a 1900MHz. Si utilizza la suddivisione FDD con entrambi i canali radio che utilizzano una banda di 200 KHz.
Lo schema di accesso multiplo è il TDMA: fino ad otto utenti condividono tale canale occupando una banda di 25KHz. La voce è codificata secondo un preciso algoritmo di compressione, ed è sottoposta a correzione degli errori e ad interlacciamento.
La continuità del servizio è assistita dal cellulare, che invia periodicamente alle celle un report della potenza del segnale. La base station decide, sulla base di tali report, se effettuare il salto della comunicazione da un canale all'altro.

General Packet Radio Service (GPRS) Systems

GPRS è nato come miglioramento al GSM introducendo il supporto allo scambio di pacchetti dati. È stato standardizzato dallo ETSI (European Telecommunication Standards Insitute) [12] e [13].
Utilizza la commutazione di pacchetti per trasferire dati ad alta velocità, ottimizzando l'utilizzo del canale radio e della rete: li considera separatamente svincolandosi così dalla particolare implementazione.
Sono definiti nuovi canali radio dove ad ogni utente viene assegnato fino ad otto unità di tempo in modalità TDMA, permettendo così velocità di trasferimento da 9Kbps fino a più di 150Kbps.
Supporta il protocollo IP permettendone il veicolamento attraverso la rete GPRS: il traffico viene incapsulato (*tunneling*), compresso e protetto da ritrasmissione per una maggiore efficienza e affidabilità. È stato progettato per supportare l'intermittenza del servizio e il trasferimento a tratti (*burst*). Sono infine stati definiti quattro tipologie di QoS.

Enhanced Data Rates for Global Evolution (EDGE)

EDGE è l'ultima miglioria effettuata per sfruttare a pieno la capacità della rete e le velocità di

trasferimento in GSM/GPRS. È stato anch'esso standardizzato dall'ETSI e offre agli operatori la possibilità di fornire servizi con transfer rate paragonabili alle reti wireless di terza generazione.
EDGE utilizza la stessa struttura di tipo TDMA, lo stesso canale logico e la stessa banda di 200KHz delle reti GSM. Introduce la modulazione 8-PSK che permette transfer rate di picco oltre i 400Kbps per utente. La comunicazione inoltre si adatta alla qualità della ricezione e introduce una ridondanza incrementale per migliorare efficienza e affidabilità. EDGE è inoltre pienamente compatibile con le reti GPRS che ancora non implementino il suo standard.

Universal Mobile Telecommunications System (UMTS)

L'UMTS è uno dei sistemi menzionati dall'Unione Internazionale delle Telecomunicazioni (UIT) nel quadro del progetto mondiale IMT 2000 volto alla definizione di sistemi mobili di terza generazione (3G). Tale scelta è applicata al fine di promuovere lo sviluppo di sistemi mobili in grado di offrire al mercato di massa una serie di servizi telefonici e multimediali mobili. L'UMTS è uno standard che si basa sulla tecnologia W-CDMA (Wideband code division multiple access) per i segnali di fonia (voce) con modalità FDD, e sulla TD/CDMA bande di frequenza asimmetriche, per la trasmissione di dati, con modalità TDD. Grazie al trasferimento dati ad alta velocità, l'UMTS consente di arrivare fino a 2Mbps per utenze a bassa mobilità, fino a 384 Kbps su micro e macro celle con una limitata mobilità. L'UMTS offre un data rate (velocità trasmissione dati) on demand (su richiesta) e le frequenze di trasmissione utilizzate sono comprese fra 1,9Ghz ed i 2,2Ghz, diversamente dallo standard GSM che trasmette a 900Mhz e a 1800Mhz.

Bluetooth

Bluetooth è una tecnologia radio a basso consumo energetico, corto raggio e bassi costi sviluppata dal Bluetooth Special Interest Group [15].
L'obiettivo del Bluetooth è quello di rimpiazzare il cablaggio per l'interconnessione di dispositivi elettronici e creare wireless *Personal Area Network* (*PAN*). Il protocollo di rete è progettato per essere robusto alle interferenze – safety – e agli attacchi – security: lo standard Bluetooth prevede meccanismi di autenticazione e crittografia nativi. Bluetooth per garantire la massima interoperabilità tra i dispositivi fa uso della banda ISM (*Industriale, Scientifica e Medica*) nell'intorno dei 2.45Ghz, libera a livello globale. Fornisce un rate trasmissivo fino a 720Kbps in un raggio di 10 metri e fino a 100 con un incremento di potenza.

Infrarosso (IrDA)

È un'altra tecnologia per trasmissioni a corto raggio tra due dispositivi. IrDA è l'acronimo di *Infrared Data Association* [16], una organizzazione fondata nel 1993 e devota a definire specifiche per comunicazioni senza fili. Quest'ultima avviene in maniera direzionale, è infatti necessaria una visuale tra i due dispositivi, e garantisce transfer rate fino a 115.2Kbps. Ulteriori migliorie hanno aumentato tale limite fino a 4Mbps.

802.11 Wireless Local Area Network (WLAN)

Una WLAN è un sistema di comunicazione che permette ad un utente di connettersi ad una LAN utilizzando tecnologie a radiofrequenza. Le wireless LAN hanno guadagnato una grande popolarità sul mercato in maniera trasversale: si pensi al campo sanitario, studentesco, alberghiero, aeroportuale, manifatturiero. Queste industrie hanno tratto profitto dai vantaggi offerti dalle WLAN, potendo usufruire di accessibilità di dati sempre e ovunque combinato alla mobilità degli utenti lungo tutta la copertura della rete. Gli amministratori di rete non necessitano la messa in posa di cavi per creare o per espandere la propria rete.

Lo standard della tecnologia adottata dalle WLAN è stato definito dalle IEEE 802.11 [14], e va sotto il nome di Wi-Fi (*Wireless Fidelity*). Esiste una famiglia di specifiche: 802.11, 802.11a, 802.11b, 802.11e, 802.11g. Verrà illustrata solo quest'ultima dato che è lo standard più recente approvato dallo IEEE.

Il rate di trasmissione assume la progressione di 6, 9, 12, 18, 24, 36, 48 Mbps e ha il massimo a 54Mbps. Risulta retro compatibile con lo standard ampiamente diffuso 802.11b ed opera, come quest'ultimo, alla frequenza dei 2.4GHz della banda ISM. Utilizza la suddivisione ortogonale di frequenza ODFM (*Orthogonal Frequency Division Multiplexing)* con tre canali non sovrapposti. La copertura garantisce un rate di trasmissione di 6Mbps teorico alla distanza di 54,8 metri

CAPITOLO 3:
I PROTOCOLLI E I DISPOSITIVI DI SUPPORTO ALLA MOBILITA

Introduzione

Fino a più di 30 anni fa Internet non esisteva. Le comunicazioni interattive si basavano sul telefono, ai costi delle linee PSTN. Lo scambio di dati era molto costoso (soprattutto per lunghe distanze) e nessuno immaginava al video interattivo (esisteva soltanto la televisione, che, com'è noto, non è interattiva).

Pochi anni fa abbiamo assistito ad alcuni importanti fenomeni: PC diffusi a larga scala, nuove tecnologie per comunicare come i telefoni cellulari e, finalmente, la grande rete: Internet; la gente ha iniziato ad utilizzare i primi servizi email, chat, ecc. e il business è rinato con il web permettendo alle persone di acquistare prodotti via Internet con un "click".

Oggi assistiamo ad una vera e propria rivoluzione nel campo della comunicazione: tutti iniziano ad usare il PC con Internet nel lavoro e nel tempo libero per scambiare dati (come immagini, suoni, documenti) e, in alcuni casi, per parlare usando applicativi come Microsoft Netmeeting o Internet Phone. In particolare inizia a diffondersi un'idea comune che potrebbe rappresentare il futuro e che permette la comunicazione vocale in tempo reale: VoIP.

La telefonia IP

VoIP sta per 'V'oice 'o'ver 'I'nternet 'P'rotocol. Come dice il termine VoIP prova a far passare la voce (prettamente quella umana) attraverso i pacchetti IP e in definitiva attraverso Internet. La tenologia VoIP può avvalersi di schede hardware acceleratrici per raggiungere tale scopo ed è

possibile il suo l'utilizzo in ambiente PC.

VoIP lavora proprio in questo modo, digitalizzano la voce i pacchetti, mandandoli in rete e riconvertendoli in voce una volta giunti a destinazione. I vantaggi del formato digitale sono notevoli: possiamo comprimere i dati, instradarli (utilissimo su Internet), convertirli nuovamente in un formato più consono al mezzo utilizzato. Sappiamo anche che il segnale digitale è più ”resistente” ai disturbi rispetto a quello analogico (vedi GSM contro TACS).

Le reti TCP/IP sono costituite di pacchetti IP contenenti un'intestazione (per controllare la comunicazione) e di una parte dati: VoIP utilizza questo paradigma per attraversare la rete ed arrivare a destinazione.

I Pacchetti di voce risiedono in pacchetti RTP (Protocollo di trasporto Real-Time) che a loro volta giacciono su pacchetti UDP-IP. Prima di tutto notiamo che VoIP non utilizza il protocollo TCP perché troppo pesante per le applicazioni multimediali (che sono, di per se stesse, ”real time”), quindi abbiamo bisogno di usare l'UDP. Secondo, con l'UDP non possiamo implicitamente controllare l'ordine di arrivo dei pacchetti o quanto impiegano ad arrivare (concetto di datagramma): entrambi sono molto importanti per ottenere una buona qualità audio della voce (per poter distinguere le parole) e una buona qualità di conversazione (la facilità con cui si segue un discorso).

Il SIP come supporto alla mobilità

il Session Initiation protocol (SIP) è un protocollo di segnalazione definito dal IETF (Internet Engineering Task Force) per stabilire delle connessioni real-time e conferenze su reti IP. Ogni sessione può includere diversi tipi di flussi dati come audio e video, sebbene ora la maggior parte delle estensioni SIP riguardino le comunicazioni audio. È un protocollo di tipo testuale e si avvicina molto ad HTTP (hypertext transfer protocol) come struttura. SIP è indipendente dal tipo di rete su cui si appoggia, è stato strutturato per essere uno standard aperto e scalabile, in modo che possa essere utilizzato per diversi scopi.

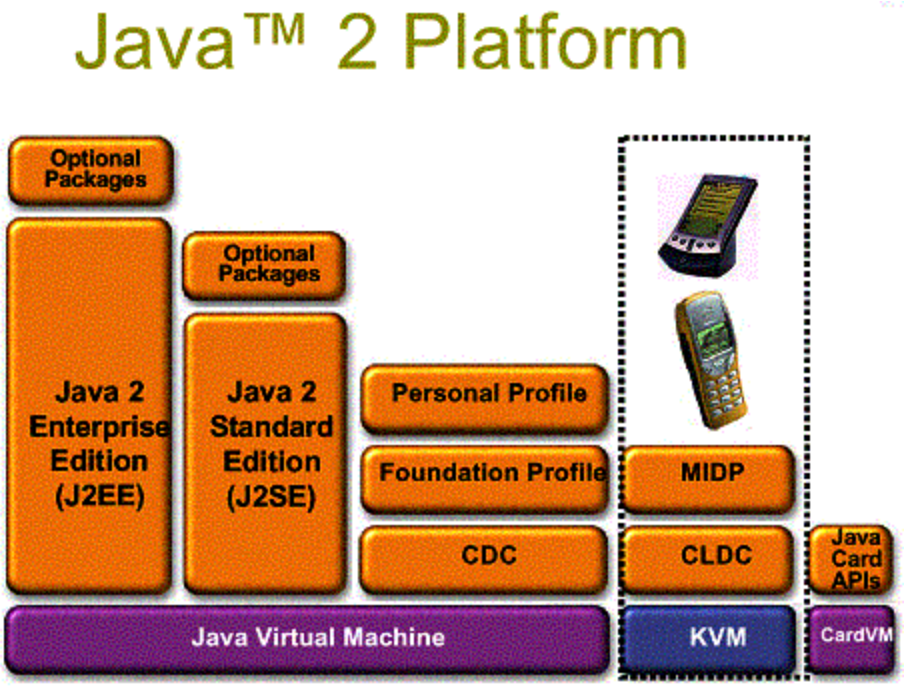
Smartphone

La continua crescita della capacità di calcolo di sistemi portabili affiancata all'avvento di avanzati sistemi operativi per sistemi handheld ha portato all'integrazione di servizi di voce, multimedia, dati e networking in un unico dispositivo portabile. Gli smartphone sono dispositivi embedded che offrono oltre i servizi tipici di un telefono cellulare altre funzionalità tipiche dei PC: la navigazione del Web, lo scambio di e-mail, accesso a database,…

Essi si sono già conquistati un ruolo da protagonisti tra i dispositivi di supporto alla mobilità.

Java Micro Edition

L'introduzione della piattaforma Java 2 Micro Edition negli smartphones permette lo sviluppo di applicazioni che offrono tutte le funzionalità necessarie per garantire la "sicurezza". J2ME è la piattaforma Java per dispositivi embedded o consumer come mobile phones, PDAs, decoder TV e molti altri ancora. J2ME esporta tutti i benefici di Java su misura per dispositivi embedded, sia connessi alla rete che meno. L'architettura J2ME definisce configurazioni, profili e package opzionali che permettono di definire un ristretto numero di classi di dispositivi in un insieme che invece è molto vasto. Una certa applicazione è compatibile con tutti i dispositivi appartenenti ad una certa classe.



Una configurazione è caratterizzata da una Java Virtual Machine e da un set minimale di librerie – core libraries – per sfruttare le funzionalità di base di una certa classe di dispositivi. Attualmente si distinguono due configurazioni: CLDC – Connected Limited Device Configuration – e CDC – Connected Device Configuration. CLDC è la configurazione per devices con una connessione alla rete non permanente e a non a banda larga, processore lento a 16 o 32 bit, autonomia limitata e memoria per l'esecuzione di applicazioni tra i 32KB e i 512KB. CDC invece è la configurazione per dispositivi con maggiore connettività, processori più veloci, e memoria di almeno 2MB per la JVM e le applicazioni associate.

Il profilo è lo strato superiore alla configurazione ed offre un ambiente di esecuzione per le applicazioni. È caratterizzato da un set di API di alto livello che offre interfacce tra l'utente, l'applicazione e servizi. Il profilo diffuso per gli smartphone è il MIDP – Mobile Interface Device Profile. MIDP offre, oltre alle interfacce utente, librerie per la connettività, memorizzazione di dati

e gestione delle applicazioni. Combinato con CLDC, il MIDP offre un ambiente di esecuzione per le applicazioni J2ME che sfrutta e ottimizza l'impiego delle risorse dei dispositivi handheld. Di MIDP si distinguono due versioni: MIDP 1.0 e MIDP 2.0. Entrambe le versioni non supportano calcoli in virgola mobile, caricamento dinamico delle classi, Java Nativa Interface, riflessione e gestione del file system. Entrambe offrono funzionalità per la gestione degli eventi, multithreading, networking, una limitata gestione degli errori, un sistema per la memorizzazione permanente delle informazioni estraneo al file system del device (RMS - Record Management System).

MIDP 2.0 offre funzionalità avanzate per i servizi di crittografia e offre una migliore interfaccia utente con form più curati. Al supporto ad HTTP aggiunge il supporto per HTTPS basato su tecnologie:

- TLS 1.0. Transport Layer Security è un protocollo aperto che opera sopra al livello trasporto, usato per permettere una comunicazione sicura tra due applicazioni, fornendo al flusso di dati servizi di autenticazione, integrità e riservatezza. Deriva da SSL.
- SSLv3
- WTLS - Wireless Transport Layer Security. Strato dello stack protocol WAP, basato su TLS.
- WAP TLS

Inoltre MIDP 2.0 supporta l'architettura push: una applicazione non in esecuzione può essere invocata da una sorgente registrata. Ad esempio alla richiesta di una connessione in ingresso su una certa porta può essere associata una determinata applicazione: quando perviene tale richiesta l'applicazione viene messa in esecuzione dal sistema operativo dello smartphone, eventualmente chiedendo conferma all'utente. Anche se MIDP 2.0 supporta l'architettura push, non tutti i devices – anche se MIDP 2.0 – sono in grado di gestire i push register.

Esempi di package opzionali per smartphones sono:

- WMA - Wireless Messaging API (JSR-120) , per la trasmissione e la ricezione di messaggi, sia testuali che meno.
- MMA -Mobile Media API (JSR-135) , per la gestione di suoni e video.
- Bluetooth API (JSR-82 No OBEX), per la gestione del Bluetooth.

SMS

Le Wireless Messaging APIs costituiscono un package opzionale di J2ME definito dal Java Community Process nel JSR 205. Sono un insieme di classi per la trasmissione e la ricezione di messaggi, inclusi i noti SMS, contenenti testo oppure dati generici. Le WMA estendono il GCF e la messagistica è connection oriented: una connessione può essere aperta sia in modalità server che in

modalità client.

Ogni messaggio implementa l'interfaccia `Message` la quale schematizza il contenuto in due parti: indirizzo e dati. La parte dati può essere a sua volta implementata come `TextMessage` oppure come `BinaryMessage`: queste due interfacce permettono di manipolare il contenuto di un messaggio come una stringa oppure come un array di byte.

RF-ID e supporto alla logistica

RFID sta per Radio Frequency IDentification e indica una tecnologia ad onde radio che consente di tracciare e controllare, in un area ristretta determinati soggetti o prodotti, in maniera automatica, che contengono un rilevatore adeguato. Il sistema prevede un lettore di tag e il tag stesso, costituito da un chip che contiene le informazioni e da una antenna che consente la ricezione/trasmissione dei dati. Anche il Telepass è una applicazione della tecnologia RFID, ma esistono tag molto più piccoli in grado di essere contenuti nelle etichette dei prodotti di largo consumo. La catena statunitense di supermercati Wal Mart ha introdotto tag RFID in tutti i prodotti che commercializza, per garantire le tracciabilità e il controllo della produzione. Tuttavia, le applicazioni sono in crescita e sono le più diverse: controllo e gestione del magazzino, controllo e gestione dei bagagli in un aeroporto, controllo giacenze e distribuzione di medicinali, controllo spostamenti di mezzi nell'area aziendale. Ma sono solo esempi. Fino ad ora il problema più evidente nell'adozione di RFID è rimasto quello legato alla gestione della privacy. Se al supermercato acquisto prodotti con tag RFID e i tag vengono associati alla mia persona posso facilmente essere tracciato e i miei gusti o abitudini possono essere registrate. Oppure le aziende potrebbero facilmente controllare gli spostamenti dei propri dipendenti, grazie al tesserino aziendale.

CAPITOLO 4:
MOBILE TRUST & SECURITY

Criticità in ambiente mobile

Gli smartphone sono dispositivi embedded che offrono oltre i servizi tipici di un telefono cellulare altre funzionalità tipiche dei PC: la navigazione del Web, lo scambio di e-mail, accesso a database,…

Uno smartphone può contenere informazioni sensibili che devono essere cifrate per preservarne la segretezza qualora il dispositivo fosse smarrito o peggio ancora rubato. Inoltre in molti contesti applicativi può rilevarsi essenziale o preferibile una comunicazione tra il dispositivo mobile ed un altro terminale che garantisca l'autenticazione, la segretezza e l'integrità delle informazioni.

Sicurezza nell'ambiente Java Wireless

Il Mobile Information Device Profile (MIDP), progettato come espansione del Connected Limited Device Configuration Profile (CLDC), permette lo sviluppo di applicazioni che possono essere scaricate on-line ("Over The Air") da reti aperte. Dopo il download dell'applicativo, il software verrà eseguito sul dispositivo dell'utente. La domanda che potrebbe sorgere è la seguente: l'utente dell'applicativo deve preoccuparsi di possibili problemi di sicurezza, quali potenziali danneggiamenti al proprio cellulare (o smartphone), cancellazione dei dati dal dispositivo o trasferimento dati verso un server remoto?

Analizzando bene l'architettura Java verranno messi in luce aspetti che descrivono come tali situazioni, non debbano essere ritenute un problema per la sicurezza del dispositivo utente.

Il meccanismo di sicurezza adottato nella versione Java 2 Standard Edition (J2SE) non è portabile nell'architettura CLDC/MIDP principalmente a causa dell'onerosa richiesta di memoria necessaria a tale meccanismo. In ogni modo, può essere utile un breve riassunto sul modello di sicurezza "sandbox" adottato con le applet per poi introdurre e discutere:

- Il modello di sicurezza CLDC/MIDP
- Spiegare il funzionamento del modello di sicurezza “sandbox” dell’architettura CLDC/MIDP
- Capire quali tradeoff sono stati scelti per raggiungere tale modello
- Discutere le funzioni eliminata dal CLDC/MIDP
- Trattare le differenze tra i due modelli di sicurezza adottati nelle due differenti tecnologie (J2SE e J2ME)
- Fornire alcune indicazioni su come implementare meccanismi di sicurezza end-to-end

La sicurezza vista nell’ambito delle applicazioni Java Wireless

I meccanismi di sicurezza descritti per la J2SE non sono riutilizzabili per i dispositivi CLDC/MIDP a causa dei notevoli requisiti in termini di memoria per l’esecuzione di questi meccanismi. Quindi sono necessari alcuni compromessi per definire il modello di sicurezza in ambiente CLDC/MIDP. La linea guida seguita si riassume nel concetto di mantenere le cose in modo semplice. L’attenzione viene incentrata su due aree:

1) sicurezza della KVM di basso-livello

2) la sicurezza di livello applicativo

La sicurezza nella KVM a basso-livello

In questa area, una applicazione MIDP scaricata sul device ed eseguita dalla K Virtual Machine (KVM) non deve assolutamente danneggiare il dispositivo nel quale è in esecuzione. Questo obiettivo può essere garantito dal class verifier Java il quale s’incarica di controllare che le classi in questione non contengano riferimenti a locazioni di memoria non valide.

Il Class Verifier

Nella versione della Java Virtual Machine J2SE, il class verifier può respingere le classi ritenute non valide. Una JVM che supporti il CLDC deve anch’essa essere in grado di respingere i file di classi non validi, tuttavia, il processo necessario per raggiungere un simile obiettivo è costoso in termini di tempo e risorse macchina; quindi, non precisamente ciò che si desidera per realtà quali i dispositivi handheld, a risorse limitate. I progettisti della KVM hanno deciso si spostare la gran parte del lavoro di verifica fuori dal dispositivo, o sul desktop dove i file di classi vengono compilati o sulla macchina server dalla quale verrà scaricata l’applicazione. Questa fase di verifica fuori dal dispositivo viene chiamata “preverifica”. Il dispositivo deve semplicemente eseguire pochi controlli sul file della classe (preverificato) per assicurarsi che è stato verificato ed è ancora valido.

La KVM non processa classi che non siano state precedentemente preverificate o ritenute non valide.

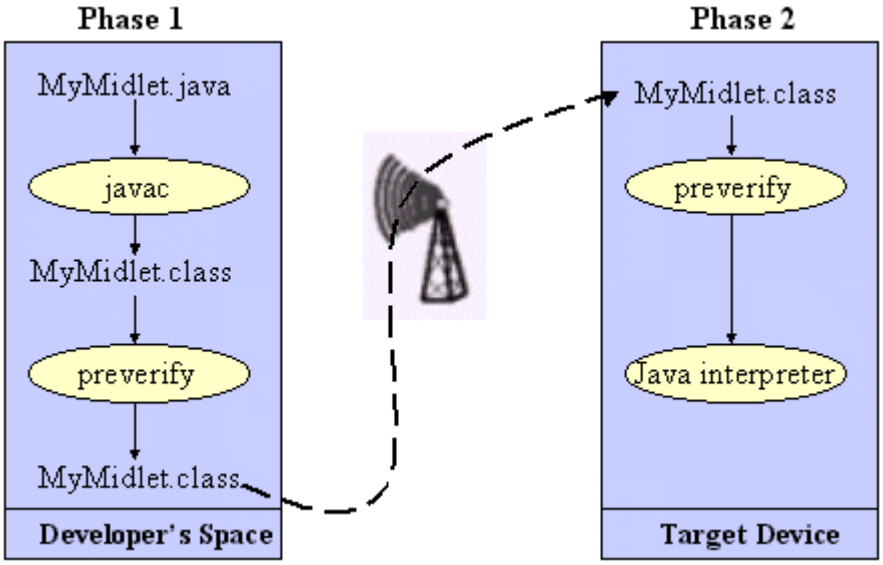


Figura 1 - Processo di verifica

In figura 1 viene mostrato il processo di verifica, per chiarezza non sono stati inseriti i processi di Jaring e Jading.
Il nuovo processo di verifica (figura 1) si compone di due fasi:

- Preverifica: Lo strumento per la preverifica è responsabile dell'inserimento inline di tutte le subroutine e dell'aggiunta di uno stack map degli attributi nella classe per facilitare la verifica a tempo d'esecuzione sul dispositivo. Il preverificatore inserisce degli attributi speciali nella classe Java. Questi attributi vengono ignorati dal J2SE class verifier convenzionale e per questo motivo le classi generate sono ancora delle classi valide J2SE.
- Verifica fatta nel dispositivo: Questa verifica viene svolta dal class verifier della KVM, il quale utilizza le informazioni generate dallo strumento di preverifica

Sicurezza di livello-applicativo

Il tipo di sicurezza che viene fornito dal class verifier si limita nello stabilire che una certa classe è una classe valida ma nulla più. Minacce per la sicurezza, quali accessi a risorse esterne (file system per esempio), dispositivi ad infrarossi o network passeranno inosservati dal verifier. Nella versione J2SE, l'accesso alle risorse esterne è controllato dal SecurityManager e da altri meccanismi Java 2 (come i controllori d'accesso e le policy di sicurezza). Ma come venne in precedenza accennato, unsimile modello, troppo costo in termini di risorse computazionali non è da preferirsi su

piattaforme a risorse limitate quali architetture CLDC/MIDP. Dunque, ora verrà descritto in quale modo il modello di sicurezza sandbox indirizzi le applicazioni in modo tale da raggiungere caratteristiche di sicurezza a livello applicativo.

La sandbox del CLDC/MIDP

La KVM fornisce un modello di sicurezza (sandbox) diverso rispetto al tradizionale modello sandbox, nel senso che gli accessi non vengono controllati attraverso il SecurityManager o attraverso le policy di sicurezza.

Questo modello di sicurezza (in accordo con le specifiche CLDC) si comporta nel seguente modo:

- Un file class Java preverificato e ritenuto valido sono considerati file class validi.
- Sono disponibili sono un limitato, e predefinito insieme di APIs per il programmatore.
- Il download e la gestione delle applicazioni Java sul dispositivo vengono effettuate dal codice nativo dentro la KVM, ed gli sviluppatori non sono autorizzati di effettuare l'override delle classi loader o ridefinerne delle loro in sostituzione.
- Gli sviluppatori non possono scaricare nessuna libreria nuova contenente funzionalità native o accedere a funzioni native che non sono parte delle librerie Java fornite dal CLDC e dal MIDP.

In sostanza, il modello sandbox di sicurezza definito dal CLDC non si avvale del SecurityManager. Le applicazioni Wireless Java possono essere eseguite in modo sicuro, in un ambiente chiuso (la sandbox) ottenuto tramite l'eliminazione di aspetti del linguaggio Java che potevano far sorgere problemi di sicurezza, in una situazione in cui è assente un pieno e completo modello di sicurezza (quale quello della J2SE per esempio). Gli aspetti eliminati per aumentare sicurezza sono:

- Nessuna Interfaccia Nativa Java (JNI): Una JVM che supporta il CLDC non implementa la JNI principalmente per motivi di sicurezza ma l'ipotetica implementazione è considerata anche dispendiosa in termini di memoria.
- Nessuna classe Loader ridefinita dall'utente: La JVM che supporta il CLDC ha un proprio loader class nativo (built-in) che non può essere ridefinito.
- Non esiste il supporto per la Riflessione: non viene fornito nessun supporto per la riflessione (il quale, ad esempio, permetterebbe di conoscere informazioni sulla JVM in esecuzione a runtime) nemmeno per il RMI e per la serializzazione degli oggetti.
- Non esistono i concetti di Gruppi di Thread e demoni thread: La JVM che implementa il CLDC fornisce il supporto per il multithreading ma non per le feature sopra indicate. Se si desidera eseguire delle operazioni su gruppi di thread, è necessario sfruttare delle tecniche a livello applicativo per memorizzare gli oggetti thread.

Wireless Network Security

Quello che ci si può domandare è cosa ha fatto Java per rendere sicuro il trasferimento dei dati su di un link wireless? La risposta è semplice e breve: questo non è un problema di sicurezza Java.

Con la sua architettura, Java ha fornito uno strumento che è la base per lo sviluppo di applicazioni su dispositivi a risorse limitate. Tale strumento è sicuro nei termini del codice che viene eseguito sul dispositivo, secondo gli aspetti discussi precedentemente. Tuttavia nel momento in cui viene utilizzato tale strumento, per la costruzione di applicazioni che necessitano, ad esempio, scambi di dati sensibili tra due parti, sarà il livello applicativo incaricato di rendere sicura la comunicazione.

Questa situazione ricade in pieno nel tipo di applicazione che ha per oggetto questo stage, e proprio attraverso tecniche crittografiche verrà creato un canale sicuro per lo scambio di dati in modo da raggiungere autenticazione, confidenzialità ed integrità dei dati. Tutto ciò viene svolto in modo cosciente del fatto che a livello di linguaggio, sono state prese tutte le misure per rendere sicuro un eseguibile su un dispositivo MID.

Questo ulteriore livello di sicurezza, necessario in applicazioni come Secure SMS Messaging, viene denominato sicurezza end-to-end.

La repentina evoluzione tecnologica, ha portato negli ultimi anni allo sviluppo di dispositivi handheld con capacità di calcolo sempre più elevate.

L’aumento delle risorse disponibili sui MID, ha permesso di allargare gli orizzonti in termini di applicativi destinati a queste piattaforme. Con il passare del tempo, è divenuto possibile sviluppare software sui dispositivi HandHeld che sfruttassero la connessione ad internet (fornita attraverso tecnologie come il GPRS, o EDGE) o interagissero con altri dispositivi tramite connessioni wireless (bluetooth, infrared a breve anche Wi-Fi su smartphone) o ancora fossero in grado di accedere a database.

In un simile panorama si intuisce che nascono, assieme alle nuove possibilità di sviluppo, anche nuove esigenze di sicurezza nel trattamento delle informazioni in gioco. Intuitivamente, se un applicativo sviluppato per un dispositivo mobile, viene creato per fare e-commerce, dovrà avere delle feature che consentano all’utente di ritenersi sicuro nell’inserire i propri dati personali. Oppure ancora, in tutte quelle applicazioni che trattano lo scambio di dati tra un utente ed un altro, nel qual caso in protocollo utilizzato per lo scambio non offra servizi di segretezza è bene, se ritenuto necessario, implementare soluzioni per aumentare sicurezza nella comunicazione.

Analizzando il caso particolare di uno smartphone, tale dispositivo può andar perso o peggio ancora rubato, involontariamente ritrovarsi tra le mani di maliziosi o ancora esposto a furti di dati. La quantità d’informazioni memorizzabili in tali dispositivi sono sempre maggiori, come sempre

maggiore è la necessità di preservare tali informazioni sensibili. Nel caso di una comunicazione tra due utenti, diventa ancor più chiaro e necessario, in alcuni casi, disporre di funzioni che permettano di raggiungere segretezza della comunicazione, autenticazione e controllo di integrità sui dati inviati.

Le tre caratteristiche elencate precedentemente, sono le principali feature che rendono “sicura” una comunicazione; grazie all’avvento della piattaforma Java 2 Micro Edition in concomitanza con le librerie crittografiche Bouncy Castle Crypto APIs si rende possibile lo sviluppo di applicazioni che supportino tali caratteristiche.

Bouncy Castle Crypto APIs

Un aiuto notevole allo sviluppo di applicazioni crittografiche è stato fornito dalle Bouncy Castle Crypto APIs, un insieme di librerie open source sviluppato dalla “Legion of Bouncy Castle”. Il package messo a disposizione, fornisce l’implementazione Java 2 Micro Edition per diversi algoritmi di cifratura. Ecco le caratteristiche del package:

* oltre 20 motori per la cifratura a chiave simmetrica e asimmetrica
  DES, Blowfish, Rijndael, IDEA, AES, RSA e RC4
* funzioni hash come MD5 o SHA
* calcolo MAC e HMAC
* scambio di chiavi
* interfacce per il calcolo e la verifica della firma digitale
* gestione di certificati

Tali implementazioni vengono distribuite tramite un file “midp.zip”.

Per rendere disponibile in package agli applicativi è necessario copiare il “midp.zip” all’interno della directory <wireless toolkit home>\apps\lib. Diversamente, se si desidera rendere disponibile tali librerie solo al progetto corrente, si deve copiare il file in <wireless toolkit home>\apps\<progetto home>\lib.

Di seguito viene mostrata una breve panoramica delle funzioni messe a disposizione dalle Bouncy Castle Crypto APIs.

Java Cryptographic Services

Cryptographic Service	Algorithms/Types	Description
SecureRandom	**SHA1PRNG**	<Generates random numbers appropriate for use in cryptography. SHA1PRNG is an implementation of the Pseudo Random Number Generator (PRNG) algorithm.>
KeyGenerator	**AES, Blowfish, DES, DESede, HmacMD5, HmacSHA1**	<Generates secret keys to be used by other services with the same algorithms.>
KeyPairGenerator	**DSA, RSA, DH**	<Generates a pair of public and private keys to be used by other services with the same algorithms.>
MessageDigest	**SHA1, MD5**	<Computes the digest of a message.>
Mac	**HmacMD5, HmacSHA1**	<Computes the message authentication code of a message.>
Signature	**SHA1WithDSA, SHA1WithRSA**	<Creates and verifies the digital signature of a message>
KeyStore	**JKS, JCEKS, PKCS12**	<Stores keys and certificates.>
CertificateFactory	**X509**	<Creates certificates.>
Cipher	**DES, TripleDES, Blowfish**	<Encrypts and decrypts messages.>
KeyAgreement	**DH**	<Lets two parties agree on a secret key without exchanging it over an insecure medium.>

Offuscatore

Le Bouncy Castle Crypto APIs, hanno una dimensione che si aggira sui 500Kb (versione J2ME). Tale occupazione, in qualche modo potrebbe non essere precisamente idonea per dispositivi a risorse limitate.

Per ridurre le dimensioni del package JAR contenente l'applicativo che sfrutta le librerie delle Bouncy Castle, è possibile utilizzare uno strumento chiamato "Offuscatore".

L'offuscatore di codice, è uno strumento che viene utilizzato principalmente, come dice il nome stesso, offuscare il codice creato. Cambiando i nomi delle classi compilate, rinominando variabili e funzioni, l'obiettivo dell'offuscatore è quello di rendere più difficile il reverse engineer dalle classi in bytecode di un'applicazione java. Allo stesso tempo però, svolge una funzione che si rivela

importante per i nostri scopi. L’offuscatore, oltre alle funzioni prima descritte, elimina dal package tutte quelle classi, metodi e campi che non vengono utilizzati realmente dall’applicazione, rendendo il package di quest’ultima molto più snello e perciò più adatto per dispositivi a risorse limitate.

Stato dell’arte

Lo straordinario sviluppo delle reti di comunicazione e dei servizi offerti mediante la tecnologia dell'Informazione, può considerarsi, senza ombra di dubbio, come la grande rivoluzione di fine secolo. Mai prima d'ora l'uomo si era trovato a disporre di un mezzo tanto potente per comunicare il proprio pensiero: oggi possiamo raggiungere con facilità, da qualsiasi posto e a costi ridotti praticamente qualsiasi altro essere umano ovunque si trovi; ed anche i nostri documenti scritti, viaggiando ad incredibili velocità, possono raggiungere in pochi istanti numerosi destinatari.

La crescente disponibilità di banda passante, unita ai sempre minori costi di connettività ed alla disponibilità sempre maggiore dei punti d'accesso, ha fatto delle moderne reti di comunicazione il vero e proprio sistema nervoso del pianeta. Eppure, anche questa magnifica costruzione ha il suo tallone d'Achille: la sicurezza. Proprio perché "reti aperte", le reti digitali sono intrinsecamente insicure: esse non sono state progettate in modo da garantire autoprotezione e difesa contro eventuali abusi.

Ne discende che esse sono particolarmente sensibili all'intercettazione ed all'alterazione dei dati trasmessi, nonché alla violazione dei supporti informatici ad essa connessi. Il problema è ancora più sentito quando si parla di commercio elettronico, o, più in generale, quando i dati trasferiti contengono informazioni riservate: la sicurezza è il presupposto fondamentale su cui si fonda il rapporto fiduciario fra acquirente e venditore, fra banche e correntisti…

Senza garanzie adeguate l'utente non avrà incentivi all'utilizzo di tali tecnologie che, sebbene siano più convenienti, sono anche più insicure.

Inoltre il desiderio dell'utente di garantire la propria riservatezza e anonimato mal si concilia con la necessità di imputabilità, cioè la possibilità effettiva di conoscere l'identità degli utenti e di ciò che stanno facendo. Il tentativo di creare siti completamente anonimi va contro le nozioni di imputabilità, autenticità, integrità, revocabilità, non ripudiazione e non può essere in armonia con la necessità di applicare la legge di fronte ad una frode
significativa.

Ideale sarebbe trovare un giusto bilanciamento fra queste diverse esigenze e tale compromesso dovrebbe essere attentamente protetto. La protezione delle informazioni trasmesse via Internet richiede tutte le attenzioni normalmente dedicate ai corrispondenti documenti cartacei.

Il passaggio dai documenti tradizionali al relativo documento elettronico deve venire gestito in

maniera tale da conservare, ed eventualmente migliorare, le tradizionali politiche di sicurezza al fine di consentire un sistema di comunicazione sicuro.

La sicurezza delle reti e delle informazioni va intesa come la capacità di una rete o di un sistema d'informazione di resistere ad eventi imprevisti o atti dolosi atti a minare la disponibilità[1], l'integrità[2] e la riservatezza[3] dell'informazione.

A protezione di questi tre vitali fattori vengono impiegate diverse misure di sicurezza (che non prescindono comunque dall'insostituibile supporto degli esperti per la fase di progettazione del sistema) tra le quali citiamo l'utilizzo di strumenti crittografici (quali IPSEC, SSL, HTTPS e VPN) e quello di strumenti tecnologici (quali firewall e Intrusion Detection System).

Tra le misure più comuni c'è l'adozione di un firewall per proteggersi dall'esterno attraverso il filtraggio dei bytes (pacchetti) in ingresso su una rete privata (il filtraggio avviene in base a un set di regole, le cosiddette policy stabilite dall'amministratore del firewall) o il controllo degli accessi tramite password e chiavi private. Queste misure sono spesso insufficienti a garantire una corretta difesa della privacy perché non escludono tentativi di intercettazione delle trasmissioni (sniffing dei dati) ed alterazione dei dati trasmessi.

In particolare sul web, il protocollo HTTP è estremamente insicuro in quanto trasmette i dati "in chiaro". Tale protocollo rappresenta, sostanzialmente, il linguaggio comune di due sistemi informatici distinti: i server web, computer che pubblicano le pagine sulla rete Internet e che, quindi, mettono a disposizione contenuti e raccolgono dati, ed i sistemi client, vale a dire quelli utilizzati da un qualsiasi browser. I dati così trasmessi sono, però, facilmente intercettabili. È per questo motivo che introdurre, ad esempio, i dati della propria carta di credito attraverso moduli o formulari proposti dalle pagine HTML può essere rischioso.

Ed è per questo che i server web prevedono sistemi quali l'SSL (Secure Socket Layer protocol, un protocollo aperto sviluppato da Netscape Communications [17] e approvato come standard dall'Internet Engineering Task Force [18]) e l'SHTTP (Secure HTTP, progettato dal W3C e

---

[1] La disponibilità dei dati è garantita se essi sono accessibili e i servizi funzionano anche in caso di interruzioni dovute alle cause più disparate.

[2] La conferma che i dati trasmessi, ricevuti o conservati sono completi ed inalterati

[3] La protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate.

dall'Enterprise Integration Technologies [19]) che permettono alle applicazioni client-server di comunicare in modo da prevenire le intrusioni, le manomissioni e le falsificazioni dei dati, garantiscono la mutua autenticazione e l'uso di firme digitali per l'integrità e la cifratura dei dati a protezione della privacy.

Protocolli Sicuri

Il World Wide Web (WWW) è un sistema ipermediale distribuito che ha acquistato vasto successo fra gli utenti di Internet. Il protocollo di applicazione del WWW client/server è l'HTTP. Alcune applicazioni di WWW richiedono la capacità di autenticare ogni scambio fra client e server. In questa direzione l'HTTP, non supporta appropriati meccanismi di crittografia. Nel seguito vengono illustrati i principali protocolli.

SSL

SSL (Secure Socket Layer protocol) è un protocollo aperto e non proprietario; è stato sottoposto da Netscape Communications all'Engineering Task Force per la sua standardizzazione, anche se di fatto è stato accettato come uno standard da tutta la comunità di Internet ancor prima del verdetto dell'IETF. La versione 3.0 del protocollo rilasciata nel novembre 1996, è un'evoluzione della precedente versione del 1994 la SSL v2.0, e rappresenta al momento una delle soluzioni più utilizzate per lo scambio di informazioni cifrate. Tale evoluzione introduce un livello di sicurezza superiore rispetto alla precedente grazie ad una maggiore attenzione nella fase di autenticazione tra client e server. Il futuro di SSL è rappresentato dal protocollo TLSv1 (SSL v3.1) sottoposto a standardizzazione nel novembre 1998.

Il protocollo SSL è nato al fine di garantire la privacy delle comunicazioni su Internet, infatti permette alle applicazioni client/server di comunicare in modo da prevenire le intrusioni, le manomissioni e le falsificazioni dei messaggi. Il protocollo SSL garantisce la sicurezza del collegamento mediante tre funzionalità fondamentali:

- **Privatezza del Collegamento:** Per assicurare un collegamento sicuro tra due utenti coinvolti in una comunicazione, i dati vengono protetti utilizzando algoritmi di crittografia a chiave simmetrica (ad es. *DES, RC4*, ecc.);
- **Autenticazione:** L'autenticazione dell'identità nelle connessioni può essere eseguita usando la crittografia a chiave pubblica (per es. *RSA, DSS* ecc.). In questo modo i client sono sicuri di comunicare con il server corretto, prevenendo eventuali interposizioni. Inoltre è prevista la certificazione sia del server che del client;

- **Affidabilità:** Il livello di trasporto include un controllo sull'integrità del messaggio basato su un apposito *MAC* (Message Authentication Code) che utilizza funzioni hash sicure (per es. *SHA*, *MD5* ecc.). In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

Gli scopi del Protocollo SSL v3.0, in ordine di priorità, sono:

- **Sicurezza del collegamento:** SSL stabilisce un collegamento sicuro tra due sistemi;
- **Interoperabilità:** Programmatori di diverse organizzazioni dovrebbero essere in grado di sviluppare applicazioni utilizzando SSL 3.0, accordandosi sui parametri utilizzati dagli algoritmi di crittografia senza necessità di conoscere il codice l'uno dell'altro;
- **Ampliamento:** SSL cerca di fornire una struttura dentro la quale i futuri metodi di crittografia a chiave pubblica e chiave simmetrica possano essere incorporati senza dover per questo creare un nuovo protocollo;
- **Efficienza:** Le operazioni di crittografia tendono a essere molto laboriose per la CPU, particolarmente le operazioni con le chiavi pubbliche. Per questa ragione l'SSL ha incorporato uno schema di session caching opzionale per ridurre il numero di collegamenti che hanno bisogno di essere stabiliti ex-novo. Particolare attenzione è stata posta nel ridurre l'attività sulla rete.

Il protocollo SSL è composto da due protocolli, SSL Record a livello inferiore ed SSL Handshake a livello superiore, che si interfaccia con una applicazione come ad esempio HTTP.

Il protocollo **SSL Handshake**, permette al server ed al client di autenticarsi a vicenda e di negoziare un algoritmo di crittografia e le relative chiavi prima che il livello di applicazione trasmetta o riceva il suo primo byte. Il client deve infatti accordarsi col server su unalgoritmo di cifratura, un algoritmo di integrità e un algoritmo per la cifratura a chiave privata; in caso contrario non viene garantita la sicurezza del canale di comunicazione la richiesta verrà scartata. La negoziazione delle Crypto-options avviene automaticamente, senza che l'utente debba intervenire. A questo punto può iniziare la trasmissione dei dati, e questi sono cifrati con la chiave concordata durante la fase di handshake.

Un vantaggio di SSL è la sua indipendenza dal protocollo di applicazione, in tal modo un protocollo di livello più alto può interfacciarsi sul protocollo SSL in modo trasparente.

Il Protocollo **SSL Record**, è interfacciato su di un protocollo di trasporto affidabile come il TCP. Questo protocollo è usato per l'incapsulamento dei dati provenienti dai protocolli superiori. Esso prende i messaggi che devono essere trasmessi, li frammenta in blocchi di dati (record di 214 byte o meno), opzionalmente li comprime, applica un MAC (Message Authentication Code che viene utilizzato per il protocollo dell’ integrità dei dati), li cifra, e trasmette il risultato. I dati ricevuti

vengono decifrati, verificati, decompressi, e riassemblati, quindi vengono trasmessi al livello più alto.

SHTTP

Il Secure HyperText Transfer Protocol (SHTTP) fornisce meccanismi di comunicazione sicura fra la coppia client/server di HTTP utile per le operazioni commerciali e altre applicazioni su rete. È disegnato per coesistere con messaggi HTTP e per essere facilmente integrato con le applicazioni HTTP. SHTTP fornisce una serie di meccanismi di sicurezza ai client e ai server HTTP, fornendo una gamma di potenziali caratteristiche che coprono tutte le possibili applicazioni sul World-Wide-Web.

Per incoraggiare il commercio elettronico su Internet, le industrie si sono mosse per stabilire uno standard di sicurezza per il World Wide Web. Il consorzio[4] per il WWW ha pensato di scegliere come standard di base per l'autenticazione e la crittografia l' SHTTP.

La forza dell' SHTTP è nella sua flessibilità e nel fatto che da anni sta continuamente evolvendo attraverso dei miglioramenti e rifiniture. SSL è più generico e non rivolto alle applicazioni poichè lo standard SSL vuole diventare un protocollo che offre servizi a livello più basso.

S-HTTP è stato progettato da E. Rescorla e A. Schiffman della EIT (Enterprise Integrated Technologic Inc.) per realizzare connessioni HTTP sicure. SHTTP fornisce servizi sicuri applicabili per:

- **transazioni confidenziali**
- **autenticazione e integrità dei dati**
- **non ripudiabilità dell'originale**

Il protocollo lascia massima flessibilità nella scelta dei meccanismi di gestione della chiave, politiche di sicurezza e algoritmi di crittografia e supporta opzioni di negoziazione fra le parti per ogni transazione**.** Non è richiesta la chiave pubblica per il client.

SHTTP contiene HTTP, poichè permette ai messaggi di essere incapsulati in vari modi.

---

[4] Il consorzio è composto da: Digital Equipment Corp., AT&T, MCI Communications Corp., IBM, Novell Inc., Netscape Communications Corp., National Center for Supercomputing Applications (NCSA), e la Microsoft Corp

L'incapsulazione può essere ricorsiva e il messaggio può subire diverse trasformazioni. SHTTP fornisce inoltre linee di testa per funzioni di gestione amministrativa come trasferimento delle chiavi e dei certificati.

SHTTP contiene dei formati standard di crittografia, in particolare: PKCS-7 e MOSS. PKCS-7 è un formato di incapsulazione di messaggi crittografati, definito dai laboratori RSA. È preferito agli altri modi di crittografia permessi dal SHTTP per la vasta possibilità di negoziazione delle opzioni. PKCS-7 è definito con la notazione ASN.1 dell' OSI come una sequenza di sei tipi diversi combinabili fra di loro:

- **Data**: Insieme di byte.
- **SignedData**: Una parte con zero o più blocchi di firme.
- **EnvelopedData**: Uno o più blocchi con parti cifrate.
- **SignedAndEnvelopedData**: La combinazione di SignedData e EnvelopedData.
- **DigestedData**: Una parte con blocco di riassunto.
- **EncryptedData**: Una parte cifrata con materiale per le chiavi esterne.

SHTTP non richiede per il client la certificazione della chiave (o la chiave pubblica). Questo è importante perchè significa che le transazioni private possono avvenire senza che gli utenti abbiano stabilito chiavi pubbliche. SHTTP fornisce transazioni sicure end-to-end, al contrario dell'HTTP nel quale i meccanismi di autorizzazione avvengono quando il client tenta l'accesso e gli viene negato. Nel SHTTP pochi dati sono trasmessi in chiaro sulla rete. Fornisce piena flessibilità degli algoritmi di crittografia, modelli e parametri. La negoziazione delle opzioni è usata per permettere al client e al server di accordarsi su come far avvenire le transazioni (ad es. se è necessaria la firma, la cifratura del messaggio o entrambi), e sugli algoritmi di crittografia da usare (RSA o DSA per la firma, DES o RC2 per la crittografia).

In SHTTP la protezione dei messaggi può avvenire in tre modi: **firma**, **autenticazione** e **crittografia**. Per ogni messaggio può essere possibile la firma, l'autenticazione, la crittografia o una combinazione di questi tre modi.

L'autenticazione è realizzata mediante la testata Content-MAC-Info: per verificare l'autenticità del messaggio spedito e indirettamente la sua integrità, SHTTP fornisce il calcolo del Message Authentication Code (MAC), un calcolo basato su funzioni hash. Questo meccanismo è anche utile per la non ripudiabilità delle transazioni.

La crittografia e la firma possono essere fatte attraverso la testata di Content-Privacy-Domain. Ad esempio se si considera per 'Privacy-Domain' il valore PKCS-7, la sicurezza mediante crittografia opera come una 'busta' sotto PKSC-7. Viene cifrato il contenuto usando un sistema DEK con le

informazioni sulla chiave specificate nella linea di testa 'Prearranged-Key-Info'. Quando occorre la firma si usa l'opzione 'SignedData' oppure 'SignedAndEnvelopedData'. In caso di firma, una certificazione appropriata deve essere unita al messaggio oppure mandata indipendentemente al mittente. Per generare i dati cifrati e firmati occorre generare prima una firma con 'SignedData' e poi cifrare i dati con 'EncryptedData', poichè il PKCS-7 non supporta una modalità per cifrare e firmare i dati contemporaneamente.
Sono realizzati meccanismi di gestione di chiavi multiple e la possibilità di mandare messaggi confidenziali a utenti che non posseggono coppie di chiavi pubblica/privata. Infatti SHTTP definisce due modi di trasferimento della chiave: uno usando la chiave pubblica del destinatario; nel secondo modo si cifra il contenuto usando una chiave transitoria, le cui informazioni sono specificate in una linea di testa.
Il client e il server negoziano quali miglioramenti vogliono usare, non usare o richiedere obbligatoriamente in riferimento alle preferenze crittografiche.
La negoziazione si riferisce sia alle preferenze crittografiche, che alle opzioni sulle chiavi da usare per migliorare la sicurezza del messaggio. Durante la negoziazione entrambe le parti esprimono le loro preferenze e richieste riguardo ai miglioramenti da adottare. La scelta finale dipenderà dalle capacità implementate nel client e nel server e dalla particolare applicazione richiesta.

IPSec

Fino ad ora tutti i lavori sulla sicurezza erano volti ad assicurare protezione a livello di sessione/presentazione (SSH e SSL), così, quello che veniva codificato e reso inaccessibile a tutti tranne che alle controparti autorizzate, erano le comunicazioni tra due processi che colloquiavano tramite un canale non sicuro: si voleva garantire la sicurezza delle applicazioni che sfruttano la rete pubblica. Con IPSEC l'idea è quella di rendere sicura l'intera rete (scendendo al livello di rete) creando un sistema che protegga attraverso metodi crittografici i datagrammi IP, un protocollo, dunque, che si vada a collocare tra il TCP (UDP) e l'IP integrandosi interamente con quest'ultimo.
È importante inoltre sottolineare che, benchè l'IPSEC non sia ancora uno standard, sono disponibili in commercio diversi prodotti proprietari che lo realizzano (RSA e CISCO), concretizzando l'esigenza di un siffatto protocollo per la realizzazione di una rete sicura queste Aziende rendono l'IPSEC uno standard "de facto".
Una realizzazione di IPSEC opera in un host o in un "Security Gateway" (SG questa dizione si riferisce a tutti quei gateway o firewall che implementano IPSEC) assicurando protezione al traffico dell'IP.

Per assicurare segretezza, autenticazione e integrità è necessario non solo provvedere a qualcosa che li realizzi operativamente, ma anche ad una struttura che li gestisca, seguendo delle direttive date da un utente o da un amministratore di rete.

Si ha bisogno di:

- Una struttura che si occupi di esaminare tutto il flusso di dati IP, sia in ingresso che in uscita, decidere quali dati debbano usufruire dei servizi IPSEC, ed in questo caso approntare tutto per assicurare il tipo di servizio più adatto.
- Una struttura che "ricordi" quale tipo di servizio è stato dato, in quale modo sia stato espletato, dove era diretto il pacchetto con quel tipo di servizio.
- Una struttura in cui siano definite tutte quelle caratteristiche da "ricordare", che sia unica per ogni connessione con il mondo esterno, e che debba essere concordata con il destinatario dei pacchetti in modo da definire al suo interno gli algoritmi di generazioni delle chiavi per la criptazione, gli algoritmi di criptazione e in generale tutto quello che necessita di essere concordato per garantire l'efficienza del servizio.

Per un analisi sul "modus operandi" di IPSEC bisogna distinguere i due flussi in ingresso e in uscita, la differenza è così marcata che per una realizzazione, gli RFC, consigliano di creare fisicamente due coppie SPD e SAD una per l'ingresso ed una per l'uscita.

Traffico in uscita

Ogni pacchetto in uscita è controllato da SPD che deve capire a quale politica fare riferimento per quello specifico pacchetto, le possibili soluzioni sono tre: il pacchetto procede per la sua strada, il pacchetto viene scartato, il pacchetto ha bisogno dei servizi di tipo IPSEC. In questo ultimo caso è necessario che:

- PD consulti SAD per vedere se esiste una SA appropriata (cioè una SA in cui il destinatario sia lo stesso di quello del pacchetto e che offra il servizio richiesto) se non c'è va creata.
- Individuata o creata la SA, si usa questa per sapere come realizzare i servizi richiesti (Individuazione della modalità e del protocollo sicuro).
- Si passa il tutto al protocollo sicuro indicato dalla SA, che a seconda della modalità (trasporto o tunnel) si occupa di modificare o di inserire ex novo l'header IP ed un proprio header, non che di criptare (caso ESP) o di fare il calcolo di ICV (Integrity Check Value) per l'autenticazione dei dati (AH o ESP).

Traffico in ingresso

Prima di compiere qualsiasi operazione i pacchetti frammentati vanno ricomposti.

Dopo è necessario identificare i datagrammi IP per sapere a quale protocollo di sicurezza fare

riferimento, inoltre è necessario risalire alla sua SA perchè in questa sono contenute le chiavi per decriptare i dati nel datagramma. In questo caso si procede:

- Si guardano i campi del datagramma che riguardano: l'indirizzo IP del destinatario (si ricorda che se si è un gateway questo indirizzo non è detto che sia banalmente il proprio!), il campo "Protocol"(IPv4) o "Next Header"(IPv6) per l'identificatiore del protocollo sicuro, il parametro SPI contenuto nell'header del protocollo sicuro.
- Con i campi individuati nel punto precedente si usa il SAD come una lookup table per l'individuazione della SA, se questo procedimento fallisce il pacchetto viene scartato.
- Una volta individuata la SA si procede a decriptare e alla verifica di autenticazione. Si deve continuare a ripetere i punti 1, 2 e 3 finchè non si incontri un header di un protocollo di livello superiore. Si deve mantenere traccia, di tutte le SA usate e del loro ordine.

Dal SAD si deve risalire alla (o all'insieme di) "politica di sicurezza" contenuta nel SPD, controllare se questa è soddisfatta, quindi eseguirla inoltrando il pacchetto al livello superiore o, nel caso di un gateway, spedendo il pacchetto ad un host (quindi se è il caso riavviare una procedura IPSEC questa volta in uscita).

Point-to-Point Tunnelling Protocol (PPTP)

Realizzato da PPTP Industry Forum[5], PPTP è stato progettato per consentire comunicazioni autenticate e crittografate tra un client e un gateway o tra due gateway, senza alcuna infrastruttura a chiave pubblica, tramite un ID utente e una password. È stato introdotto sul mercato nel 1996, due anni prima rispetto a IPSec e L2TP, con l'obiettivo di ottenere un supporto di facile impiego, multiprotocollo e trasversale per una vasta gamma di reti IP. Il protocollo PPTP (Point-to-Point Tunneling Protocol) utilizza una connessione TCP per la gestione del tunnel e frame PPP incapsulati GRE (Generic Routing Encapsulation) per i dati sottoposti a tunneling. È possibile crittografare e/o comprimere i payload dei frame PPP incapsulati. L'impiego dei frame PPP consente di negoziare l'autenticazione, la crittografia e i servizi di assegnazione degli indirizzi IP

[5] US Robotics (ora 3Com), 3Com/Primary Access, Ascend, Microsoft e ECI Telematics

Layer 2 Tunneling Protocol (L2TP)

Si tratta di una combinazione di PPTP e L2F, che si è sviluppata nel corso dell'elaborazione degli standard IETF. L2TP è un protocollo di tracking standard IETF ormai affermato e ampiamente implementato. L2TP effettua l'incapsulamento dei frame PPP (Point-to-Point Protocol) da inviare sulle reti IP, X.25, Frame Relay o ATM (Asynchronous Transfer Mode). Dopo aver configurato il protocollo L2TP per l'utilizzo di IP come trasporto, è possibile adottarlo come protocollo di tunneling VPN in Internet. L2TP su IP utilizza la porta UDP 1701 e include una serie di messaggi di controllo L2TP per la gestione del tunnel. Tramite la porta UDP, L2TP invia inoltre frame PPP incapsulati L2TP come dati sottoposti a tunneling. I frame PPP possono essere crittografati o compressi. Quando i tunnel L2TP vengono visualizzati come pacchetti IP, essi sfruttano la protezione IPSec standard utilizzando la modalità di trasporto IPSec per integrità, risposta, autenticità e protezione della privacy avanzate. L2TP è stato progettato appositamente per le connessioni client ai server di accesso remoto e per le connessioni tra gateway. Grazie all'impiego di PPP, L2TP acquisisce il supporto multiprotocollo per protocolli quali IPX e Appletalk. PPP rende inoltre disponibile una vasta gamma di opzioni per l'autenticazione dell'utente, quali CHAP, MS-CHAP, MS-CHAPv2 e EAP (Extensible Authentication Protocol), in grado di supportare i meccanismi di autenticazione di token card e smart card. L2TP/IPSec implementa quindi funzionalità di tunneling ben definite e interoperabili, con sicurezza IPSec avanzata e interattiva. Rappresenta inoltre un'ottima soluzione per la sicurezza dell'accesso remoto e delle connessioni tra gateway.

Virtual Private Network (VPN)

Una rete VPN (Virtual Private Network) permette a computer ubicati in sedi fisiche diverse di stabilire un collegamento tramite Internet. Questa soluzione elimina la necessità di ricorrere a costose linee dedicate poiché la connessione a Internet permette di collegare sia sedi diverse sia utenti remoti. Poiché le connessioni a Internet sono connessioni pubbliche, e quindi non protette per definizione, sono esposte al rischio che i pirati informatici possano intercettare e modificare i dati trasmessi sul Web. Con una rete VPN è tuttavia possibile crittografare i dati e inviarli solo ad un computer (o gruppo di computer) specifici o, in altre parole, di creare una rete privata che è accessibile solo agli utenti autorizzati a differenza del Web che è accessibile a tutti. La rete in questione è però una rete virtuale poiché il collegamento tra i computer remoti non è fisico ma basato sul Web. Per poter utilizzare un'applicazione installata sui sistemi della propria azienda, i dipendenti che lavorano fuori sede devono semplicemente collegarsi ad un sito Web specifico e immettere una password.

Per poter essere protetti, i dati scambiati sulla rete VPN devono essere incapsulati tramite un processo chiamato “tunneling”, che ha lo scopo di collocare i dati in buste digitalizzate. Il termine “tunnel” è stato scelto poiché indica uno spazio protetto creato nell'ambito della connessione al Web. Naturalmente, le aziende e gli utenti remoti devono utilizzare programmi software specifici a ciascuna uscita del "tunnel" per poter crittografare e decrittografare i dati con lo stesso formato. Nel modello di trasmissione viene spesso aggiunta una fase di compressione dei dati che ha lo scopo di evitare che la rete si saturi a causa dell'elevato numero di pacchetti crittografati. È necessario anche un server VPN, ossia il computer che gestisca le richieste di connessione degli utenti e dei router remoti (nel caso di sedi dislocate in altre ubicazioni).
Per consentire agli utenti di ciascuna uscita del tunnel di leggere i dati, è necessario, naturalmente, che tutti i componenti della rete VPN utilizzino lo stesso protocollo. Esistono naturalmente vari protocolli con livelli di protezione diversi: PPTP (Point-to-Point Tunneling Protocol), L2F (Layer Two Forwarding), L2TP (Layer Two Tunneling Protocol) e IPSec. I protocolli PPTP e IPSec offrono il livello di protezione più elevato.
Il protocollo PPTP permette di incapsulare i pacchetti dati in un datagramma IP al fine di creare una connessione punto-a-punto. In questo caso, i dati vengono protetti a due livelli poiché i dati sulla rete locale (come gli indirizzi dei PC) vengono incapsulati in un messaggio PPP che è a sua volta incapsulato in un messaggio IP. IPSec offre tre moduli (Authentication Header, Encapsulating Security Payload e Security Association) che ottimizzano la protezione, garantendo la riservatezza, l'integrità e l'autenticazione dei dati.

IDS distribuiti

L’individuazione delle intrusioni è definito essere il problema dell’identificazione di individui che stanno usando un sistema senza autorizzazione (*crackers*), a di coloro che, seppur avendo accesso legittimo al sistema, stanno però violando i diritti concessi loro (minacce dall’interno o *insider threat*). [21]
Un Sistema di Rilevamento delle Intrusioni (Intrusion Detection System o IDS) è una combinazione di metodi ed entità atte a determinare la presenza e l’ubicazione di attività non autorizzata su una rete di computer. IDS individua e segnala vulnerabilità nella sicurezza, oltre che registrare utenti interni malintenzionati per proteggere l’affidabilità. [22]
Esistono in letteratura[23] due grandi categorie di approcci alla tematica dell’Intrusion
Detection:

- **Anomaly Detection:** in questo tipo di approccio si cerca di studiare il comportamento dell’utente, confrontandolo con un profilo di comportamento “normale”, modellato secondo

varie tecniche. Il sistema individua in modo statistico qualsiasi deviazione “significativa”, segnalandola all’amministratore come “sospetta”. I sistemi di questo tipo vengono anche detti “*behavior based*”

- **Misuse Detection:** in questo tipo di approccio, viceversa, il sistema cerca di individuare direttamente un comportamento “anomalo”, solitamente basandosi su qualche forma di base di conoscenza che contenga un catalogo di attacchi noti (“firme” o “signatures”). I sistemi di questo tipo vengono anche detti “*knowledge based*”.

Ciascuno di questi approcci ha pregi e difetti. I sistemi basati sulla anomaly detection, per esempio, non richiedono un’immisione di conoscenza “a priori”, né richiedono continui aggiornamenti delle “firme” d’attacco, essendo teoricamente in grado di rilevare i “cattivi comportamenti” sulla base di una descrizione di “normalità”. Tuttavia, per costruire un modello di “comportamento normale” serve innanzitutto uno studio architetturale preciso su quale tipo di modello usare, e in secondo luogo una fase più o meno prolungata di addestramento in cui il modello viene “tarato” sullo specifico utente e sullo specifico sistema. Inoltre, questi sistemi sono drammaticamente proni ad errori e falsi positivi.
I sistemi basati sulla misuse detection, viceversa, richiedono uno studio estensivo delle forme d’attacco per la produzione delle “firme” necessarie al loro funzionamento. Dalla qualità delle firme e dal loro aggiornamento costante dipende inevitabilmente l’efficacia del sistema (si può notare immediatamente un parallelo con i meccanismi e le problematiche tipiche del software antivirus). Stranamente, il problema dei falsi positivi ma soprattutto degli alert indesiderati affligge drammaticamente anche i sistemi di questo tipo, che dovrebbero essere meno vulnerabili. Ciò che si nota, infine, è che mantenere una base di conoscenze vasta e in continuo aggiornamento con i “pattern” degli attacchi è una impresa improba, e spesso inutile.
Un’altra classificazione molto importante distingue tra sistemi *host-based* e *network-based*:

- I sistemi “host-based” controllano una singola macchina e a volte una singola applicazione, e dipendono dal sistema operativo (a cui sono spesso collegati strettamente, nello specifico molti moduli di intrusion detection host based sul sistema linux vengono realizzati come moduli del kernel) per tracciare chiamate di sistema, utilizzo delle risorse, comandi eseguiti e i passaggi da un livello di privilegi a un altro. Altre tipiche fonti di dati per un sistema hostbased sono i log.
- I sistemi “network-based”, viceversa, sono collegati in posizioni opportune ad una rete di computer, e cercano di controllare tutto il traffico che la attraversa (mediante degli sniffer di

rete), cercando nel flusso di pacchetti le indicazioni di possibili attacchi.

Come sempre, entrambi gli approcci presentano vantaggi e svantaggi. Uno dei vantaggi principali di un IDS network-based è la possibilità di usare un numero di sonde relativamente piccolo per controllare anche reti di grandi dimensioni. Però vi sono alcuni tipi di intrusione che un sistema network-based non può, realisticamente, individuare: esempi tipici sono tutte le attività che coinvolgono canali crittografici.

Per esempio, un IDS di rete può intercettare ed analizzare tentativi di attacco rivolte ad una web application (per esempio, mandando dati mal formattati ad un campo di una form), ma se questi ultimi viaggiano in una sessione criptata (per esempio su SSL) le “firme” dell’IDS di rete sono sostanzialmente inutili.

Uno dei potenziali vantaggi di un IDS network-based è la possibilità di operare una “passive analysis”, in cui il sistema raccoglie i pacchetti di rete senza che la sua presenza sia rilevabile: operativamente questo si ottiene dotando la macchina che esegue l'IDS di una scheda di rete posta in modalità promiscua e con un indirizzo IP nullo (0.0.0.0), in maniera tale che essa non possa trasmettere alcunché ma riceva ed analizzi qualsiasi pacchetto indirizzato a qualsiasi indirizzo. In questo modo diventa molto difficile per un intruso a rilevare la presenza dello sniffer. Tuttavia una serie di ricerche hanno dimostrato la possibilità di rilevare la presenza di interfacce poste in modalità promiscua.

Gli IDS Network-Based devono affrontare i seguenti compiti:

- Individuare violazioni all’integrità dell’host guardando passivamente il traffico di rete. Questo può essere effettuato utilizzando appositi sensori e piazzandoli su appositi servizi sugli host o, più tradizionalmente, sui gateways.
- Rispondere a tentate violazioni bloccando indirizzi IP esterni. Abbattere le connessioni a ambo i capi di una comunicazione rilevata. È possibile inoltre inserire regole nei firewall di confine (*Border Firewall*) della rete.
- Rispondere a intrusioni dall’esterno bloccando indirizzi IP esterni. Individuare tentativi di apertura di porte non permesse su server anche mediante indirizzi IP “flypaper”(carta moschicida, o trappola per mosche).
- Trovare e segnalare inconsistenze di utilizzo che indicano un furto di identità o di diritti. Determinare che gli account autorizzati nelle varie postazioni sono le stesse che usano gli altri sevizi di login.
- Individuare violazioni monitorando le informazioni

- Fare log e stabilire la relazione tra il traffico e l’utente in modo da facilitare confronti futuri.

Reti Wireless e di sensori

La necessità di mobilità e di copertura in ambienti aperti o difficili da raggiungere tramite cavi (es: ospedali, aereporti o palazzi antichi) hanno favorito la diffusione delle tecnologie wireless. Esistono diverse metodologie di trasmissione dati via etere, quali ad esempio il GPRS, Bluetooth e 802.11, detta anche Wireless Ethernet o Wi-Fi (Wireless Fidelty). Tutte queste tecnologie sono state ampiamente discusse nel capitolo precedente.

Esistono però dei rischi di sicurezza collegati all'uso delle tecnologie wireless. Alcuni di questi rischi esistono anche nelle reti di tipo tradizionale, ma vengono esasperati dalla tipologia di collegamento senza fili. La trasmissione attraverso onde radio non è confinabile ad uno spazio ben definito, quale può essere quello della trasmissione via cavo: come per l'ascolto di una radio, è possibile per un potenziale intruso avvicinarsi all'esterno del palazzo e "captare" le onde radio. Così come per le reti cablate, attraverso appositi strumenti, è possibile visualizzare i dati che vengono ricevuti e inviati, rendendo disponibile all'eventuale intruso preziose informazioni quali utenze e password, e, in alcune situazioni, addirittura accedere ai database e corrompere i dati. Un altro fattore di rischio molto importante, ma spesso sottovalutato, è che un eventuale intruso non abbia nessun interesse a prendere informazioni sulla rete attaccata, ma voglia utilizzare la rete vittima come "ponte" per attaccare una terza entità, con cui spesso si ha una relazione di fiducia. L'intruso sarà solito usare il "ponte" per offuscare le proprie traccie: da un punto di vista puramente giuridico, l'amministratore della rete wireless violata sarà formalmente responsabile dell'atto di pirateria informatica nei confronti della terza entità, fino a quando le autorità giudiziali non troveranno prova dell'avvenuta intrusione.

La Wireless Ethernet dispone di un sistema di sicurezza che viene chiamato Wired Equivalent Privacy, detto comunemente WEP. Questa specifica, nata per garantire la privacy delle utenze, è basata però su di un sistema di crittografia debole che si è rilevata controproducente: attraverso un’analisi probabilistica di una piccola quantità di dati cifrati, è possibile risalire alla chiave di crittografia e pertanto accedere alla rete.

I rischi descritti nei paragrafi pecendenti possono rendere vulnerabile la propria rete ad attacchi. Possiamo evidenziare tre macro tipologie di attacchi: all'apparato radio, alla rete aziendale o interna e al client wireless.

- **Attacchi agli apparati radio**. Le insicurezze del WEP permettono agli intrusi di eludere la crittografia dei dati trasmessi, così da poter analizzare il traffico wireless e da poter ricavare

il contenuto dei dati trasmessi (es: login e password) per futuri attacchi. Inoltre, si possono eseguire attacchi più specifici, come la modifica dei dati in transito, il “replay” di sessioni eseguite dai client e il disturbo del segnale radio (Radio Jamming). Un altro tipo di attacco è l'inserimento di un finto Access Point. Per dirottare la connessione dei dispositivi wireless verso la rete pirata, gli hacker installano un punto di accesso con un segnale più potente nelle loro vicinanze. Gli utenti tenteranno di collegarsi ai falsi server, fornendo nome utente e password e qualsiasi altra informazione riservata.

- **Attacchi alla rete aziendale o interna**. Il WEP è l'unico modo protocollo nello standard IEEE 802.11 per autenticare gli utenti, pertanto un aggressore può facilmente entrare nella rete aziendale senza dover preoccuparsi di autenticarsi alla rete. Inoltre, non esiste nessun controllo di accesso verso le risorse della rete interna: un intruso può effettuare qualsiasi operazione sulla rete senza nessuna limitazione.
- **Attacchi ai client wireless**. Molte architetture prevedono che i client wireless vengano visti come risorse interne, anzichè risorse esterne (o untrusted). Eventuali aggressori possono compromettere i client wireless per ottenere preziose informazioni o per usarli come “ponte” per penetrare nella rete aziendale.

Le contromisure ad ogni tipo di attacco sono molteplici, e vanno da dei semplici accorgimenti fino all’utilizzo di protocolli di comunicazione e di autenticazione appositi. Nel seguito viene fatta una breve panoramica delle possibilità.

Accorgimenti da utilizzare

Una corretta configurazione degli apparati è un buon inizio per proteggere la rete wireless. Grazie ad alcuni accorgimenti, è possibile “sviare” un eventuale intruso nascondendo dettagli preziosi e rendendo più difficile l'identificazione della rete su cui si sta collegando.

- **Cambiare gli SSID di defaule e utilizzarne di non descrittivi.** Il Service Set Identifier (SSID) identifica univocamente ogni punto di accesso all interno della rete. Tramite una configurazione opportuna, soltanto i dispositivi che utilizzano la corretta SSID possono comunicare con i punti di accesso. Molti dei dispositivi hanno già preconfigurato un SSID di default: un intruso può usare questi nomi per cercare di accedere ad AP che hanno ancora la configurazione di fabbrica.
- **Disabilitare il Broadcast SSID.** Gli AP mandano ad intervalli regolari Beacon Frames per la sincronizzazione con i client, i quali contengono il SSID. Queste frames servono ai client per configurarsi automaticamente la rete di accesso, ma servono anche a potenziali

aggressori durante la ricerca delle reti wireless.

- **Cambiare le password.** Come per gli SSID, è importante cambiare le password di default degli AP. È buona norma che la password sia lunga almeno otto caratteri e che includa caratteri speciali e numeri.
- **Chiavi WEP.** Anche se è stato dimostrato che WEP non è adeguato a proteggere una rete wireless, rappresenta comunque un deterrente per gli intrusi occasionali. Serve catturare dai 100 Mb a 1 Gb di traffico per provare a ricavare la chiave WEP, pertanto l'aggressore deve essere ben motivato per tentare l'intrusione. Cambiare spesso le chiavi WEP di crittografia sugli AP fa in modo che una rete compromessa, non lo sia a tempo indeterminato: un intruso, infatti, dovrebbe di fatto riprovare a ricavare la chiave WEP, scoraggiandolo da un secondo tentativo. Cambiare le chiavi WEP è abbastanza oneroso: alcuni Access Point supportano la dynamic WEP-key exchange per cambiare la chiave WEP per ogni adattatore.
- **Abilitare il MAC filtering.** Molti produttori includono nei loro Access Point la possibilità di abilitare soltanto alcune schede di rete, usando come metodo discriminatorio il loro MAC address.
- **Minimizzare l'intensità del segnale.** Gli intrusi sfruttano il fatto che le onde radio non si possono limitare a dei luoghi ben definiti, esempio l'ufficio vendite, ma riescono ad espandersi fuori dalle mura perimetrali dall'ufficio. Da qui la definizione del nome “parking lot attack”, o più semplicemente attacchi provenienti dal parcheggio. È pertanto importante scegliere un'adeguata collocazione dell'Access Point all'interno dell'edificio, in modo che il segnale sia sufficiente a garantire il collegamento solo ed esclusivamente alla zona interessata.

Point-to-Point Protocol over Ethernet (PPPoE)

Questa tecnologia permette di incapsulare il protocollo PPP, usato nella sua accezione più comune sui collegamenti via modem, sul mezzo trasmissivo ethernet.

Analogamente alle tecnologie ADSL e cable modem, la wireless LAN è in grado di emulare una rete ethernet. Anche in ambito wireless è possibile sfruttare quindi la tecnologia PPPoE, con i benefici descritti precedentemente, ad esempio fornendo servizi personalizzati all'utente quali l'IP address fisso e access lists basate a livello utente.

Il protocollo PPP e di conseguenza PPPoE, offre un'architettura di crittografia chiamata Microsoft Point-To-Point Encryption Protocol (MPPE). Questa estensione del Compression Control Protocol (CCP) è stata introdotta da Microsoft per applicare la sicurezza nel protocollo di VPN chiamato

Point-to-Point Tunneling Protocol (PPTP). MPPE è basato sull'algoritmo Rivest-Shamir-Adleman (RSA) RC4 per effettuare la crittografia dei pacchetti e può usare una chiave crittografica fino a 128-bit. Inoltre MPPE può negoziare una modalità detta *stateless* che permette di cambiare la chiave di crittografia ogni qual volta esso si collega. Il protocollo PPP e di conseguenza PPPoE, offre un'architettura di crittografia chiamata Microsoft Point-To-Point Encryption Protocol (MPPE). Questa estensione del Compression Control Protocol (CCP) è stata introdotta da Microsoft per applicare la sicurezza nel protocollo di VPN chiamato Point-to-Point Tunneling Protocol (PPTP). MPPE è basato sull'algoritmo Rivest-Shamir-Adleman (RSA) RC4 per effettuare la crittografia dei pacchetti e può usare una chiave crittografica fino a 128-bit. Inoltre MPPE può negoziare una modalità detta *stateless* che permette di cambiare la chiave di crittografia ogni qual volta esso si collega.

IEEE 802.1x

Lo standard IEEE 802.1x permette di identificare in maniera sicura gli utenti, collegati ad una determinata porta ethernet o ad un Access Point, ed applicare di conseguenza il livello di sicurezza necessario: ad esempio ad un nostro partner possiamo dare la possibilità di navigare solamente su internet, mentre l'amministratore delegato può accedere al database principale. IEEE 802.1x è nato per l'identificazione e l'autorizzazione dell'utente su reti wireless e più in
generale su reti ethernet, permettendo servizi personalizzati quali il raggruppamento di una classe di utenti in una determinata Virtual LAN.

Il protocollo è basato su Extensive Authentication Protocol Over Lan (EAPOL) che prevede differenti tipologie di autenticazione, tra cui MD5 e TLS. Sebbene questo protocollo sia l'ideale per riconoscere un utente e dare l'accesso alla rete, si possono evidenziare tre sue implicazioni. La prima é che IEEE 802.1x non definisce un sistema di crittografia: questo protocollo si limita ad autenticare l’utente, anche se in seguito verrà descritto in che modo é in grado di “integrarsi” con WEP. Il secondo problema é che molti degli Access Point esistenti non dispongono di 802.1x. Quegli AP che non dispongono della possibilità di essere aggiornati via software devono essere sostituiti. Inoltre é probabile che i futuri AP a basso costo, tipicamente pensati per l’utenza domestica e piccoli uffici, non disporranno di 802.1x, che necessita comunque di una infrastruttura RADIUS.

Al fine di poter identificare e autorizzare l’utente finale IEEE ha scelto di incapsulare su ethernet il protocollo Extensible Autentication Potocol. EAP é un framework di autenticazione inizialmente pensato per il Point-to-Point Protocol (PPP) che supporta differenti schemi di autenticazione. EAP

non definisce uno specifico metodo di autenticazione, bensì permette di negoziare il protocollo di autenticazione tra i due interlocutori, ovvero l'utente e il server di autenticazione (tipicamente Radius). Sono stati definiti alcuni schemi di autenticazione EAP, i più famosi dei quali sono: MD5, TLS, TTLS, LEAP, PEAP, SecurID, SIM e AKA.

Wi-Fi Protected Access (WPA)

Il protocollo Wi-Fi Protected Access (WPA) é uno sforzo dei produttori nel tentativo di colmare le lacune derivate da WEP.

Il WPA richiede che un client si autentichi per accedere alla rete, sia esso attraverso un *Pre-Shared Key* (utenti SOHO) che attraverso *IEEE 802.1x/EAP*, e introduce un framework di crittografia per la confidenzialità dei dati che si appoggia ad algoritmi quali WEP, TKIP e AES. Il WEP usato in WPA ha un impatto minore rispetto al WEP tradizionale, in quanto le chiavi verranno cambiate in modo differente. Anche se WEP é supportato, WPA usa di default il *Temporary Key Integrity Protocol* (TKIP) per crittografare i dati, aumentando la chiave dai 104-bit di WEP, fino a 128-bit. Contrariamente a WEP, dove le chiavi venivano

impostate staticamente, in TKIP vengono generate dinamicamente e distribuite attraverso il protocollo 802.1x/EAP. Inoltre TKIP include un *Message Integrità Check* (MIC) che permette di evitare le alterazioni dei pacchetti trasmessi attraverso la rete wireless. Il MIC viene calcolato separatamente dal client e dall'Access Point e se risultasse differente il pacchetto verrebbe scartato.

Il TKIP aumenta la difficoltà di decriptare i dati su una rete wireless: specialisti crittografi infatti hanno analizzato il Wi-Fi Protected Access e hanno affermato che i problemi legati al WEP sono stati risolti facendo di WPA un ottimo deterrente contro attacchi conosciuti.

VoIP

Il protocollo Voice Over IP, come il nome suggerisce, convoglia il traffico voce prodotto in pacchetti IP e li invia attraverso la rete con le modalità inaffidabili che sono prima state esposte. La mole di traffico prodotto è notevole e risulta direttamente proporzionale alla qualità audio desiderata. L'implementazione di misure di sicurezza come quelle sopra citate per la sicurezza del canale o della cifratura del pacchetto (IPSec o SSL) causa l'aumento della dimensione occupata e delle risorse di calcolo necessarie per la crittografia.

L'aspetto critico è che VoIP ha una bassa tolleranza alla perdita di pacchetti, e i dispositivi mobili hanno hardware ancora limitato e tale per cui il processo di cifratura e decifratura può essere oneroso. Risulta necessario trovare il giusto compromesso nel trade-off tra Security e qualità della

voce.

L’occupazione della banda può essere un fattore secondario, soprattutto il dispositivo si avvale di una connessione di tipo UMTS o Wi-Fi verso un Access Point.

RFID

Per quanto riguarda la tecnologia RFID, di recente fatta avanti l’ipotesi di una minaccia alla sicurezza e alla privacy. La possibilità che i tag ed i lettori RFID diventino veicoli di virus e worm. Alcuni ricercatori della Vrije Universiteit di Amsterdam hanno dimostrato con dei test pratici che il sistema RFID è particolarmente esposto ad attacchi di diversi tipi o come veicolo di infezioni virali. A partire dagli attacchi di tipo DoS (Denial of Service), che possono impedire il corretto utilizzo del sistema le altre minacce potrebbero provenire da tecniche di Spoofing, Replay oppure temuti attacchi ai database con tecniche di SQL Injection. Utilizzando lo Spoofing, malintenzionati potrebbero simulare autentici tag RFID usando appositi trasponder. In questa maniera sarebbe abbastanza facile sbloccare l'antifurto di una automobile. Più a rischio potrebbero essere i nuovi passaporti digitali che alcuni stati vorrebbero introdurre oppure i diffusi sistemi di pagamento di tipo “contactless”, quali il Telepass. Con la tecnica del Replay Attack è possibile captare e ritrasmettere query o codice maligno. Sottolineando la possibilità dei Buffer Overflows una grave minaccia arriva dall'architettura di back-end che sta dietro al sistema RFID. I tag RFID non sono altro dei veicoli di informazioni, che pio vengono trasmesse e gestite tramite un database. Se il database viene infettato da un virus la situazione diventa molto critica. Anche un semplice attacchi di tipi SQL Injection potrebbe azzerare qualsiasi sforzo compiuto nell'implementazione

CAPITOLO 5:
MOBILITA NELLA COLLABORAZIONE TRA IMPRESE

History Case

L'evolversi delle tecnologie ha portato grandi benefici alla mobilità delle attività umane attenuando le barriere geografiche e favorendo la collaborazione tra imprese.

Vengono presentati di seguito due casi di studio di enti e aziende dove è forte l'integrazione tra le tecnologie "mobili" e le attività del personale. Il primo riguarda l'ambiente sanitario, dove la tecnologia Wi-Fi agevola il lavoro del personale medico e paramedico. Il secondo invece tratta di come la tecnologia RF-ID snellisca, ottimizzi e avvantaggi la logistica della merci di azienda finlandese.

University Hospital di Leipzy – Germania

L'ospedale Universitario di Leipzig ha sviluppato un progetto legato alla mobilità che prevede cartelle cliniche in formato elettronico accessibili da tutto il personale medico e paramedico per mezzo di tablet PC messi loro a disposizione e sfruttando la WLAN.

L'ospedale universitario di Leipzig conta circa 4200 dipendenti e 48000 ricoverati e 260000 pazienti ambulatoriali. l'anno. L'obiettivo della struttura consiste nell'offrire ai pazienti le migliori cure possibili contenendo i costi. Il mobility project è un progetto realizzato con la collaborazione di grosse società quali Intel, e Fujitsu-Siemens.

RFID per la logistica Just-in-Time di ABB Oy – Finlandia

Abb Oy Driver produce, nella propria fabbrica di Pitäjänmäki (Helsinki), Low-Voltage AC driver con la procedura JIT (just-in-time) definita "kanban". Questo termine giapponese, che letteralmente

significa “cartellino”, è il più noto dei sistemi JIT per il controllo degli approvvigionamenti di materie prime. Prevede che all’avvio di un ordine per quello specifico componente avvenga solo quando il contenitore di quel componente è vuoto. Il kanban, indicante la tipologia del materiale usato per una lavorazione, è apposto su un contenitore che una volta vuotato deve essere rifornito.

Le esigenze di ABB Oy nascevano dalla considerazione che i prodotti gestiti sono caratterizzati da volumi di produzione particolarmente elevati generando flussi d’ordine (e la conseguente movimentazione dei contenitori kanban) particolarmente consistenti. ABB Oy vedeva quindi la necessità di ottimizzare ulteriormente il processo di gestione in kanban per l’approvvigionamento dei semilavorati da una quindicina circa di fornitori del suo stabilimento.

La proposta di Vivant Systems Oy, system integrator finlandese partner di ACEN, è stata quella di gestire il processo kanban attraverso un sistema automatizzato di ordini che sincronizzasse il flusso dei contenitori con il flusso gestionale di trasmissione degli stessi e di ricezione del materiale. La scelta tecnologica proposta da Vivant Systems si è rivolta alle etichette intelligenti RFID in UHF che, valutata sul campo da ABB contro le possibili alternative, è risultata essere la vincente.

Il processo kanban automatizzato ha inizio quando una cassa ormai vuota e dotata di un tag RFID è portata alla baia di carico/scarico merci. Il transito attraverso il varco RFID attiva automaticamente l’emissione di un ordine da parte del sistema informativo aziendale. L’ordine viene immediatamente inviato al fornitore di quel componente attraverso una rete extranet in formato XML. Il fornitore può quindi processare l’ordine ancor prima di ricevere il contenitore kanban relativo. Una volta preparati i componenti necessari alla spedizione il fornitore provvede ad inserire elettronicamente all’interno del tag RFID che equipaggia il contenitore pieno di componenti, tutte le informazioni del documento di consegna.

All’arrivo della merce in ABB nuovamente il transito del materiale attraverso il varco consentirà l’acquisizione di tutte le informazioni relative a quel contenitore, informazioni che verranno automaticamente trasferite nel sistema ERP aziendale.

L’azienda ha potuto ottenere: l’eliminazione del lavoro manuale per la verifica e la gestione documentale sia alla spedizione che al ricevimento, la riduzione significativa del ciclo ordine/consegna con eliminazione dei tempi morti e conseguente riduzione delle giacenze in magazzino, l’accessibilità immediata delle informazioni sulla disponibilità di materiale, la riduzione drastica degli errori dovuta alla quasi totale assenza dell’intervento umano, il reporting accurato dell’attività e dei flussi di materiale.

BIBLIOGRAFIA

[1] **Mobility: An Extended Perspective** - Masao Kakihara & Carsten Sørensen, *Department of Information Systems, London School of Economics and Political Science (2002)*

[2] **Mobility and Security** – Luca Cardelli, *Microsoft Research (1999)*

[3] **Digital Nomad** - T. Makimoto and D. Manners, *Chichester: John Wiley & Sons (1997)*

[4] **Sociology beyond Societies: Mobilities for the Twenty-First Century** - J. Urry, *London: Routledge (2000).*

[5] **Information, Internet, and Community: Notes Towards an Understanding of Community in the Information Age** - S.G. Jones, *S.G. Jones ed. CyberSociety 2.0:Revisiting Computer-Mediated Communication and Community, Thousand Oaks, CA: Sage Publications (1998)*

[6] **Being Digital** - N. Negroponte, *London: Coronet Books. Hodder and Stoughton (1995)*

[7] **Extending the EnterpriseNetwork Through Mobility** – Hewlett Packard *(2005)*

[8] **Forecast: Wireless LAN Equipment, Worldwide, 2002-2009.** - Gartner *(2005)*

[9] **Magic Quadrant for Global Campus LANs** – Gartner *(2004)*

[10] **Design and Performance of 3G Wireless Networks and Wireless LANs** – Chuah and Zhang, *Springer Ed.(2006)*

[11] **GSM Standards** - *MobileIN.com*

[12] **Digital Cellular Telecommunications System (Pahse 2+); General Packet Radio Service (GPRS); Overall Description of the GPRS Radio Interface; Stage 2 (GSM 03.64, v.5.1.0)** – ETSI, *(Novembre 1997)*

[13] **General Packet Radio Service (GPRS); Service Description; Stage 1 GSM 03.64, v.7.0.0** –ETSI, *(Aprile 1998)*

[14] **IEEE 802.11 working group**

[15] **Bluetooth Special Interest Group**

[16] **Infrared Data Association**

[17] **The SSL Protocol version 3.0** http://wp.netscape.com/eng/ssl3/draft302.txt

[18] **Internet Engineering Task Force**

[19] **W3C, World Wide Web Consortium**

[20] **Enterprise Integrated Technologic Inc**

[21] **DIDS(Distributed Intrusion Detection System) – Motivation, Architecture and An Early Prototype** Computer Security Laboratory Division of Computer Science *University of California (1991)*

[22] ***Distributed IDS*** , Darian Jenik – *Queensland University of Technology (2001)*

[23] **Un Sistema di Intrusion Detection Basato su tecniche di Apprendimento non Supervisionato** - Stefano Zanero, *Politecnico di Milano(2002)*

[24] **Sicurezza Nelle Wireless LAN** - Giuseppe Paternò, *E-book liberamente consultabile (2003)*

[25] ABB Oy Drives - Finlandia