

Attacchi Internet

Marco Bozzetti, Francesco Zambon

Negli ultimi tempi la stampa quotidiana ha dato ampio spazio e rilevanza ai numerosi attacchi ai sistemi informatici e di telecomunicazione (nel seguito indicati con il termine ICT, Information and Communication Technology) , in particolare ai siti web, connessi in Internet. Il fenomeno, dopo quello dei virus sui PC, ha fortemente risvegliato l'attenzione del grande pubblico sul problema della sicurezza ICT , visti anche i riflessi negativi sulle quotazioni in borsa e sui disservizi causati, in particolare nell'ambito del commercio elettronico e della fornitura dei servizi via rete.

I problemi della sicurezza ICT e dei suoi impatti sulla quotidiana vita, data la pervasività dei sistemi ICT e della nostra forte dipendenza dal loro corretto funzionamento non sono più fantasie di scrittori di gialli fantascientifici, ma iniziano a pervadere tutti gli utenti, sia in ambito professionale che domestico.

Facendo riferimento in particolare agli attacchi via Internet subiti nello scorso febbraio da siti quali Yahoo, CNN, Amazon, TD Waterhouse, E*Trade, Ebay.com, Buy.com, e che hanno provocato anche delle cadute dei rispettivi titoli quotati in Borsa, il presente articolo intende esaminare i principali metodi di attacco in ambito Internet, con riferimento a numerosi siti ove approfondire tali tematiche, e che occorre meglio conoscere per meglio difendersi.

Vengono considerati solo attacchi contro sistemi ICT, e non vengono considerate tutti i crimini e frodi perpetrati tramite l'utilizzo, proprio o improprio, di mezzi ICT (es. pedofilia, riciclaggio denaro sporco, ecc.) Si ipotizza che il lettore abbia una conoscenza di base delle funzionalità di Internet, e si forniscono i riferimenti ai siti specialistici per approfondimenti sulle tematiche considerate, che spesso richiedono specifiche competenze.

Per un approfondimento sul concetto di computer crime, e più in generale sulla sicurezza ICT, si rimanda al volume edito dalla Franco Angeli " 2° Osservatorio sul crimine ICT in Italia di FTI-Sicurforum" ed al sito <http://www.forumti.it>.

Senza alcuna pretesa accademica, ma con il solo intendo di semplificare e rendere più semplice la lettura degli attacchi nel seguito considerati, si seguirà la seguente "macro" classificazione:

- Attacchi alla rete:
 - Diretti al protocollo IP
 - Ai protocolli/servizi di rete : TCP, UDP, DNS, ICMP, routing, ecc
 - alle unità di rete (router, hub, multilayer switching, ecc.)
- Attacchi ai server che supportano servizi, ed in particolare ai server che supportano i siti web (www). Tali attacchi dipendono anche dal tipo di sistema operativo, principalmente NT o Unix (Linux, AIX,) ed includono virus, agenti ostili, cavalli di troia, ecc.. In tale casistica si considerano come server anche i gateway, firewall, ecc.
- Attacchi specifici agli applicativi/servizi (e-mail, database, ecc.)
 - Attacchi agli elenchi identificativi degli utenti e delle loro password
 - Attacchi ai protocolli applicativi : SNMP, SMTP, POP, IMAP, NFS, Telnet, FTP, X11, EDIFACT, ecc.
 - Attacchi ai sistemi di pagamento on line quali SET, IOTP, ecc.....
 - Attacchi agli applicativi (package, ERP,) ed alle banche dati/file systems
- Attacchi ai singoli client che accedono ad Internet (agenti ostili, virus, ecc.) ed ai programmi residenti

Molti attacchi sono una combinazione di più attacchi elementari, e gli obiettivi possono essere ricondotti nella seguente macro classificazione:

- Compromissione o blocco dell'erogazione di un servizio in rete (DoS, Denial of Service)
- accesso non autorizzato al sistema, carpando gli identificativi e le password d'utente il più delle volte mascherandosi come "gestore" dello stesso per utilizzare in maniera non autorizzata (spesso ciò significa banalmente "gratuitamente") o per poter compiere i due sottostanti più gravi attacchi

- accesso non autorizzato alle informazioni, che si suppongono riservate o comunque non disponibili gratuitamente;
- modifiche non autorizzate alle informazioni.

La maggior parte degli strumenti di attacco sono disponibili gratuitamente in Internet. Propedeutici alla maggior parte degli attacchi sono gli strumenti di analisi, quali i port scanner, che consentono di analizzare dall'esterno una rete, in termini di opportuno insieme di indirizzi di Internet e delle porte a più alto livello. Tra i molti possibili attacchi, per i quali si rimanda all'ampia letteratura disponibile (per una bibliografia aggiornata si rimanda a www.first.org, <http://www.zdnet.com/zdtv/cybercrime/>, <http://www.antonline.com/>), alcuni sono "tipici" del mondo Internet in quanto:

- a) sfruttano i protocolli della pila TCP/IP, come ad esempio per gli attacchi distribuiti per il "denial of service" nel seguito approfonditi;
- b) sfruttano i programmi ed i meccanismi di interazione client-server quali i browser, le interfacce applicative, gli applet, i plug-in, gli allegati della posta elettronica, ecc.;
- c) sfruttano le dimensioni globali e l'anonimicità possibile nell'ambito Internet.

Nel seguito verranno considerati due tipologie tra le più diffuse di attacchi via Internet ai sistemi informativi: il Distributed Denial of Service e l'attacco alle password. Ad essi si aggiungono e si affiancano altri tipi di attacchi, dallo spamming con la posta elettronica (invio di messaggi inutili per intasare una risorsa di rete) alla diffusione di virus, spesso trasportati come allegati nella posta elettronica (famosi in Internet i virus Melissa, Explore.zip, Happy99). Un'altra area di crescente criticità tipica di Internet è la comparsa di attacchi portati tramite applet o più facilmente ActiveX, ossia piccoli moduli di programmi scambiati tra client e server, che nascondono al loro interno cavalli di troia o virus che compiono azioni non volute sul sistema attaccato.

DoS e DDoS

La maggior parte degli attacchi recentemente perpetrati su Internet è inquadrabile come "DoS", Denial of Service: sono attacchi che tendono a compromettere/bloccare la disponibilità di un sistema/servizio tramite l'intasamento della piattaforma e/o delle linee di comunicazione, senza che le informazioni gestite siano danneggiate, disperse o proditoriamente copiate.

Lo sferrare l'attacco da più di un sistema, anche nell'ottica di non farsi riconoscere, prende il nome di DDoS, distributed denial-of-service. Un DoS o DDoS non provoca la distruzione o la manipolazione di informazioni, e l'esperienza ha dimostrato che spesso è di difficile identificazione. L'attaccante in logica criminale ricatta la vittima obiettivo (normalmente un provider) con la minaccia di provocare disservizi tali da causare significativi danni economici e di immagine.

I recenti attacchi sono stati condotti prevalentemente con programmi simili, chiamati Trinoo, Tribe Flood Network (in due versioni l'ultima denominata ovviamente 2000) e Stacheldraht (filo spinato in tedesco).

Nel seguito viene brevemente descritta la logica di tali attacchi. Per maggiori dettagli su questi programmi si rimanda a <http://staff.washington.edu/dittrich/misc/trinoo.analysis> o [tfn.analysis](http://staff.washington.edu/dittrich/misc/tfn.analysis) o [stacheldraht.analysis](http://staff.washington.edu/dittrich/misc/stacheldraht.analysis), ed al rapporto N.2319 del CIAC al sito <http://ciac.inl.gov/>

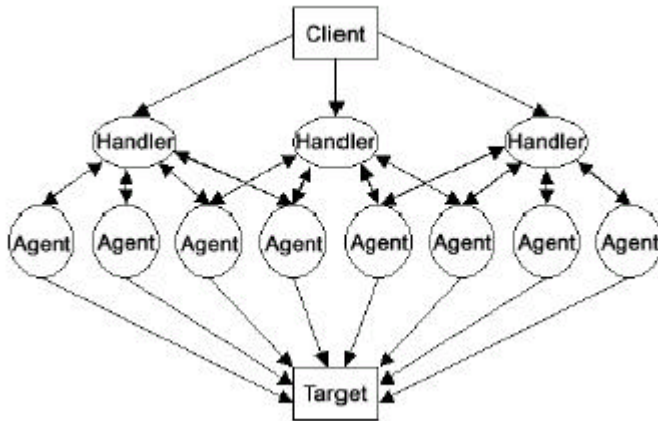
I sorgenti di questi programmi sono liberamente disponibili in rete, e possono pertanto essere variamente modificati in modo da meglio mimetizzarsi e meglio nascondere le loro comunicazioni nella rete. Per i consigli su come reagire un buon riferimento è il rapporto del CERT (<http://www.cert.org/advisories/CA-200-é1.htm>).

I sistemi di DDoS si basano tutti su una comune architettura basata su quattro categorie di sistemi:

- Un "client" funge da console per dirigere l'attacco.
- Un "target" funge involontariamente da bersaglio ma l'attacco può avere conseguenze anche su altri host della sottorete del "target"

- Un serie di sistemi “handler” diretti dal “client” comandano le operazioni di attacco eseguite dagli “agent”, i sistemi che di fatto inviano il messaggio di attacco al “target”.

Handler e Agent sono programmi che risiedono su calcolatori dei quali l'attaccante ha preso il controllo nella lunga fase di preparazione dell'attacco. L'attaccante ha dovuto installare i programmi “handler” o “agente” come server del sistema ospite, silenti ma in attesa di un ordine.



Da: CIAC 2319 Distributed Denial of Service 2/00

Molte sono le tecniche per prendere il controllo di un sistema remoto; la letteratura sui sistemi Unix e Linux é estesissima, più ridotta quella sui sistemi Microsoft anche perchè solo con WinNT e Win95/98 tali sistemi possono operare in rete. In questo caso, per la prima volta, il controllo di svariati sistemi Windows è stato ottenuto usando Back Orifice 2000 (<http://www.bo2k.com/>) un programma per controllo remoto che può usare molte strade, tra cui gli allegati della posta, come cavallo di troia.

L'attacco di tipo DDoS si svolge inviando una impressionante massa di messaggi al target in modo da consumarne tutte le risorse ed impedirgli di svolgere il suo lavoro o anche di essere in condizione di attivare filtri e protezioni.

Gli attacchi sono caratterizzati dal fatto che il tempo per elaborare il messaggio, magari solo per segnalare un errore é maggiore del tempo richiesto per inviare il messaggio. Inoltre vengono i usati messaggi che non richiedono che l'indirizzo del destinatario sia corretto introducendo una prima barriera a chi tenta di individuare l'attaccante.

La seguente tabella schematizza alcuni dei protocolli e messaggi usati per sferrare attacchi di tipo DDoS.

ATTACCO	DESCRIZIONE
Icmp Flood	Il messaggio “icmp_echorequest” richiede al target una risposta; poiché l'indirizzo del destinatario é fasullo, anche il calcolatore che ha ricevuto una risposta non richiesta chiederà spiegazioni al target
Smurf attack	Sfrutta la possibilità di richiedere un “broadcast” a tutti gli host della sottorete; la sottorete funge allora da casa di risonanza per messaggi “icmp_echorequest” e “icmp_echoreply”
Syn Flood	Viene sfruttato Tcp, un protocollo reliable, che prevede una forma di mutuo riconoscimento degli interlocutori. Viene attivata una connessione e si lascia il target in attesa di un acknowledgement che non arriverà mai e il target é costretto a gestire le richieste pendenti.

Targa3 attack	I pacchetti IP sono in vario modo scorretti: il target e' costretto a diagnosticare l'errore e a segnalarlo
Upd Flood	Con Upd, il protocollo senza connessione, si possono inviare messaggi a port scelti a caso; come minimo il target deve rispondere che il port non era raggiungibile

Visto che la preparazione dei messaggi è molto semplice e che può essere effettuata da molti calcolatori, nei recenti attacchi si è arrivati ad utilizzare una banda di 1 gigabit/sec (In Europa basta molto meno per bloccare tutte le linee).

L'attacco è di per sé semplicissimo, blocca l'operatività, in genere senza creare altri danni anche se qualche sistema può crollare se non è in grado di controllare perfettamente le risorse esorbitanti che vengono richieste.

Le comunicazioni tra client, handlers e agents sono tutte crittate (con robusti algoritmi (come Cast e Blowfish), i port di connessione sono estremamente variabili o addirittura scelti tra un pool in modo casuale; nessun messaggio contiene il mittente rendendo molto difficile risalire dal target al client. Inoltre i programmi sono difficilmente riconoscibili nelle directories o tra i registri per i nomi dei files o per qualche stringa ASCII contenuta nel binario dei programmi stessi. In un caso anche i testi inclusi nei binari erano crittati.

Molti siti hanno ospitato agenti, anche per lungo tempo, senza saperlo, ossia senza accorgersene. Più sofisticati e tecnologici gli attacchi, più difficile prevenire e poi reprimere gli attacchi.

Sono stati rapidamente realizzati programmi capaci di riconoscere le copie dei programmi handler e agent sui server occupati per l'attacco ma le facili metamorfosi dei programmi possono rendere rapidamente inefficaci questi strumenti.

Una seconda parte delle difese si rivolge all'individuazione dei messaggi scambiati tra i programmi attaccanti: anche in questo caso la facilità con cui vengono modificati i port TCP e la difficoltà di riconoscere i messaggi crittati rende spesso inefficaci tali difese.

Da ultimo è necessario uno sviluppo delle funzioni di router e firewall che consenta di individuare e filtrare rapidamente i messaggi che non hanno un mittente legale o che possono rappresentare un attacco. Tipico esempio è il pacchetto SYN. Esso è normalmente il primo pacchetto di sincronizzazione in uno scambio TCP, ed è seguito da un SYN-ACK che conferma la corretta ricezione del SYN. Con un SYN flood, il pacchetto SYN-ACK non è mai ritornato alla sorgente di SYN. Vari prodotti di router della fascia alta e di firewall hanno controlli "anti-syn".

Il collasso della rete potrà essere evitato e/o limitato solo se saranno effettivamente e largamente implementati quei protocolli, previsti in IPv6, che consentono di controllare la percentuale di banda assegnata ad ogni tipo di traffico. Questo consente ai sistemi sotto attacco la possibilità di reagire in vari modi, ad esempio di bloccare il traffico in entrata da certi indirizzi o di un certo tipo, quali messaggi icmp, udp, ftp, ecc.

I più moderni router e firewall sono in grado di fornire questo genere di funzionalità, e quindi di reagire meglio a, se non di prevenire e bloccare, questo genere di attacchi.

A seguito degli attacchi Ddos il governo americano ha organizzato un gruppo di esperti delle società di software e di sicurezza che mantengono aggiornato un documento intitolato "The consensus roadmap for defeating Distributed Denial of Service Attacks

(http://www.sans.org/ddos_roadmap.htm). Il documento suggerisce che, per prevenire gli attacchi con IP spoofing per nascondere la provenienza dell'attacco, ogni organizzazione si assicuri che tutti i pacchetti che escono dalla loro sottorete abbiano un indirizzo che appartiene alla stessa rete. Questo consente almeno di isolare l'area da cui provengono gli attacchi. Inoltre il documento suggerisce di impedire che messaggi broadcast o multicast siano reindirizzati (forwarded) da un host all'altro, in modo da impedire che il "broadcast" venga utilizzato per amplificare l'attacco.

Attacchi all'autenticazione di un utente

L'identificazione e autenticazione di un utente su internet e nelle intranet/extranet aziendali è per lo più affidata alle password. Si tratta di una logica adeguata per i sistemi tradizionali, raggiungibili da un numero limitato di persone interconnesse tramite una rete privata, ma ora del tutto inadeguata con sistemi raggiungibili da un numero elevato, se non praticamente illimitato, di utenti. Anzi le password danno una falsa sensazione di fiducia, sensazione che aumenta la pericolosità dell'approccio. La falsa sicurezza è il peggior nemico della sicurezza reale di un sistema ICT!!!

Le password degli utenti di un sistema o di un applicazione sono tipicamente memorizzati in un file (o in una tabella di database o di Ldap) e possono essere agevolmente raggiunte dal chi ha una autorizzazione come "superuser".

Nei tempi passati non era difficile raggiungere tale file senza avere alcuna autorizzazione, ora, almeno per i sistemi con sicurezza C2 (tutti i sistemi Unix, i mainframe con TopSecret o Racf, ed anche Wnt se opportunamente configurato) la cosa è più difficile ma, poiché i sistemi oggi sono in rete anziché cercare di raggiungere il file è possibile cercare di catturare le password mentre vengono trasmesse in rete. Questa operazione è comunemente chiamata sniffing. Operazione fattibile sia con opportuni dispositivi, ad esempio quelli di messa a punto e di test, messi in parallelo su un mezzo trasmissivo, o con programmi software operanti o su qualche elemento della rete, ad esempio un router, o su un client o un server nell'ambito di una rete locale.

Premesso che è possibile esaminare solo in traffico proveniente/destinato a sistemi specifici, in modo di non affondare in enormi file di log, il filtraggio dei dati che passano sulla nostra rete locale consente di selezionare:

- Il tipo di protocollo a livello 2 (IP nel nostro caso) ma anche gli alti protocolli come Sna o netbios, possono essere analizzati se serve.
- Il protocollo di livello 3. Le alternative sono tcp, udp e icmp.

Viene filtrato successivamente il port; ogni protocollo/server di internet ha associati uno o più ports, in base al port e' possibile sapere a quale server è indirizzato il traffico. Con questo meccanismo e' possibile focalizzarsi, in modo selettivo, sul traffico:

- Telnet: connessione alfanumerica ad un terminale: si tratta, ad esempio, del protocollo usato per programmare i router. Per passare da intercettazioni sulla rete locale a quelle sulla WAN il possesso della password del router può essere molto comoda.
- ftp: trasferimento di file
- smtp: la posta quando viene trasportata fino alla mailbox del destinatario
- pop o imap: la posta quando viene prelevata dalla mailbox
- http: il web
- e molto altri

I messaggi trasmessi da questi protocolli sono testi ASCII, sono perfettamente leggibili o, al massimo, sono codificati in modo da non utilizzare il primo bit di ogni byte. Le codifiche usate sono ben note: uudecode e base64 sono le più comuni e sono facilmente traducibili in testo leggibile. Trattandosi di testi ascii è possibile utilizzare dei semplici filtri che catturino solo i messaggi interessanti. Tipici esempi:

- Pop: filtrare il port 110, solo i pacchetti contenenti "user" e "pass"
- Sntp: filtrare il port 25
- http (proxy): si tratta delle password usate per accedere da una intranet all'internet attraverso un firewall che chiede di autorizzare l'utente: filtrare solo i pacchetti contenenti "Proxy-authorization:" indirizzati al port del firewall
- http (web pass): si tratta delle password (basic authentication) che autorizzano l'accesso a parti riservate di un sito. Per intercettarle basta filtrare i pacchetti http (port 80 tipicamente) contenenti "Authorization:"

- http – password applicative: in qualche caso l'applicazione non utilizza i meccanismi messi a disposizione dal server ma introduce un meccanismo proprio: in questo caso e' necessario studiare il formato del pacchetto, ma essendo tutto in chiaro le intercettazioni sono banali e non e' nemmeno necessario decodificare userid e password che sono scritte direttamente in chiaro anzichè usare una codifica base64. Ad esempio, nel caso di hotmail, intercettare i pacchetti contenenti: "hotmail", "login", "passwd" e "doklogin"

Per le password di accesso ad un sistema operativo, trasmesse da un sistema ad un altro (ad esempio l'autenticazione in un dominio di sistemi Windows) e' appena più complessa in quanto, in questo caso la password è crittata. Trattandosi di un "hash" non e' in generale possibile ricostruire la password ma, per tentativi, e' molto probabile si possa individuare la stringa che ha generato la stringa crittata. Forse qualche password richiederà una prova esaustiva di tutte le possibilità, ma in genere i tentativi basati sui ricchi dizionari disponibili in rete sono più che sufficienti. Un programma che lavora in background vi risolverà il problema senza disturbare il vostro lavoro.

La letteratura è ricca di strumenti di sniffing e di password cracking (programmi che provano tutte le possibili combinazioni fino a trovare la password che funziona) per i sistemi Unix e Linux. Per i sistemi windows il numero di strumenti è più limitato ed include:

- SpyNet di Laurentiu Nicula (per intercettare e filtrare i messaggi sulla rete locale)
- L0phtcrack (elle zero pi...) di "Cult of the Dead Cow" per intercettare e decodificare le password dei sistemi Windows-NT che passano per la rete
- mime64: nel caso non sappiate come decodificare una string base64

Alle intrinseche debolezze dell'identificativo d'utente e della sua password sopra evidenziate, si aggiungono, in particolare in ambito Internet, le difficoltà gestionali delle password stesse.

La password è un segreto condiviso tra l'utente ed il sistema. L'utente e' costretto a ricordare le password usate per ciascun sistema, o applicazione a cui ha accesso. Per l'utente si tratta di un compito complesso in quanto e' impossibile trovare una mediazione tra password sicure e cambiate frequentemente e che siano contemporaneamente facili da ricordare, quando oltretutto i sistemi che richiedono le password (quando addirittura la password non viene fissata dai gestori) aumentano in continuazione. Con l'aumento del numero delle password il meccanismo lato utente degrada rapidamente

Nel server e' necessario invece memorizzare la userid e la password, possibilmente crittata assieme ai diritti di accesso dell'utente.

Difficile, anche memorizzando le password su sistemi Ldap gestire milioni di utenze che hanno diritto di accedere alla stessa applicazione allocata su parecchi server, anche geograficamente lontani, per problemi di distribuzione del carico.

Difficile assicurare la corretta gestione dell'elenco specie per quanto riguarda la cancellazione di autorizzazioni scadute

Praticamente impossibile per una azienda sospendere tutte le autorizzazioni date nel tempo ad un dipendente o ad un esterno che ha terminato la collaborazione con l'azienda, per non parlare della gestione automatica di autorizzazioni più complesse come: "per una sola volta", "se sono presenti le seguenti persone.....", "per la durata del contratto...".....

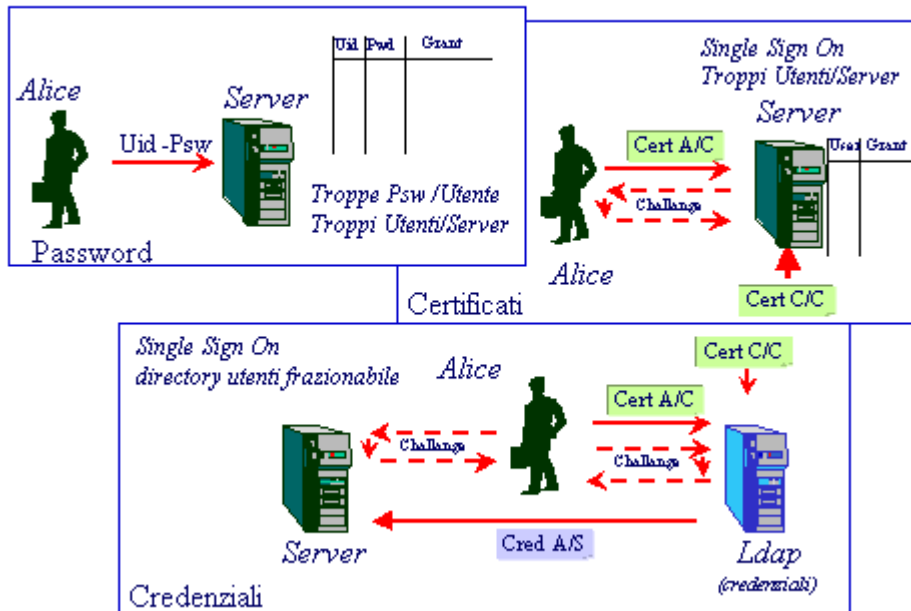
Impossibile non lasciare del tutto accessibili ai gestori dei sistemi le autorizzazioni emanate dall'azienda ed oggi, con l'outsourcing e il ricorso agli ASP (application service providers), e' improbabile che il gestore del sistema abbia legami con l'azienda della quale gestisce parti importanti sistema informativo.

Le nuove tecniche di identificazione ed autenticazione forte basate su smart card ed algoritmi crittografici a chiave pubblica consentono di superare le debolezze sopra evidenziate per quanto concerne sia gli attacchi all'algoritmo (come usare tritolo o lancia termica) sia gli attacchi al protocollo (come farsi dire la combinazione o scippare la chiave).

La tecnologia delle "credenziali" è ancora in fase di consolidamento (per approfondimenti si rimanda a Spki (<http://www.ietf.org/html.charters/spki-charter.html>) e KeyNote (ftp://ftp.isi.edu/in-notes/rfc2704.txt) mentre la tecnologia dei certificati X509 (o meglio PKIX in Internet <http://www.ietf.org/html.charters/pkix-charter.html>) e' ormai matura e risolve alla radice il problema delle intercettazioni delle password e della gestione delle stesse per l'utente (l'utente avrà una sola

password per attivare/proteggere la propria chiave privata o il Pin della smart card) oltre ad essere anche la tecnologia da usarsi per la firma digitale di documenti e transazioni. La figura che segue schematizza i principali pro e contro nell'uso delle tradizionali password, dei certificati e dei crediti.

Certificati vs Password



Conclusioni

Se gli attacchi ai siti più famosi hanno portato la Sicurezza di Internet in prima pagina, negli ultimi mesi vi è stato un lungo susseguirsi di iniziative ed eventi, meno pubblicizzati ma con maggiori conseguenze che stanno ridisegnando il problema.

Dal punto di vista dell'hacking l'evento rilevante è la distribuzione free di BackOrifice 2000, piattaforma estensibile che rende accessibili a molti, sui sistemi Windows, le più sofisticate tecniche di attacco e monitoraggio dei sistemi. La preparazione necessaria per eseguire un attacco si è abbassata drasticamente mentre è cresciuta esponenzialmente la quantità di persone capaci di eseguire un attacco serio.

Contemporaneamente il governo americano ha finalmente rivisto la legislazione sull'export dei sistemi di crittografia, almeno quelli per il mercato consumer. Non si tratta certo dei sistemi ad elevata sicurezza ma si tratta di sistemi che per diversi anni possono garantire autenticazione, privacy e transazioni economiche sicure in tutto il mondo e non solo negli Usa.

Da lato del Parlamento Europeo, tralasciando Echelon (<http://www.jya.com/atpc.htm>) di cui si parla ora poiché è ormai residuo della guerra fredda, l'evento rilevante è la firma elettronica. Con questa legislazione viene dato un supporto importante alla diffusione su larga scala dei certificati, certificati che possono essere usati per firmare i documenti ma che possono essere contemporaneamente usati per rendere sicure le connessioni ai server Internet (Tls – ex SSL – è il protocollo di riferimento). Ed in tale settore l'Italia ha emanato una delle più avanzate legislazioni oggi disponibili. (<http://www.interlex.it/docdigit/indice.htm>)

Ritornando agli attacchi possiamo notare che se i recenti interventi legislativi tolgono vincoli a tecnologie ormai mature che possono rendere sicure molte operazioni su internet. La sicurezza intrinseca della rete non dipende invece tanto dall'uso della crittografia quanto da un radicale ridisegno del protocollo IP (oggi IPV4). Tale ridisegno è in corso da anni (si tratta di un progetto estremamente complesso) ed sta ora volgendo alla conclusione. Casualmente o no i recenti attacchi rendono evidente l'urgenza di un passaggio a Ipv6. Si tratta di un passaggio costoso e complesso che senza forti pressioni della domanda probabilmente Internet provider e corporate tenderebbero a rimandare nel tempo.

Come rilevato dalle sempre più numerose analisi ed osservatori, il numero crescente di punti di debolezza dei sistemi è dovuto più di tutto alla scarsa preparazione del personale, alle configurazioni scorrette dei sistemi, alla crescente complessità dei sistemi stessi spesso non progettati con adeguata percezione delle esigenze di sicurezza. Il problema della sicurezza, al di là degli aspetti tecnici, è in primo luogo organizzativo e di management.

.....
Gli autori

Marco Bozzetti. (nato a Milano il 15-1-51)

Laureato in ingegneria elettronica al Politecnico di Milano, è attualmente dirigente ENI. Da più di 25 anni attivo professionalmente nell'ambito ICT presso primarie imprese di produzione e di consulenza, è stato uno degli ideatori di EITO, European Information Technology Observatory, il rapporto annuale di riferimento per il mercato ICT europeo, per il quale è curatore scientifico e redige lo stato dell'arte tecnologico. Autore di saggi ed articoli, è Socio fondatore dell'FTI, Presidente di Sicurforum-Italia e Vicepresidente del ClubTI.

Francesco Zambon (nato Treviso il 18-7-46)

Laureato in Matematica, dopo alcuni anni presso l'Università di Padova ha lavorato all'Ente spaziale Europeo (progetto Meteosat). Successivamente, nel Gruppo Eni, si è occupato di simulazione di processi industriali e di processi aziendali, di applicazioni di tecniche di intelligenza artificiale e di software engineering, coordinando progetti internazionali e svolgendo attività di consulenza per clienti e per l'UE.

Attualmente è Responsabile Soluzioni Innovative (applicazioni internet, datawarehouse, e-business) in Enidata. È socio IEEE, ACM, ClubTI