

Sono trascorsi più di due anni dai tragici eventi di New York e Washington ed è ormai assodato che la perdita di alcuni diritti digitali può essere stabilmente inclusa nell'elenco dei danni collaterali. «Le cyberlibertà sono state minacciate e le fondamentali libertà digitali amputate» rilevava già nel 2002 l'annuale rapporto di **Reporter sans frontières** (www.rsf.fr). Ad essere sotto accusa non sono Paesi tradizionalmente schierati contro ogni forma di dissenso politico, Cina o Corea per fare solo due nomi, quanto altri di consolidate radici e tradizioni democratiche. Analogamente a quanto avvenuto negli USA si è più volte documentato inoltre il clima tutt'altro che sereno, che ha portato all'approvazione di norme molto restrittive in materia di cyberterrorismo, come ad esempio il Regulations of Investigatory Powers (RIP) in Gran Bretagna.

D'altra parte una quota considerevole di cittadini occidentali è intimamente convinta di essere controllata in maniera capillare e quotidiana. Certo prima di Echelon era difficile immaginare a quale livello e ampiezza le tecniche di intercettazione fossero arrivate, né immaginare che il tutto avvenisse in maniera perfettamente legale. Ma con le prime timide rivelazioni sul sistema d'intercettazione statunitense quelle sensazioni hanno trovato un riscontro puntuale e drammatico. Gli eventi hanno mostrato quanto sia facile acquisire dati relativi alle comunicazioni di cittadini, aziende e organi statali; a questa nuova consapevolezza si è poi aggiunta un'altra considerazione altrettanto inquietante, vale a dire che ciò non sempre avviene per ragioni relative alla "cosiddetta difesa nazionale".

L'acquisizione di informazioni ha obiettivi differenziati. Già si è detto dell'onnicomprensiva definizione di difesa nazionale; ma l'informazione è altrettanto utile nella gestione degli affari e i governi, sempre più consapevoli al riguardo, si stanno attrezzando per mettere a punto sofisticati sistemi d'intercettazione in grado di fornire una messe sterminata di dati.

Complice la necessità di "garantire la sicurezza del Paese", si diffondono anche a livello governativo gli strumenti per leggere i messaggi di posta elettronica. Come tutelare, oggi, l'integrità e la riservatezza delle nostre e-mail? **Giuseppe Badalucco**

CRITTOGRAFIA VUOLE DIRE PRIVACY?



SICUREZZA



Un duro colpo alla privacy dei cittadini è stato portato ancora di recente, in seguito alle rivelazioni relative a un programma (*Carnivore* - vedi www.fbi.gov/hq/lab/carnivore/carnivore.htm) sviluppato dall'Fbi che consentirebbe di controllare qualsiasi messaggio di posta elettronica passante attraverso i server dei provider.

La posta elettronica in transito su Internet viene spesso paragonata alla corrispondenza cartacea e in particolare alle cartoline postali in transito negli uffici postali: privacy nulla, rischio di possibili manomissioni molto alto. I maggiori rischi derivanti da questa intrinseca vulnerabilità sono così sintetizzati da **Vincenzo Campanale** - Product Manager Security and Management di **Microsoft** (www.microsoft.com): «Alterazione del contenuto della mail, che una volta inviata in rete può essere manipolata nei suoi contenuti; integrità; lettura non autorizzata; violazione della riservatezza; alterazione del mittente».

Un software dedicato può condurre ricerche per parole chiave, per nomi di mittente/destinatario, per indirizzi ecc. e la posta interessante può essere automaticamente copiata e analizzata in seguito. Il tutto naturalmente a completa insaputa degli utilizzatori, almeno fino a quando sistemi di questo genere non vengono rivelati e catapultati all'attenzione di cittadini e governi.

Azioni simili possono ovviamente essere condotte da semplici malintenzionati. La dis-

seminazione di software passivo lungo il percorso compiuto dall'e-mail è una delle tecniche più diffuse; intercettate le mail più interessanti, contenenti password, numeri di carta di credito, informazioni commerciali pregiate, il passo successivo sarà l'utilizzo diretto o indiretto del moltiplo.

IL PRIMO FU GIULIO CESARE

La crittografia è definita come una misura attiva di sicurezza che ha come obiettivo la protezione delle informazioni; essa rappresenta oggi la tecnica più utilizzata e affidabile per garantire la sicurezza dei dati attraverso l'inibizione sia dell'accesso al contenuto (confidenzialità), sia della loro modifica (integrità).

Contrariamente a quanto si ritiene l'obiettivo principale della crittografia non è tanto quello di nascondere il messaggio quanto di celarne il significato a chi non ne sia il legittimo destinatario.

Crittografia e crittoanalisi sono scienze antiche come il mondo. Erodoto, il primo storico dell'antichità, nelle sue Storie, descrive l'impiego di una prima rudimentale tecnica di crittografia, la steganografia. Giulio Cesare crittografava le proprie missive utilizzando un rudimentale algoritmo eponimo di cifratura ancora oggi conosciuto. Spesso i due termini sono impiegati indifferentemente per indicare le tecniche di decrittazione dei codici, violazione degli schemi di autenticazione e in generale, mutuando dall'inglese il termine, di rottura degli algoritmi utilizzati.

Il principio di Kerchoff, che postula la sicurezza di un sistema crittografico nella segretezza della chiave impiegata e non nell'algoritmo, segna secondo numerosi teorici la cesura principale tra l'antica e moderna scienza crittografica. "Egli dimostrò già nel 1883 che la garanzia di sicurezza di un messaggio cifrato deve risiedere interamente nella chiave utilizzata e non nel metodo di cifratura, che può essere noto, come del resto avviene per buona parte degli algoritmi crittografici attuali" sottolinea **Elio Molteni**, Business Technologist per le soluzioni di sicurezza di **Computer Associates** (www.ca.com).

Una chiave segreta di cifratura, adeguatamente protetta e dalle caratteristiche idonee a garantire il livello di sicurezza richiesto coincidente o comunque derivante da quella di decifratura sarà definita crittografia simmetrica. Diversamente con chiavi di cifra e decifra differenti saranno in presenza di crittografia a chiave asimmetrica. Nel primo caso mittente e destinatario dovranno necessariamente conoscere algoritmo e chiave utilizzata, mante-



Vincenzo Campanale
Product Manager
Security and
Management
di Microsoft

(RIP)OSA IN PACE PRIVACY

In Gran Bretagna i controlli telematici sono consentiti dalla legge Regulation of Investigatory Powers (Rip) che obbliga i provider a fornirli di appositi strumenti che consentano alla polizia di controllare la posta elettronica e i dati dei cittadini inglesi. Per evitare che i provider possano trasferirsi all'estero ed eludere la legge, il Governo britannico ha addirittura stanziato un finanziamento che li agevoli nell'aggiornarsi con le apparecchiature necessarie.



Elio Molteni, Business Technologist per le soluzioni di sicurezza di Computer Associates

nendo segreta quest'ultima e sostituendola di frequente. Nella crittografia asimmetrica le chiavi sono generate senza soluzione di continuità; chi le genera ne conserva una riservata, la chiave privata, e ne rende contestualmente disponibile l'altra, detta appunto chiave pubblica, a chiunque ne faccia richiesta.

Gli algoritmi di crittografia a chiave simmetrica sono una componente fondamentale di molti sistemi crittografici. Essi svolgono diversi compiti: servono ad autenticare un messaggio; sono utilizzati per la costruzione di generatori pseudo casuali impiegati per la creazione di chiavi crittografiche; servono per ottenere funzioni di hash e inoltre forniscono il meccanismo base per garantire la confidenzialità di una comunicazione su un canale insicuro.

L'algoritmo di cifratura a chiave simmetrica più conosciuto è probabilmente il DES (Data Encryption System), oggi impiegato soprattutto nella variante Triplo DES. Introdotto nel 1975 da IBM e adottato un paio d'anni dopo come standard ufficiale per la trasmissione di informazioni non classificate dal governo statuni-

tense, DES è anche il primo algoritmo coperto da copyright di cui siano stati forniti tutti i dettagli implementativi. Piuttosto diffuso è anche IDEA (International Data Encryption Algorithm), mentre relegati ad ambiti più circoscritti sono rispettivamente AES (Algorithm Encryption Standard) e RC4 (vedi Box: "Gli algoritmi di cifratura a chiave simmetrica").

In un sistema di crittografia asimmetrico ogni soggetto dispone di una chiave pubblica e di una privata, tali per cui partendo da quella pubblica non è computazionalmente praticabile ricavare la chiave privata.

Va rilevato che i cifrari asimmetrici sviluppano performance molto più basse rispetto alla velocità sviluppata dai cifrari simmetrici. Questo spiega perché i primi sono impiegati soprattutto per crittografare le chiavi simmetriche di sessione a loro volta utilizzate per cifrare il messaggio originale usando un cifrario simmetrico. Per garantire l'autenticità di un messaggio si procede in maniera analoga con la sola differenza che il mittente cifra il messaggio utilizzando la propria chiave privata.

L'algoritmo a chiavi pubbliche più utilizzato è RSA, il cui nome deriva dalle iniziali dei suoi ideatori Rivest, Shamir e Adleman. Sfruttando i vantaggi derivanti dalla fattorizzazione di numeri molto grandi, RSA è un algoritmo che attraverso l'utilizzo di chiavi di lunghezza pari ad almeno 1024 bit assicura il raggiungimento di un discreto livello di sicurezza.

Tuttavia per la creazione di chiavi di particolare importanza, come è ad esempio il caso della chiave di firma dei certificati utilizzata da una Certification Authority, una lunghezza pari ad almeno 2048 bit è quantomeno consigliabile. Un altro cifrario asimmetrico molto conosciuto è l'algoritmo DSA (Digital Signature Algorithm). La sua particolarità è quella di sfruttare la debolezza del logaritmo discreto. A differenza di RSA utilizzato sia per la crittografia sia per la firma digitale, DSA è impiegato esclusivamente per l'apposizione di firme digitali. Se a parità di lunghezza di chiave il livello di sicurezza di entrambi gli algoritmi è comparabile, la maggior diffusione di RSA rappresenta senza dubbio un vantaggio considerevole.

ATTACCHI CRITTOGRAFICI

Siamo partiti dalle manipolazioni che la posta elettronica in transito su Internet (o all'interno delle LAN aziendali) può subire e di fatto subisce. Abbiamo accennato ad alcuni dei principali algoritmi che sono alla base della crittografia e alle modalità con le quali possono es-

GLI ALGORITMI DI CIFRATURA A CHIAVE SIMMETRICA

DES cifra a blocchi di 64 bit utilizzando una chiave di 56 bit effettivi, giudicati oggi insufficienti in ragione della potenza di calcolo raggiunta dai calcolatori. Per questo motivo viene impiegata la variante "triplo DES" che applica in cascata l'algoritmo per 3 volte a ogni blocco di dati utilizzando tre chiavi differenti; in tal modo la lunghezza effettiva della chiave è di 168 bit, lunghezza di tutto rispetto per assicurare un buon livello di sicurezza. AES nasce per sostituire il DES. AES cifra a blocchi di 128 bit con una chiave a lunghezza variabile, 128, 196 o 256 bit corrispondenti rispettivamente ad altrettanti algoritmi AES-128, AES-196 e AES-256. AES è un algoritmo dalla struttura particolarmente efficiente in implementazioni hardware.

RC4, a differenza di DES e AES, è un algoritmo che non cifra a blocchi di bit. RC4 si presta in particolare ad implementazioni di tipo software risultando di circa 10 volte più veloce del DES. RC4, sviluppato da Ronald Rivest, ha fatto la sua comparsa nel 1987 e mantenuto segreto da RSA Data Security. Nel 1994 è stato scoperto e reso pubblico su Internet da un anonimo hacker.

IDEA (International Data Encryption Algorithm) nasce con l'obiettivo di imporsi come standard sostitutivo di DES, oggetto di numerosi attacchi brute force. Come DES anche IDEA cifra a blocchi da 64 bit di dati utilizzando lo stesso algoritmo sia per la codifica sia per la decodifica. Il fattore che conferisce a IDEA un livello di sicurezza maggiore è dato dalla lunghezza della chiave, che è di 128 bit. Sulla base di analisi di tipo prestazionale IDEA raggiunge velocità simili a quelle di DES; tuttavia data la lunghezza della chiave il vantaggio rispetto a quest'ultimo aumenta considerevolmente (fattore di grandezza di 10) il tempo necessario per il successo di un attacco brute-force. Studi successivi hanno però dimostrato che l'algoritmo presenta problemi di debolezza proprio nella chiave, carpibile sferrando un attacco di tipo chosen-plaintext.



Max Uggeri,
responsabile offerta
IT Security ONION -
NetFORCE

sere utilizzati per proteggere e autenticare i dati. Sappiamo che è possibile applicare tecniche di autenticazione mediante algoritmi di hash e firma digitale per consentire lo scambio di messaggi garantendo la confidenzialità, l'autenticazione e il non ripudio, a due o più soggetti che utilizzano un canale di comunicazione insicuro e operano in un contesto distribuito ed eterogeneo. Occupiamoci ora delle debolezze e degli attacchi agli algoritmi.

Gli algoritmi di crittografia disponibili attualmente non sono né immuni agli attacchi né completamente sicuri. Le tipologie di attacco alla crittografia sono molto numerose. Nel box ne sono riportate alcune classificate sulla base della qualità dell'informazione in possesso del crittoanalista.

In linea generale la cifratura a chiave pubblica richiede calcoli molto più gravosi rispetto (nell'ordine di grandezza di 1 a 1000) a quella simmetrica. Nel 1991, anno di diffusione pubblica di PGP, i chipset più avanzati erano gli Intel 386, la stragrande maggioranza dei Pc montava processori di classe 286 e ancora molto diffusi erano i vetusti 8086. Perciò l'implementazione di PGP per applicazioni reali era di fatto ostacolata dall'inadeguatezza della tecnologia disponibile. Zimmerman, l'ideatore del programma, scelse perciò di implementare PGP a moduli utilizzando un approccio ibrido in grado di sfruttare al meglio le opportunità offerte dalla cifratura a chiave pubblica e simmetrica. Il problema, data la capacità di calcolo dei processori odierni, di fatto non rappresenta più un ostacolo insormontabile.

Un altro esempio è quello suggerito da Molteni. "La prima "sfida" all'algoritmo DES con

chiave a 56 bit (vale a dire oltre 72 miliardi di chiavi possibili) risale al 1997 e richiese la bellezza di 149 giorni con l'ausilio di circa 15.000 computer in rete per violarlo. Nel 1999 in sole 22 ore e 15 minuti, con uno speciale computer multi-processore e alcune workstation, si ottenendo lo stesso risultato.

Una delle pratiche più diffuse per intercettare la posta elettronica in transito è di disseminare di software passivo (sniffer) lungo il percorso compiuto dalla stessa. Se PGP è installato su un host remoto, passphrase e messaggi saranno probabilmente inviati in chiaro all'host, a meno che non siano aperte sessioni utilizzando SSH o DESlogin. Comuni analizzatori di pacchetti installati tra il terminale dell'utilizzatore e l'host sono in grado di catturare e analizzare queste informazioni, consentendo così la lettura dei messaggi prima che siano crittografati.

In genere gli attacchi portati con queste tecniche sono economici, difficili da individuare e tutto sommato semplici nella loro eleganza; come vedremo si tratta di attacchi "sferrati" direttamente al sistema operativo ospite, in particolare l'ambiente Windows, sfruttando Trojan o Backdoor esistenti. L'obiettivo è quello di ottenere il controllo delle risorse (DLL e API) che pilotano la gestione dei certificati, permettendo così il furto dell'identità" osserva **Max Uggeri**, responsabile offerta IT Security ONION - NetFORCE (www.onion.it).

Come sappiamo lo scambio delle chiavi pubbliche è il primo passo da compiere per avviare una comunicazione crittografata, indipendentemente dal canale impiegato per il loro trasferimento. Ipotizzando che su entrambi i lati della comunicazione le chiavi siano inter-

TIPOLOGIE DI ATTACCHI DA CRITTOANALISI

Definire una tipologia degli attacchi perpetrabili è impresa ardua. Ne abbozziamo una classificando gli attacchi in ordine crescente di qualità dell'informazione in possesso del crittoanalista.

1. attacco ciphertext-only: il crittoanalista possiede il solo testo cifrato. Possiamo ipotizzare che il testo sia stato ottenuto analizzando (sniffando) i pacchetti in transito sulla rete. Le chance di successo di questo tipo di attacco sono molto basse, il crittoanalista necessitando di un'enorme quantità di dati cifrati;
2. attacco known-plaintext: il crittoanalista dispone sia del testo cifrato sia del testo in chiaro. Disponendo di quest'abbondanza di informazioni è teoricamente possibile risalire alla chiave segreta;
3. attacco chosen-plaintext: partendo dalla scelta di un eventuale testo in chiaro, l'attaccante calcola il testo cifrato cercando di ottenere la stessa sequenza di dati cifrati in suo possesso;
4. una variante dell'attacco di tipo chosen-plaintext è l'attacco adaptive-chosen-plaintext: con questo attacco si modifica la scelta del testo in chiaro sulla base del risultato dell'analisi effettuata in precedenza;
5. attacco chosen-ciphertext: diversamente dall'attacco chosen-plaintext, qui è il crittoanalista a scegliere il testo cifrato con l'intenzione di decrittarlo e ottenere il testo in chiaro in suo possesso. Si tratta di una tipologia di attacco applicato in genere in sistemi a chiave pubblica;
6. attacco adaptive-chosen-ciphertext: iniziando dal testo cifrato, la scelta di quest'ultimo viene modificata in base ai risultati dell'analisi precedente.

Tratto da *Sicurezza dei sistemi informatici*, Apogeo, 2001. Elaborazione Data Manager

cezzate e sostituite con altrettante chiavi pubbliche contraffatte, si concretizzerà il maggiore pericolo derivante dall'utilizzo di tecniche di crittografia a chiave pubblica, il cosiddetto attacco man-in-the-middle.

Sulla carta si tratta di un meccanismo assai semplice ed efficace. I pacchetti IP in transito su una LAN devono essere convertiti in pacchetti gestibili per la rete locale stessa. Ethernet identifica le macchine con un indirizzo MAC di 48 bit (Media Access Controllers). «L'host attaccante manda delle false reply ARP alle vittime, associando all'indirizzo IP del corretto destinatario il proprio indirizzo MAC dirotta il flusso della comunicazione verso di sé. La decrittazione di una chiave è poi questione di tempo, inversamente proporzionale alla complessità della chiave stessa» spiega **Lorenzo Grillo**, amministratore delegato di **Ubizen Italia** (www.ubizen.com).

COME TI TROVO LA CHIAVE

Intercettato il primo messaggio, il malintenzionato cercherà di decrittare il contenuto con la chiave pubblica di cui è entrato in possesso, inviando a B un messaggio di risposta crittato con l'altra chiave intercettata, potendo altresì modificare il contenuto del messaggio per i propri scopi. L'attacco man-in-the-middle, come rileva **Giuliano Bertoletti**, e-Security Manager di **Intrinsic** (www.intrinsic.it), è la principale falla della crittografia a chiave pubblica in generale: «Tutto dipende dal modello di sicurezza con cui si ha a che fare. La domanda da porsi è: "Chi sono A e B e perché vogliono comunicare privatamente?". La risposta a questo interrogativo ci consentirà di ottenere validi indizi su come procedere».

La contromisura più semplice è quella di fare in modo che i soggetti coinvolti si scambino, ad esempio telefonicamente, parti della propria chiave pubblica. Se il riconoscimento delle voci da parte di entrambi avrà luogo senza problemi la contromisura sortirà l'effetto desiderato. Tuttavia come rileva **Yann Bongiovanni**, presidente di **Live Network Security** (www.lns.it): «Per chi non usa la PKI, ma si scambia i certificati usando la posta elettronica, è buona prassi verificare telefonicamente o per fax che il "fingerprint" (un valore esadecimale di quaranta cifre derivato dal certificato) del certificato ricevuto/inviato corrisponda effettivamente». Qualora non ci sia corrispondenza di "fingerprint" si può essere certi che il certificato è stato sostituito o manipolato.

Tuttavia secondo Grillo le contromisure rispetto a questo attacco sono piuttosto deboli,



Lorenzo Grillo, amministratore delegato di **Ubizen Italia**



Yann Bongiovanni, presidente di **Live Network Security**

sottolineando che gli stessi sistemi di Intrusion Detection «si limitano a rilevare l'attacco senza riuscire però ad evitarlo. Il modo più sicuro per evitare queste appropriazioni? Utilizzare un sistema a chiave privata RSA basato su smart card, che evita il problema dello scambio delle chiavi».

Secondo altri, il metodo più efficace per fronteggiare questo genere di attacchi è quello di ricorrere ad una Trusted Third Party, la Certification Authority, che, apponendo la propria firma, assicura la corrispondenza tra la chiave pubblica contenuta nel certificato e il titolare dello stesso. «Adottando un approccio molto più integrato all'ambiente delle PKI, la soluzione Security Box utilizza i meccanismi che danno le maggiori garanzie sull'identità del titolare di un certificato e quindi di una chiave pubblica, necessari e non prescindibili nell'utilizzo di tali tipi di tecnologie in ambito business», ci spiega **Massimiliano Micucci**, Product Marketing Manager di **Finmatica Advanced Technologies** (www.finmatica.com)

Anche per RSA, la sicurezza è in relazione alla difficoltà di fattorizzare numeri molto grandi sebbene nessuno abbia ancora dimostrato che questa sia l'unica tecnica efficace d'attacco.



Massimiliano Micucci,
Product Marketing
Manager di Finmatica
Advanced
Technologies

Inoltre è sempre possibile che qualcuno metta a punto una tecnica più efficiente per fattorizzare i numeri; a questo proposito potremmo citare le recenti brillanti intuizioni nella teoria dei numeri, che stanno rendendo questa operazione sempre meno complicata e considerare che, solo nel 1977, un crittografo rilevava che la fattorizzazione di un numero a 125 cifre avrebbe richiesto 40 quadrilioni di anni, mentre già nel 1994 la stessa operazione (ma su un numero a 129 cifre) è stata possibile utilizzando l'idle time dei computer su Internet in soli otto mesi.

D'altra parte il cosiddetto "time to break", vale a dire il tempo ritenuto necessario per violare il meccanismo di crittografia a parità di chiave, è di gran lunga maggiore nei sistemi basati sulle curve ellittiche che non nel sistema a fattorizzazione dei numeri primi come per l'algoritmo RSA. «Il sistema a curve ellittiche ECC (Elliptic Curve Cryptography) con chiave lunga 106 bit offre per esempio lo stesso "time to break" di un sistema RSA con chiave a 512 bit. Aumentando la lunghezza della chiave, questo rapporto a favore dell'ECC cresce; per esempio un ECC con chiave a 210 bit ha il medesimo "time to break" di un RSA a 2048 bit» osserva Molteni.

La stessa inarrestabile crescita della potenza di calcolo dei sistemi è un'altra minaccia costante alla robustezza di RSA, indipendentemente dal sistema di fattorizzazione adottato. D'altra parte per gli utilizzatori di RSA la contromisura più efficace rimane tuttora quella di aumentare la grandezza delle chiavi. Perciò se le capacità di calcolo sono raddoppiate negli ultimi 18 mesi, la creazione di una chiave pubblica che sia un trilione di volte più difficile

da fattorizzare dovrebbe rappresentare una buona difesa.

RSA effettua calcoli che richiedono tempi differenti. Partendo da questa constatazione chi attacca potrebbe, in teoria, utilizzare le rilevazioni relative alle differenze di durata nelle computazioni effettuate dal sistema per tentare di calcolare la chiave privata. Siamo di fronte a un attacco passivo in quanto limitato al monitoraggio dei tempi di calcolo impiegati da RSA. La contromisura più intuitiva è quella di mascherare in modo temporaneo con qualche stratagemma la disponibilità di questi dati che saranno in un secondo tempo recuperati consentendo ai calcoli effettuati da RSA di impiegare una quantità di tempo random.

Consideriamo ora l'esempio di un'azienda che distribuisca la versione aggiornata di un software conosciuto di cui non sia la legittima licenziataria e al cui interno sia stato celato un trojan. Posto che l'ignaro utilizzatore installi il programma e si connetta a Internet, il software potrebbe a questo punto aprire automaticamente una porta che consenta l'accesso al sistema. Accedendo al file system l'intrusore si trova nella condizione di leggere tutti i messaggi non crittografati. Un trojan più evoluto potrebbe essere incorporato in un software che offra una maggiore facilità di utilizzo di PGP. Il programma potrebbe funzionare benissimo e tutto potrebbe sembrare a posto, ma contemporaneamente potrebbe registrare la passphrase della chiave privata collegarsi al modem e inviare il tutto a qualcuno. Anche il codice sorgente di PGP può essere facilmente modificato. Come abbiamo visto un malintenzionato può inserire una back door e lasciare il programma in balia di qualche sito sulla rete. Il truccetto però può essere facilmente scoperto controllando l'hash MD5 sul codice compilato; la pigrizia in questo è un ottimo indicatore delle probabilità di successo.

La cancellazione sicura dei file e le tecniche di encrypting disk sono probabilmente tra le misure di sicurezza più efficaci utilizzando PGP. Per la cancellazione, l'unico problema riguarda i file di grosse dimensioni che spesso richiedono tempi non trascurabili per sovrascrivere più volte i settori del disco interessati. «La creazione di una partizione virtuale cifrata appoggiata sul (e non integrata nel) file-system fisico crea sprechi di spazio, poiché viene allocato all'atto della creazione. Inoltre se sul disco fisico si rovinano alcuni cluster, è probabile la perdita dei dati. Ma il vero problema è che non è possibile cifrare l'unità C:\ che

LA SICUREZZA? DIPENDE

La sicurezza comprende un insieme di attività complesse, che vanno dall'analisi e individuazione delle vulnerabilità alla definizione dei rischi procedurali organizzativi e tecnologici accettabili, passando attraverso la definizione di cosa proteggere e da chi, nonché delle linee guida per la tutela del patrimonio aziendale e delle attività di selezione del software in grado di soddisfare i requisiti di sicurezza richiesti. Il prodotto deve poi essere implementato, mantenuto e gestito periodicamente nel tempo. Il tutto senza dimenticare l'importanza della verifica mediante controlli puntuali dei livelli di sicurezza e delle linee guida stabilite.

Una tale serie di operazioni potrebbe indurre a chiedersi: "Ma da dove iniziare?". Non è importante seguire la catena dall'inizio alla fine, sottolineano i responsabili di **Met Sogeda** (www.metsogeda.it), poiché molto dipende dalla situazione del cliente, dalle politiche di sicurezza già implementate o dalla necessità di eliminare un virus.

Resta comunque chiaro che è impossibile raggiungere la sicurezza totale, anche perché il fattore umano è più critico in un sistema di sicurezza, e molto dipende dalla criticità del business di un'azienda e dal budget disponibile.

è quella in cui la maggior parte dei programmi creano i file temporanei» rileva Bertoletti.

CRITTOANALISI FORTE

Passiamo ora a discutere di alcuni dei problemi che possono sorgere nella crittografia. In prima battuta possiamo in qualche modo ribadire che tutti gli algoritmi di crittografia presentano vantaggi e svantaggi e perciò non è possibile dire quale sia migliore di tutti gli altri. In termini di velocità alcuni sono più efficienti se implementati in dispositivi hardware, altri al contrario software; altri ancora assorbendo meno risorse e quantità di memoria si prestano meglio ad essere impiegati su piattaforme con limiti particolari quali ad esempio le smartcard.

Abbiamo già rilevato che la natura degli attacchi è strettamente correlata alle caratteristiche dell'algoritmo adottato. Occupiamoci allora del modo in cui lo si implementa. A questo proposito un buon punto di partenza è ritenere la memorizzazione segreta in un punto facile da violare una pessima idea per alcuni buoni motivi; utilizzando poniamo il 3-DES la chiave sembrerebbe sempre semplice da attaccare. Niente di più sbagliato: la memorizzazione in locale nei PC dei segreti è impossibile senza un altro segreto. In breve: utilizzando una chiave conosciuta il miglior algoritmo disponibile è inutile. Per la crittografia, affinché raggiunga il suo obiettivo, è fondamentale codificare le informazioni da tenere segrete con un altro segreto; con un piccolo problema: in genere gli utenti non riescono facilmente a memorizzare una nuova password e per questo chiedono all'applicazione client di ricordare per loro la password.

Un secondo problema sollevato da una cattiva implementazione della crittografia è rappresentato dal segreto universale. Il segreto universale si determina quando i prodotti che contengono algoritmi sono autorizzati a dialogare senza doversi scambiare chiavi di sessione autenticate; disposte così le cose la violazione è solo una questione di tempo.

Per esempio l'algoritmo DVD (Digital Versatile Disk) infranto nel settembre 1999 si avaleva di un algoritmo a 40 bit detto CSS (Content Scrambling System). Il problema del segreto universale in questo caso in relazione all'algoritmo CSS è che possedendo il codice di sblocco del lettore DVD diventa possibile decodificare tutti i DVD posseduti. Altri esempi nei quali il segreto universale rappresenta un problema sono dati dalle schede DSS (Digital Satellite System) e smart card con valore memorizzato.

Il processo di degrado o di tendenza al disordine rappresenta nella formulazione di Merriam-Webster il concetto di entropia. In relazione alla crittografia il postulato genera una considerazione tanto semplice quanto inattuabile: l'algoritmo più robusto diventerà completamente inutile se l'utente utilizzerà una password risibile. Si considerino Steganos II o ancora PGP, applicativi entrambi che pur utilizzando algoritmi forti si affidano alle password decise dall'utente la cui robustezza è direttamente proporzionale alla lunghezza dei bit adottata per una chiave crittografica.

Praticamente ogni giorno si verificano attacchi brute force contro i sistemi crittografici (per una definizione di attacco a forza bruta è possibile consultare il seguente link: www.tuxedo.org/esr/jargon/html/entry/bruteforce.html).

L'utilizzo della forza bruta si esplicita attraverso la prova di tutte le combinazioni possibili di chiave all'interno di uno spazio prestabilito fino all'identificazione di quella corretta, operazione questa che potrebbe richiedere tempi esageratamente lunghi. Come detto, attacchi di questo genere sono sferrati con frequenza impressionante ma non sempre con fini dolosi. È possibile infatti che il network engineer di un'azienda per garantire la conformità collaudi le policy della propria azienda servendosi di applicativi quali LOPhtCrack per le pw di NT/2000/XP oppure Crack e John The Ripper per quelle di Unix. Oppure si può ricorrere a dispositivi hardware dedicati.

Una delle lezioni che si imparano osservando i guru della crittografia è che non ci si dovrebbe fidare degli algoritmi segreti. Sebbene quelli disponibili pubblicamente debbono essere considerati inaffidabili se non superano anni di attacchi condotti da teste d'uovo, è importante sapere che se un algoritmo è senza dubbio particolare non riceve soverchia attenzione da parte degli esperti e non lo attaccano.

Ideare un algoritmo forte che superi i test più sofisticati e in grado di resistere ad anni di attacchi sopravvivendo alle sempre più dure aggressioni crittoanalitiche, lo si sarà intuito, non è un'impresa facile. La storia in tal senso parla chiaro: poche persone ci sono riuscite e raggiungendo quasi sempre solo successi parziali. D'altra parte sebbene la quantità di persone in grado di violare un algoritmo di crittografia sia destinata presumibilmente ad aumentare, il loro numero rimane ancora piuttosto limitato considerando che la competenza richiesta è almeno pari a quella degli autori. **DM**

