

Materiale didattico
validato da AICA
Certificazione EUCIP
IT Administrator
Modulo 5 -
IT Security
Sicurezza Informatica



"AICA Licenziataria esclusiva in Italia del programma EUCIP (European Certification of Informatics Professionals), attesta che il materiale didattico validato copre puntualmente e integralmente gli argomenti previsti nel Syllabus IT Administrator e necessari per il conseguimento della certificazione IT Administrator IT Security. Di conseguenza AICA autorizza sul presente materiale didattico l'uso del marchio EUCIP, registrato da EUCIP Ltd e protetto dalle leggi vigenti"

Riferimento Syllabus 2.0 (curriculum ufficiale AICA)
5.7.9 Intrusion detection

► Sicurezza di rete – Intrusion detection e VPN

Difendersi dai nemici all'interno

La settima lezione di Eucip IT Administrator Sicurezza Informatica copre un campo vastissimo: la sicurezza di rete. L'abbiamo suddivisa in cinque parti per coprire tutti i temi. In questa ultima puntata ci occupiamo dei sistemi di prevenzione delle intrusioni e delle reti private virtuali (VPN), due elementi fondamentali di protezione attiva. I contenuti sono composti da tre elementi: un articolo sulla rivista, un articolo molto più esteso in formato PDF e un corso multimediale completo su DVD

di [Giorgio Gobbi](#)

I sistemi di rilevamento delle intrusioni, o *Intrusion Detection Systems* (IDS), sono sistemi hardware o software che automatizzano il processo di monitoraggio degli eventi che avvengono in un sistema o in una rete, analizzandoli alla ricerca d'indicatori riconducibili a problemi di sicurezza.

Un'intrusione è qualunque attività non autorizzata su un sistema o sulla rete di un individuo o di un'organizzazione. Può manifestarsi, ad esempio, come l'azione di un utente legittimo per procurarsi privilegi superiori a quelli che gli sono concessi, il tentativo di un utente remoto non autorizzato di compromettere un servizio di sistema per creare un account, l'installazione di codice maligno trasportato dalla posta elettronica, o in tanti altri modi.

Non esiste una definizione legale d'intrusione che sia univoca e di facile applicazione. I criteri variano da nazione a nazione e non sono uniformi, neppure in ambito nazionale. Non sempre è chiaro se un'intrusione è illegale (si pensi alla scansione delle porte, un'attività pressoché costante su Internet che, in sé, non è un atto ostile, ma può preludere a un tentativo di attacco).

Su un piano concreto, l'intrusion detection è il processo di monitorare gli eventi che avvengono in un sistema, o in una rete, e di analizzarli alla ricerca di segni d'intrusione, intesi come tentativi di compromettere riservatezza, integrità e disponibilità delle informazioni (i cardini della politica di sicurezza) o di aggirare i meccanismi di sicurezza di un computer o di una rete.

Il termine IDS indica un'ampia classe di prodotti e tecnologie. La caratteristica che hanno in comune è quella di rilevare segni d'intrusione, cioè possibili violazioni della politica di sicurezza. In generale, un IDS si limita a rilevare le intrusioni senza impedirle; le informazioni raccolte ser-

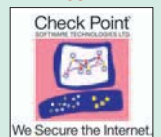
vono per predisporre le contromisure e ridurre gli effetti delle violazioni. Questa non è, comunque, una regola assoluta; esistono modalità e strumenti di risposta attiva (*active response*), a volte implementati tramite applicazioni esterne, che permettono a un IDS di attuare una risposta immediata e automatica all'attacco, così da minimizzarne (o annullarne) gli effetti dannosi.

Nel 2003 varie campagne di marketing iniziarono a promuovere gli *Intrusion Prevention Systems* (IPS) come eredi degli IDS, presentati come un fallimento perché non impedivano gli attacchi e fornivano troppi *falsi positivi*, cioè messaggi d'intrusione che si rivelavano falsi allarmi. A qualche anno di distanza, dissipato il polverone delle promesse

I contenuti delle 8 lezioni

- Lezione 1:** Informazioni generali
Lezione 2: parte 1 Crittografia - fondamenti e algoritmi
Lezione 2: parte 2 Crittografia - applicazioni
Lezione 3: Autenticazione e controllo degli accessi
Lezione 4: Disponibilità dei dati
Lezione 5: Codice maligno
Lezione 6: Infrastruttura a chiave pubblica
Lezione 7: parte A Sicurezza di rete Ethernet e TCP/IP
parte B Sicurezza in mobilità e on line
parte C Impedire accessi non autorizzati
parte D Posta elettronica e firewall
parte E Difendersi dai nemici all'interno
Lezione 8: Aspetti sociali e legali della sicurezza IT

In collaborazione con:



se non mantenute dagli IPS, lo scenario è più chiaro. Gli IDS continuano a evolversi e hanno consolidato la loro presenza nell'industria. Lo standard di fatto degli IDS, Snort, sviluppato a livello individuale da Marty Roesch (fondatore della società Sourcefire) nel 2005 è stato acquisito da Check Point. Anche se Snort verrà integrato nei prodotti Check Point, continuerà comunque a essere sviluppato e distribuito come software libero sotto GPL (*General Public License*) per una comunità di centinaia di migliaia di utenti.

Anche gli IPS proseguono nella loro evoluzione, spesso integrandosi con i firewall, con cui condividono la funzione di bloccare traffico illegale o sospetto. D'altra parte, IDS e IPS hanno ruoli e collocazioni diversi. Un IDS non è intrusivo come un firewall o un IPS, e agisce in primo luogo allo strato di rete, sebbene ci siano IDS in grado di esaminare anche lo strato applicativo. Un IPS, per essere efficace, deve invece essere in grado di far fronte alle complessità dello strato applicativo, senza farsi ingannare dalle tecniche di evasione. Inoltre, un IPS deve essere tarato con molta precisione per riconoscere gli attacchi e, insieme, evitare di bloccare traffico lecito. IDS e IPS sono complementari; anche in presenza di IPS sulla rete, solo l'utilizzo degli IDS a monte e a valle delle protezioni può confermare l'efficacia dei blocchi attuati da firewall e IPS. Un IDS è, di fatto, l'ultima risorsa per rilevare tentativi di attacco passati indenni attraverso le altre barriere.

Oltre a non essere intrusivi, gli IDS hanno il vantaggio di non introdurre complessità di controllo del traffico difficili da gestire. E' vero, tuttavia, che nessun IDS è efficace in assenza di una struttura di supporto competente e tempestiva nell'azione di monitoraggio e negli interventi correttivi. Solo personale esperto è in grado di eseguire il *tuning* (taratura) delle regole di riconoscimento e dei criteri di segnalazione, in modo da isolare gli eventi significativi e limitare il numero di segnalazioni, solitamente ingente.

Tipologie di sistemi di Intrusion Detection

Il tipo di traffico maligno che allerta un IDS dipende dal tipo di IDS e dalla sua collocazione. Gli IDS sono generalmente classificati in base alle seguenti categorie:

1. *Network-Based Intrusion Detection System* (NIDS), cioè IDS basati su rete;
2. *Host-Based Intrusion Detection System* (HIDS), IDS basati su host;
3. *Distributed Intrusion Detection System* (DIDS), IDS distribuiti o ibridi.

Un'ulteriore categoria, *Application-Based IDS*, può essere considerata un subset di quella HIDS, e comprende IDS che analizzano gli eventi nell'ambito di un'applicazione software.

Network-Based IDS

Come suggerisce il nome, i NIDS tengono sotto controllo un intero segmento di rete (o sottorete). A tale scopo, modificano la modalità operativa della scheda di rete a cui sono connessi, da non promiscua (il default) a promiscua. Ciò significa che la scheda passa agli strati di rete superiori non solo i pacchetti diretti all'indirizzo MAC (*Media Access Control*) della scheda, ma tutti i pacchetti che transitano in quel punto della rete, qualunque sia il destinatario. L'IDS si comporta quindi da sniffer di tutto il traffico in transito, che viene analizzato con metodi diversi.

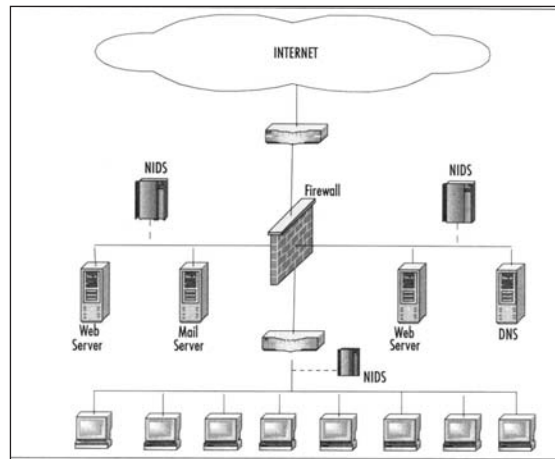
Qualunque sia la terminologia usata dai produttori per promuovere i propri metodi di analisi, i meccanismi fondamentali usati per riconoscere segni d'intrusione sono tre:

1. **Pattern matching**, ovvero il riconoscimento dei pacchetti a fronte di un database di "firme" che identi-

cano i vari tipi di attacco; nella maggior parte dei casi, gli IDS supportano anche uno *stateful pattern matching*, dove i pacchetti sono esaminati nel contesto della connessione, rendendo così più difficile a un cracker aggirare la protezione.

2. **Analisi dei protocolli**: meno specifica del pattern matching, esamina il *pattern* (la struttura) del traffico, anziché il campo dati dei pacchetti. Qui sono verificati gli header e la loro coerenza con la struttura dei pacchetti.

3. **Rilevamento delle anomalie**: suddivisibili in anomalie basate sul comportamento e in anomalie basate sul protocollo. Il rilevamento delle anomalie si basa sull'esame del traffico a livello superiore rispetto al pattern matching e all'analisi dei protocolli. Anziché i singoli pacchetti, si osserva il traffico nel suo complesso; ci sono vari modi per implementare questa metodologia. Un esempio è il monitoraggio delle connessioni tra gli host: se compaiono pacchetti non corrispondenti allo stato della connessione o vistosamente fuori sequenza, scatta l'allarme. Un altro esempio è un Web server che inizi ad accettare connessioni su una porta alta (>1023) anziché la consueta 80, oppure che origini una connessione con un host su Internet. Anche picchi di traffico dovuto ad applicazioni peer-to-peer (solitamente illegali in azienda perché implicano un controllo esterno sui sistemi interni) possono ricadere in tale categoria.



Generalmente, gli IDS sul mercato utilizzano una combinazione dei tre metodi di analisi sopra citati. Di solito il motore centrale utilizza un metodo specifico, e si affida a pre e post-processor per l'implementazione degli altri due metodi. Vediamo un esempio pratico: Snort articola il proprio operato in varie fasi e componenti. Innanzitutto, utilizza una serie di decoder che scompongono i pacchetti ai vari strati (data link, IP, TCP). Una volta completata la scomposizione, invoca alcuni *preprocessor* che si occupano, ad esempio, di seguire lo stato della connessione e di riconoscere eventuali anomalie in tale ambito. Il traffico passa quindi al *detection engine* vero e proprio, che verifica circa 2.500 regole generali di vario tipo. Un'altra classe di componenti, i cosiddetti *output plug-in*, permette di configurare i log (che cosa registrare dell'attività svolta) e gli allarmi.

Un NIDS esamina il traffico di rete senza né modificare il contenuto, né influenzarne il transito. Ciò permette d'installare i sensori con facilità; d'altra parte, l'assenza di controllo sul traffico richiede un accurato dimensionamento e configurazione del sistema e dell'IDS, per riuscire a eseguire l'analisi su tutti gli strati previsti (*stateful inspection*, analisi dei dati applicativi) senza perdere pacchetti. Altrimenti, si può lasciar passare un attacco e perdere lo stato delle connessioni. A pesare ulteriormente sul carico del sistema possono contribuire particolari tecni-

Esempio con tre
Network-Based Intrusion
Detection System (NIDS)

5.7.9.1: Conoscere
le principali tipologie
di *Intrusion
Detection Systems*
(IDS)

Esempio di utilizzo di
Host-Based Intrusion
Detection System (HIDS)

che di attacco, come la frammentazione dei pacchetti.

Un IDS come Snort, dopo anni di evoluzione e dopo la riscrittura del *detection engine* attraverso un algoritmo di ricerca *multipattern* che verifica più regole in parallelo, ha raggiunto le prestazioni necessarie per ispezionare una rete dell'ordine dei gigabit/secondo. In generale, se il motore dell'IDS (e il resto del sistema) non è abbastanza sofisticato per reggere un alto carico di lavoro, bisogna limitare la complessità dei controlli a forme di pattern matching sul *payload* (campo dati) dei pacchetti e di controlli sugli header TCP/UDP/IP. Analisi più approfondite possono essere demandate a una consolle centralizzata, anziché essere eseguite in tempo reale; in tal caso, le azioni correttive vengono ulteriormente ritardate.

L'automazione delle azioni di risposta (*active response*), quando supportate, si limita di solito all'invio di pacchetti *TCP Reset* per interrompere connessioni pericolose, o all'aggiunta dinamica di regole di filtraggio sul firewall. Tali azioni vanno usate tuttavia con cautela, per non rischiare di bloccare traffico legittimo in risposta a pacchetti falsificati (un esempio è il blocco del traffico DNS a causa di pacchetti contraffatti apparentemente provenienti dal nameserver).

L'installazione di uno o più NIDS non ha impatti sul funzionamento della rete, ma può averne sulla sua topologia. La strategia di controllo può essere centralizzata (una consolle centrale controlla il monitoraggio e il reporting), parzialmente distribuita (monitoraggio centrale e reporting a una o più postazioni), o completamente distribuita (monitoraggio basato sull'uso di agenti e decisioni prese nel punto di analisi). Inoltre, il traffico può essere raggruppato e suddiviso tramite switch, in modo da sottoporre ai sensori solo il traffico che è opportuno analizzare, isolato dal traffico meno interessante. In caso contrario, i sensori dovranno essere più numerosi e dimensionati per gestire una maggiore quantità di traffico e di controlli.

Un problema generale degli IDS è quello del *tuning* per ridurre i *falsi positivi* (falsi allarmi) e i *falsi negativi* (attacchi passati inosservati). Se ci si limita a ispezionare ogni pacchetto e a eseguire semplici controlli di pattern matching si usa un approccio troppo generale, che produce molti *falsi positivi*. Se il pattern matching diventa molto specifico, si rischia di mancare gli attacchi (*falsi negativi*). Il *tuning* della configurazione e l'uso dei *preprocessor* per riconoscere le anomalie fanno parte della soluzione.

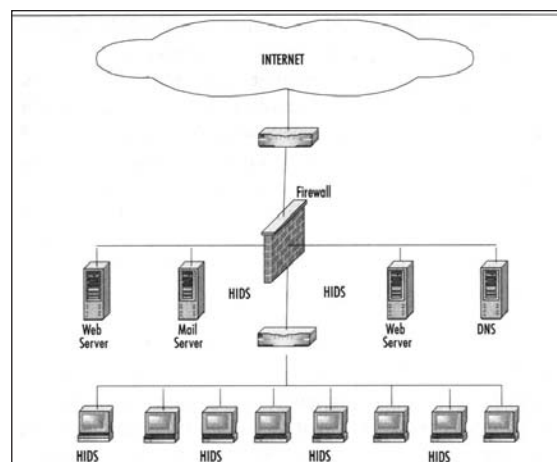
Come nella difesa a più livelli (detta anche *defense in depth*, o difesa in profondità) citata a proposito dei firewall, anche gli IDS dovrebbero essere collocati in ogni punto in cui una rete si connette a un'altra rete: connessioni Internet, DMZ (*Demilitarized Zone*), banchi di modem, gateway VPN (*Virtual Private Network*) e via dicendo. Inoltre, un IDS dovrebbe essere presente ovunque ci siano server la cui compromissione sia ritenuta una grave violazione di sicurezza.

Di fronte alla enorme quantità di dati (log, messaggi, dump) che possono essere prodotti dagli IDS, un requisito vitale è la presenza di un amministratore competente nella sicurezza delle reti e nel *tuning* degli IDS, così da minimizzare i *falsi positivi* e utilizzare gli appropriati strumenti di analisi per estrarre le informazioni utili da migliaia (o centinaia di migliaia) di record.

Una fonte eccellente di informazioni su Snort e gli IDS in generale è Snort 2.1, Second Edition, di vari autori, Syngress Publishing, 2004.

Host-Based IDS

Un IDS basato su host (HIDS) differisce da un NIDS in due modi: protegge solo il sistema su cui è installato (anziché la sottorete), e la scheda di rete del sistema su cui è installato funziona in modo non promiscuo (non ascolta i pacchetti destinati agli altri nodi della sottorete). Di conseguenza, il carico di lavoro di un HIDS è inferiore e il set di



regole su cui esso opera può essere personalizzato in modo molto specifico per il particolare sistema host (per esempio, non occorre monitorare i servizi non attivi).

Il rovescio della medaglia è che un HIDS dev'essere compatibile con il sistema operativo installato sul sistema, il che costituisce un inconveniente soprattutto negli ambienti multi-piattaforma. Un altro aspetto è che l'installazione di un HIDS su un host, soprattutto un server, causa un incremento del carico di lavoro che potrebbe essere mal sopportato.

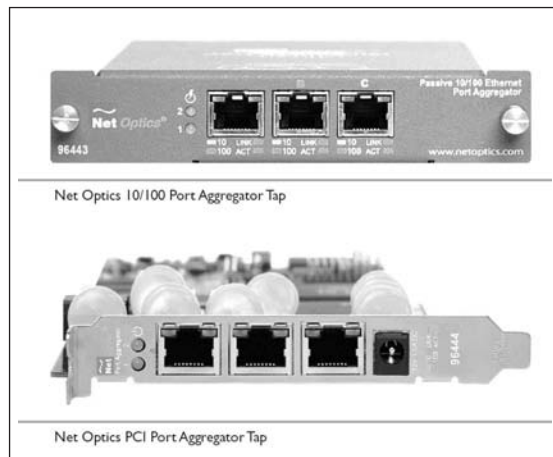
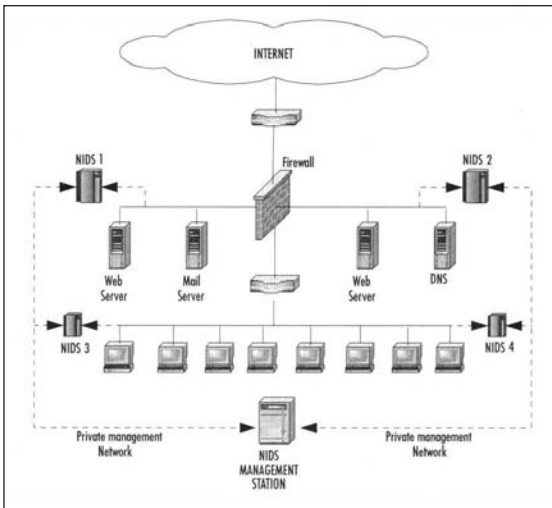
Le caratteristiche degli HIDS possono essere molto varie. In particolare, i sensori possono avere diverse tipologie:

1. sensori che esaminano i log di sistema e applicativi; sono poco intrusivi, ma la loro efficacia è condizionata dalle informazioni che il sistema e le applicazioni registrano nei file di log.
2. sensori che rilevano le modifiche apportate ai file critici di sistema e al registry di Windows, che potrebbero essere effetto d'intrusioni; tra i prodotti della categoria *change audit* (monitoraggio e registrazione dei cambiamenti) citiamo, ad esempio, quelli di Tripwire e di Active Reasoning.
3. sensori collocati tra il software (servizi, sistema, applicazioni) e la rete, che intercettano il traffico e possono bloccare le attività sospette o pericolose. Tali sensori, capaci di attività preventiva, sono presenti in diversi personal firewall commerciali; rispetto ai NIDS, hanno il vantaggio di una maggiore disponibilità d'informazioni sul contesto in cui avviene il traffico con la rete, inclusa l'applicazione che invia e riceve i dati.
4. sensori che intercettano le chiamate di sistema di un processo, con possibilità di segnalarle o di bloccarle; tali sistemi, per lo più sperimentali, richiedono una valutazione del carico di lavoro aggiunto al sistema. Gli HIDS di questo e del precedente tipo sono spesso utilizzati per proteggere singole applicazioni, come i Web server.

Gli HIDS hanno una caratteristica comune agli antivirus: in caso di malfunzionamento o compromissione del sistema, anche l'HIDS può essere bloccato o disattivato. Un comportamento tipico del software maligno è individuare e cercare di chiudere gli antivirus e i personal firewall; in particolare, il firewall di Windows XP può essere disattivato tramite la sua stessa API (*Application Programming Interface*).

Distributed IDS

Un IDS distribuito, o DIDS, è una combinazione di sensori NIDS e sensori HIDS, distribuiti attraverso la rete aziendale, che riportano le informazioni a un sistema centrale di coordinamento. I log degli attacchi sono generati sui sensori e trasferiti, periodicamente o continuamente, alla stazione server centrale dove possono essere archiviati in un database. Le firme dei nuovi attacchi sono caricate sulla



Esempio di rete con Distributed Intrusion Detection System (DIDS)

Esempi di network tap

stazione di management man mano che si rendono disponibili, e quindi vengono trasferite ai sensori secondo necessità. Da notare che gli sviluppatori di Snort, entro pochi giorni - se non ore - dal rilascio di un nuovo malware, aggiornano il ruleset di Snort sulla mailing list di NANOG (North American Network Operators' Group).

I diversi tipi di sensori possono essere gestiti o meno dallo stesso server, e i server di gestione sono spesso distinti dai server che raccolgono i log. Ogni sensore può avere un set di regole personalizzato per le necessità della rete o dell'host monitorati dai sensori. I messaggi di allerta possono essere inoltrati a un sistema di messaggistica ubicato sulla stazione centrale di coordinamento, in modo da tenere informato l'amministratore dell'IDS.

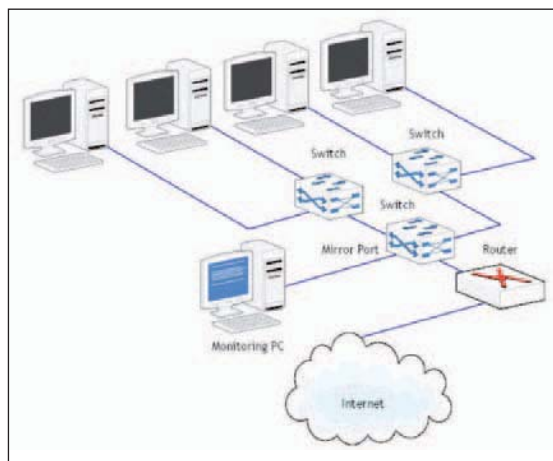
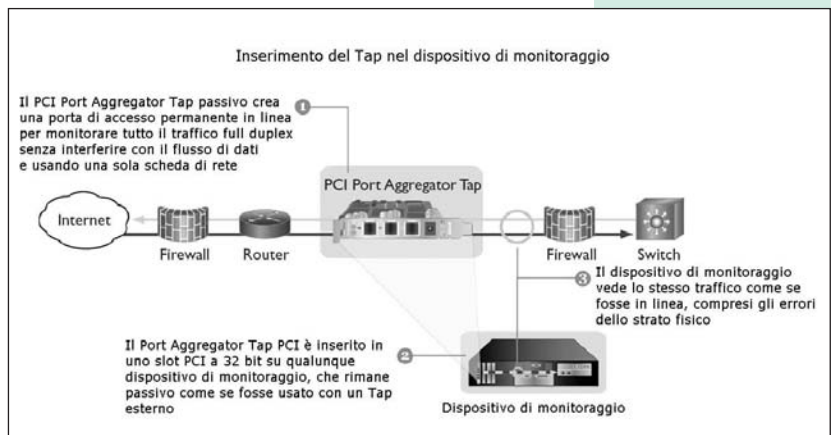
Le transazioni tra sensori e stazione di gestione possono avvenire su una rete privata, come nello schema dell'esempio, oppure sulla rete aziendale. In quest'ultimo caso è vitale che tutti i messaggi riguardanti la sicurezza e il rilevamento delle intrusioni siano cifrati, magari utilizzando una VPN.

Accesso al traffico

L'avvento delle reti switched (basate su switch anziché su hub) ha ostacolato il monitoraggio in modo promiscuo delle reti. La soluzione è stata di configurare gli switch in modo da replicare i dati di tutte le porte o VLAN (Virtual LAN) su una singola porta di mirroring (che deve supportare il traffico cumulativo delle porte da controllare). Tale funzione ha diversi nomi, come *Port Mirroring*, *Spanning Port*, *Monitoring Port*, *SPAN port* e *Link Mode Port*. Spesso *Port Mirroring* indica la capacità di copiare il traffico da una singola porta a una porta di mirroring, disattivandone il traffico bidirezionale. *Spanning Port* indica la possibilità di copiare il traffico da tutte le porte a una singola porta, disattivandone anche in questo caso il traffico bidirezionale. Per Cisco, SPAN significa *Switch Port Analyzer*. Alcuni switch non permettono alle porte SPAN di trasmettere pacchetti, impedendo di usare contromisure di risposta attiva come il *TCP Reset*.

Un'alternativa al mirroring o span delle porte di uno switch (soluzione costosa e sotto il controllo del gruppo di networking, anziché del gruppo di sicurezza) è l'uso dei *network tap* (*test access port*), dispositivi hardware che si innestano direttamente nel cavo di rete e che inviano una copia del traffico di rete a un altro dispositivo. I *network tap* possono essere usati con i NIDS e con gli analizzatori di rete, come Ethereal. A differenza delle porte span, i *tap* forniscono il 100% del traffico di pacchetti, compresi gli errori di strato 1 (fisico) e 2 (data link), normalmente filtrati dagli switch.

Un NIDS può operare in modo invisibile (*stealth mode*),



Uso di un network tap all'interno del dispositivo di monitoraggio (ad esempio un IDS)

Monitoraggio tramite la porta mirror del root switch

ovvero non visibile dalla rete che tiene sotto controllo. Ciò avviene solitamente evitando di assegnare un indirizzo IP all'interfaccia di rete del NIDS, e usando un *network tap* che consente solo la ricezione e non l'invio di traffico. Un fattore chiave per impedire agli attaccanti di accorgersi del NIDS.

Honeypots/Honeynets

Un honeypot è un sistema esca, distinto e complementare rispetto a un IDS, progettato per attirare gli attaccanti lontano dai sistemi critici. Gli scopi degli honeypot sono:

1. sviare gli attaccanti dall'accesso ai sistemi critici;
2. raccogliere informazioni sulle attività degli attaccanti;
3. incoraggiare gli attaccanti a restare nel sistema abbastanza a lungo perché gli amministratori attuino una risposta.

Gli honeypot possono comporre una honeynet, che simula una rete vulnerabile, attirandovi l'attaccante con l'illusione di trovare materiale interessante. Nessun utente legittimo accedrebbe all'honeypot o honeynet, quindi qualunque accesso a questa parte della rete è sospetto. Il sistema è attrezzato con monitor sensibili (IDS) e logger degli eventi, in modo da raccogliere tutte le informazioni utili.

L'implementazione e configurazione di tali strumenti deve essere accurata e realistica. Se l'attaccante si accorge della trappola, evita l'honeypot e inizia ad attaccare i sistemi reali; per questo, l'uso di honeypot non deve creare false aspettative di sicurezza che potrebbero rivelarsi controproducenti (ad esempio, notando troppo tardi che la quiete sull'honeynet non significa assenza di attacchi, ma attacco alle altre reti). Inoltre, un attaccante che ha scoperto un honeypot lo può sfruttare come base di partenza per attaccare i sistemi e le reti reali.

Per queste considerazioni, gli honeypot dovrebbero essere usati in sinergia con gli IDS per prevenire, rivelare e rispondere agli attacchi. A differenza di un sistema di produzione sotto attacco, un honeypot può essere facilmente analizzato, visto che tutte le attività sono ostili e che il sistema può essere messo offline ed esaminato a piacere. L'attacco a un honeypot può anche attivare meccanismi di difesa più efficaci, fino allo shutdown dei sistemi reali in base alle policy di sicurezza e alle informazioni sugli attacchi in corso.

Padded Cell

Anziché attirare un attaccante in un honeypot tramite l'esca di informazioni apparentemente interessanti, una padded cell (cella imbottita) opera in coppia con un IDS. Quando l'IDS riconosce un attaccante, lo trasferisce in modo trasparente a uno speciale host con funzione di padded cell, che contiene un ambiente simulato dove l'attaccante non può fare danno. Come con l'honeypot, l'attaccante deve essere indotto a credere che l'attacco stia avendo successo. Anche una padded cell deve essere ben equipaggiata di strumenti di monitoraggio per osservare e registrare le azioni di attacco.

I vantaggi di honeypot e padded cell sono chiari:

1. gli attaccanti sono sviati verso obiettivi che non possono danneggiare;
2. gli amministratori guadagnano tempo per decidere come reagire;
3. le azioni d'attacco possono essere monitorate in modo esauriente, contribuendo a migliorare le contromisure;
4. gli honeypot sono efficaci nel catturare anche gli insider che curiosano intorno alla rete, fuori dalle aree di lavoro legittime.

Ci sono anche svantaggi:

1. potrebbero esserci implicazioni legali da considerare;
2. l'efficacia di tali strumenti è ancora da approfondire;
3. un attaccante che si accorge di essere manipolato diventa più accanito;
4. gli amministratori e i manager di sicurezza devono avere un alto grado di competenza per utilizzare tali sistemi in modo appropriato.

Monitoraggio dei file di log

I file di log sono una delle fonti di informazioni che possono indicare attacchi e tentativi d'intrusione. L'analisi manuale dei file di log è praticabile solo occasionalmente, quando si affronta un problema specifico. Su base regolare, servono strumenti automatici che selezionino le informazioni d'interesse immediato e le forniscano tempestivamente agli amministratori. In ambienti di tipo Unix, il daemon syslogd di raccolta dei messaggi può essere configu-

rato in modo da inviare sulla console i messaggi di livello *emerg*, ma non offre la flessibilità necessaria per scegliere i messaggi in base ai criteri necessari di volta in volta.

Swatch (*Simple Watch*) è un esempio di strumento capace di monitorare attivamente i messaggi che sono registrati man mano nei file di log, e di selezionarli in base a un set di regole. Ciò evita agli amministratori di essere sommersi sotto un diluvio di messaggi, selezionando ad esempio solo quelli che indicano possibili violazioni o tentativi d'intrusione, o quelli che rappresentano anomalie rispetto allo schema abituale degli eventi.

L'esame dei log può essere periodico o avvenire in tempo reale, con dispendio di risorse di calcolo. Un buon compromesso è installare uno scanner periodico su ciascun server e uno scanner real time sui log server centralizzati. Swatch (<http://sourceforge.net/projects/swatch>) è uno strumento adatto per la scansione real time, mentre Logcheck è un programma che si presta per le scansioni periodiche (<http://sourceforge.net/projects/sentrytools>).

Swatch è molto potente, ma piuttosto complesso da configurare. Può monitorare in tempo reale non solo i log di sistema, ma qualunque file, e può eseguire qualsiasi comando in base ai messaggi riconosciuti (per esempio, può cancellare i file più vecchi di una settimana se riceve un messaggio di file system temporaneo pieno).

Logcheck esamina i log di sistema e riporta, anche via e-mail, le anomalie riscontrate. Gli utenti definiscono gli eventi da ignorare e le violazioni in corrispondenti file di configurazione. Le violazioni sono distinte in *Active System Attacks*, *Security Violations*, e *Unusual Activity*.

Ricevere troppe informazioni, sperando di avere maggiore controllo, è negativo quanto riceverne troppo poche, perché per la maggior parte non sono utili e finiscono per essere ignorate, impedendo di notare i messaggi di reale emergenza. Pertanto, un sistema di segnalazione efficace richiede una *tuning* delle regole di selezione adattato all'ambiente specifico, in modo da escludere tutti i messaggi che rientrano nella routine e isolare le condizioni di allerta.

Sistemi di Intrusion Prevention

Gli IDS hanno il compito di riscontrare attività sospette e intrusioni, sia di tipo classificato e riconoscibile tramite pattern matching, sia di tipo sconosciuto in virtù di qualche anomalia di comportamento o di uso scorretto dei protocolli. In generale, non impediscono un attacco, ma forniscono segnalazioni che vanno valutate per stabilire una risposta. Anche quando si utilizzano tecniche di risposta attiva, la reazione automatica, di solito, non va più in là dell'interrompere una connessione TCP. Lo spoofing degli indirizzi di origine rende molto rischioso rifiutare ogni connessione con determinati indirizzi IP, che potrebbero rivelarsi necessari per le normali attività di un'azienda. In qualche caso, la connessione con un determinato indirizzo viene sospesa per un tempo limitato, in modo da ridurre i danni se l'indirizzo di origine è contraffatto.

Come è avvenuto nei personal firewall commerciali (per uso individuale), che da qualche anno incorporano funzioni di prevenzione delle intrusioni capaci di riconoscere un assortimento di tipologie di attacco, anche i firewall aziendali, in molti casi, si sono arricchiti di funzioni analoghe. In altri casi, i sistemi IPS (*Intrusion Prevention Systems*) sono stati realizzati, spesso come evoluzione degli IDS o a essi combinati, sotto forma di appliance, cioè dispositivi hardware autonomi dotati di un proprio sistema operativo embedded. Questi, nei prossimi anni, si andranno progressivamente integrando con le prossime generazioni di firewall di fascia medio-alta, sia pure in ritardo rispetto alle appliance.

Anziché limitarsi a monitorare il traffico, vengono in-

5.7.9.3. Essere informati sui sistemi di prevenzione delle intrusioni (*Intrusion Prevention Systems*)

5.7.9.2: Sapere in che modo monitorare i log di sicurezza e eventi di sistema

stallati in linea, di fronte alla rete o al servizio da proteggere, in modo da bloccare il traffico ostile. I facili entusiasmi dei primi tempi e il tentativo di screditare gli IDS presentando gli IPS come loro eredi hanno ceduto il passo a una visione più equilibrata, dove gli IPS sono ben accetti se effettivamente bloccano la maggior parte degli attacchi (pochi *falsi negativi*) senza interferire con il traffico lecito (pochi *falsi positivi*). Ciò richiede la capacità di esaminare in profondità (incluso lo strato applicativo) i pacchetti e il traffico, e di utilizzare più tecnologie simultanee per neutralizzare le tecniche evasive messe in campo dagli attaccanti.

I maggiori protagonisti del mercato delle appliance IPS sono 3Com, Check Point, Cisco, DeepNines, Internet Security Systems, Juniper Networks, McAfee, NFR Security, NitroSecurity, Radware, Reflex Security, Sourcefire, StillSecure, Symantec, Top Layer Networks e V-Secure Technologies.

Configurazione di un IDS

Premesso che un'adeguata descrizione di Snort occupa le 700 pagine del citato Snort 2.1 Second Edition, in questa sezione vediamo alcuni aspetti di un'installazione di Snort come NIDS. Consideriamo un sistema con singola interfaccia, anche se Snort può essere configurato in modalità inline controllando il traffico tra due interfacce e utilizzando iptables per ricevere i pacchetti, anziché la libreria pcap.

Il primo requisito hardware è che la scheda di rete utilizzata da Snort e una delle porte dello switch siano configurate in modo promiscuo, in modo da acquisire il traffico di tutta la sottorete. Un altro requisito è che lo switch non sia talmente impegnato da non riuscire a replicare tutti i pacchetti sulla porta SPAN (la porta SPAN deve avere la banda necessaria). Ove ci siano più switch, l'IDS va collegato allo switch root del segmento di rete, altrimenti riceverebbe solo una porzione del traffico.

Snort è affiancato da numerosi pacchetti di terze parti, che ne migliorano la gestione e le prestazioni e ne estendono le funzionalità. Tra di essi citiamo: ACID (*Analysis Console for Intrusion Databases*), uno strumento di browsing e analisi dei dati con supporto MySQL e PostgreSQL; SGUIL (*Snort GUI for Lamers*), un front-end client/server per analizzare i dati prodotti da Snort; Barnyard, un processore degli eventi analizzati da Snort che libera Snort dalle incombenze di formattare l'output e inviarlo a destinazione; Swatch, monitor di log in tempo reale che invia avvisi via email; Snortsam, Fwsmort e Snort-inline, che aggiungono a Snort capacità di risposta attiva; IDSCenter, un front-end di gestione di Snort per Windows; IDS Policy Manager, una console di amministrazione di Snort per Windows; Oinkmaster, uno script Perl per tenere aggiornato il ruleset di Snort; Snortlog, uno script Perl che riassume i log di Snort; SnortSnarf, altro script Perl che produce un report HTML degli eventi recenti; Snortplot.php, che mostra graficamente gli attacchi alla rete; Razorback, un programma di analisi real time dei log per Linux; Incident.pl, uno script Perl che crea un report degli eventi basato sul log di Snort; PigSentry, che usa l'analisi statistica per segnalare picchi nei tipi di segnalazioni fornite da Snort.

Sia Snort (www.snort.org), sia i programmi complementari sono disponibili sui siti dei relativi produttori; rispetto alle versioni preconfezionate è preferibile scaricare le ultime versioni, nonché gli aggiornamenti delle regole. Le applicazioni sono disponibili sia in forma binaria eseguibile, sia come sorgenti da compilare.

La compilazione di Snort richiede la libreria libpcap e le librerie di sviluppo. Una volta installato Snort, è necessario configurarlo. Il file di configurazione è tipicamente `/etc/snort/snort.conf`; in Windows, può essere

`C:\snort\etc\snort.conf`. È un file voluminoso, ma contiene esempi e indicazioni per la personalizzazione. Una delle variabili da modificare è probabilmente `HOME_NET`, a cui si assegna l'indirizzo della propria LAN (per esempio 192.168.0.0/24). La variabile `EXTERNAL_NET` dovrebbe mantenere il valore di default `any`.

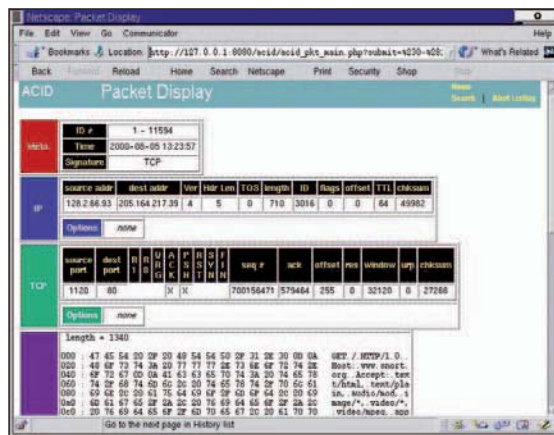
Quindi, è necessario scaricare le regole aggiornate e installarle in una directory, come `/etc/snort/rules` o `C:\snort\rules`. Tale directory dovrà essere assegnata come valore della variabile `RULE_PATH` nel file di configurazione.

A questo punto, si può provare Snort con un comando del tipo:

```
/usr/local/bin/snort -i eth0 -A full -g snort -u snort -c snort.conf -l /var/log/snort
```

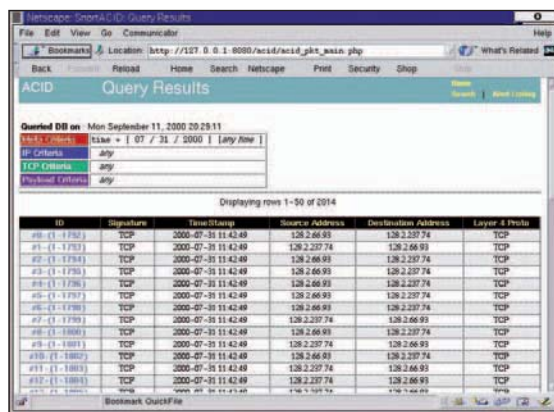
che indica in `/var/log/snort` la directory di logging, che deve essere scrivibile per l'utente `snort` (indicato con l'opzione `-u`). Si può usare l'opzione `-s` per dirigere il logging su syslog.

In seguito, è opportuno sia esaminare il contenuto di

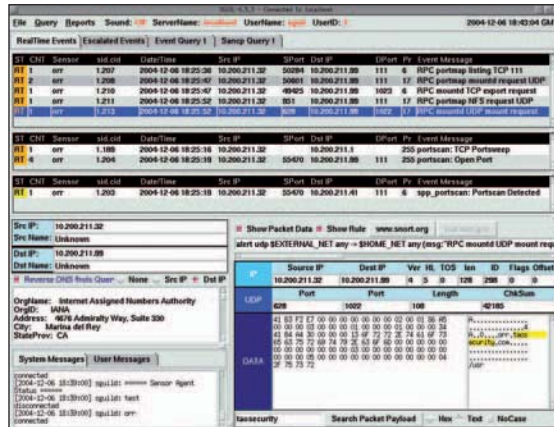


5.7.9.4 Essere in grado di allestire e configurare in maniera essenziale un sistema di Intrusion Prevention System (IDS)

Esame dei pacchetti con ACID



Analisi del traffico con ACID



Esame del traffico con SGUIL

5.7.10 Reti private virtuali

snort.conf per affinare la configurazione, sia utilizzare un file *init*. In molte distribuzioni i parametri della riga di comando possono essere configurati in */etc/sysconfig/snort*.

È possibile scrivere plug-in personalizzati basandosi sia su quelli esistenti, sia sul manuale utente o sui libri su Snort in commercio.

Una volta verificato il funzionamento di Snort, inizia la fase più impegnativa di *tuning* del programma e delle applicazioni complementari per rendere efficiente il riconoscimento delle intrusioni e la gestione degli allarmi. Occorre tenere presente che l'usabilità ed efficienza della rete hanno la precedenza sul rilevamento delle intrusioni, quindi si dovrà fare attenzione a non creare colli di bottiglia e a non sovraccaricare switch e sistemi.

Reti Private Virtuali

Per decenni le connessioni dedicate (*leased lines*), che in Italia hanno preso il nome di *Circuiti Diretti Numerici* (CDN), hanno permesso la realizzazione di collegamenti digitali punto-punto o punto-multipunto. Le linee, affittate dalle compagnie telefoniche, servivano ad esempio per collegare fisicamente due sedi di una società. Il canale così creato è privato, e la velocità di trasmissione dei dati è scelta in funzione del numero di utenti che si vogliono connettere e del volume di traffico della rete. Lo svantaggio di tale soluzione è il costo elevato, perciò, con la diffusione di Internet, un numero sempre maggiore di organizzazioni ha abbandonato le connessioni dedicate a favore delle reti private virtuali (VPN, *Virtual Private Networks*), che utilizzano Internet e diverse tecnologie di sicurezza (cifratura e autenticazione) per ottenere molti dei vantaggi delle reti private al basso costo della rete pubblica.

Una VPN è una rete virtuale, costruita sulla base di reti fisiche esistenti, in grado di fornire un meccanismo di comunicazione sicura dei dati e delle informazioni IP trasmessi in rete. Le reti fisiche possono essere sia reti locali aziendali, sia reti pubbliche come Internet. L'utilizzo di Internet per la trasmissione di informazioni riservate non soltanto è meno costoso rispetto alle connessioni dedicate prese in affitto, ma è anche molto più flessibile, perché è utilizzabile indipendentemente dall'ubicazione fisica degli host. Di conseguenza, oltre ai collegamenti tra aziende o tra sede e filiali, (*gateway-to-gateway*), le VPN permettono collegamenti sicuri tra il personale esterno (ad esempio telelavoro o dipendenti in viaggio) e l'azienda (*host-to-gateway*), e anche collegamenti da computer a computer (*host-to-host*), per esempio per l'amministrazione remota di un server.

Sicurezza dello strato di rete

Dopo anni di evoluzione, che hanno visto l'utilizzo di vari stack di protocolli, il successo di Internet e la diffusione della famiglia TCP/IP anche per le LAN hanno uniformato le VPN sul modello TCP/IP, arricchito di una serie di protocolli di sicurezza per consentire connessioni sicure attraverso una rete insicura. Per meglio comprendere il motivo per cui le VPN proteggono principalmente la connessione allo strato di rete, prendiamo in considerazione le problematiche generali ai vari strati del modello TCP/IP.

1. **Strato applicativo.** A questo strato ogni applicazione deve prevedere controlli separati, con modifiche al codice per ogni specifica protezione. Il grado di controllo e flessibilità sono elevati, ma lo è pure l'investimento. Inoltre, è molto difficile progettare protocolli applicativi crittografici e implementarli correttamente, senza lasciare punti deboli. Il software commerciale spesso non prevede tali protezioni, e anche quando sono protetti i dati applicativi, le applicazioni non sono in grado di proteggere i dati TCP/IP degli strati inferiori, su cui non hanno competenza. Quan-

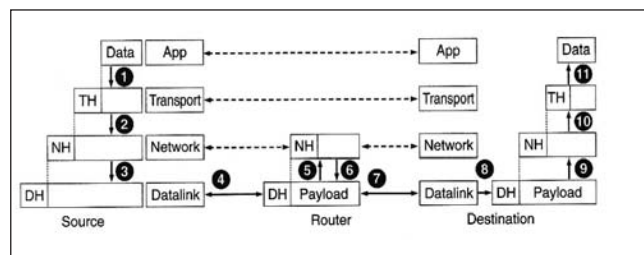
do utilizzata, la protezione allo strato applicativo dovrebbe basarsi su standard accettati e ben collaudati, come nell'esempio di PGP (*Pretty Good Privacy*) per la cifratura della posta elettronica.

2. **Strato di trasporto.** A questo strato si può proteggere una sessione di comunicazioni tra due host. Poiché le informazioni IP sono aggiunte allo strato di rete (cioè sotto allo strato di trasporto), non possono essere protette dallo strato di trasporto. L'utilizzo principale dei protocolli di sicurezza allo strato di trasporto è per proteggere il traffico HTTP. Vengono usati SSL (*Secure Sockets Layer*) e, soprattutto, la sua versione standardizzata TLS (*Transport Layer Security*). A differenza dei controlli allo strato applicativo, che richiedono estese personalizzazioni, i controlli allo strato di trasporto sono molto meno invasivi perché si limitano a proteggere le comunicazioni in rete senza entrare nel merito dei dati applicativi. Sebbene possa richiedere la modifica di qualche applicazione, TLS è un protocollo ben collaudato ed è stato incluso in molte applicazioni, perciò è un'opzione molto meno rischiosa rispetto ad aggiungere protezioni allo strato applicativo. Un inconveniente di TLS è che protegge solo comunicazioni basate su TCP, e non anche su UDP.

3. **Strato di rete.** A questo strato i controlli si applicano indistintamente a tutte le applicazioni, e tutte le comunicazioni tra due host sono protette senza modificare le applicazioni né sui client, né sui server. In molti ambienti, controlli come IPsec (*IP Security*) forniscono una soluzione molto migliore rispetto a quelle di strato applicativo o di trasporto, che richiedono l'aggiunta di controlli alle singole applicazioni. Inoltre, dato che le informazioni IP sono inserite a questo strato, i controlli possono proteggere sia i dati contenuti nei pacchetti (passati dagli strati superiori), sia le informazioni IP di ogni pacchetto. D'altro canto, i controlli allo strato di rete forniscono meno controllo e flessibilità nel proteggere specifiche applicazioni di quanto possano fare i controlli agli strati applicativo e di trasporto.

4. **Strato data link.** I controlli di questo strato sono applicati a tutte le comunicazioni lungo uno specifico collegamento fisico come, ad esempio, il circuito dedicato tra due edifici o la connessione modem con un ISP (*Internet Service Provider*). I controlli di strato data link per circuiti dedicati sono esercitati solitamente da dispositivi hardware specializzati (come i *data link encryptor*), mentre per altri tipi di collegamenti (per esempio via modem) sono forniti dal software. Dato che lo strato data link è sotto allo strato di rete, i controlli proteggono dati e header IP dei pacchetti; si tratta di controlli semplici e facili da implementare, che supportano anche strati di rete diversi dall'IP. Dato che i controlli di tipo data link sono specifici per un certo tipo di collegamento fisico, non si prestano a proteggere connessioni composte da link multipli, come una VPN attraverso Internet. Questa è normalmente costituita da una catena di numerosi link fisici eterogenei, per cui si dovrebbe dislocare una serie di controlli data link separati per ogni tratta, e non è fattibile.

Visto che i controlli allo strato di rete possono proteggere molte applicazioni senza richiedere modifiche, sono quelli più usati per la sicurezza delle comunicazioni su Internet. Forniscono una soluzione unificata per tutte le ap-



Il flusso dei dati in una rete TCP/IP

plicazioni e proteggono sia i dati, sia le informazioni IP. In qualche caso, altri tipi di protezione possono essere più indicati; se, ad esempio, occorre proteggere una sola applicazione, controllare l'intero strato di rete può essere una misura eccessiva.

Tra gli strumenti di protezione delle comunicazioni allo strato di rete, IPSec (*Internet Protocol Security*) è emerso come quello più comunemente utilizzato. IPSec è un complesso di standard aperti volti ad assicurare comunicazioni private su reti IP. A seconda di come è implementato e configurato, può assicurare una combinazione dei seguenti tipi di protezione:

1. Riservatezza. IPSec può impedire che i dati siano letti da estranei, utilizzando la cifratura simmetrica e una chiave temporanea nota solo alle due parti che scambiano dati.
2. Integrità. IPSec è in grado di determinare se i dati sono stati modificati durante il transito. Viene usato un MAC (*Message Authentication Code*) calcolato come hash dei dati e ricalcolato a destinazione; se i due MAC differiscono, il messaggio è stato alterato.
3. Autenticazione. Ogni *endpoint* (punto terminale) IPSec conferma l'identità dell'altro *endpoint* IPSec con cui desidera comunicare, garantendo che il traffico di rete e i dati provengano dall'host previsto.
4. Protezione da replay. Gli stessi dati non possono essere inviati più volte, né inviati con forte alterazione della sequenza. IPSec non garantisce, tuttavia, che i dati siano recapitati nell'esatto ordine di invio.
5. Protezione da analisi del traffico. Un'entità che tenga monitorato il traffico di rete IPSec non è in grado di riconoscere chi sono gli interlocutori, quanto spesso comunicano o quanti dati si scambiano. Può tuttavia contare il numero di pacchetti scambiati.
6. Controllo d'accesso. Gli *endpoint* IPSec possono esercitare un'azione di filtraggio per assicurare che solo gli utenti IPSec autorizzati possano accedere a determinate risorse di rete; possono anche permettere o bloccare certi tipi di traffico di rete.

Crittografia

Le VPN utilizzano un ampio repertorio di tecnologie crittografiche, tra cui cifratura simmetrica (come AES, *Advanced Encryption Standard*, e 3DES, *Triple Data Encryption Standard*), cifratura asimmetrica (a chiave pubblica, come RSA e DSA, *Digital Signature Algorithm*), hashing (come MD5, *Message Digest 5*, e SHA-1, *Secure Hash Algorithm 1*) e protocolli di scambio e gestione delle chiavi.

Architettura gateway-to-gateway

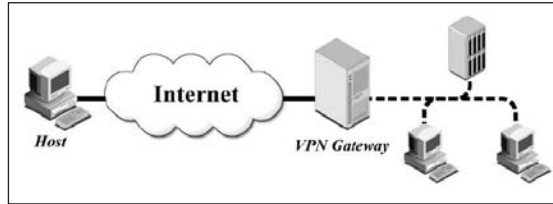
La comunicazione sicura tra due reti, attraverso Internet (o altra rete TCP/IP), è realizzata dislocando un gateway VPN in ciascuna delle due reti. Il gateway, molto spesso, è incorporato in un firewall o router, ma può essere un dispositivo dedicato, come un server o un'appliance.

Nell'illustrazione, il tratto continuo indica la connessione protetta, che è solo quella tra i due gateway; le connessioni tra i gateway e gli host sulle reti locali (tratteggiate) non sono protette. Questo è il modello più semplice da realizzare: la VPN è trasparente per gli utenti, che

non devono eseguire un'autenticazione separata per accedere alla VPN e non hanno bisogno di alcun software client VPN. Tra due gateway in connessione stabile la protezione richiesta è superiore rispetto a una connessione occasionale, e l'autenticazione avviene solitamente tramite certificati digitali.

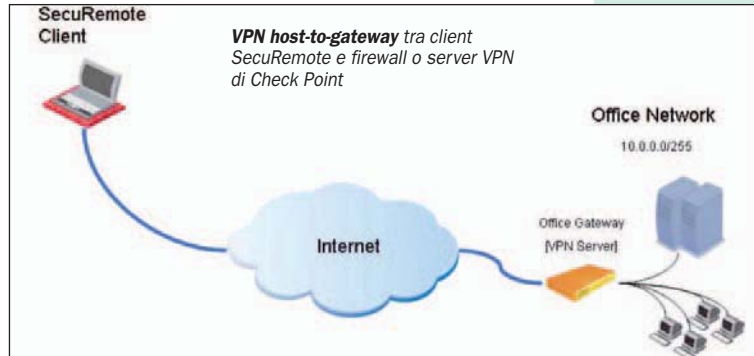
Architettura host-to-gateway

Nell'architettura *host-to-gateway*, un utente remoto (che può anche essere un amministratore) accede alla rete in modo sicuro. La protezione si estende dall'host remoto fino al gateway aziendale.



VPN host-to-gateway
(per esempio tra dipendente in viaggio e azienda)

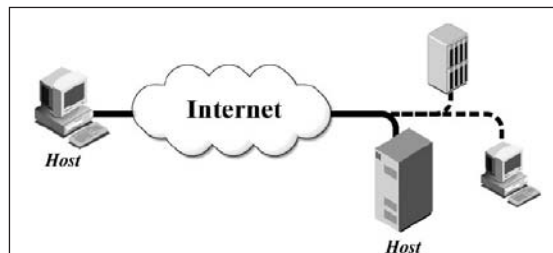
Quando l'utente remoto ha bisogno di connettersi alla rete aziendale, inizia la comunicazione con il gateway VPN. L'host ha bisogno di un software client che può essere fornito dal sistema operativo o essere un'applicazione commerciale. Ad esempio, Check Point distribuisce gratuitamente SecuRemote, un software che rende molto più facile e veloce configurare un host come punto terminale di una connessione VPN; in tal caso, il gateway è un firewall o un server VPN dello stesso produttore.



Quando l'host desidera stabilire una connessione VPN con il gateway, quest'ultimo gli chiede di autenticarsi prima che la connessione possa essere attuata. Lo scambio d'informazioni avviene tramite certificati (il metodo preferibile) o chiavi condivise, secondo i tipi di VPN e il grado di sicurezza richiesto, finché le due parti non si sono reciprocamente autenticate.

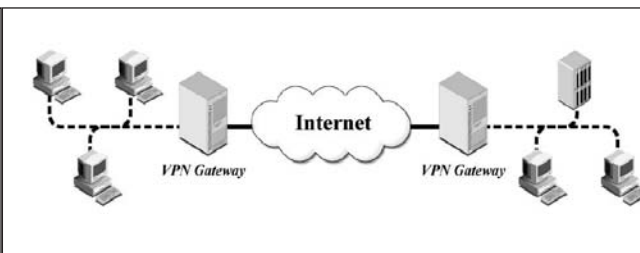
Architettura host-to-host

Si tratta del modello di VPN usato meno di frequente, e serve per scopi particolari, come l'amministrazione remota di un singolo server (normalmente, l'amministratore remoto può utilizzare la connessione *host-to-gateway*). Il server deve essere configurato in modo da fornire servizi VPN,



VPN gateway-to-gateway
(per esempio tra due aziende)

VPN host-to-host
(per esempio tra amministratore remoto e server)



5.7.10.1 Conoscere i protocolli IPSEC/IKE

e l'host dell'amministratore funge da client VPN. Anche in questo caso il client origina la richiesta di connessione, che viene stabilita dopo la fase di autenticazione e scambio di informazioni. Il più delle volte, la VPN *host-to-host* è usata quando un piccolo numero di utenti fidati ha bisogno di amministrare un sistema remoto che richiede l'uso di protocolli insicuri, e che può essere aggiornato in modo da supportare servizi VPN che incapsulino le comunicazioni insicure.

VPN basate su IPsec/IKE

La principale suite di protocolli usata per creare VPN è IPsec (*Internet Protocol Security*), sviluppata dall'IETF (Internet Engineering Task Force) e documentata in una lunga serie di RFC, di cui citiamo un minimo subset di base:
RFC 2401: Security Architecture for the Internet Protocol
RFC 2402: IP Authentication Header (AH)
RFC 2406: IP Encapsulation Security Payload (ESP)
RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409: The Internet Key Exchange (IKE)

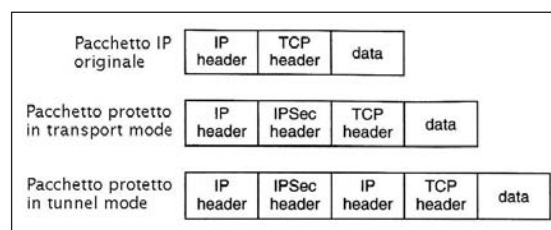
IPsec fornisce funzioni di autenticazione e di cifratura a livello del protocollo IP. Nella pratica, protegge i datagrammi IP definendo un metodo per specificare il traffico da proteggere, come quel traffico deve essere protetto e a chi il traffico è inviato. Un IP datagramma protetto con IPsec è pur sempre un pacchetto IP, quindi si possono nidificare i servizi di sicurezza e fornire, ad esempio, l'autenticazione end-to-end tra due host e inviare i dati protetti da IPsec attraverso un tunnel, a sua volta protetto da gateway di sicurezza che utilizzano IPsec.

Il modo in cui IPsec protegge i pacchetti IP è attraverso l'uso di uno dei suoi due protocolli, ESP (*Encapsulation Security Payload*) o AH (*Authentication Header*). AH fornisce la prova di origine dei pacchetti ricevuti, l'integrità dei dati e la protezione da replay. ESP offre tutto ciò che fornisce AH con, in più, la riservatezza ottenuta attraverso la cifratura del traffico. Il protocollo IKE (*Internet Key Exchange*) fornisce un modo dinamico automatico per autenticare gli interlocutori, negoziare i servizi di sicurezza e generare chiavi condivise. L'uso di chiavi asimmetriche (troppo lento per la cifratura del traffico) è limitato all'autenticazione iniziale durante lo scambio di chiavi, dopo di che, sono usate chiavi simmetriche per la cifratura dei dati e per il calcolo dei MAC (*Message Authentication Code*, usati per l'integrità dei dati).

La RFC2401 definisce l'architettura di base, riferimento per tutte le implementazioni di IPsec. Definisce i servizi di sicurezza forniti, come e dove possono essere usati, come sono costruiti ed elaborati i pacchetti e l'interazione tra l'elaborazione IPsec e la politica di sicurezza.

I protocolli IPsec, AH e ESP, possono essere usati per proteggere l'intero *payload IP* (il pacchetto ricevuto dallo strato di trasporto), o solo la parte dati relativa ai protocolli di strato superiore. Tale distinzione si riflette nelle due modalità d'uso di IPsec. Il *Transport mode* è usato per proteggere i protocolli di strato superiore; il *Tunnel mode* serve per proteggere interi datagrammi.

In *Transport mode*, un header IPsec è inserito tra l'header



der IP e l'header del protocollo superiore (ad esempio TCP). In *Tunnel mode*, l'intero pacchetto IP da proteggere è incapsulato in un altro IP datagramma, e un header IPsec viene inserito tra il nuovo header IP esterno e l'header IP interno. Sia AH, sia ESP possono operare in *Transport* o *Tunnel mode*.

Il *Transport mode* può essere usato solo per proteggere pacchetti laddove il punto terminale della comunicazione coincida con il punto terminale crittografico. Il *Tunnel mode* può essere usato al posto del *Transport mode* e permette, inoltre, di essere utilizzato dai gateway di sicurezza per fornire servizi a beneficio di altre entità della rete, come una VPN. In tal caso, i punti terminali della comunicazione sono specificati dall'header IP interno, che è protetto, e i punti terminali crittografici sono quelli dell'header IP esterno. Un gateway di sicurezza estrae il pacchetto IP incapsulato a conclusione dell'elaborazione IPsec, e inoltra il pacchetto alla sua destinazione finale.

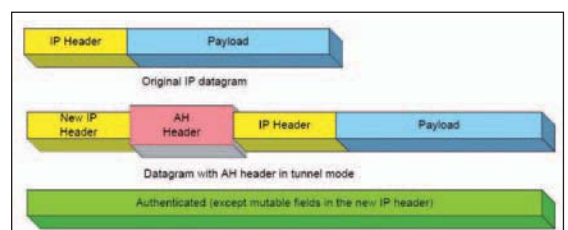
Per poter incapsulare ed estrarre i pacchetti IPsec, è necessario un modo per associare i servizi di sicurezza e una chiave con il traffico da proteggere e con l'interlocutore con cui viene scambiato il traffico. Tale costruzione prende il nome di *Security Association* (SA). È unidirezionale: definisce i servizi di sicurezza in una direzione, associati ai pacchetti in uscita o in entrata. Tali servizi sono identificati da un *Security Parameter Index* (SPI) presente negli header IPsec, dal protocollo IPsec e dall'indirizzo di destinazione associato alla SA. Le SA esistono tipicamente in coppie (una per direzione), e sono create dinamicamente dal protocollo IKE. Le SA risiedono nel *Security Association Database* (SADB). Un'altra struttura centrale di IPsec è il *Security Policy Database* (SPD); ogni suo record definisce il traffico da proteggere, come proteggerlo e con chi la protezione è condivisa. Per ogni pacchetto che entra o esce dallo stack IP, l'SPD viene consultato per verificare la possibile applicazione di servizi di sicurezza. Gli schemi che seguono mostrano il formato dei pacchetti AH ed ESP in entrambe le modalità, *Tunnel* e *Transport*, con alcuni commenti.

Authentication Header

Il protocollo AH di IPsec assicura l'autenticazione d'origine, l'integrità e la protezione da replay dei datagrammi IP in modo *connectionless*, ovvero pacchetto per pacchetto. L'integrità è garantita dalla *checksum* generata da un *Message Authentication Code* (MAC); l'autenticazione dell'origine dei dati è assicurata inserendo una chiave condivisa nei dati da autenticare; la protezione da replay è ottenuta tramite un numero di sequenza nell'header AH.

AH viene usato in *Tunnel mode*, ad esempio, in un'architettura *gateway-to-gateway* (detta anche *site-to-site*), oppure *LAN-to-LAN* (tra LAN della stessa azienda). L'indirizzo di destinazione nel nuovo header IP è l'indirizzo della VPN di destinazione. La funzione di autenticazione si applica all'intero pacchetto, eccetto che per alcuni campi nel nuovo header IP (come il *time to live*, un campo decrementato da ogni router che instrada il pacchetto), che possono venire modificati durante il percorso verso destinazione. Tali campi sono anche chiamati campi mutevoli.

L'autenticazione copre sia l'indirizzo di origine, sia quel-

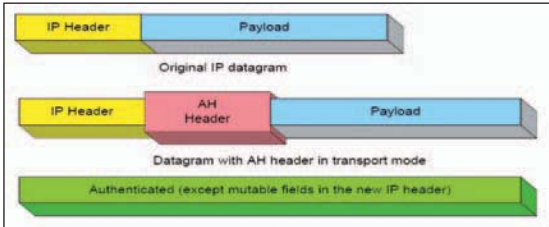


Transport mode e Tunnel mode

AH in Tunnel mode

lo di destinazione. Ciò permette al ricevente di riconoscere eventuali attacchi con spoofing del mittente.

AH è usato in *Transport mode*, ad esempio, nell'architettura *host-to-host*. La differenza principale è che viene mantenuto l'header IP originale. L'autenticazione riguarda ancora l'intero pacchetto. L'autenticazione non fornisce alcuna riservatezza, una funzione che spetta al protocollo ESP.



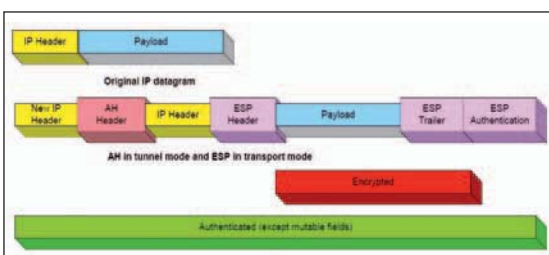
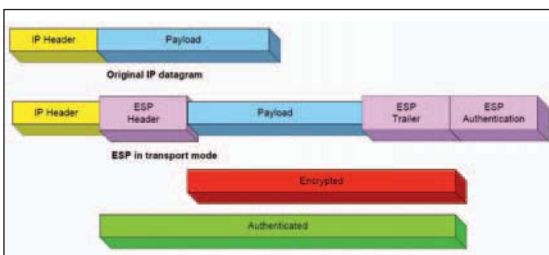
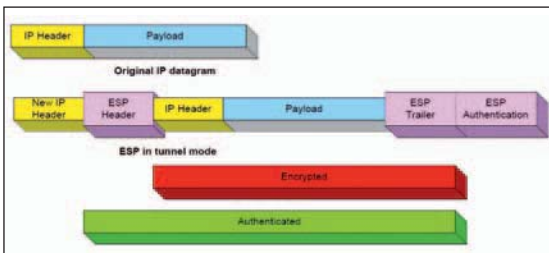
Encapsulation Security Payload

Il protocollo ESP di IPSec assicura sempre la riservatezza (tramite cifratura) e, opzionalmente, l'integrità, l'autenticazione dell'origine dei dati e la protezione da replay. Quando è usato per fornire le funzioni di autenticazione, ESP utilizza gli stessi algoritmi impiegati da AH, ma con una diversa copertura: i campi autenticati non comprendono il nuovo header IP, quindi ESP non fornisce protezione contro lo spoofing dell'indirizzo di origine.

Lo schema del pacchetto ESP in *Tunnel mode* mostra l'aggiunta di un header ESP. L'indirizzo di destinazione nel nuovo header IP è l'indirizzo della VPN di destinazione. L'autenticazione non include il nuovo header IP.

Anche lo schema del pacchetto ESP in *Transport mode* mostra l'aggiunta dell'header ESP; la principale differenza è che viene mantenuto l'header IP originale. A differenza del *Transport mode* di AH, l'autenticazione non include l'header IP.

Le funzioni AH ed ESP possono essere utilizzate insieme. Una potenziale combinazione è usare ESP in *Transport mode* e AH in *Tunnel mode*.



In questa combinazione di AH ed ESP, il *payload* originale e il *trailer* (coda) *ESP* sono le uniche porzioni che vengono cifrate (come ESP in *Transport mode*). L'autenticazione copre l'intero pacchetto, tranne per i campi mutevoli del nuovo header IP.

Internet Key Exchange

IKE è un protocollo che ha la funzione di negoziare in modo protetto le SA (*Security Associations*) e fornire il materiale autenticato usato per la costruzione delle chiavi. I processi che implementano IKE possono essere usati per la negoziazione delle VPN e per fornire a un utente remoto (con indirizzo IP non noto in anticipo) l'accesso sicuro a un host o a una rete. IKE richiede il completamento di due fasi prima che il traffico possa essere protetto con AH o ESP.

Lo scopo della prima fase è che i due endpoint IPSec negozino con successo un canale sicuro attraverso il quale possa essere negoziata una SA IPSec. Il canale sicuro così creato è detto IKE SA; il suo scopo è fornire una cifratura e un'autenticazione bidirezionale per gli altri scambi IKE: le negoziazioni della fase due, il trasferimento delle informazioni di stato e di errore, e la creazione di informazioni per la costruzione delle chiavi attraverso l'algoritmo *Diffie-Hellman* di scambio chiavi (che ha dato origine alla crittografia asimmetrica).

La fase uno può avvenire in due modi: *main mode*, che prevede tre paia di messaggi, o *aggressive mode*, che utilizza solo tre messaggi, ma è meno flessibile e sicuro.

Lo scopo della fase due è di stabilire una SA per l'effettiva connessione IPSec (detta IPSec SA). A differenza della IKE SA, che è bidirezionale, le IPSec SA sono unidirezionali, quindi una connessione IPSec tra due sistemi richiede due SA.

L'utilizzo di IPSec può riservare due difficoltà. La prima è relativa alla *Network Address Translation* (NAT). La SA è legata agli indirizzi di mittente e destinatario, quindi, se viene modificato un indirizzo nel pacchetto durante il percorso, l'autenticazione fallisce.

Ciò non permetterebbe a IPSec di attraversare un router che applica la NAT. Ci sono diverse soluzioni per l'uso di NAT con IPSec:

1. eseguire la NAT prima di applicare IPSec (per esempio, il gateway può eseguire prima la NAT e poi IPSec per i pacchetti in uscita);
2. usare UDP per l'incapsulamento dei pacchetti ESP in *Tunnel mode*. L'incapsulamento UDP aggiunge un header UDP a ogni pacchetto che fornisce un indirizzo e porta UDP utilizzabili da NAT/NAPT; ciò elimina conflitti tra IPSec e NAT nella maggior parte dei casi (vedere le RFC 3947 e 3948).
3. nelle abitazioni e piccoli uffici si può configurare il router ADSL che esegue la NAT in modo da permettere l'attraversamento di IPSec.

Una seconda difficoltà riguarda la gestione, in caso di *Tunnel mode*, dei parametri legati alla *Class of Service* (CoS - gestione del traffico per tipo, ad esempio posta, trasferimento file, streaming video, con classi di priorità diverse). Infatti, non è ovvio se e come i parametri CoS del pacchetto incapsulato debbano essere utilizzati dal gateway per il nuovo header generato, o se esso ne debba generare di propri; in questo caso, il link cifrato potrebbe non rispettare i requisiti dell'header interno senza che, però, la cosa risulti evidente al mittente.

Alcune ottime fonti di informazioni su IPSec e VPN sono: IPSec di N. Doraswamy e D. Harkins (l'autore di IKE), Prentice Hall, 1999; Guide to IPSec VPNs, National Institute of Standard and Technology, US Department of Commerce, pubblicazione 800-77, dicembre 2005; Virtual Private Networks and Their Use in Support of National Security and Emergency Preparedness, National Communication System, US Department of Homeland Security, 2002.

AH in Transport mode

ESP in Tunnel mode

ESP in Transport mode

Combinazione di AH in Tunnel mode e ESP in Transport mode

5.7.10.2 Conoscere le reti private virtuali basate su tecnologia MPLS

VPN basate su MPLS

Il *Multiprotocol Label Switching* (MPLS) è un meccanismo di trasporto dei dati che emula alcune proprietà di una rete a commutazione di circuito su una rete a commutazione di pacchetto. Nel modello OSI, MPLS si colloca in una posizione intermedia tra gli strati 2 (data link) e 3 (rete), che è spesso chiamata *strato 2,5*. MPLS è un metodo ad alte prestazioni per l'inoltro dei frame attraverso una rete; mette in grado i router ai bordi della rete di applicare semplici etichette ai frame e gli switch ATM (*Asynchronous Transfer Mode*), o i router all'interno della rete possono commutare i pacchetti in base alle etichette con un minimo costo di elaborazione.

Nel modello di routing convenzionale di una rete *connectionless* (dove ogni pacchetto è instradato individualmente), ogni router utilizza un algoritmo di routing di strato 3 (rete o IP). Man mano che il pacchetto attraversa la rete, ogni router sul percorso prende una decisione indipendente sull'inoltro del pacchetto. Usando le informazioni nell'header del pacchetto e le informazioni ottenute dall'algoritmo di routing, il router sceglie la destinazione del salto (*hop*) successivo per il pacchetto. Il processo implica trovare una corrispondenza tra l'indirizzo di destinazione di ogni pacchetto e una route specifica ottenuta dalla routing table; l'analisi e classificazione dell'header IP è, perciò, dispendiosa in termini di risorse di calcolo. Inoltre, le informazioni contenute nella maggior parte degli header non consentono al router di inviare il pacchetto fino alla destinazione finale; i router non hanno una visione completa del percorso dei pacchetti, e i criteri di decisione per l'instradamento (economia, percorso più breve, ecc.) non assicurano obiettivi di qualità del servizio (QoS), alta disponibilità e flessibilità.

In un ambiente MPLS i percorsi ottimali attraverso la rete sono identificati in anticipo. Perciò, appena i pacchetti di dati entrano nella rete MPLS, i dispositivi di ingresso usano le informazioni di strato 3 per assegnare i pacchetti a uno dei percorsi predeterminati. A tale scopo, viene inserita nel pacchetto un'etichetta (*label*) che specifica il percorso da seguire. L'etichetta accompagna il pacchetto dati man mano che attraversa la rete. I router successivi sul percorso usano le informazioni nell'etichetta per determinare il dispositivo di destinazione del salto successivo. MPLS utilizza un header che consiste di una serie di etichette, detta *label stack*. Ogni elemento dello stack è lungo 32 bit, e comprende quattro campi:

1. il valore dell'etichetta (20 bit);
2. un campo sperimentale di 3 bit per uso futuro;
3. un flag di fondo stack di 1 bit (vale 1 per l'ultima etichetta dello stack);
4. un campo TTL (*time to live*) di 8 bit.

Il pacchetto MPLS viene trasmesso da mittente a destinatario su circuiti virtuali in base alle informazioni contenute nelle etichette, che determinano il percorso. In tal modo, si ottiene la massima flessibilità nella definizione dei percorsi unita all'efficienza dell'instradamento (solo il router d'ingresso della rete MPLS deve eseguire calco-

li impegnativi). Inoltre, MPLS permette di scegliere un percorso (route) in base alla qualità del servizio richiesta (in termini di larghezza di banda, tempi di ritardo o perdita di pacchetti).

In particolare, ci sono due approcci per fornire il routing con QoS (*Quality of Service*) in ambito MPLS: tramite informazioni di *Classe di Servizio* (CoS) nell'etichetta MPLS, usate per ottenere adeguata priorità di routing, oppure attraverso più percorsi messi a disposizione dalla rete MPLS, ciascuno con un diverso livello di servizio, in modo che il traffico segua il percorso appropriato quando entra nella rete.

Lo standard MPLS supporta diversi protocolli di rete, tra cui IPv4, IPv6, IPX e AppleTalk. Inoltre, supporta diversi tipi di strato data link, inclusi Ethernet, Token-Ring, FDDI (*Fiber Distributed Data Interface*), ATM (*Asynchronous Transfer Mode*), Frame Relay e collegamenti punto a punto. Lo standard viene progressivamente esteso ad altri protocolli e tipi di rete.

Uno degli impieghi tipici di MPLS è la realizzazione di circuiti virtuali (ad esempio su reti ATM), che sono visti dagli utenti come un singolo collegamento di strato 2 (data link) tra mittente e destinatario anche se, in realtà, attraversano più nodi di una rete geografica. La tecnologia MPLS è trasparente al traffico IP; allo strato 3 (rete) il traffico di due circuiti MPLS può essere completamente separato, anche se essi condividono gli stessi apparati e collegamenti fisici. Tali circuiti virtuali hanno un'affidabilità non inferiore a quella di una linea dedicata presa in affitto.

Nel complesso, MPLS combina l'intelligenza del routing con la velocità dello switching, offrendo benefici notevoli a reti di vario tipo: con pura architettura IP, con abbinamento di IP e ATM, o con un mix di tecnologie di strato 2. MPLS è impiegato principalmente nel nucleo della rete dei servizi provider. I router periferici della rete applicano le etichette ai pacchetti, e gli switch ATM o i router dentro la rete commutano i pacchetti in base alle etichette, col minimo sforzo. In pratica, MPLS integra le prestazioni e le capacità di gestione del traffico di strato 2 con la scalabilità e flessibilità dello strato 3.

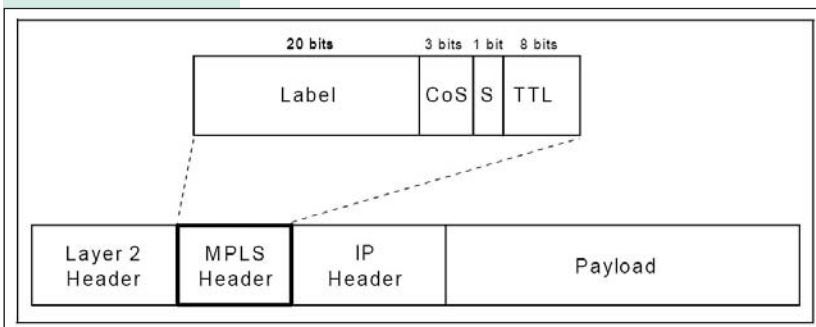
Vantaggi e svantaggi delle diverse tecnologie

Negli ultimi anni si sono costituiti due gruppi di lavoro dell'IETF (Internet Engineering Task Force) focalizzati su tre componenti delle VPN: sicurezza Internet, standardizzazione del label switching e qualità del servizio (QoS - *Quality of Service*). Nell'Area Routing dell'IETF, il gruppo di lavoro dell'MPLS ha sviluppato meccanismi per supportare l'allocazione di risorse agli strati di rete superiori, la QoS e la definizione del comportamento degli host. Contemporaneamente, nell'Area Sicurezza dell'IETF, il gruppo di lavoro IPsec si è concentrato sulla protezione dello strato di rete attraverso meccanismi di sicurezza crittografici che supportano in modo flessibile varie combinazioni di autenticazione, integrità, controllo d'accesso e riservatezza. L'IETF ha lasciato la questione dell'integrazione tra MPLS e IPsec alla discrezione dei produttori di networking. Il risultato è che sono emerse due architetture, una basata su MPLS e i circuiti virtuali, e l'altra basata su IPsec e la cifratura; le due architetture sono comunque complementari, anziché esclusive.

L'autenticazione e la cifratura dei pacchetti tramite IPsec offrono, rispettivamente, garanzie di integrità e di riservatezza. Tali proprietà sono controllate dal mittente e dal destinatario, indipendentemente dalla rete attraverso cui sono trasmessi i pacchetti. Pertanto, questa tecnologia può essere usata su Internet anche tra host e tra sedi re-

5.7.10.3 Sapere quale livello di sicurezza è garantito dalle differenti tecnologie

L'header MPLS (è mostrata una sola etichetta)



mote, dislocate in qualunque parte del mondo. Tuttavia, non viene offerta alcuna garanzia di disponibilità: la trasmissione dei pacchetti continua ad avvenire secondo il principio di "best effort", che caratterizza il traffico IP: si eseguono controlli, ma i pacchetti sono consegnati singolarmente, in ordine casuale e senza garanzia che arrivino tutti a destinazione. La disponibilità di banda può essere contrattata attraverso meccanismi di CoS (*Class of Service*), ma senza garanzie; IPSec non si occupa direttamente di qualità del servizio, mentre alcuni produttori hanno sviluppato soluzioni per mantenere la classificazione QoS dei pacchetti all'interno di un tunnel IPSec.

Al contrario, la qualità del servizio è ottenuta in MPLS attraverso l'assegnazione di una banda garantita a un circuito virtuale, preservata da tutti gli apparati che realizzano il circuito. Inoltre, le capacità di *traffic engineering*, ovvero la flessibilità con cui si possono definire percorsi alternativi, contribuiscono alla protezione del traffico e alla robustezza della rete. D'altro canto, anche questa tecnologia ha i suoi limiti. La riservatezza e l'integrità del traffico non sono garantite da un estremo all'altro della connessione, e il traffico attraverso il circuito in chiaro, quindi potrebbe essere intercettato. La valutazione del rischio è legata all'affidabilità del gestore sia in termini di correttezza, sia di gestione della sicurezza al proprio interno. La protezione del traffico è garantita solo se gli apparati sono configurati in modo appropriato. Le conseguenze di errori di configurazione includono:

1. perdita di efficacia dei meccanismi di disponibilità (ad esempio, in caso di guasto hardware);
2. vulnerabilità ad attacchi agli apparati attraverso i circuiti MPLS che essi supportano (gli stessi dispositivi hardware possono supportare circuiti MPLS di aziende concorrenti e di provider);
3. perdita di isolamento del traffico su circuiti diversi.

Si deve anche tenere conto che, solitamente, la disponibilità di circuiti MPLS è legata all'infrastruttura di un singolo gestore, quindi l'attivazione di protezione tra due host su reti diverse collegate a Internet non è immediata come con IPSec. Infine, la tecnologia MPLS può avere costi notevoli, specialmente in conseguenza della banda garantita, mentre IPSec può essere utilizzata con costi trascurabili. Entrambe le tecnologie possono convivere con vantaggio, specialmente se la VPN è utilizzata per realizzare tratte geografiche della propria intranet.

Altre tecnologie di incapsulamento

IPSec offre la flessibilità e sicurezza che lo rendono la soluzione preferita per la maggior parte delle VPN. Esistono diverse alternative, che possono essere raggruppate secondo lo strato di rete a cui si applicano.

Protocolli VPN di strato data link

Mentre IPSec opera allo strato di rete e supporta solo il protocollo IP, i protocolli VPN di strato 2 (data link) possono essere usati con diversi protocolli di rete, come IP, IPX e NetBEUI (oggi IPX e NetBEUI sono obsoleti).

I più comuni protocolli VPN di strato 2 sono usati tipicamente in abbinamento al *Point-to-Point Protocol* (PPP), e per lo più servono a rendere sicure le connessioni via modem. PPP, non il protocollo VPN, fornisce tipicamente i servizi di autenticazione e cifratura del traffico. Tuttavia, lo standard PPP prevede solo la cifratura DES (*Data Encryption Standard*, obsoleto perché insicuro) e l'autenticazione via PAP (*Password Authentication Protocol*) e CHAP (*Challenge Handshake Authentication Protocol*), anch'essi insicuri, mentre i protocolli VPN di strato 2 utilizzano spesso pro-

tolcolli aggiuntivi per offrire autenticazione e cifratura più robuste. I protocolli VPN più usati sono i seguenti:

1. Point-to-Point Tunneling Protocol (PPTP) Version 2. Fornisce un tunnel protetto tra un client (per esempio un personal computer) e un server, entrambi abilitati a PPTP. Richiede agli utenti l'installazione e la configurazione del software client (incluso in Windows). Per il trasporto dei dati, PPTP utilizza il protocollo IP 47 (GRE, *Generic Routing Encapsulation*), che viene bloccato dalla maggior parte dei dispositivi di filtraggio dei pacchetti, quindi può essere necessaria una loro riconfigurazione per lasciarlo passare. Oltre alla connessione GRE, PPTP apre un canale di controllo usando la porta TCP 1723. Microsoft ha creato un proprio meccanismo di cifratura per PPTP, l'IMPPE (*Microsoft Point-to-Point Encryption*), che usa una chiave da 40 o 128 bit con l'algoritmo RC4 di RSA. Microsoft ha anche sviluppato MS-CHAP e MSCHAPv2 per fornire un'autenticazione più robusta, ma neppure questi protocolli sono esenti da vulnerabilità. Il PPTP originale era affetto da gravi lacune di sicurezza. PPTPv2 ha risolto molti problemi, ma i ricercatori hanno individuato punti deboli che ne sconsigliano l'utilizzo, se non per connessioni occasionali senza alti requisiti di sicurezza. PPTP può essere utilizzato, ad esempio, per connettersi alla rete domestica o SOHO (*Small Office-Home Office*) quando si è in viaggio.

2. Layer 2 Tunneling Protocol (L2TP). Alla pari di PPTP, protegge le comunicazioni tra un client e un server entrambi abilitati a L2TP. Sui computer degli utenti dev'essere installato e configurato un client L2TP. A differenza di PPTP, L2TP utilizza un proprio protocollo di tunneling che fa uso della porta UDP 1701. Inoltre, L2TP supporta sessioni multiple nello stesso tunnel. Oltre ai metodi di autenticazione forniti da PPP, L2TP supporta altri metodi, come l'uso dei server di autenticazione RADIUS e TACACS+. Spesso, L2TP utilizza IPSec per i servizi di cifratura e gestione delle chiavi.

3. Layer 2 Forwarding (L2F). A differenza di PPTP e L2TP, L2F è destinato all'uso tra dispositivi di rete, come il server di accesso alla rete di un ISP (*Internet Service Provider*), e il gateway VPN di un'azienda. Gli utenti stabiliscono una connessione non protetta dal loro computer all'ISP. Quest'ultimo riconosce che il traffico degli utenti deve essere incapsulato in un tunnel verso l'azienda, perciò autentica ogni utente e il gateway dell'azienda, quindi fornisce la protezione del traffico tra il proprio server e l'azienda. L'uso di L2F richiede il supporto e la partecipazione dell'ISP. Poiché L2F non è basato sui client, i sistemi non hanno bisogno di software client o di configurazione, ma la comunicazione tra i computer degli utenti e l'ISP non è protetta. Come L2TP, anche L2F può usare protocolli di autenticazione come RADIUS e TACACS+, ma L2F non supporta la cifratura dei dati.

L2TP è stato introdotto per rimpiazzare PPTP e L2F. Quando configurato in modo appropriato, L2TP combinato con IPSec può fornire autenticazione forte e cifratura. PPTP non dovrebbe essere usato per proteggere le comunicazioni, a causa dei suoi punti deboli. Poiché L2F fornisce solo una protezione limitata a porzioni delle comunicazioni che coinvolgono un ISP partecipante, si dovrebbe usare L2TP al posto di L2F. L2TP con IPSec è un'opzione valida per fornire riservatezza e integrità alle comunicazioni dial-up (chiamata via modem), specialmente per organizzazioni che contrattano servizi VPN con un ISP.

Oltre a proteggere le connessioni dial-up, i protocolli VPN di strato data link sono usati anche negli ambienti ad alta sicurezza per proteggere particolari collegamenti fisici, come i circuiti dedicati tra due edifici. La VPN può essere creata collocando un gateway di cifratura e decifratura alle estremità del circuito, oppure aggiungendo servizi VPN a punti terminali come gli switch. Si parla di *Provisioner-provided VPN* (PPVPN) quando il service provider del collegamento offre la protezione VPN del collegamento stesso. In

5.7.10.4 Conoscere altri protocolli d'incapsulamento (PPTP, IP over UDP, etc.), e il relativo impiego

5.7.10.5 Essere in grado d'installare un client VPN

tal caso, la gestione e manutenzione della VPN sono a carico del provider, non dell'azienda utente. Il gruppo di lavoro Layer 2 Virtual Private Networks (L2VPN) dell'IETF sta sviluppando gli standard per le PPVPN di strato 2.

Protocolli VPN di strato 4 (trasporto)

I protocolli di strato 4 come TLS (*Transport Layer Security*) sono utilizzati principalmente per fornire comunicazioni sicure a singole applicazioni basate su HTTP, benché possano proteggere sessioni di comunicazione di altro tipo. Dato che tutti i principali browser supportano SSL e TLS, gli utenti non hanno bisogno d'installare un client software o di riconfigurare il sistema (salvo attivare TLS nel browser se non è attivo per default). Una differenza importante tra le protezioni TLS e IPsec è che IPsec autentica automaticamente ciascun punto terminale con l'altro, mentre l'autenticazione TLS è tipicamente monodirezionale, dal server (provvisto di certificato) al client (la maggior parte delle implementazioni non sfrutta l'opzione di autenticare anche il client dotandolo di certificato).

Uno sviluppo recente è l'uso dei reverse proxy server TLS (chiamati anche SSL proxy server, TLS VPN e SSL VPN) per offrire una soluzione VPN più robusta agli utenti remoti. L'utente remoto che ha bisogno di usare un'applicazione aziendale inserisce nel browser l'URL (*Uniform Resource Locator*) del proxy server, a cui si connette in modo HTTP protetto da TLS. L'utente viene autenticato dal proxy server, quindi può accedere all'applicazione desiderata, come specificato nei controlli d'accesso del proxy. L'utente non si collega all'applicazione direttamente; il suo sistema usa una connessione HTTP protetta da TLS con il proxy server, che a sua volta stabilisce un'altra connessione con il server applicativo che può essere protetta o meno, secondo necessità. Tale metodo può essere adattato anche ad applicazioni non Web, tramite appositi client software forniti dai produttori e da installare sulle macchine degli utenti.

In generale, il metodo del proxy server è adatto soprattutto per proteggere un numero significativo di applicazioni Web, altrimenti non offre vantaggi sostanziali rispetto alla protezione individuale delle applicazioni tramite TLS.

Protocolli VPN di strato applicativo

Ogni protocollo di strato applicativo è in grado di proteggere una singola applicazione; in molti casi, la protezione riguarda solo una parte dei dati applicativi. Per esempio, programmi di cifratura come PGP (*Pretty Good Privacy*) e GPG (*GnuPG*) possono essere usati in combinazione con un client di e-mail per cifrare il corpo di un messaggio di posta elettronica, ma non l'intestazione (che include le informazioni sugli indirizzi). Protocolli VPN applicativi possono anche essere incorporati nelle applicazioni per fornire la protezione dei dati senza richiedere applicazioni separate. Se il software in commercio o in distribuzione non comprende protezione allo strato applicativo, la protezione deve essere aggiunta attraverso un altro prodotto (allo strato applicativo, oppure a un altro strato), per esempio avvolgendo l'applicazione basata su HTTP con TLS o realizzando una VPN basata su IPsec.

Un protocollo di strato applicativo comunemente usato è *Secure Shell* (SSH), che contiene i sostituti sicuri di parecchi protocolli applicativi, tra cui telnet, rcp e FTP. Lo stesso programma SSH client, in sé, fornisce la protezione per il login remoto a un altro sistema. Alcune aziende estendono l'uso dell'applicazione SSH stabilendo tunnel SSH tra host, e quindi facendo passare altre comunicazioni attraverso i tunnel. Ciò permette di proteggere più applicazioni alla volta attraverso un singolo tunnel, il che, tecnicamente, fa di SSH un protocollo VPN di strato 4 (trasporto), anziché di strato applicativo. Tali strumenti sono utilizzati soprattutto dagli amministratori, a causa della competenza tecnica necessaria per installare e configurare il software SSH.

Configurazione di un client IPSEC

Descriviamo la configurazione di base per un computer portatile con Windows XP configurato come client IPsec in grado di collegarsi a un gateway IPsec. Forniamo anche alcune indicazioni applicabili a un gateway Linux, pur tralasciandone la configurazione.

La configurazione IPsec di Windows XP (se non si usa un client IPsec fornito da un produttore) richiede l'uso del protocollo L2TP (descritto nella sezione precedente), che permette d'incapsulare i frame di strato 2 (destinati a un server PPP, per essere estratti sulla rete locale) in pacchetti IP. Sul gateway Linux è necessario installare e configurare il *daemon pppd* e il *daemon l2tpd*, che è disponibile in molte distribuzioni (vedere anche www.jacco2.dds.nl per software e istruzioni).

Il *daemon l2tpd* deve essere configurato per essere accessibile solo dai tunnel IPsec. Alcune misure da prendere sono:

1. per L2TP/IPsec si devono abilitare alcune porte e protocolli: UDP 500 (IKE), protocollo IP 50 (ESP) e porta UDP 4500 (NAT-T, necessaria se i client sono dietro un router NAT);

2. bloccare il traffico destinato alla porta 1701 (L2TP) su tutte le interfacce, ad esempio tramite iptables;

3. mettere l2tpd in ascolto solo sull'indirizzo della rete interna (per proteggerlo da accessi esterni), per esempio 192.168.1.98, e ridirigendovi il traffico proveniente dal tunnel con un comando

```
iptables -t nat -append PREROUTING -i ipsec0 -p udp -sport 1701 -j DNAT --to-destination 192.168.1.98
```

dopo di che, occorre utilizzare una patch necessaria per legare (bind) l2tpd a un determinato indirizzo IP (quello della rete interna), scaricabile da www.jacco2.dds.nl/networking/tarballs/l2tpd-10jdl.tgz.

Il *daemon l2tpd* permette di portare al gateway qualsiasi pacchetto incapsulato nel protocollo L2TP, quindi se ne dovrà tenere conto nel configurare il firewall. E' opportuno verificare anche se la distribuzione di sistema operativo utilizzata presenta particolarità relative al supporto L2TP (si veda anche www.jacco2.dds.nl/networking/freeswan-l2tp.html).

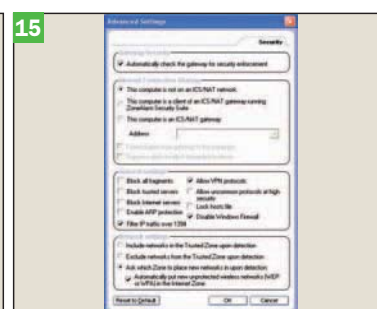
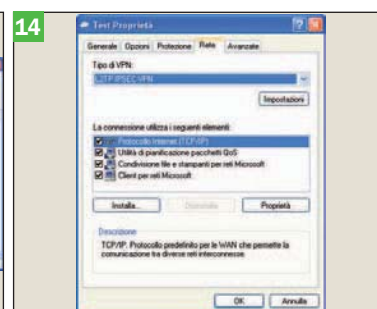
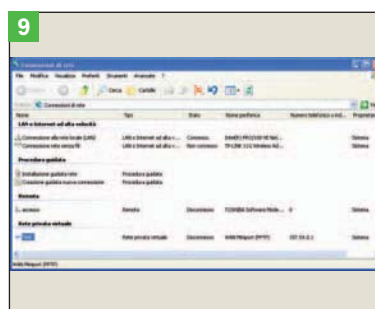
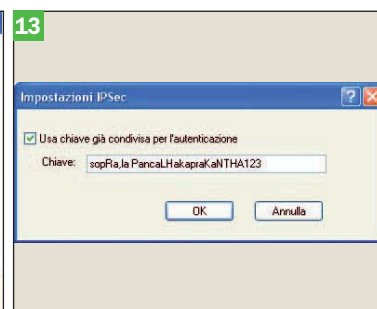
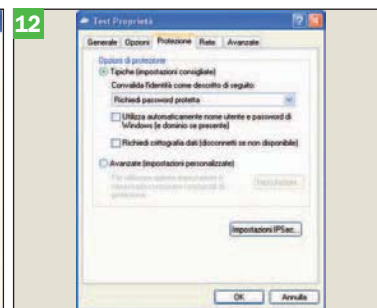
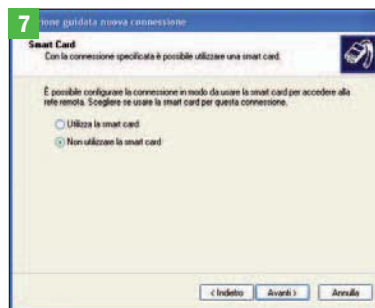
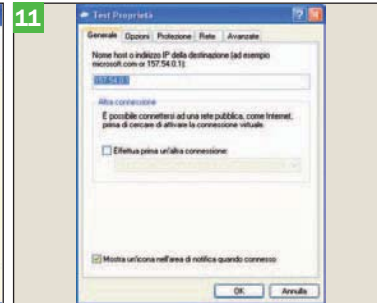
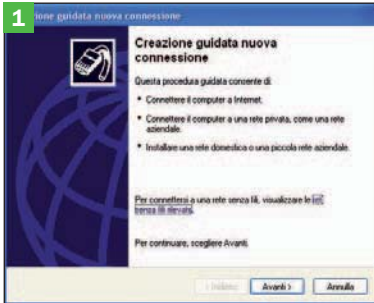
La configurazione del client Windows XP prevede i seguenti passi:

1. Attivare la procedura guidata per creare una nuova connessione di rete tramite *Start > Tutti i programmi > Accessori > Comunicazioni > Creazione guidata nuova connessione*
2. *Avanti*
3. *Connessione alla rete aziendale > Avanti*
4. *Connessione VPN > Avanti*
5. *Inserire un nome (ad esempio Test) > Avanti*
6. *Non effettuare alcuna connessione > Avanti*
7. *Inserire l'indirizzo IP pubblico del gateway VPN > Avanti*
8. *Non utilizzare la smart card > Avanti > Fine*
9. Ora nella finestra *Connessioni di rete* è presente la nuova connessione *Test* sotto *Rete privata virtuale*; fare doppio clic su *Test*.
10. Clic su *Proprietà*
11. Clic su *Protezione*
12. Rimuovere *Richiedi crittografia dati* (riguardante il traffico PPP), dato che se ne occupa IPsec
13. Clic su *Impostazioni IPsec*
14. Inserimento di una chiave condivisa (sebbene sia la configurazione più semplice e meno sicura, è semplice e adatta per il test della connessione; si usi comunque una chiave complessa) > *OK*
15. Selezionare il tab *Rete*
16. Selezionare *L2TP IPSEC VPN* come Tipo di VPN
17. Verificare la configurazione del protocollo TCP/IP

18. Nella sezione *Avanzate*, se necessario, è possibile modificare le opzioni del firewall di Windows XP per tale connessione. Se si usa un altro firewall software, si verifichi che lasci passare i protocolli VPN e, in caso contrario, si attivi tale funzione. Se si utilizza un server Linux, il nome utente e la pas-

sword devono essere inseriti nella configurazione CHAP, generalmente in `/etc/ppp/chap-secrets`.

Una volta collaudata la connessione tramite chiave condivisa, si potrà riconfigurare la protezione della connessione in modo da utilizzare un certificato digitale per l'autenticazione del client. ■



- 1 Avvio della procedura guidata di creazione della connessione VPN
- 2 Selezione del tipo di connessione
- 3 Selezione della modalità di connessione
- 4 Assegnazione del nome della connessione
- 5 Opzione di collegamento a Internet prima della connessione VPN
- 6 Inserimento dell'indirizzo IP pubblico del gateway VPN
- 7 Opzione di utilizzo di Smart Card
- 8 Completamento della procedura guidata
- 9 La connessione VPN è elencata in Connessioni di rete
- 10 Finestra di connessione e configurazione
- 11 Proprietà generali della connessione VPN
- 12 Impostazioni generali di protezione
- 13 Inserimento di una chiave condivisa
- 14 Proprietà IPSec della connessione
- 15 Esempio di abilitazione dei protocolli VPN in un personal firewall (ZoneAlarm)

GLOSSARIO

3DES (Triple DES)

tripla applicazione del DES. L'algoritmo alla base di 3DES è lo stesso di DES, l'algoritmo più studiato e collaudato di tutti i tempi. 3DES è molto robusto e affidabile, ma è stato progettato circa 30 anni fa ed è stato concepito per l'implementazione in hardware.

Accountability

Vedi rendicontabilità.

Accuratezza

tutte le funzioni intese a garantire l'accuratezza delle informazioni.

AES

pubblicato dal NIST nel 2001, è l'algoritmo richiesto per proteggere le informazioni riservate, ma non classificate, del governo statunitense. Nel 2003 il governo USA ha autorizzato l'uso di AES per la cifratura di documenti classificati fino al livello di secret con chiave di 128 bit, e di top secret con chiave di 192 o 256 bit. E' previsto che risulti sicuro per decenni a venire, ed è utilizzabile senza il pagamento di royalty.

Affidabilità del servizio

una vasta categoria di contromisure, perché sono diverse le aree che potrebbero compromettere l'affidabilità dei servizi informatici.

Agente

l'entità che mette in atto la minaccia viene chiamata agente. Esempi di agenti di minaccia sono un intruso che entra in rete attraverso una porta del firewall, un processo che accede ai dati violando le regole di sicurezza, un tornado che spazza via il centro di calcolo o un utente che, inavvertitamente, permette ad altri di vedere le password.

Algoritmo (o cifrario)

un insieme di regole logiche e matematiche usate nella cifratura e nella decifratura.

Analisi del rischio

si classificano le informazioni e le risorse soggette a minacce e vulnerabilità, e si identifica il livello di rischio associato a ogni minaccia.

Autenticità

garantisce che eventi, documenti e messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro.

Bene

un bene è qualsiasi cosa, materiale o immateriale, che abbia un valore e debba, quindi, essere protetta.

Blowfish

Blowfish è un cifrario simmetrico a blocchi di 64 bit con chiavi di lunghezza fino a 448 bit. Durante la cifratura, i dati sono sottoposti a 16 fasi di funzioni crittografiche. Blowfish è un algoritmo molto robusto ed è stato scritto da Bruce Schneier, uno degli autori più citati nel campo della crittografia.

BS 7799

Le linee guida BS 7799, oggi ISO/IEC 17799 e BS 7799-2, hanno una storia che risale agli inizi degli anni '90, quando il Department of Trade and Industry britannico istituì un gruppo di lavoro con l'intento di fornire alle aziende linee guida per la gestione della sicurezza delle informazioni. Nel 1993 questo gruppo pubblicò il *Code of practice for information security management*, un insieme di buone regole di comportamento per la sicurezza delle informazioni.

Business Continuity

(talvolta chiamata *business continuance*) descrive i processi e le procedure che un'organizzazione mette in atto per assicurare che le funzioni essenziali rimangano operative durante e dopo un disastro.

Busta elettronica

una busta elettronica (*digital envelope*) consiste di un messaggio che usa la cifratura simmetrica a chiave segreta e una chiave segreta cifrata in modo asimmetrico.

Qualunque messaggio formattato con CMS può essere incapsulato dentro un altro messaggio CMS, applicando ricorsivamente la busta elettronica. Ciò permette agli utenti di firmare una busta digitale, di cifrare una firma digitale o di eseguire varie altre funzioni.

CBC (Cipher Block Chaining)

uno dei principali cifrari a blocchi. Utilizza il blocco di testo cifrato precedente e lo combina in XOR (*OR esclusivo*, un'operazione tra due bit che produce come risultato 1 se i bit sono diversi, o 0 se sono uguali) con il blocco successivo di testo in chiaro prima della cifratura. Il primo blocco è combinato in XOR con un Vettore di Inizializzazione (IV, *Initialization Vector*), scelto con forti proprietà di pseudocasualità in modo che testi diversi producano lo stesso testo cifrato. La decifratura funziona nel modo opposto: ogni blocco è decifrato e combinato in XOR con il blocco precedente. Il primo blocco è decifrato e combinato in XOR con il vettore d'inizializzazione.

CEN (Comitato Europeo di Normalizzazione, www.cenorm.org)

un organismo europeo composto dagli enti di standardizzazione dei paesi membri dell'Unione Europea e dell'EFTA (European Fair Trade Association - tra cui l'UNI per l'Italia).

CERT (Computer Emergency Response Team)

(squadra di intervento per le emergenze informatiche) ha la missione di operare con la comunità di Internet per facilitare la risposta agli eventi riguardanti la sicurezza degli host (i computer collegati a Internet), prendere iniziative per sensibilizzare la comunità sugli aspetti della sicurezza, e condurre ricerche rivolte a incrementare la sicurezza dei sistemi esistenti.

CERT-CC

il primo CERT (www.cert.org) è diventato il CERT Coordination Center (CERT-CC), ed è situato presso il Software Engineering Institute, finanziato dal governo USA e gestito dalla Carnegie Mellon University di Pittsburgh. Si focalizza sulle violazioni alla sicurezza, allerta sulle nuove minacce, reagisce agli attacchi (i cosiddetti *incidents*) e fornisce assistenza, informazioni sulla vulnerabilità dei prodotti e istruzione con documenti e tutorial.

Certification Authority (CA)

la CA garantisce le chiavi pubbliche delle entità del proprio dominio mediante l'emissione dei "certificati digitali" in formato standard, contenenti: 1) una serie d'informazioni, tra cui il nome del titolare del certificato, la sua chiave pubblica, il periodo di validità del certificato e altre informazioni che concorrono a identificare il titolare e l'autorità che emette il certificato; 2) la firma digitale, apposta alle suddette informazioni utilizzando la chiave privata della CA.

Chiave

la sequenza segreta di bit che governa l'atto della cifratura o della decifratura.

Chiave privata

una delle due chiavi usate nella crittografia asimmetrica. E' segreta e viene mantenuta in possesso del solo proprietario.

Chiave pubblica

una delle due chiavi usate nella crittografia asimmetrica. E' pubblicamente disponibile a chiunque voglia comunicare con il suo proprietario.

Chiave segreta

la chiave usata nella crittografia simmetrica e comune sia al mittente, sia al destinatario. Deve essere mantenuta segreta perché la sua conoscenza consente di decifrare qualsiasi messaggio cifrato alla fonte.

Cifrare o cifratura

l'azione di trasformare i dati in formato illeggibile.

Cifrario a blocchi

opera sui dati un blocco alla volta (le dimensioni tipiche dei blocchi sono di 64 o 128 bit), e ogni operazione su un

blocco è un'azione elementare.

Cifrario a flusso

opera invece un bit o un byte alla volta; una volta inizializzati con una chiave, producono un flusso di bit e si prestano alla cifratura di grandi quantità di dati.

CMS (Cryptographic Message Syntax)

il formato con cui sono codificati i messaggi creati con la cifratura asimmetrica è definito dallo standard PKCS #7 *Cryptographic Message Syntax* (CMS). Altre proprietà del formato CMS: 1) gestisce la firma congiunta di più firmatari, 2) gestisce la firma per un numero arbitrario di destinatari, 3) consente di aggiungere attributi firmati al messaggio, come la data e l'ora della firma, 4) consente di allegare al messaggio i certificati dei firmatari, agevolando la verifica della firma, 5) include gli identificatori degli algoritmi crittografici utilizzati e gli elementi che facilitano la decifratura e la verifica della firma.

Common Criteria

criteri standard di valutazione di applicabilità globale che allinea i criteri di valutazione esistenti ed emergenti: TCSEC, ITSEC, il canadese CTCPEC (*Canadian Trusted Computer Product Evaluation Criteria*) e i criteri federali USA. Il progetto è stato sviluppato attraverso la collaborazione degli enti nazionali di standardizzazione di Stati Uniti, Canada, Francia, Germania, Regno Unito e Olanda. I benefici di questo sforzo comune comprendono la riduzione della complessità del sistema di valutazione, la disponibilità di un unico linguaggio per le definizioni e per i livelli di sicurezza e, a beneficio dei produttori, l'uso di un unico insieme di requisiti per vendere i prodotti sul mercato internazionale.

Controllo degli accessi

le funzioni di sicurezza che verificano se il processo o l'utente, di cui è stata autenticata l'identità, ha il diritto di accedere alla risorsa richiesta.

Controllo del rischio

vengono individuate le modalità che l'azienda intende adottare per ridurre i rischi associati alla perdita della disponibilità di informazioni e risorse informatiche, e della integrità e riservatezza di dati e informazioni.

Contromisure

le contromisure di sicurezza sono le realizzazioni e le azioni volte ad annullare o limitare le vulnerabilità, e a contrastare le minacce.

Contromisure di carattere fisico

Queste contromisure sono generalmente legate alla prevenzione e al controllo dell'accesso a installazioni, locali, attrezzature, mezzi di comunicazione.

Contromisure di tipo procedurale

definiscono passo per passo le operazioni per eseguire un certo compito, oppure regolano il comportamento degli utenti per gli aspetti che riguardano la sicurezza delle informazioni e delle risorse.

Contromisure di tipo tecnico informatico

sono le contromisure realizzate attraverso mezzi hardware, firmware e software, e prendono anche il nome di funzioni di sicurezza.

Correttezza

è un attributo intrinseco di un prodotto (o componente o procedura) che riflette il grado di corrispondenza tra le effettive funzioni svolte dal prodotto e le sue specifiche.

Criteri di valutazione della garanzia

sono i metodi con cui viene valutata la fiducia, che può essere accordata ai sistemi e ai prodotti informatici di sicurezza.

Tra le pubblicazioni disponibili, le tre più significative sono i criteri americani TCSEC (*Trusted Computing Security Evaluation Criteria*, 1985), i criteri europei ITSEC (*Information Security Evaluation Criteria*, 1991) e i criteri internazionali ISO/IEC 15408, noti come *Common Criteria* e pubblicati nel 1999.

Crittoanalisi

la pratica di ottenere il messaggio in chiaro dal messaggio cifrato senza disporre della chiave, o senza scoprire il sistema di cifratura.

Crittografia

la scienza della scrittura nascosta (o segreta) che permette di memorizzare e trasmettere dati in una forma utilizzabile solo dagli individui a cui essi sono destinati.

Crittografia a curve ellittiche (ECC)

tecnologia di cifratura asimmetrica con chiavi molto più corte rispetto a RSA. Una chiave ECC di 163 bit equivale a una chiave RSA di 1024 bit. Le curve ellittiche sono una branca della teoria dei numeri e sono definite da certe equazioni cubiche (di terzo grado); le loro proprietà permettono di creare algoritmi crittografici asimmetrici, vista l'estrema difficoltà di eseguire i calcoli a ritroso per ricostruire la chiave privata dalla chiave pubblica e dalle condizioni iniziali.

Crittografia asimmetrica

la chiave di cifratura è diversa da quella di decifratura. Detta anche crittografia a chiave pubblica.

Crittografia simmetrica

la chiave di cifratura è la stessa usata per la decifratura, o possono essere derivate facilmente una dall'altra. Detta anche crittografia a chiave segreta.

Crittologia

lo studio della crittografia e della crittoanalisi.

Crittosistema

l'implementazione hardware o software della crittografia, che trasforma un messaggio in chiaro (*plaintext*) in un messaggio cifrato (*ciphertext*) e poi, di nuovo, nel messaggio in chiaro originario.

CSIRT (Computer Security Incident Response Team)

squadre di intervento per gli incidenti di sicurezza informatica coordinate dal CERT-Coordination Center.

Custode dei dati

ha la responsabilità della manutenzione e della protezione dei dati.

Decifrare o decifratura

l'azione di trasformare i dati in formato leggibile.

DES (Data Encryption Standard)

è l'algoritmo di cifratura più conosciuto, ed è stato il primo di cui sono stati forniti tutti i dettagli di implementazione. È stato incluso nella maggioranza dei prodotti commerciali dotati di funzionalità crittografiche, ed è stato usato dagli enti governativi. Per oltre un decennio DES è stato considerato uno degli algoritmi più efficaci ed efficienti, finché la NSA smise di supportarlo nel 1988, prevedendo la sua vulnerabilità a fronte della crescita della potenza di calcolo dei computer.

Diffie-Hellmann

algoritmo di crittografia asimmetrica, è utilizzato per lo scambio delle chiavi, dove i due interlocutori si scambiano le chiavi pubbliche e, con le proprie chiavi private, costruiscono una chiave segreta condivisa.

Digest

vedi hash.

Disaster Recovery

nel contesto informatico, è la capacità di un'infrastruttura di riprendere le operazioni dopo un disastro.

Disponibilità

è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono.

DMZ (Demilitarized Zone)

il termine, di origine militare, indica un'area tampone tra una zona fidata e una non fidata all'interno della quale non sono consentite le armi. Applicata al networking, una DMZ è una sottorete alla quale sono connessi sistemi accessibili da reti con diversi livelli di fiducia e criticità.

DSA (Digital Signature Algorithm)

una variante dell'algoritmo di cifratura asimmetrica ElGamal è il DSA, o *Digital Signature Algorithm*, sviluppato

dalla NSA e pubblicato dal NIST (National Institute of Standards and Technology), e diventato uno standard del governo USA.

DSS (Digital Signature Standard)

Lo standard federale americano per la firma elettronica di cui DSA è l'algoritmo di firma, e SHA è l'algoritmo di hash.

Dynamic packet filtering

Vedi Stateful inspection.

ECB (Electronic Code Book)

uno dei principali cifrari a blocchi. Ogni blocco di testo in chiaro viene trasformato in un blocco di testo cifrato. Lo stesso blocco di testo, con la stessa chiave, produce sempre lo stesso blocco di testo cifrato, il che consente ai malintenzionati di compilare un codice (*code book*) di tutti i possibili testi cifrati corrispondenti a un dato testo in chiaro.

ECDSA

una variante più efficiente del DSA basata sulle curve ellittiche.

Efficacia

una proprietà che mette in relazione la contromisura (prodotto, procedura o altro) con il contesto in cui è utilizzata, in particolare le vulnerabilità, la gravità e la probabilità di attuazione delle minacce.

ElGamal

algoritmo di cifratura asimmetrica. Può essere usato sia per la cifratura, sia per l'autenticazione con firma digitale. È un algoritmo sicuro, e ha la caratteristica di generare un testo cifrato lungo il doppio del testo in chiaro.

ETSI (European Telecommunications Standards Institute)

un'organizzazione europea indipendente, riconosciuta dalla Commissione Europea e dall'EFTA. Ha sede a Sophia Antipolis (Francia), ed è responsabile per la standardizzazione delle tecnologie informatiche e di comunicazioni (ICT) in Europa.

Firma digitale

una firma dev'essere difficile da falsificare, non ripudiabile (non può essere cancellata o disconosciuta), inalterabile (dopo l'apposizione della firma, non deve essere possibile modificare il documento) e non trasferibile (da un documento a un altro). La firma digitale si basa sulla cifratura asimmetrica di un hash, o digest, calcolato sul contenuto del documento o messaggio.

FIRST (Forum for Incident Response and Security Teams)

I CERT o CSIRT delle varie nazioni sono collegati in una struttura internazionale, il FIRST, che permette la rapida condivisione delle informazioni utili a fronteggiare minacce e attacchi.

FTP bounce

un attacco (rimbalzo FTP) che sfrutta una vulnerabilità del protocollo FTP per cui un attaccante è in grado di usare il comando *PORT* per chiedere accesso alle porte indirettamente, attraverso l'uso del server FTP come intermediario nella richiesta.

Funzionalità

applicato alla sicurezza, conserva il significato generale che ha in altri settori; è l'insieme di ciò che un prodotto o un sistema informatico fornisce in relazione alla protezione delle informazioni e, di riflesso, delle risorse e dei servizi informatici.

Funzioni di sicurezza

Vedi contromisure di tipo tecnico informatico.

Garanzia

concetto introdotto da chi si occupa di sicurezza per esprimere il grado in cui l'implementazione di una funzionalità riduce una vulnerabilità o la possibilità di attuazione di una minaccia.

Gestione del rischio

nella gestione del rischio si possono individuare due fasi distinte. 1) Analisi del rischio. 2) Controllo del rischio.

Hash

un numero binario di lunghezza fissa, ricavato da un input

(file, messaggio, blocco di dati, ecc.), di lunghezza variabile, che funge da "impronta" del dato di partenza.

HMAC

Un tipo speciale di MAC specificato nella RFC 2104. HMAC è anch'essa una funzione *keyed hash*, ma in realtà costituisce un *keyed hash* all'interno di un *keyed hash*.

IAB (Internet Architecture Board)

un gruppo tecnico consultivo della Internet Society, responsabile della selezione dello IESG, della supervisione dell'architettura, della supervisione del processo di standardizzazione e della procedura di appello, della serie delle RFC (*Request For Comment*), dei collegamenti esterni e di consiglio all'ISOC.

IANA (Internet Assigned Numbers Authority)

mantiene le funzioni di coordinamento centrale dell'Internet globale nel pubblico interesse. La IANA custodisce i numerosi parametri e valori di protocollo unici necessari per il funzionamento di Internet e per il suo sviluppo futuro.

ICANN (Internet Corporation for Assigned Names and Numbers)

azienda non-profit che fu creata per assumere la responsabilità dell'attribuzione degli spazi d'indirizzamento IP, dell'assegnazione dei parametri dei protocolli, della gestione del sistema dei domini e della gestione del sistema dei server root, funzioni che in precedenza erano eseguite, sotto contratto con il governo USA, dalla IANA e da altre entità. È l'autorità per l'assegnazione dei nomi di dominio a livello globale.

IDEA

IDEA è un cifrario simmetrico a blocchi di 64 bit, suddivisi in 16 sotto-blocchi sottoposti a otto serie di manipolazioni matematiche. IDEA presenta similitudini con DES, ma è molto più robusto. La chiave è lunga 128 bit. IDEA è brevettato ed è concesso in licenza dalla società svizzera Mediacrypt.

Identificazione e autenticazione

Le funzioni di questa categoria servono a identificare un individuo o un processo, e ad autenticarne l'identità.

IESG (Internet Engineering Task Group)

è responsabile della gestione tecnica delle attività dell'IETF e del processo di standardizzazione di Internet. Come parte dell'ISOC, amministra tale processo secondo le regole e le procedure che sono state ratificate dai fiduciari dell'ISOC. Lo IESG è direttamente responsabile delle azioni associate all'avvio e alla prosecuzione dell'iter di standardizzazione, inclusa l'approvazione finale delle specifiche come Standard Internet. Lo IESG coordina e approva gli standard tecnici.

IETF (Internet Engineering Task Force)

una vasta comunità internazionale di progettisti, operatori, produttori e ricercatori nel campo del networking, interessati all'evoluzione dell'architettura di Internet e all'affidabilità del suo funzionamento.

Impatto

è la conseguenza dell'attuazione di una minaccia.

Integrità

è la fedele conservazione del contenuto originario di un documento archiviato o trasmesso in rete, attestata da strumenti che segnalano se il documento ha subito alterazioni.

Internet Society - ISOC

un'organizzazione privata senza fini di lucro che riunisce professionisti nel mondo del networking, e che ha la missione di garantire il continuo funzionamento di Internet e il suo potenziamento.

IRTF (Internet Research Task Force)

ha la missione di promuovere attività di ricerca che possano contribuire in modo significativo al futuro sviluppo di Internet. Opera creando gruppi di ricerca focalizzati sui seguenti temi: protocolli, applicazioni, architettura e tecnologia.

ISO (International Organization for Standardization)

la maggiore organizzazione internazionale di standardizzazione e comprende gli enti di standardizzazione nazionali di 146 paesi (l'UNI è il membro italiano).

ISO/IEC 17799

una serie di linee guida e di raccomandazioni compilata a seguito di consultazioni con le grandi aziende. I 36 obiettivi e le 127 verifiche di sicurezza contenuti nel documento sono suddivisi in 10 aree, o domini, riportati nel riquadro A, I dieci domini formano una piramide che scende dalla prospettiva organizzativa (1, 2, 3, 4, 9, 10) verso quella operativa (6, 7, 8), con inclusi gli aspetti tecnici (5).

ITSEC (Information Security Evaluation Criteria)

il primo tentativo di stabilire un unico standard di valutazione degli attributi di sicurezza da parte di molti paesi europei.

ITU (International Telecommunication Union)

un'organizzazione internazionale, nell'ambito dell'ONU, dove governi e settore privato coordinano le reti e i servizi globali di telecomunicazioni. Ha sede a Ginevra e comprende i settori ITU-T (standardizzazione), ITU-R (radiocomunicazioni) e ITU-D (sviluppo).

Keyed hashing

Far dipendere l'hash del messaggio da una chiave segreta. Il keyed hashing viene usato nella crittografia simmetrica per produrre i codici MAC utilizzati per autenticare i messaggi e garantirne l'integrità.

Keyspace

(spazio delle chiavi) l'insieme di tutti i possibili valori che una chiave può assumere.

MAC (Message Authentication Code)

un hash calcolato su un messaggio con l'aggiunta di una chiave segreta condivisa, usato per verificare all'altro capo della comunicazione l'integrità del messaggio.

man-in-the-middle

tipo di attacco dove il nemico finge rispettivamente di essere l'altro interlocutore nei confronti di due sistemi tra i quali si è interposto. Intercetta il traffico dell'uno prima di ritrasmetterlo all'altro e viceversa, fingendo ogni volta di essere il mittente e il destinatario corretto per ciascuna comunicazione.

MD5

algoritmo di hash evoluzione di MD4, è stato sviluppato da Ron Rivest all'MIT nel 1991 ed è descritto nella RFC 1321 (www.ietf.org/rfc). MD5 è molto popolare, ma la crescita della potenza di calcolo e i primi successi degli attacchi sia basati su forza bruta, sia di tipo crittoanalitico (basati sull'analisi dell'algoritmo) inducono a considerare MD5 vulnerabile.

MIME (Multipurpose Internet Mail Extensions)

è lo standard che specifica come devono essere trasferiti i dati multimediali e gli allegati di e-mail.

Minaccia

è un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza.

Non ripudio

impedisce che un evento o documento possa essere sconosciuto dal suo autore.

Norme e linee guida

segnaliamo le linee guida ISO/IEC 13335 e le norme BS (British Standard) 7799.

Norme funzionali

sono relative ai prodotti e hanno lo scopo principale di ricercare l'interoperabilità dei prodotti informatici. Coprono argomenti quali i protocolli di comunicazione, il formato dei dati (per esempio in un certificato digitale o in una smartcard), e così via.

Obiettivi

gli obiettivi di sicurezza sono il grado di protezione che si intende predisporre per i beni, in termini di disponibilità, integrità e riservatezza.

one-way hash function

produce una trasformazione a senso unico, dove a N possibili input corrisponde un output, da cui non è possibile risalire all'input. L'*hashing one-way* viene usato nella crittografia asimmetrica per produrre le firme digitali (ad esempio con gli algoritmi RSA o DSA), anche in questo caso per assicurare l'autenticità e l'integrità dei dati trasmessi o archiviati.

Packet filter

il tipo più semplice di firewall che consiste di un router che include una funzione di controllo d'accesso per i singoli pacchetti governata da una serie di regole (*ruleset*) eseguite in sequenza.

PGP (Pretty Good Privacy)

un programma di sicurezza per la posta elettronica realizzato da Phil Zimmermann e pubblicato inizialmente nel 1991 come freeware. Le funzioni di PGP sono: firma digitale, cifratura dei messaggi, compressione, conversione in ASCII (in base 64) e segmentazione dei messaggi; di queste, le prime due rientrano nel contesto delle applicazioni crittografiche.

PKCS (Public Key Cryptographic Standard)

comprende un'intera serie di standard che hanno l'obiettivo di agevolare l'implementazione delle tecnologie PKI (per esempio, *PKCS #1* descrive lo standard di cifratura RSA). *PKCS #7* specifica i formati binari usati per la firma digitale e per la "busta elettronica". Lo standard *PKCS #7* è stato adottato dall'IETF nella RFC 2315, aggiornata dalla RFC 2630.

Politica di sicurezza

è un documento sintetico in cui il management superiore, o un comitato delegato allo scopo, delinea il ruolo della sicurezza nell'organizzazione o in un suo aspetto particolare.

Privacy

consiste nella salvaguardia dei dati privati degli utenti, anche in conformità alla legge 196/2003 sulla protezione dei dati personali.

Proprietario dei dati

un membro del management superiore, il massimo responsabile della protezione delle informazioni e della sicurezza in generale.

Proxy

(procuratore) un server che si frappone fra un'applicazione client (come un browser) e un reale server (come un Web server). Al server, il proxy appare come se fosse il client, mentre al client esso appare come se fosse il vero server.

Proxy firewall

un firewall basato su proxy (detto anche *application gateway*, *proxy gateway* e *proxy server*) che richiede un'applicazione specifica per ogni protocollo. Vengono usate applicazioni che accettano connessioni dai client, esaminano il traffico e aprono corrispondenti connessioni verso i server.

RC4

RC4 è il più noto dei cifrari a flusso. E' stato creato nel 1987 da Ron Rivest per RSA Security. Utilizza un keystream di dimensioni variabili (ma solitamente di 128 bit), e opera su un byte alla volta. In origine il cifrario era segreto, ma fu fatto filtrare su Internet. L'algoritmo è molto robusto se utilizzato con chiavi di lunghezza adeguata (tipicamente 128 bit), casuali e non riutilizzate.

RC5

RC5 è un cifrario simmetrico a blocchi dotato di parecchi parametri per assegnare le dimensioni del blocco, la lunghezza della chiave e il numero di passaggi di trasformazione da eseguire. E' stato creato da Ron Rivest (la R di RSA). Di solito si utilizzano blocchi di 32, 64 o 128 bit, e la chiave può raggiungere i 2.048 bit. RC5 è stato brevettato da RSA Security nel 1997. Il basso consumo di memoria lo rendono adatto per smartcard e altri dispositivi simili.

Recovery Point Objective (RPO)

il momento nel tempo a cui il sistema è riportato.

Recovery Time Objective (RTO)

il lasso di tempo che intercorre prima di ripristinare l'infrastruttura.

Rendicontabilità (accountability)

le funzioni che permettono di attribuire la responsabilità degli eventi agli individui che li hanno causati.

Reverse proxy

indica un proxy utilizzato per la protezione di un server, tipicamente un Web server (HTTP/HTTPS) su Internet. Gli usi più comuni dei reverse proxy riguardano il bilanciamento del carico e la continuità del servizio, che costituiscono anche un aspetto di disponibilità.

RIPEMD-160

algoritmo di hash sviluppato nell'ambito del progetto European RACE Integrity Primitives Evaluation (RIPE) da un gruppo di ricercatori che avevano conseguito parziali successi nell'attaccare MD4 e MD5.

Rischio

Concettualmente, il rischio è la possibilità che si verifichi un evento dannoso ed è tanto maggiore quanto è forte l'impatto causato dall'evento, e quanto è alta la probabilità che esso si verifichi.

Riservatezza

consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate, e si applica sia all'archiviazione, sia alla comunicazione delle informazioni.

Riutilizzo degli oggetti

le funzioni che permettono di riutilizzare oggetti contenenti informazioni riservate: supporti magnetici, supporti ottici riscrivibili, aree di memoria RAM, zone di memoria dei processori (registri, cache, ecc.), buffer di periferiche e simili.

RSA

dell'omonima azienda, è il cifrario asimmetrico più utilizzato. Può essere usato sia per la cifratura (per ottenere la riservatezza), sia per la firma digitale (per ottenere l'autenticazione), sia per lo scambio delle chiavi (come nell'esempio di cui sopra).

S/MIME (Secure/Multipurpose Internet Mail Extensions)

è un protocollo che aggiunge la cifratura e la firma elettronica ai messaggi MIME descritti nella RFC 1521 (Mechanisms for Specifying and Describing the Format of Internet Message Bodies).

Scambio dati sicuro

le funzioni destinate a garantire la sicurezza delle trasmissioni. Il modello *OSI Security Architecture* (ISO 7498-2) le classifica nelle seguenti sottoclassi: autenticazione, controllo dell'accesso, riservatezza, integrità (dell'hardware, dei dati e dei flussi di pacchetti trasmessi sia in modo *connectionless*, come UDP, sia *connection-oriented*, come TCP, anche ai fini della corretta sequenza dei pacchetti) e non ripudio.

Screened subnet

a differenza di una DMZ, che è una piccola sottorete collocata tra il router Internet e l'interfaccia esterna del firewall, una *screened subnet* è una rete isolata accessibile solo attraverso una delle interfacce del firewall, e non connessa direttamente alla rete interna.

Secure Shell (SSH)

un protocollo per realizzare un collegamento remoto sicuro da un computer a un altro attraverso una rete insicura. Supporta il login remoto sicuro, il trasferimento sicuro di file e l'inoltro sicuro del traffico di tipo TCP/IP e X Window. SSH è in grado di autenticare, cifrare e comprimere i dati trasmessi.

Secure Sockets Layer (SSL)

è un protocollo per la protezione di un canale di comunicazione attraverso una rete e funziona allo strato di trasporto, tra i protocolli di trasporto e di applicazione.

Come altri protocolli di sicurezza di rete, SSL utilizza la crittografia simmetrica e asimmetrica e le funzioni di hash per fornire l'autenticazione del server (e in opzione anche del client), la cifratura dei messaggi e l'integrità dei dati.

SHA (Secure Hash Algorithm)

uno standard FIPS (*Federal Information Processing Standard*) statunitense. SHA genera un digest di 160 bit che viene passato a DSA o a un altro degli algoritmi di firma digitale ammessi dal governo USA (RSA ed ECDSA, *Elliptic Curve Digital Signature Algorithm*).

SHA-1

è stato sviluppato dal NIST, ed è stato pubblicato come standard federale USA nel 1993 con il nome di *Secure Hash Algorithm* (SHA, FIPS 180), e riveduto nel 1995 come SHA-1 (FIPS180-1). SHA-1 riceve in input un messaggio di lunghezza massima inferiore a 264 bit (una dimensione equivalente a 2.147 Gbyte e, perciò, praticamente illimitata), suddiviso in blocchi di 512 bit, e produce un hash di 160 bit.

Sicurezza attiva

le misure di sicurezza che proteggono le informazioni in modo proattivo, in modo cioè da anticipare e neutralizzare i problemi futuri. Questo viene ottenuto non solo impedendo agli estranei di accedere alle informazioni (sicurezza passiva o difensiva), ma rendendo le informazioni intrinsecamente sicure a livello applicativo, proteggendone la riservatezza (*confidentiality*, chiamata anche confidenzialità), l'integrità e l'autenticità.

Sicurezza passiva

un approccio fondamentalmente difensivo o passivo, che valuta quali rischi accettare, quali delegare a terzi e quali controllare, riducendoli o azzerandoli.

Skipjack

Skipjack è un cifrario a blocchi sviluppato dalla NSA nel 1987, messo in servizio nel 1993 e declassificato nel 1998.

Social engineering

è la pratica di manipolare ad arte le persone per indurle a compiere azioni (come l'esecuzione di software maligno), oppure a rivelare informazioni (come le password) utili a ottenere accesso a dati e risorse.

Stateful inspection

tutti i filtri di pacchetti che implementano qualche forma di *stateful inspection* mantengono in memoria lo stato di tutte le comunicazioni che attraversano il firewall e determinano se bloccare i singoli pacchetti in base a interi flussi di comunicazione, non semplicemente sulla base dei singoli pacchetti. Perciò, i firewall del tipo *stateful inspection* (o *stateful packet inspection*, SPI) permettono o bloccano il passaggio di un pacchetto non solo in base a indirizzi IP e porte, ma anche utilizzando SYN, ACK, numeri di sequenza e altri dati contenuti nell'header TCP (strato 4).

Static packet filtering

Vedi Packet filtering

TCSEC (Trusted Computing Security Evaluation Criteria)

un sistema per valutare la funzionalità e garanzia di un prodotto, usato soprattutto negli USA e descritto nel cosiddetto Orange Book, un volume dalla copertina arancione. Serve per valutare sistemi operativi, applicazioni e prodotti di vario genere.

Testo cifrato (ciphertext)

dati in forma cifrata o illeggibile.

Testo in chiaro (plaintext o cleartext)

dati in forma leggibile o intelligibile.

Time Stamp Authority (TSA)

una terza parte fidata che attesta il tempo di produzione o d'invio di un documento tramite una "marca temporale", che è di fatto una controfirma del documento contenente un hash del documento, il riferimento temporale e altre informazioni.

TLS (Transport Layer Security)

un protocollo definito dall'IETF nella RFC 2246, simile a

SSL, ma con differenze soprattutto negli algoritmi crittografici utilizzati.

UNINFO

una libera associazione a carattere tecnico, con lo scopo di promuovere e di partecipare allo sviluppo della normativa nel settore delle tecniche informatiche. L'UNINFO è associato all'UNI, l'ente nazionale italiano di unificazione (www.uni.com/it) e rappresenta l'Italia presso CEN e ISO.

Verifica (audit)

le funzioni che registrano gli eventi in un file di logging, con informazioni riguardo a errori e a violazioni di sicurezza.

Vulnerabilità

una vulnerabilità è un punto debole del sistema informatico (hardware, software e procedure) che, se colpito o sfruttato da una minaccia, porta alla violazione di qualche obiettivo di sicurezza.

Work factor (fattore di lavoro)

il tempo, lo sforzo e le risorse che si stimano necessari per violare un crittosistema.