Tecnologie di **security** e tecniche di attacco

Una breve rassegna delle principali tecnologie di security sviluppate con uno sguardo alle più comuni tecniche di "attacco" oggi diffuse attraverso internet.

Quando si tratta di sicurezza, si pensa spesso alla crittografia. Crittografia significa letteralmente "scrittura segreta", ma nel linguaggio informatico indica il processo che permette l'identificazione e l'autenticazione degli utenti e assicura la riservatezza delle comunicazioni salvaguardando l'integrità dei dati. Gli argomenti relativi alla crittografia includono lo studio dei crittosistemi, degli algoritmi di cifratura e decifratura, le tecniche di autenticazione, gli schemi di firma, i certificati digitali, la distribuzione delle chiavi crittografiche. Sono argomenti tecnici, resi complessi dal profondo utilizzo degli strumenti propri del calcolo numerico, in particolare dell'aritmetica modulare. I termini e concetti relativi alla sicurezza elettronica più ricorrenti nelle descrizioni dei prodotti commerciali sono di seguito illustrati.

Encryption e Decryption

Cifratura e decifratura, sono le operazioni con cui i messaggi scambiati sono modificati per essere resi incomprensibili e successivamente riportati allo stato originario.

Chiave crittografica

Informazione pubblica o privata utilizzata per la cifratura e decifratura dei messaggi. Si tratta di un'informazione che può avere diversa natura (un numero, una lettera, una sequenza di bit…) a seconda del sistema in cui è utilizzata.

Crittosistema a chiave segreta (privata)

Scenario in cui due interlocutori utilizzano una "chiave" per rendere incomprensibile la comunicazione a estranei che non sono a conoscenza di tale segreto. Esempio classico è il cifrario di Giulio Cesare, i cui messaggi utilizzavano un alfabeto composto dalle stesse lettere e nello stesso ordine di un alfabeto normale, ma spostate di posizione. Per comprendere i messaggi così cifrati bisognava conoscere il numero di posizioni di cui erano state spostate le lettere. Le variazioni sul tema sono numerose, con l'aggiunta di inversioni d'ordine, spostamenti di blocchi di lettere e così via.

Crittosistema a chiave pubblica asimmetrica

Scenario in cui il mittente cifra il messaggio con una chiave pubblicata su una directory visibile a tutti e il ricevente li decifra utilizzando una chiave nota solo a lui.

Integrità dei dati

Indica che i dati trasmessi non sono stati modificati da terze persone.

Identificazione

Procedura volta a verificare la corrispondenza tra identità reale e identità digitale.

Autenticazione

Tecniche per verificare l'identità (digitale) degli interlocutori

Firma digitale

Tecniche per autenticare le parti coinvolte in una comunicazione

VPN le reti inaccessibili

Virtual Private Network significa rete privata virtuale, cioè una rete non accessibile a tutti e dove non tutte le macchine sono direttamente connesse tra di loro. Si tratta di reti geografiche che in alcuni tratti utilizzano mezzi trasmissivi non privati (tipicamente Internet) per la connessione di spezzoni di reti locali, al limite costituiti da un unico terminale. L'esempio più semplice di VPN è costituito da una normale rete aziendale collegata a Internet tramite un router a cui si collega remotamente il computer portatile di un dipendente in trasferta. Uno scenario più complesso è quello delle VPN che connettono due LAN di due sedi di un'azienda.
Il servizio VPN permette quindi di utilizzare una linea di comunicazione insicura per il collegamento di due entità remote, ricreando virtualmente un'unica rete. Grazie alla VPN è possibile risparmiare sugli elevatissimi costi di affitto di una linea dedicata o sui costi di telefonate per connessioni dial-up di computer portatili. La cifratura delle informazioni viene affidata ai terminali della comunicazione (router), che attraverso algoritmi e protocolli creano sulla rete pubblica un "tunnel" sicuro entro il quale gli interlocutori possono trasmettere i propri dati.
Tipicamente, nelle VPN la codifica delel informazioni è fatta utilizzando l'IP Layer Security Protocol (IPSEC). Questa sigla raggruppa una serie di protocolli standard aventi il fine di garantire la trasmissione sicura di pacchetti di dati tramite Internet. In particolare, lo standard Authentication Header (AH) fornisce servizi di integrità e autenticazione per i pacchetti IP, mentre lo standard Encapsulated Security Payload (ESP) fornisce riservatezza, integrità e autenticazione dei dati.
In genere, Le VPN sono affiancate da PKI (public Key Infrastructure). Usare solo un apassword come metodo di autenticazione a una VPN è infatti troppo rischioso, in quanto le sole password sono considerate assolutamente inadeguate per la protezione di informazioni sensibili.

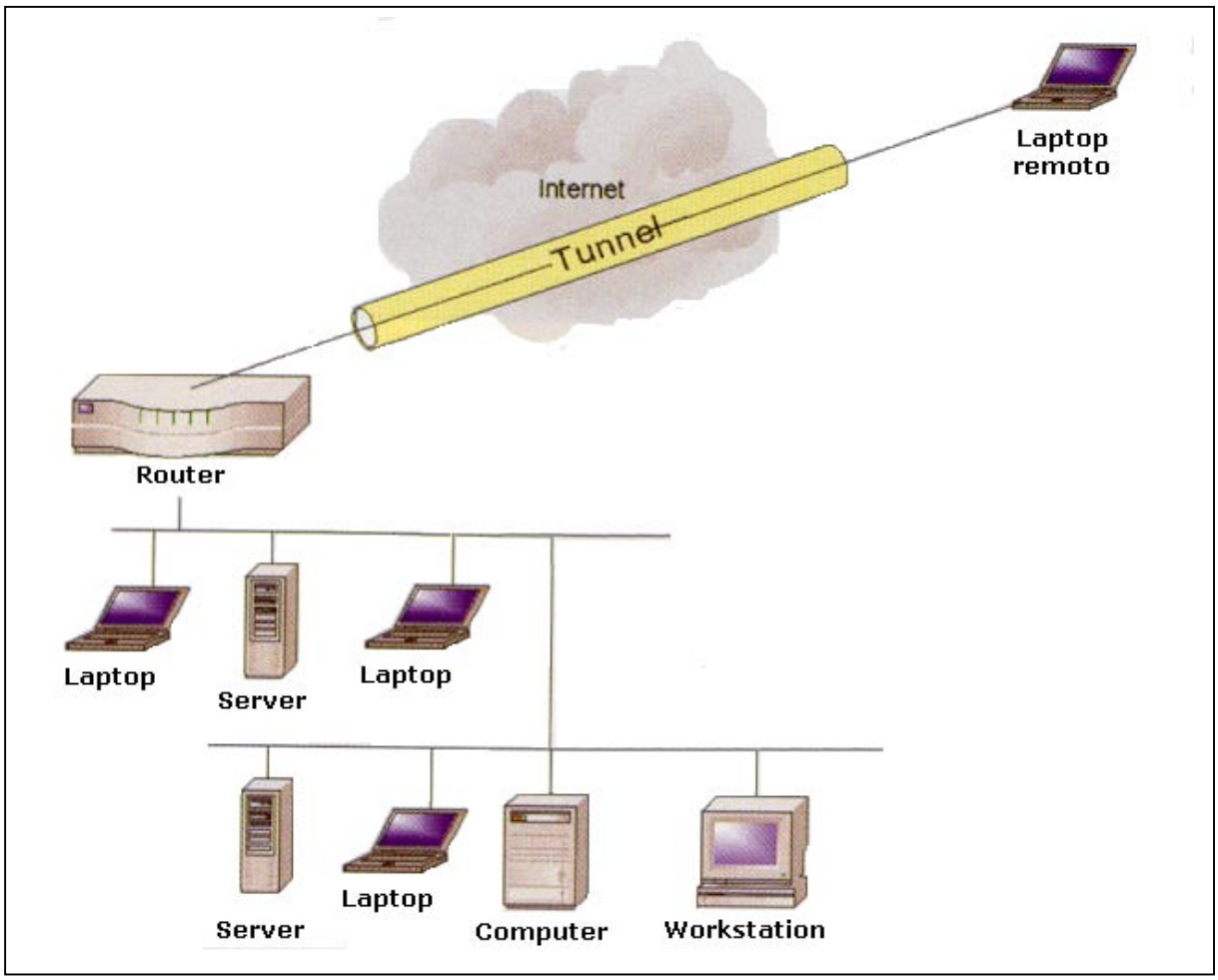

Figura 1 – Semplice VPN per dare accesso alla LAN aziendale a dipendenti esterni

Le vulnerabilità introdotte da una VPN con login e password possono essere così riassunte

- Le password sono memorizzate su macchine locali e macchine di rete, spesso facili da trovare
- L'utente tende ad utilizzare la stessa password su macchine differenti per semplificare la gestione del sistema, aumentando la portata del rischio
- L'implementzione di molti schemi di autenticazione con username/password prevede l'invio in rete della password in chiaro
- Un hacker può mascherarsi da utente legittimo agendo da qualunque postazione
- Esistono tool (password cracking tools) che permettono di trovare le password anche in modo facile, ma mai così facile come leggere i post-it con username e password appiccicati sul monitor del PC.

Le soluzioni più complete per portare la sicurezza delle VPN ad un livello adeguato prevedono l'utilizzo di una PKI per la gestione dei certificati digitali e di sistemi di strong authentication con smart card, token o lettori di tipo biometrico per proteggere l'accesso alle credenziali digitali.

FIREWALL accesso controllato

Letteralmente “Firewall” sarebbe “muro di fuoco”, ma in ambito di sicurezza indica una “struttura tagliafuoco”. Sebbene la prima interpretazione sia più suggestiva, con l’idea di utenti indesiderati che vengono “bruciati”, il ruolo del firewall è di separare il mondo pericoloso esterno dalla LAN (o dal computer) da proteggere, creando una barriera di protezione perimetrale capace di bloccare o di chiudere le connessioni non considerate legali (trusted) e consentendo la comunicazione solo sulle porte TCP/UDP desiderate.
Tecnicamente, il firewall è un programma funzionante in background che interviene al verificarsi di determinati eventi. Riceve le richieste di connessione, le confronta con un elenco di regole e decide se consentire o meno l’accesso. Trattandosi di un software in genere non troppo impegnativo dal punto di vista delle risorse richieste per il suo funzionamento, un firewall può essere installato (embedded) su hardware dedicato, il che permette di evitare l’acquisto di un computer completo da desinare unicamente al suo supporto. Spesso il firewall è integrato direttamente sul router.

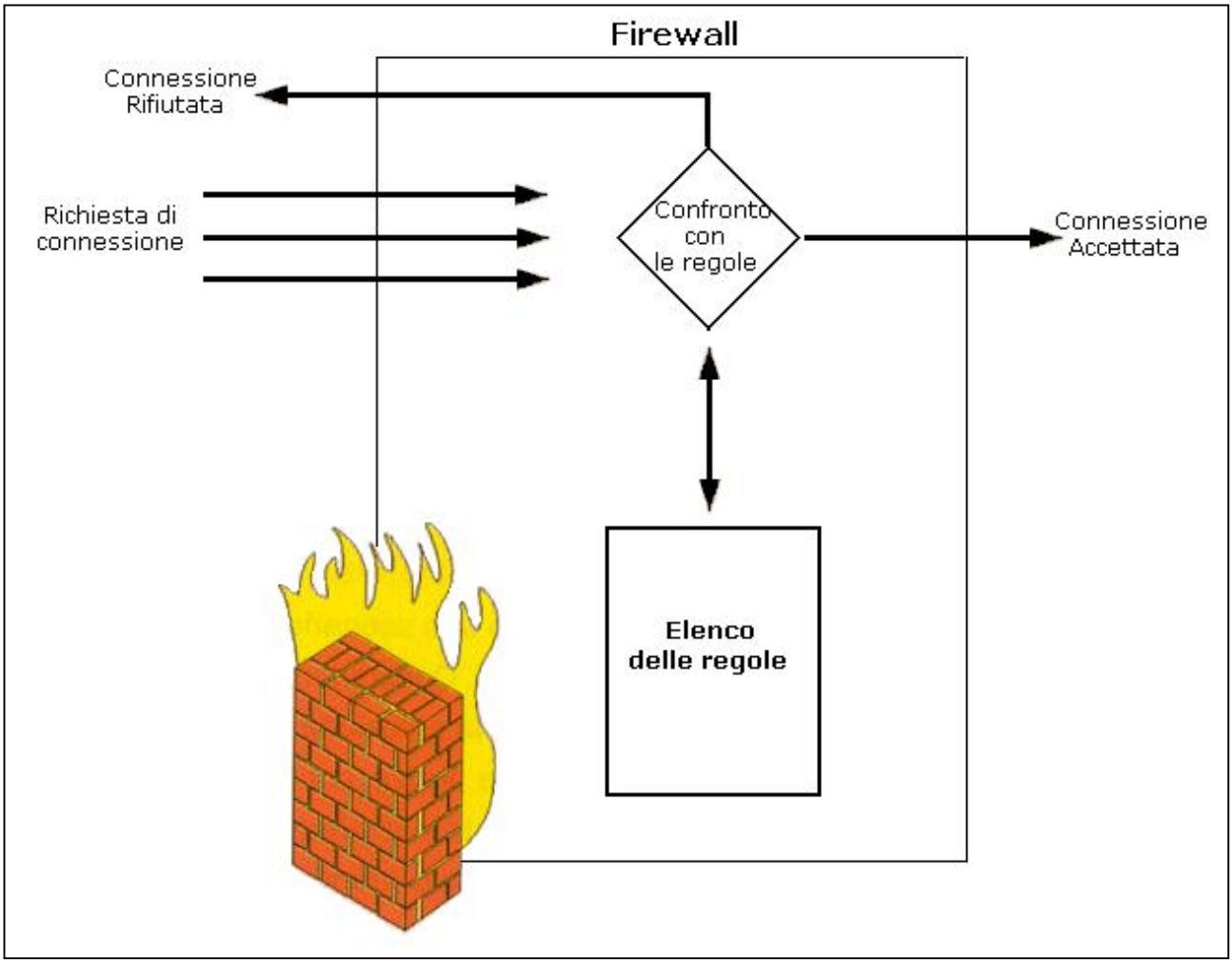

Figura 2 – Schema generale di un Firewall

Virus, worm e altri malanni

La sicurezza elettronica prevede la protezione di qualunque risorsa presente nella rete aziendale, sia hardware che software. Sebbene l'idea di e-security faccia pensare agli attacchi da parte di hacker, buona parte dei danni subiti dai sistemi informativi è causata da software pericoloso. I maggiori responsabili sono sicuramente i virus, gli internet worm, le nuke e i programmi "modificati" incautamente scaricati da Internet.

I **virus** sono programmi annidati all'interno di file eseguibili o contenenti informazioni elaborate da altri applicativi (Macro di Word, codice Visual Basic, Applet Java, codice ActiveX). Sono creati per infettare altri file (copiando il proprio codice) e per produrre danni ai dati presenti su disco, eventualmente rendendo il sistema inutilizzabile.

I **worm** (vermi) sono programmi auto-replicanti inseriti all'interno di piccole applicazioni; una volta eseguiti aprono backdoor nel sistema ospite e si spediscono automaticamente a tutti i destinatari presenti nella rubrica del proprietario della macchina. Attraverso la backdoor gli hacker possono penetrare nel sistema.

Le **nuke** (bombe atomiche) sono spezzoni di codice o pacchetti TCP/IP in formato non valido che una volta interpretati possono mandare in crisi il programma che li elabora. L'esempio più tipico è il Win Nuke, che sfruttando un baco di Windows (la possibilità di inviare un codice non valido al NetBios) "congela" il sistema operativo mostrando sul monitor la classica schermata blu. Esistono bombe anche per programmi di messaging e sharing, pe esempio per ICQ e per i client IRC.

Pericolosa fonte di danno per il sistema sono i programmi modificati che sono pubblicati su alcuni siti Internet. Possono essere software freeware o shareware liberamente distribuibili, contenenti all'interno virus, worm o spezzoni di codice modificati per mandare in crash il sistema o produrre danni ai dati. Anche programmi commerciali infettati in modo non doloso possono essere distribuiti nei circuiti dei pirati informatici.

Per difendersi da tutti questi attacchi al software sono stati sviluppati gli **antivirus**, programmi in grado di analizzare i file presenti sul disco, riconoscere (con analisi deterministiche o euristiche) virus e vermi all'interno del codice e rimuovere i file così identificati. Un buon software antivirus andrebbe installato su ogni macchina per prevenire attacchi causati da codice proveniente via mail, via rete o introdotto involontariamente dagli utenti su qualche supporto di memorizzazione utilizzato all'esterno. Aziende con reti grandi o con dati particolarmente sensibili dovrebbero installare **Gateway** antivirali che consentano la scansione preventiva dei file prima che entrino nella rete locale.

Questi problemi sono vitali per chi utilizza Internet per lo scambio di dati, sia attraverso posta elettronica, che con file-sharing o download/upload. La posta elettronica in particolare aumenta il tasso di rischio perché si possono ricevere e-mail indesiderate contenenti codice pericoloso. Per risolvere i problemi delle aziende con traffico dati molto importante sono state sviluppate tecniche di **Stateful Inspection** per la scansione dei file in transito sui firewall o sui server di posta.

Sicurezza in ambito wireless

Le LAN wireless rappresentano uno scenario interessantissimo per il futuro delle reti locali. Questa tecnologia potrebbe rappresentare la svolta per la creazione di LAN in spazi quali aeroporti, stazioni, fiere e piazze, conducendo ad un nuovo livello la filosofia dell'Internet always-on. L'utilizzo dell'etere come mezzo trasmissivo introduce problemi di sicurezza a lungo studiati sia in ambito militare che civile. Una comunicazione radio è sempre intercettabile attraverso un RF jammer, di conseguenza le informazioni sono disponibili a chiunque rientri nel raggio dell'apparecchio. Occorre una protezione per le informazioni in transito che tenga in considerazione questa realtà. Il protocollo wireless 802.11b è stato da tempo "bucato" e le vulnerabilità riscontrate sono descritte ampiamente su molti siti. Si rende necessaria una soluzione che garantisca la protezione end-to-end della comunicazione, badando che il sistema complessivo non presenti falle intermedie, per esempio durante la conversione da un protocollo di sicurezza ad un altro.
L'esigenza di una protezione end-to-end trova riscontro anche nelle nuove applicazioni dei telefoni cellulari (GSM e GPRS). Gli algoritmi di sicurezza del GSM non garantiscono più un livello di protezione sufficiente e lo stesso vale per la sicurezza crittografica del COMP128 utilizzato nello standard GPRS. Anche il WAP (Wireless Application Protocol), che utilizza in trasmissione il protocollo WTLS, potrebbe creare problemi di sicurezza nei punti del sistema dove le comunicazioni criptate sono decifrate. La comunicazione in tali situazioni risulta non protetta e un intruso con il controllo della macchina su cui avviene la decrittazione potrebbe avere accesso a tutte le informazioni in transito.