I.T.I.S. “E. MAJORANA”
MARTINA FRANCA(TA)

TESINA: *SICUREZZA RETI*
MATERIA: *SISTEMI*

DATA EMISSIONE: 20-06-2005
AUTORI: *ANGELO SPALLUTO*

INDICE: SICUREZZA RETI

SICUREZZA RETI 2

1 AMBIENTI DI UTILIZZO **2**
1.1 SICUREZZA NEI WEB SERVER *3*
2 OBIETTIVI **3**
3 MODALITÀ DI AUTENTICAZIONE **3**
3.1 AUTENTICAZIONE USER-TO-HOST *4*
3.2 AUTENTICAZIONE USER-TO-HOST *4*
3.3 UTILIZZO DI PASSWORD *5*
3.4 AUTENTICAZIONE TRAMITE INDIRIZZO IP *5*
3.5 AUTENTICAZIONE CON SFIDA SIMMETRICA *5*
3.6 AUTENTICAZIONE CON SFIDA ASIMMETRICA *6*
3.7 AUTENTICAZIONE CON SISTEMI BIOMETRICI *6*
3.8 ONE-TIME PASSWORD (OTP) *6*
4 PROTOCOLLI DI AUTENTICAZIONE **7**
4.1 KERBEROS *7*
4.2 NTLM AUTHENTICATION *11*
4.3 LM (LAN MANAGER) *12*
4.4 ALTRI PROTOCOLLI DI AUTENTICAZIONE *12*
5 TECNICHE DI ATTACCO **12**
5.1 DENIAL OF SERVICE *13*
5.2 IP SPOOFING *13*
5.3 ATTACCHI A SNIFFER *14*
5.4 ATTACCHI A SESSIONE TELNET *14*
5.5 DIROTTAMENTO DEL PROTOCOLLO TCP (TCP HIJACK) *14*
6 ARCHITETTURE PER RETI SICURE **14**
6.1 FIREWALL *15*
6.2 PROXY SERVER *16*
6.3 BASTION HOST *17*
6.4 DMZ (DE-MILITARIZED ZONE) *17*
7 SICUREZZA RETI VOIP **17**
7.1 VoIP (Voice over Internet Protocol) *18*
7.2 TELEFONATA TRA PC E TELEFONO TRADIZIONALE *18*
7.3 TELEFONATA TRA TELEFONO FISSO E TELEFONO FISSO *19*
7.4 TELEFONATA TRA PC E PC *19*
7.5 SICUREZZA RETI VOIP *19*
8 ASPETTI LEGALI **20**
SITOGRAFIA **21**

SICUREZZA RETI

1 AMBIENTI DI UTILIZZO

Lo sviluppo dei sistemi interconnessi ad Internet e la diffusione del servizio web, ha incentivato sempre più la nuova tecnologia ad elaborare sistemi informatici in grado di assicurare maggiori livelli di sicurezza e garantire maggiore affidabilità nelle trasmissioni di informazioni.
Inoltre, la presenza di molti servizi collegati ad Internet, e lo sviluppo esponenziale legato alla loro crescita, fa intuire come la probabilità di queste risorse renda vulnerabile la rete a fronte di attacchi che mirano alla violazione o addirittura alla distruzione delle informazioni trasmesse all'interno della rete su cui l'utente accede.
I servizi che utilizzano la rete come attività commerciale sono i siti web che gestiscono dei veri e propri negozi on-line (esempio:ebay) disponibili in qualsiasi ora della giornata. Servizi di questo genere utilizzano sistemi di autenticazione,

per permettere la validità delle transazioni che avvengono sul web ma soprattutto per rendere lo scambio dei dati in maniera privata al di fuori di utenti estranei. Le garanzie che vengono fornite da questi servizi sono:

- ✓ Il servizio può utilizzare i dati solo per operazioni che vengono consentite dall'utente.
- ✓ Non è possibile leggere o falsificare le transazioni che avvengo attraverso l'utilizzo di questo servizio.

Queste operazioni avvengono mediante l'utilizzo di protocolli sicuri (HTTPS e SSL) che gestiscono il flusso delle informazioni in maniera più privata, a differenza di come invece accade nei normali protocolli utilizzati per il trasferimento dei dati (HTTP).

1.1 SICUREZZA NEI WEB SERVER

I protocolli descritti nel paragrafo precedente vengono utilizzati all'interno di applicazioni di tipo Web Server, che vengono configurati per fornire file HTML oppure servizi di posta elettronica. Il protocollo sicuro utilizzato per lo scambio di ipertesti viene chiamato HTTPS (oppure Secure HTTP anche se è più sconosciuto), l'obiettivo di questo protocollo è quello di proteggere il canale di comunicazione quando si ricevono o si spediscono dati.
Altri protocolli invece che vengono considerati insicuri all'interno di un Web Server sono: i servizi di posta elettronica SMTP (SIMPLE MAIL TRANSFER PROTOCOL) e i servizi che permettono il download dei dati da parte di sistemi collegati in remoto FTP (FILE TRANSFER PROTOCOL).
La posta elettronica è uno dei servizi più comuni offerti da Internet, e modificarne il proprio contenuto non è un operazione complessa. I problemi più comuni con la posta elettronica sono dovuti agli attacchi di *flooding* (catene di San'Antonio) ed alle persone che inviano dati riservati fidandosi della confidenzialità del servizio.
Le stesse problematiche sono legate anche al protocollo di tipo FTP che viene utilizzato maggiormente dagli amministratori di Web Server, ogni qualvolta che vogliono aggiornare i propri servizi.

2 OBIETTIVI

Come è stato gia evidenziato nei paragrafi precedenti, l'utilizzo di sistemi di autenticazione all'interno di reti private e della stessa rete Internet, rappresenta da un punto di vista applicativo un sbarramento per rendere sicure le modalità di trasferimento dati.
All'interno di questa specifica verranno trattati in maniera più accurata i seguenti punti:

- ✓ Protocolli di autenticazione e le loro modalità di funzionamento;
- ✓ Descrizione dei principali attacchi;
- ✓ La sicurezza nelle reti;
- ✓ Reti VoIP e la loro sicurezza;
- ✓ Aspetti Legali;

3 MODALITÀ DI AUTENTICAZIONE

All'interno di una rete locale la figura dell'amministratore di rete ha il compito garantire il corretto funzionamento della rete, a partire dall'autenticazione degli utenti fino al monitoraggio e al mantenimento delle funzionalità degli apparati.
In un sistema informativo distribuito, l'autenticazione riguarda la verifica dell'identità di un utente, i metodi di autenticazione si possono suddividere in diverse modalità:

- ➢ *User-to-Host* (Da utente a Host) Metodi usati dall'host per identificare gli utenti.
- ➢ *Host-to-Host* (da Host a Host) Tecniche utilizzate da host per convalidare l'identità di altri host, in modo da evitare eventuali comunicazioni errate.
- ➢ *User-to-user* (da utente a utente) Questo è il classico metodo che viene utilizzato ogni qualvolta si vuole verificare che l'utente mittente non si spaccia per qualcun altro.

Le tecniche che vengono utilizzate per sfruttare questi metodi sono:

SYH: (Something You Have) L'utente viene identificato mediante qualcosa che possiede , detto token che può essere incluso all'interno di un tesserino elettronico, smart card o in un bancomat. Attraverso il token che generalmente

corrisponde ad una password oppure ad un codice PIN, l'utente viene identificato. Ma questo tipo di metodologia può presentare alcuni inconvenienti che sono:

- Il token può essere smarrito, clonato oppure viene reso non disponibile.
- L'utilizzo del token può comportare anche delle spese elevate dal punto di vista economico.
- L'utilizzo del token comporta svantaggi anche dalle spese legate alle infrastrutture hardware o software che devono essere create per permettere agli utenti di potersi identificare da più luoghi distanti fra loro.

SYA: (Something You Are) L'utente viene identificato sulla base di alcuni aspetti fisici (esempio: impronta digitale, tono vocale). In questa tecnica le problematiche principali sono:

- Alta percentuale di errore;
- Rischio di intrusione nei sistemi di rilevazione;
- Costo elevato delle attrezzature da utilizzare;

SYK: (Something You Know) L'utente viene identificato per mezzo di qualcosa che sa, un tipico esempio è il riconoscimento per mezzo di una password segreta. Questo a livello economico rappresenta la tecnica migliore per evitare dei grossi dispendi, inoltre, abbinata a tecniche crittografiche molto efficienti le password sono molto sicure.

Tutte queste tecniche possono effettuare l'autenticazione mediante alcuni fattori che possono essere a fattore unico, oppure a due o più fattori. Quando si parla di "fattori" si sta ad indicare l'entità utilizzata per far avvenire l'autenticazione (esempio: username e password).
Un esempio a fattore unico è la password utilizzata all'interno di autenticazioni che avvengono per login, dove l'utente deve conoscere solo la password, mentre l'username è visibile a tutti.
Un esempio a due fattori si basa sulla memorizzazione di un'entità e sul possesso di un'altra, esempio: possesso di una card e conoscenza di un PIN. Questa come soluzione è l'ideale, ma risulta di scarsa praticità nei sistemi informatici.

3.1 AUTENTICAZIONE USER-TO-HOST

Come è stato descritto precedentemente l'autenticazione può avvenire in diversi modi, in questo paragrafo analizzeremo come l'accesso ad un sistema avviene tra utente e host. Nel caso seguente ogni utente deve dimostrare al sistema la propria identità, mediante tecniche che identificano l'utente in maniera univoca.
Un utente può identificarsi con una semplice fase di login inserendo username e password (tecnica peggiore) oppure utilizzando un sistema elettronico, attraverso l'utilizzo di carte magnetiche. Con carte magnetiche l'autenticazione avviene in maniera più sicura, infatti, i dati che permettono l'autenticazione vengono incisi all'interno di questa carta magnetica, e non vengono resi pubblici ad utenti estranei. Se invece, c'è bisogno di rendere l'autenticazione sicura, allora questa può avvenire utilizzando sistemi biometrici, dove l'accesso ad un sistema informatico si verifica per mezzo di caratteristiche fisiche.
Un esempio di identificazione biometria è l'utilizzo di impronte digitali, del tono della voce, o di qualche altra caratteristica fisica; come la dimensione della faccia o il colore degli occhi.
E' possibile intuire che le tecniche descritte nel paragrafo precedente possono essere utilizzate all'interno di sistemi informatici sulla base di due fattori che sono:

- Risorse economiche;
- Importanza nel rendere il più sicuro possibile l'autenticazione;

Inoltre, nei sistemi di nuova generazione è possibile permettere l'autenticazione degli utenti con più fattori contemporaneamente, questo può avvenire utilizzando anche più di due fattori. Una tecnica di questo genere prende il nome di *factors authentication*.

3.2 AUTENTICAZIONE USER-TO-HOST

Mentre nel caso precedente l'autenticazione avviene tra utente e macchina, in questo caso avviene tra due host. All'interno di un sistema informativo non ci sono solamente utenti che operano, ma anche delle procedure, dei processi che molto spesso operano in modo automatico anche in assenza di un operatore umano. Anche in questi processi, alcune volte c'è bisogno che un elaboratore per ottenere una funzionalità, un servizio o dei dati deve autentificarsi nei confronti di un altro elaboratore. In questo caso, l'identità del programma o del processo che ha iniziato a svolgere questa funzione può coincidere o meno con quello dell'utente che ha iniziato l'attività.

Realizzare un sistema di questo genere comporta un operazione complessa, in quanto a causa dell'assenza di un operatore, l'autenticazione mediante le tecniche descritte precedentemente non può avvenire. Le soluzioni che sono state proposte per risolvere questo inconveniente sono state:

- ✓ Utilizzare indirizzi di rete (cioè abilitare i processi solo a determinati elaboratori);
- ✓ Memorizzare password all'interno del codice di un programma (la password in questo caso non è sicura);

3.3 UTILIZZO DI PASSWORD

La tecnica che oggi ha avuto maggiore diffusione nei sistemi di autenticazione è quella con l'utilizzo di un'username e password. Questa tecnica è fortemente sconsigliabile solo se sussistono alcuni fattori come:

- ✓ Se la password può essere letta durante la sua trasmissione;
- ✓ Se la password viene conservata in chiaro all'interno di un file. In questo caso è veramente un operazione banale leggerla, ma anche nel caso in cui la password sia mantenuta in forma crittografata, cioè cifrata, diventa pericoloso se questa entra nelle mani di un utente estraneo.

Sulle password conservate all'interno dei file è possibile svolgere mediante l'utilizzo di programmi presenti sulla rete degli attacchi di tipo *dictionary attack* dove: confrontano la password rilevata con possibili password presenti all'interno di altri file è possibile risalire alla chiave segreta. Altri attacchi che possono rivelare l'identità della chiave sono :*brute force* oppure attacchi che avvengono con più computer che lavorano in concorrenza in un ambiente distribuito.
Una raccomandazione nell'utilizzo delle password è quella di non utilizzare password con soli caratteri alfabetici, ma fondere al suo interno lettere, cifre e caratteri di punteggiatura con un minimo di otto caratteri. Inoltre, si consiglia di non mantenere sempre la stessa password per lungo tempo.

3.4 AUTENTICAZIONE TRAMITE INDIRIZZO IP

Un'altra possibilità di autenticare sia un utente che un servizio, è quello di fare affidamento sugli indirizzi di rete, cioè identificare l'utente in base alla sua postazione di lavoro. Questo avviene utilizzando le classi degli indirizzi di rete IP, infatti la maggior parte delle volte questa tecnica viene utilizzata quando si vuole far accedere solo determinate postazioni di lavoro presenti, all'interno di una grande rete aziendale.
Ovviamente le persone che accedono con questi indirizzi, effettuano prima una fase di autenticazione per permettere l'accesso solo a determinati utenti. Ma questo tipo di autenticazione è molto debole, in quanto è molto facile falsificare gli indirizzi IP su un normale PC, pertanto l'autenticazione basata sugli indirizzi di rete è da sconsigliare fortemente in ambienti con grado di sicurezza medio/alto.

3.5 AUTENTICAZIONE CON SFIDA SIMMETRICA

I sistemi di autenticazione descritti fino ad ora non garantiscono dei buoni risultati dal punto di vista funzionale, infatti, vengono implementati solamente in ambienti dove la sicurezza non è essenziale.
Alcuni sistemi che invece garantiscono migliori risultati nella sicurezza dei dati sono i sistemi cosiddetti di autenticazione a sfida simmetrica, in questo caso oltre all'utente anche il sistema conosce la password. Il funzionamento di questi sistemi avviene mediante alcune fasi che sono:

1. L'utente che vuole accedere al sistema, invia un primo pacchetto che specifica l'username (ID) dell'utente che ha inoltrato la richiesta. Il valore di questo ID è valore univoco per ogni utente.

2. A fronte di questa richiesta di accesso, il sistema che al suo interno ha l'elenco degli identificativi e le relative password di tutti gli utenti, invia all'utente che ha sollecitato la richiesta un messaggio di sfida. Tale sfida consiste nell'inviare un numero random N, che viene cifrato utilizzando come chiave la password relativa a quel utente.

3. Se l'utente che ha inviato la richiesta è quello giusto, allora deve essere in grado di ricavare il numero N mediante la password che gli corrisponde, utilizzando lo stesso algoritmo adottato dal sistema.

4. Se l'utente non riesce a decifrare quel numero, significa che un utente estraneo ha cercato di spacciarsi con un'identità estranea.

I vantaggi che presenta questo metodo sono legati al fatto che la password è conosciuta solamente dal fornitore del servizio e dall'utente. Inoltre, nella fase di trasmissione dei dati la password viene solo utilizzata per cifrare un numero, quindi, un utente estraneo che sniffa i messaggi sul canale, non potrà mai sapere quale sarà stata la chiave utilizzata, in quanto non viene trasmessa. Bisogna evitare nella fase di autenticazioni successive, di ripetere lo stesso numero casuale che è stato utilizzato per un'autenticazione precedente, infatti può rappresentare un grande rischio se viene letto da un utente estraneo che cerca di disturbare la comunicazione.
L'inconveniente di questo metodo è che il valore della chiave segreta viene reso disponibile anche al fornitore del servizio.

3.6 AUTENTICAZIONE CON SFIDA ASIMMETRICA

Questo sistema elimina il problema che si verifica nell'autenticazione a sfida simmetrica, infatti il contenuto della chiave privata è solo a conoscenza dell'utente. Questo metodo utilizza per lo scambio di dati due chiavi che sono: una privata e una pubblica, quella privata viene utilizzata solo per decifrare il messaggio da parte dell'utente, mentre quella pubblica viene utilizzata da coloro che devono inviare un messaggio a questo utente, ed è conosciuta da tutti. Il sistema su cui viene effettuata l'autenticazione, memorizza solamente gli ID che identificano univocamente l'utente
Le fasi che determinano l'autenticazione dell'utente sono le seguenti:

1. L'utente che vuole accedere al sistema, invia il proprio certificato a chiave pubblica contenente il proprio identificativo e la propria chiave pubblica.

2. Il sistema sulla base della chiave pubblica che ha ricevuto da questo certificato, identifica l'utente e gli manda una sfida. La sfida consiste sempre nel solito numero N casuale che viene crittografato con la chiave pubblica del destinatario.

3. A questo punto il destinatario per autenticarsi decifra il numero cifrato con la sua chiave privata, pertanto una volta ricavato il numero originario se è lo stesso viene riconosciuto, altrimenti, l'operazione viene considerata nulla.

Anche in questo caso, chi osserva il traffico nella rete non può in alcun modo desumere quale sia la chiave privata dell'utente per poi in futuro spacciarsi per l'utente soggiogato.
Nella realtà queste tecniche vengono utilizzate nelle firme digitali, dove si utilizzano le due chiavi per il riconoscimento dell'utente destinatario, inoltre, vengono utilizzati anche algoritmi crittografici di tipo asimmetrico in cui la riservatezza dei dati viene garantita efficientemente, tipo: il TRIPLE-DES (DATA ENCRYPTION STANDARD) che utilizza una chiave a 128 bit, anche se i nuovi software riescono a cifrare con chiavi superiori a 128 bit.

3.7 AUTENTICAZIONE CON SISTEMI BIOMETRICI

Per evitare che una password venga scoperta oppure che una smart card venga smarrita in mani malintenzionate, si è pensato di implementare alcuni sistemi senza l'utilizzo di nessuna chiave o identificativo, in grado di identificare l'utente con applicativi biometrici. Si utilizzano principalmente tre tipi di tecniche. Infatti, esistono dei dispositivi in grado di abilitare l'utilizzo di carte magnetiche solo dopo aver effettuato il riconoscimento di un impronta digitale, oppure del tono vocale dell'utente o, se dotato di una piccola telecamera oculare, effettuando lo scanner dei vasi sanguigni presenti sul fondo della nostra retina.
Tutte queste tecniche sono valide solo da un punto di vista teorico, infatti ancora non sono disponibili delle attrezzature che riescono a svolgere determinate funzioni con una percentuale minima di errore. Il problema principale legato a questa tecnica è legato soprattutto dai possibili rifiuti che le apparecchiature di input possono avere a seguito di una conferma di autenticazione. Le apparecchiature che sono state create momentaneamente non sono efficienti al massimo, infatti, presentano un errore di circa il 10% pertanto sono ancora in fase di progettazione. Comunque queste forme di autenticazione ribalteranno il funzionamento di un sistema di autenticazione già efficiente in questo periodo, rendendolo ancora più sicuro.

3.8 ONE-TIME PASSWORD (OTP)

Un metodo per gestire l'utilizzo delle password e per evitare che nella fase di comunicazione un utente utilizzi la stessa password nelle autenticazioni successive è *one-time password* (usa e getta) password valida solo una volta.

Questo metodo si divide in due versioni, la prima afferma che: quando il sistemista abilita un utente ad accedere ad un sistema, gli fornisce un range di password numerate in maniera tale da utilizzare ognuna per ogni autenticazione futura.
Utilizzare un sistema di questo genere garantisce dei vantaggi all'utente, infatti, anche se un estraneo osserva la password durante la trasmissione dei dati, questa non potrà mai essere valida per una futura autenticazione. Inoltre, una volta che l'utente avrà terminato le password a disposizione dovrà recarsi dal sistemista per avere un altro elenco di password.
Nella seconda versione l'autenticazione avviene sempre nella stessa maniera cioè con password usa e getta, ma la differenza sta nel fatto che queste vengono calcolate da un programma che viene fornito da fornitore del servizio.
In base all'istante di tempo in cui avviene l'identificazione, attraverso questo programma viene calcolata una password che identifichi l'utente solo per quel istante. Ovviamente, il valore delle password cambia con una certa approssimazione di tempo (ogni 60 secondi), inoltre, la data del sistema con cui l'utente sta effettuando l'autenticazione deve coincidere con quella dell'utente stesso, e se c'è una differenza di orario tra i due sistemi l'autenticazione fallisce. Questa versione in confronto a quella precedente è molto più efficiente in quanto una password non potrà mai essere ritrasmessa nella comunicazione. L'inconveniente di questa versione è: se l'utente malintenzionato riesce ad impossessarsi dell'algoritmo utilizzato dal programma.

4 PROTOCOLLI DI AUTENTICAZIONE

La maggior parte dei sistemi di rete usa uno schema di autenticazione basato sulle password. Quando un utente si autentica per accedere a un server di rete deve fornire un username e una password per tutti i servizi che richiedono l'autenticazione. La trasmissione delle informazioni di autenticazione per molti servizi non è cifrata, quindi rappresenta un rischio per le informazioni che vengono manipolate sulla rete. Qualunque utente che ha accesso alla rete e che può utilizzare un analizzatore di pacchetti di rete (vedremo successivamente) può intercettare le password che attraversano la rete, compromettendo gli account degli utenti e l'integrità della sicurezza dell'infrastruttura. Pertanto, sono stati creati protocolli che hanno come scopo principale di eliminare la trasmissione delle informazioni di autenticazione attraverso la rete. Uno dei protocolli che ha avuto larga diffusione in questo campo è: Kerberos, comunque sono stati implementati diversi protocolli.

4.1 KERBEROS

IL 27 Maggio del 1983 il MIT (L'istituto di Ingegneria più grande dell'America) supportato dalla IBM e dalla Digital, varò un progetto denominato Athena della durata di cinque anni, avente come scopo di integrare la potenza di calcolo e la capacità grafica degli elaboratori, al fine di ottenere degli ottimi risultati dal punto di vista elaborativi. Il progetto non ebbe ottimi risultati, ma nel 1991dal MIT furono presentati delle importanti tecnologie quali il sistema X Window e il sistema di autenticazione di Kerberos. Kerberos (nella mitologia greca indica il cane a tre teste guardiano delle porte dell'inferno) è un protocollo di autenticazione che ha lo scopo di non di inviare password attraverso la rete nel momento in cui avviene l'autenticazione, ed impedisce agli utenti non autorizzati di intercettare le password inviate all'interno del protocollo. Kerberos si serve della crittografia a chiave segreta e utilizza un sistema fidato denominato KDC (Key Distribution Center) per autenticare gli utenti su una rete e consentire loro di accedere ai servizi desiderati. Inizialmente Kerberos utilizzava l'algoritmo DES, ma visto che oggigiorno il DES è stato riconosciuto, allora utilizza algoritmi di crittografia più forti come 3DES e IDEA. Il sistema Kerberos può essere utilizzato sia per offrire un'autenticazione semplice (solo con un utente) che in mutua autenticazione, inoltre questo protocollo si basa su due fattori che sono:

- ***REALM*** Una rete basata su Kerberos, formata da uno o più server (chiamati anche KDC) e da un insieme di client che offrono servizi "kerberizzati";
- ***TICKET*** Rappresenta la struttura dati per l'autenticazione del client per un particolare servizio.

Un ***TICKET*** è un insieme di dati che permette ad un servizio di identificare un client. Un ticket al suo interno è costituito da campi che lo identificano univocamente, questi sono:

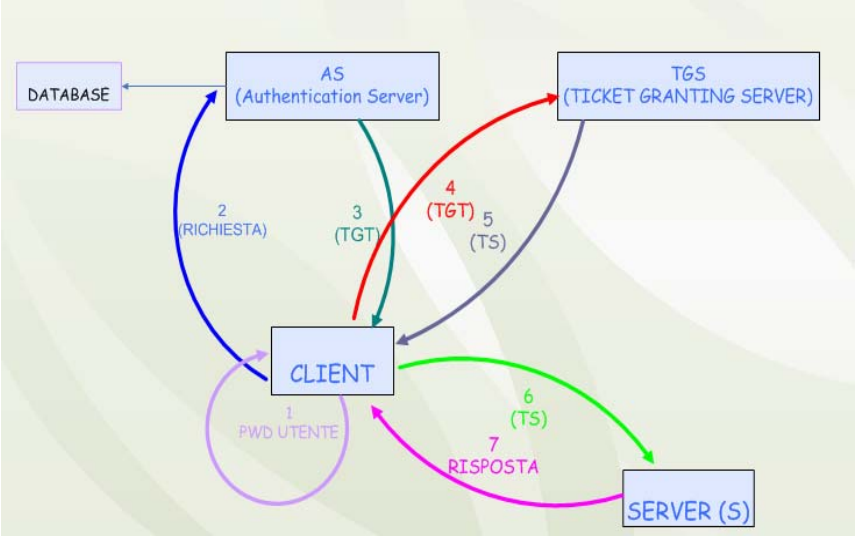
- ID del Server a cui il client si connette per ricevere un servizio;
- ID identificativo del Client che utilizza il ticket;
- IP del Client che utilizza il ticket;
- Data e ora dell'emissione del ticket (questo avviene memorizzando i dati con un campo di tipo timestamp);
- Durata di vita di un ticket (mediamente i ticket rimangono in memoria sino ad 8-10 ore);
- Una chiave crittografata per permettere eventualmente al client e al server di effettuare delle comunicazioni cifrate;

Per evitare che i ticket possano essere manipolati dagli utenti, tutti questi dati presenti al loro interno vengono cifrati con la chiave KS del server a cui sono destinati. In questo modo, quando un utente riceve un ticket per usufruire di un servizio, l'unica cosa che può fare è trasmettere questo ticket al server a cui desidera ricevere un servizio. Il Client non può in nessun modo modificare il contenuto del ticket perché non conosce la chiave per aprire il ticket. I ticket possono di diverso tipo, ognuno con un compio diverso, questi sono:

- ✓ ***INITIAL O PRE-AUTHENTICATED***: Questo ticket viene emesso dal protocollo del server di autenticazione. L'utilizzo di questo ticket avviene per aggiungere informazioni addizionali nella fase di autenticazione oppure quando viene emesso il TGT, tutto questo avviene mediante le opzioni PRE-AUTHENT e HW-AUTHENT.
- ✓ ***PROXIABLE E PROXY***: In alcuni casi ci potrebbe essere che un utente permetta ad un servizio di effettuare delle operazioni a suo posto. Il servizio deve essere in grado di autenticarsi come se fosse il client, per fare questo viene utilizzato un ticket proxy.
- ✓ ***FORWARDABLE***: Questo è un ticket proxy particolare, infatti viene utilizzato quando l'utente si collega al server e vuole che l'autenticazione avviene come se fosse in locale.
- ✓ ***RENEWABLE***:Un ticket di questo tipo è caratterizzato da due tempi di scadenza, che sono: il tempo di scadenza associato al ticket stesso, ed il massimo tempo di rinnovo possibile. I ticket rinnovabili vengono utilizzati quando si vogliono ridurre i danni nel caso di furto di un ticket.
- ✓ ***INVALID***: Il ticket non è valido;
- ✓ ***POSTDATED***: Il ticket viene generato per essere utilizzato in seguito.

I ticket utilizzando degli standard Internazionali per permettere che questo avvenga correttamente. Questi standard sono: ISO 8824-1, 8824-2, 8824-3, 8824-4 e ISO 8825-1, 8825-2.

FUNZIONAMENTO KERBEROS:



Il funzionamento di Kerberos avviene in base ad alcune fasi distinte, queste sono state elencate successivamente e sono:

1. Nel momento in cui un utente accede ad una postazione di lavoro di tipo client fornisce localmente la propria password, la quale rimane sempre memorizzata all'interno del client.

2. A questo punto un client per usufruire dei servizi di un'applicazione deve prima fornirsi un ticket di autorizzazione che acquista da un Server di Autenticazioni (AS). Per avere l'autorizzazione il client invia in chiaro un messaggio al server di autenticazione, questo messaggio è composto da due parti una in chiaro e una cifrata. Nella prima è contenuta una richiesta per ottenere il TGS che permette l'accesso al servizio a cui l'utente vuole collegarsi, mentre nella seconda sono presenti i dati necessari per AS o al KDC per verificare l'identità del client, questi dati sono: nome del sistema client e marcatore orario e vengono cifrati con la chiave segreta del client. La verifica dei dati del client avviene mediante alcune fasi che il KDC esegue, queste sono:

    - ✓ AS utilizza la chiave segreta presente all'interno del database di KDC, per decifrare la parte cifrata;

- ✓ Una volta decifrato il messaggio confronterà il principal (nome del client) che risiede sul db con quello che ha inoltrato la richiesta, se è uguale allora l'identificazione è avvenuta correttamente altrimenti, sarà inviato un messaggio di errore. Il marcatore di orario è necessario perchè farà sì che la richiesta non verrà ripresentata nuovamente;

3. Se la richiesta è avvenuta correttamente l'AS invierà al client un messaggio di risposta TGT (Ticket Granting Ticket) composto da due parti che sono: la prima viene cifrata dalla chiave segreta del client, che conterrà al suo interno la chiave di sessione (CS), mentre la seconda sarà cifrata con la chiave segreta del servizio TGS (Ticket Granting Server) a cui l'utente deve collegarsi, quindi questa parte è accessibile solo al TGS.

4. A questo punto il Client dopo aver ricevuto il TGT invierà al TGS un messaggio composto da tre parti distinte che sono: La prima indica il testo in chiaro contenente la richiesta di un TGS per il servizio S che l'utente ha richiesto, la seconda contiene il nome del client e un marcatore orario che vengono cifrati con la chiave segreta del client , infine l'ultima parte è costituita dal TGT ottenuto dall'AS nella fase precedente.

5. Il TGS risponderà con un messaggio composto da due parti distinte, una cifrata con la chiave segreta del client e quindi accessibile solamente da quest'ultimo, dove al suo interno sarà contenuta la chiave di sessione (CS) che l'utente utilizzerà per usufruire del servizio S che ha richiesto, e nell'altra parte sarà invece contenuto il ticket che avrà al suo interno sempre la CS, ma, questa volta cifrata con la chiave segreta del server.

6. Nell'ultima fase il client si presenta al servizio S con i dati che ha ricevuto dal TGS, con un messaggio composto da due parti cifrate. La prima che al suo interno è composta dal nome del client e un marcatore di orario, cifrata con la CS (Authenticator) che ha restituito il TGS, mentre la seconda contiene il ticket ricevuto dal TGS, ma questa volta viene cifrato con la chiave segreta del Servizio S.

7. Il servizio S risponderà con un messaggio contenete il marcatore orario ricevuto nel precedente messaggio del client. Questo messaggio viene cifrato con la CS estratta dal messaggio ricevuto dal client.

Come si può notare, i punti descritti precedentemente riportano sempre casi in cui le richieste vanno a buon fine, ma nel caso in cui la risposta ha un esito negativo, allora kerberos gestisce anche gli eventuali errori.
I messaggi di errore non vengono cifrati, al loro interno sono contenute informazioni come: data e ora dell'errore, la versione di kerberos utilizzata, il tipo di messaggio generato e l'ora sia del client che del server.
La durata dei ticket come abbiamo già detto varia dalle 8 alle 10 ore, quindi non è necessario accedere in continuazione al server di autenticazione, per essere identificati. Un'avvertenza che va fatta è cancellare il ticket allocato nella memoria della postazione, alla fine della sessione di lavoro.
Kerberos a differenza degli altri protocolli di autenticazione è quello che ha avuto una larga diffusione, ma questo sistema, viene implementato su reti con un protocollo di trasporto non connesso come l' UDP che utilizza la porta 88 per interfacciarsi dal KDC verso l'esterno. Inoltre, kerberos può essere utilizzato solo sul sistema operativo Windows 2000. Nel momento della descrizione delle fasi per verificare l'identità del client, sono stati usati termini tecnici come: principal e realm. Il principal è il nome unico di un utente o un servizio, il nome del principal ha la seguente forma: *root[/instance]@ realm* .
Tramite kerberos si riesce a proteggere la rete dagli attacchi più comuni, ma a volte potrebbe risultare complesso da implementare, per varie ragioni:

- ✓ Affinché una applicazione di rete possa usare Kerberos, è necessario modificare il suo codice sorgente per effettuare le chiamate alle librerie Kerberos. Per altre applicazioni, occorre invece modificare il protocollo di comunicazione utilizzato tra server e client. Le applicazioni "a sorgente chiusa" che non supportano Kerberos di default risultano quelle più problematiche.

- ✓ Kerberos parte dal presupposto che stiate usando host fidati su una rete non sicura. Il suo obiettivo principale è di impedire che le password in solo testo vengano inviate lungo questa rete. Tuttavia, se qualcuno diverso dall'utente effettivo ha accesso fisico a uno degli host, specialmente quello che emette i ticket usati per l'autenticazione, l'intero sistema di autenticazione è a rischio.

- ✓ Se si decide di utilizzare kerberos sulla rete bisogna ricordarsi tutte le password trasferite a un servizio che non lo supporta, poiché l'autenticazione rischia di essere intercettata dai packet sniffer. Per proteggere la rete con Kerberos bisogna *"kerberizzare" tutte* le applicazioni che inviano password in testo oppure evitate del tutto di utilizzarle.

Il funzionamento di Kerberos può risultare inefficiente ogni volta che l'autenticazione di un utente per un servizio che non utilizza kerberos avviene per mezzo di una password di testo. Quindi è sconsigliabile utilizzare servizi che non prevedono kerberos, come per esempio gli applicativi Telnet e FTP,mentre è più sicuro per protocolli come SSH e SSL.
Nelle problematiche viste precedentemente, si vuole sottolineare quanto sia pericoloso utilizzare applicativi che non supportano kerberos per trasportare le password. Questo avviene principalmente quando accedo ad un sistema Kerberos da remoto, ad esempio se voglio utilizzare la macchina kerberizzata da casa. In questa maniera per accedere da remoto alla macchina kerberizzata devo inviare una password , ma questa potrebbe essere intercettata dai racket sniffer.
Per risolvere questo inconveniente, si è pensato in alcune versioni di kerberos di utilizzare un'interfaccia simile a quella dei sistemi one-time password, a sfida simmetrica o a sfida asimmetrica.

Una delle possibili tecniche che abbiamo visto precedentemente per permettere di nascondere la password nel trasferimento dei dati è: *one-time password.* Il problema che ci si pone in questa tecnica è come fornire all'utente sempre nuove password, perché queste verranno esaurite in brevissimo tempo. Le soluzioni che abbiamo riscontrato quando abbiamo parlato di questa tecnica, erano scrivere le password su un foglietto oppure munire l'utente con un programma che generi password.
Un'implementazione del primo tipo è quella fatta dal sistema chiamato S/KEY. In questa tecnica l'utente sceglie un segreto (chiamato anche seme o seed) il quale non è altro che un numero binario casuale, dopodichè l'utente calcola autonomamente un numero N di password a piacere. La modalità di come avviene è in questo modo:

1. La password numero 1 viene calcolata applicando una funzione di hash al seme S

2. La password numero 2 è data dalla stessa funzione di hash applicata alla password 1;

3. Si generano in questa maniera un numero consistente di password;

4. Per poi poter accedere al server, viene memorizzata l'ultima password (n);

Ogni volta che voglio effettuare un login o accedere ad un servizio fornito dal server, il server stesso ci chiederà le password in ordine inverso a quello con cui sono state generate. Ad esempio: il server ci chiederà la password n-1, perché al suo interno conteneva il valore della numero n. Mediante funzioni di hash il server dalla password n-1 ricaverà la password n, se è uguale a quella memorizzata nel db allora significa che l'utente è stato autenticato correttamente, altrimenti non avviene la conferma. Sotto viene riportato un esempio:

- ✓ Il Server ha memorizzato al suo interno l'ultima password es. 10;

- ✓ Quando l'utente fa la richiesta di login, il server chiede la password 9;

- ✓ Il server con una funzione di hash sulla password 9 determina il valore della password 10. Se il valore coincide l'utente viene autenticato, altrimenti non avviene il login.

- ✓ Una volta che l'utente fa nuovamente un'altra richiesta di accesso, il server chiederà la password 8. Questo processo avviene fino a quando non si arriva al numero 0.

Una volta capito il funzionamento di questo sistema, dobbiamo considerare il caso quando è più conveniente usare delle password scritte su di un foglio, oppure utilizzare un programma. Per fare questa distinzione nel caso in cui è più conveniente utilizzare un metodo invece di un altro, bisogna tener conto della sicurezza e delle garanzie che la postazione di lavoro ci garantisce. Se al nostro sistema possiamo accedere tramite una postazione sicura, quindi una postazione in cui noi ci fidiamo sia del software installato che del hardware, allora è possibile fornire il seme alla nostra postazione, e fare in modo che sia lei a calcolarne la password da inviare.
Se invece non ci fidiamo della postazione oppure non utilizziamo sempre la stessa postazione, possiamo scrivere le password calcolate su di un foglietto.
La tecnica descritta precedetemente è simile alla prima versione dell'OTP. Mentre nella seconda versione dell'OTP si utilizza una filosofia diversa nel calcolare le password, infatti, prima le password venivano calcolate una dopo l'altra, mentre ora vengono calcolate in funzione del tempo. Nei sistemi one-time password basati sul tempo, le password dipendono sia dal seme scelto dall'utente che dall'istante di tempo in cui viene creata.
La password viene calcolata con una funzione di hash applicata sul seme e sul tempo. Per far si che il server possa convalidare la password all'utente, allora entrambi devono condividere tre cose: il segreto S, il riferimento di tempo e l'algoritmo che viene applicato.
Molte aziende hanno adottato sulla base dell'OTP un sistema indipendente dalla postazione di lavoro e meno ingombrante, in grado di rendere la creazione delle password molto velocemente, utilizzando i cosiddetti autenticatori hardware. Questi sono delle minicalcolatrici portatili che effettuano per noi il calcolo necessario per il sistema di autenticazione. Queste componenti hardware assomigliano a delle normali calcolatrici, che hanno il formato di una carta

di credito, dotata di un tastierino alfanumerico, su ci l'utente deve battere un PIN per abilitare la carta con le sue funzioni. Il PIN abilita il calcolo dell'algoritmo sulla CPU presente all'interno di questo autenticatore. La CPU calcola la password mediante una funzione di hash, sulla base di un riferimento temporale e di un segreto S presente all'interno della scheda. Una volta calcolata, la password viene visualizzata su un display della carta.

4.1.1 SISTEMA A SFIDA SIMMETRICA

Nei sistemi a sfida il problema principale è come permettere all'utente di conservare il segreto o la chiave e come calcolare il valore della F che è il risultato della funzione che viene applicata sul messaggio. Bisogna evitare di rendere l'accesso solo su determinate macchine, in maniera tale da rendere il sistema indipendente da qualsiasi dispositivo di memoria e di calcolo. Quindi, il problema può essere eliminato utilizzando un qualcosa di simile agli autenticatori hardware. Normalmente, per i sistemi a sfida si utilizzano le criptocalcolatrici.
Per i sistemi basati su sfida simmetrica si usano delle criptocalcolatrici basate sull'algoritmo DES. In questo caso il segreto corrisponde con la chiave di cifratura DES e la funzione F corrisponde all'algoritmo che viene utilizzato.
L'autenticatore hardware ha al suo interno la chiave segreta, e nel momento che arriva la sfida, con l'utilizzo dell'algoritmo presente all'interno del criptocalcolatore decifra il valore.
E' compito dell'utente battere la risposta che è stata ottenuta sulla tastiera, per fornirla al sistema che ci ha sfidato.

4.1.2 SISTEMA A SFIDA ASIMMETRICA (SMART-CARD)

Nel caso di sfide asimmetriche, vengono utilizzate le smart-card (carta intelligente) che sono delle criptocalcolatrici di tipo asimmetrico. Le smart-card possono essere considerate anche quelle che vengono fornite dai distributori di benzina, ma quelle che vengono utilizzate per le sfide asimmetriche utilizzano alcuni componenti elettronici per permettere la memorizzazione e la creazione di password.
Le smart-card a sfida asimmetrica sono dotate di chip in grado di effettuare calcoli crittografici, ma al loro interno c'è anche un microcontroller che svolge funzioni di CPU. Per memorizzare i dati queste carte utilizzano delle piccole memorie RAM, inoltre, dispongono anche di memorie ROM, EEPROM che contengono informazioni che risiedono sulla scheda per permettere di implementare algoritmi di crittografia. Normalmente, questa scheda si interfacciano con altri dispositivi per ricevere informazioni di tipo I/O, è la loro velocità raggiunge i 9600 bit/s.
Per rendere queste smart-card compatibili su tutti i sistemi, sono stati definiti alcuni standard definiti dall'ISO. Gli standard sono validi solo nel caso in cui le smart-card svolgono funzioni crittografiche, e definiscono il formato fisico, elettronico e logico. Il numero dello standard è 7816. La dimensione di memoria di queste smart-card varia intorno gli 8 Kbyte.

4.2 NTLM AUTHENTICATION

NTLM (NT LAN MANAGER) è protocollo di autenticazione che viene utilizzato e implementato in alcuni server distribuiti nella rete. A differenza di Kerberos NTLM ha delle caratteristiche diverse per autenticare un utente, infatti si è sviluppato in due versioni in cui alcune caratteristiche del programma sono state modificate. La differenza che sta tra la prima e la seconda versione è la lunghezza delle chiavi, infatti nella prima si utilizza una chiave a 56 bit, mentre nella seconda una chiave a 128 bit. Le caratteristiche che questi due versioni hanno in comune sono: la password non viene mai inviata e, che l'autenticazione avviene utilizzando la password elaborata in modo irreversibile ed uno schema challenge-response. NTLM sfrutta la conversione unicode dei caratteri, ogni carattere unicode è composto da 16 bit. L'algoritmo che viene utilizzato in questa tecnica cerca di bypassare alcuni programmi noti per la decodifica di messaggi (LC noto per decodificare le password).
Una volta ottenuto questo risultato, il messaggio viene sottoposto all'algoritmo MD4 che produce 16 byte finali. La password che viene utilizzata ha una lunghezza massima teorica di 128 bit, ma per limitazioni in Windows NT la lunghezza massima è di 14 caratteri. Questo protocollo può essere implementato su quasi tutte le versioni di Windows.
Il funzionamento di questo protocollo in http avviene mediante alcune fasi distinte, che sono:

1. Il client effettua una richiesta HTTP con una GET anonima al server;
2. Il server risponde con un HTTP 401 e include i metodi di autenticazione;
3. Il client richiede la pagina;
4. Il server risponde sempre con un HTTP 401 ed include un valore generato casualmente;

5. Il client a questo punto cifra un hash codificato con quello della password, e viene inviato al server sulla stessa connessione. A questo punto solo un utente con il giusto hash della password ed il valore della password può generare il nuovo hash.

6. Il server invia l'hash, username ed il valore del challenge, al domain controller, che controlla se il valore dell'utente è uguale a quello inviato dal server. Se i valori coincidono il domain controller autentica l'utente, e la pagina viene visualizzata.

4.3 LM (LAN MANAGER)

Questo protocollo utilizza l'algoritmo del DES, è la password non viene mai inviata durante l'autenticazione, ma i dati viaggiano in chiaro. Questo protocollo utilizza una parola chiave con una lunghezza fissa di 14 caratteri, se l'utente sceglie una parola chiave più corta allora, i caratteri mancanti vengono riempito con il valore di 0, se invece i caratteri utilizzati sono di più di 14 allora la password viene troncata al quattordicesimo carattere. Dopo aver definito la parola chiave, questa converte tutte le lettere minuscole in maiuscolo e la stringa ottenuta verrà divisa in 7 caratteri ciascuna.
Dalle due chiavi ottenute verrà aggiunto un bit di controllo, a questo punto le chiavi ad 8 byte verranno utilizzate all'interno dell'algoritmo DES. Nell'algoritmo DES viene utilizzata una costante per ricavare la password, questa è "0xAAD3B435B51404EE", dopo aver determinato la password i due blocchi vengono concatenati, e formano una password di 16 byte.
Infine, la password ricavata viene salvata all'interno del registro di configurazione. Questo protocollo può essere implementato nelle versioni Windows 2000/NT4.0/ 95/98.

4.4 ALTRI PROTOCOLLI DI AUTENTICAZIONE

Altri protocolli di autenticazione implementati nelle versioni di windows sono:

- ✓ EAP (Extensible Authentication Protocol): Questo è un estensione del protocollo PPP (Point-to-Point Protocol) ed è stato sviluppato per permettere l'autenticazione attraverso l'utilizzo di smart-card, token card e certificati digitali.

- ✓ CHAP (Challenge Handshake Authentication Protocol):La password non viene mai inviata e l'autenticazione avviene utilizzando la password elaborata con l'algoritmo di MD5 ed uno schema challenge response.

- ✓ MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) Questa è una versione proprietaria del protocollo CHAP è si divide in due versioni MS-CHAPv1 e MS-CHAPv2. Questa utilizza lo schema di autenticazione di LM e invia i dati utilizzando il protocollo MPPE, inoltre permette di cambiare le password se scadono durante la procedura. La differenza tra la prima e la seconda versione è che nella prima supporta l'autenticazione dal client verso il server mentre nella seconda, supporta la mutua autenticazione. Questo protocollo può essere implementato su tutte le versioni di Windows.

- ✓ SPAP (Shiva Password Autentication Protocol):Questa è una versione proprietaria del PAP e durante il processo di autenticazione la password viene inviata cifrata con un algoritmo reversibile. I dati vengono inviati in chiaro e non permette di modificare la password se questa scade nella procedura di autenticazione. Può essere implementato in tutte le versioni di Windows.

- ✓ PAP (Password Autentication Protocol): Questo protocollo è molto semplice invia sia i dati che la password in chiaro e non permette di modificare la password se scade durante l'autenticazione. Può essere implementato in tutte le versioni di Windows.

5 TECNICHE DI ATTACCO

Nel paragrafo precedente sono state descritte le tecniche necessarie per rendere incomprensibile le informazioni che viaggiano sulla rete. Ora verranno descritte le tecniche di attacco che vengono utilizzate, da coloro che vogliono alterare il contenuto delle informazioni che viaggiano nella rete.
Lo scopo principale degli attacchi che avvengono contro una rete o una organizzazione da parte degli attaccanti, è impadronirsi di un sistema per poi modificarne dei dati oppure reperire delle informazioni. Molte volte un utente può impadronirsi di un sistema utilizzando una tecnica denominata *Social Engineering* (quando un utente si spaccia per l'utente corretto). Un'altra tecnica è basata di indovinare username e password facendo dei tentativi.

Entrambe le tecniche non sono molto pericolose, anche perché molte volte non risulta facile indovinare una password. Pertanto esistono delle tecniche che possono causare dei veri disagi all'interno del sistema, alcune di queste sono: *Denial of Service*, *Spoofing*, *Sniffing* e altre.

5.1 DENIAL OF SERVICE

Un attacco di questo genere nega l'accesso ad un servizio presente in rete. Un attacco di questo genere crea uno stato di inefficienza del servizio che viene preso di mira, infatti, attacchi di questo genere utilizzano tecniche di flooding (inondazione) un attaccante spedisce ad un sistema o ad una rete una lunga sequenza di messaggi in modo da occupare interamente o quasi la CPU ed altre risorse del sistema. In questo modo, il sistema spende la maggior parte del tempo a rispondere ai messaggi, e non riesce a fornire il servizio che risiede su quella macchina a tutti gli utenti che si collegano. Gli attacchi di tipo flooding sono considerati poco interessanti per coloro che vogliono mettere in crisi un sistema, anche perché risultano troppo semplici.
I servizi che vengono colpiti da questi attacchi sono molte volte i siti di commercio elettronico, dove un attacco di questo genere rende il sito non più disponibile. Molte volte capita che situazioni di questo genere si verificano quando ad un sistema si collegano molti utenti (non malintenzionati) che richiedono un servizio, pertanto, i server non riescono a soddisfare tutte le richieste, e diventano non accessibili.

5.2 IP SPOOFING

La tecnica di spoofing consiste nella capacità di sostituirsi a qualcuno o a qualcosa. Le tecniche di spoofing possono avvenire in diversi modi, quali:

- *User Account spoofing:* In questo caso l'hacker utilizza la username e la password di un altro utente senza averne il diritto. Questi dati vengono reperiti mediante un'altra tecnica che vedremo in seguito (sniffing);

- *DNS Spoofing:* Questa tecnica prevede che l'hacker invia una risposta del DNS al Server presente nella rete della vittima, anche se alcune volte risulta difficile da effettuare.

- *IP Address spoofing:* Questo è l'attacco più diffuso, in quanto si basa sul fatto che la maggior parte dei routers all'interno di una rete controllano solamente l'indirizzo IP di destinazione e non quello sorgente. Questo attacco può avvenire mediante alcune fasi che sono:

    1. L'hacker cambia il proprio indirizzo IP in modo da farlo corrispondere all'indirizzo IP del client valido, in questo caso si parla di indirizzo spoofato.
    2. L'hacker poi costruisce un percorso con il server, in maniera tale da creare un collegamento diretto per fare in modo che i pacchetti viaggiano tra se ed il server;
    3. L'hacker utilizza il percorso di origine per inviare al server una richiesta del client;
    4. Il server accetta la richiesta dell'hacker come se questa provenisse dal client valido, e poi restituisce la risposta all'host dell'hacker;
    5. Ogni risposta alle richieste da parte del client valido viene inviata all'host del client.

- *IP Address spoofing e TCP:* Questo metodo fu quello che venne utilizzato da Kevin Mitnick contro Tsutomu Shimamura. Questa tecnica sfrutta il numero di sequenza del pacchetto per poter instaurare una connessione con il server, è avviene mediante alcune fasi:

    1. L'hacker apre diverse connessioni TCP per capire come viene generato il numero di sequenza TCP sull'host della vittima.
    2. L'hacker invia un pacchetto a B pretendendo di essere A ed imposta il flag SYN nel pacchetto.
    3. B a questo punto risponde ad A con un pacchetto di ACK e SYN. Ma A non può rispondere a B perché ha subito un attacco di flooding. Ora l'hacker deve riuscire a capire qual è la sequenza di quel pacchetto basandosi sulle considerazioni che ha fatto nel punto 1.
    4. Una volta capito il numero di sequenza l'hacker invia un pacchetto a B con il numero di sequenza indovinato. Se il valore del sequence number del TCP è giusto, allora incomincerà una comunicazione tra B e l'hacker.

    Molte volte gli hacker sfruttano dei debug del software. Questi debug possono essere:

        - Il programma più è complesso e più è la probabilità che si verificano errori;

- Alcuni programmatori inseriscono nella parte del codice del software alcune chiavi che, se vengono richiamate, il programma si comporta in una certa maniera (trapdoors).

5.3 ATTACCHI A SNIFFER

La tecnica che consente di leggere quando i pacchetti attraversano la rete, è packet sniffing. Se inviamo informazioni non cifrate in rete, lo sniffing è uno strumento di utilizzo immediato per la loro cattura. Coloro che utilizzano questo tipo di tecnica mirano sempre ad attaccare macchine che sono meno sicure.
Gli attacchi a sniffer passivo rappresentano il primo passo prima che un hacker esegua un attacco di tipo spoofing. Lo sniffing avviene mediante alcune fasi, ma prima di tutto l'hacker per entrare nella rete deve avere un ID e una password. Una volta che l'hacker ha i diritti per accedere in rete, allora, con l'utilizzo di un programma sniffer può raccogliere tutte le informazioni possibili sull'utente che desidera attaccare.
Un altro metodo per effettuare sniffing è quello che viene denominato attacco mascherato. In un attacco di questo genere l'hacker inizia la sessione inviando al server un pacchetto di sincronizzazione, utilizzando come IP di origine quello del client. A questo punto il server risponderà con una conferma, e l'hacker può cosi iniziare la comunicazione catturando le informazioni necessarie per poi effettuare un attacco spoofing. Una tecnica di questo genere ha comunque dei problemi che sono :

1. Se il client sostituito è attivo sulla rete riceverà il pacchetto di conferma dal server, e quindi risponderà con un pacchetto di reset per indicare che lui non ha effettuato nessuna connessione. Per evitare questo inconveniente, l'hacker utilizzerà un attacco di tipo denial of service sulla macchina del client in modo tale da permettergli di non rispondere;

2. L'hacker se non riesce ad effettuare un attacco di tipo denial of service non riuscirà ad instaurare nessun rapporto con il server, ma potrà ascoltare la conversazione con un programma di sniffer se i dati viaggiano in chiaro. Un vantaggio di cui può disporre l'hacker è :quando sia il client che l'hacker, condividono lo stesso canale di comunicazione, quindi se le informazioni passano prima dall'hacker allora, sarà semplice instaurare una connessione.

5.4 ATTACCHI A SESSIONE TELNET

Gli hacker possono intercettare anche le comunicazioni di rete che avvengono mediante sessioni Telnet. L'hacker prima di interferire nella sessione, osserva passivamente la trasmissione. Nel momento opportuno l'hacker invia una grande quantità di dati nulli al server con la sequenza (NOP=no operation), telnet interpreta questi dati come valore nullo e li rimuove dal canale. Ma la ricezione di questi dati, interrompe la comunicazione e genera una sessione desincronizzata, a questo punto l'hacker può entrare nella sessione spacciandosi come client.
Gli hacker possono utilizzare questo metodo solo se la sessione può trasportare dati nulli, ma anche se il server supporta la gestione di questi dati, non è un operazione semplice.

5.5 DIROTTAMENTO DEL PROTOCOLLO TCP (TCP HIJACK)

Questo attacco rappresenta la più grave minaccia per i server connessi a Internet. Questo attacco ottiene l'accesso alla rete costringendo alla rete stessa di essere accettato utilizzando il proprio IP come se fosse un indirizzo fidato, e quindi l'hacker non è costretto a provare indirizzi IP. L'obiettivo di questo attacco è sostituirsi ad un computer che si collega alla rete, e per fare questo, disconnette tale computer ed inganna il server. A questo punto l'hacker sostituisce IP del computer disconnesso con il suo, fatto questo il server risponderà esclusivamente all'hacker. Con un attacco simile l'hacker può impadronirsi di un intero sistema senza utilizzare password.

6 ARCHITETTURE PER RETI SICURE

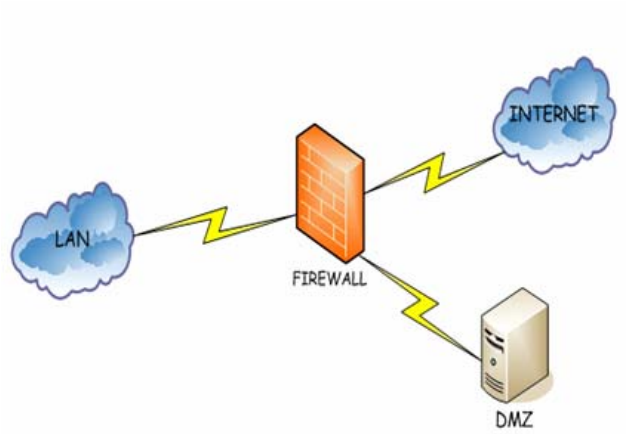
L'interesse che il pubblico ha dimostrato verso la rete internet ha stimolato il settore commerciale a fornire nuovi servizi per la vendita e la presentazione dei prodotti. Molti siti presenti in rete permettono l'acquisto di beni attraverso transazioni economiche. Oltre a siti di questo genere sono presenti anche siti che non vendono prodotti ma, che forniscono informazioni aziendali importanti e accesso completo a sistemi informativi. Il problema maggiore di queste tipologie di installazioni è impedire che persone non autorizzate possano accedere alla rete interna utilizzando tecniche che abbiamo già descritto. Per evitare che una rete interna possa essere attaccata da utenti estranei si ricorre all'utilizzo

di alcuni dispositivi hardware o software. Il dispositivo che viene utilizzato per risolvere questi problemi è il firewall oppure altre tecniche come proxy server, DMZ.

6.1 FIREWALL

Il firewall è un componente posizionato fra la rete locale e Internet e può essere sia un software che un dispositivo hardware. Il suo compito è impedire che persone non autorizzate possano accedere alla rete interna sfruttando debolezze delle strutture informatiche e telematiche. Il firewall si possono distinguere sostanzialmente in tre categorie: Application level Firewall, Packet Filter Firewall e Hardware Firewall.

FIREWALL:



6.1.1 APPLICATION LEVEL FIREWALL

Questo tipo di firewall gestisce il traffico a livello applicazione. Questo tipo di firewall si basa su delle regole prestabilite dall'utente e dal produttore, che personalizzano il software in base all'applicazioni che possono avere accesso alla macchina. A livello applicativo l'utilizzo di un firewall di questo genere può garantire delle ottime prestazioni su particolari attacchi, ma rallenta in maniera drastica il funzionamento della macchina in rete.
Firewall di questo genere vengono utilizzati generalmente da normali utenti che utilizzano Internt da casa oppure da un ufficio. Un fiewall di questo genera garantisce una sicurezza solo da un punto di vista applicativo ma, sicuramente non sono affidabili in reti LAN dove oltre a diminuire le prestazioni di una macchina, rendono la rete meno sicura, in quanto da parte di utenti estranei può essere facile entrare all'interno della rete. I più famosi personal firewall sono: Zone Alarm, Tiny Firewall, McAfee Firewall.

6.1.2 PACKET FILTER FIREWALL

Il packet filtering funziona sfruttando le informazioni di livello 3 e 4 del modello ISO OSI. I sistemi di packet filtering instradano in maniera selettiva i pacchetti tra host interni ed host esterni, vietando il transito a determinati pacchetti che vengono segnalati nella politica di sicurezza effettuata da un operatore specializzato. Generalmente i firewall che vengono utilizzati in queste applicazioni hanno anche funzionalità di routing. Il router utilizzato per queste funzionalità prende il nome di *screening router*.
Il firewall analizza ogni singolo pacchetto in transito ed estrae gli indirizzi di sorgente e destinazione oltre alla porta dove questi frame sono diretti. Una volta analizzati, questi pacchetti vengono messi in relazione con una tabella contenenti le sorgenti e le destinazioni che possono accedere al sistema. I pacchetti che rientrano nella politica adottata dal firewall vengono scartati,questo può avvenire scartando il pacchetto in modo silenzioso oppure generando una segnalazione di errore al mittente. E' consigliabile scartare in maniera silenziosa e fornire il minor numero possibile di informazioni alla rete esterna, per evitare che questi messaggi diventino dati preziosi per ulteriori strategie di attacco.
Il router è anche i grado di analizzare la parte dati di un pacchetto, assicurandosi che il pacchetto sia valido. Un router di questo genere mantiene traccia di una connessone memorizzando ad esempio: il numero di pacchetti trasmessi o ricevuti da un host oppure pacchetti che sono stati frammentati.
Le differenze che intercorrono tra un router normale e un screening router sono: che il router normale controlla semplicemente l'IP di destinazione di ogni pacchetto e seleziona il percorso ottimale per raggiungere la destinazione mentre, lo screening router analizza i pacchetti molto attentamente, decidendo se instradarli oppure scartarli. Router di questo genere ma che sono più sofisticati riescono anche a modificare il contenuto di un pacchetto per effettuare il NAT, riescono a spedire il pacchetto ad una destinazione diversa da quella prevista e possono anche modificare le tecniche di filtering. Dispositivi di filtering che tengono traccia delle connessioni e della storia del pacchetto prendono il nome di *stateful packet filter*.

Configurare un router di filtering non è un operazione semplice, in quanto bisogna personalizzare il router in base all'esigenze dell'azienda che dispone di una rete locale. L'amministratore che compie queste operazioni deve tener conto di alcuni fattori della rete su cui si vuole implementare un dispositivo di questo genere, infatti deve impostare il router in maniera tale da permettere ai pacchetti che viaggiano nella LAN di raggiungere la destinazione correttamente.
Se la rete interna utilizza Internet solamente per il WEB è opportuno bloccare porte che permettono l'accesso ad altri applicativi come : Telnet, FTP, SMTP e POP3.
I vantaggi che presenta un firewall di questo genere come si può intuire sono legati soprattutto a rendere la rete interna molto sicura, ma sono anche dispositivi che non comportano grandi spese economiche.
Gli svantaggi sono: che questi dispositivi non sono facili da configurare per via delle regole e delle complessità operative, inoltre alcune volte se vengono attivati servizi di posta o connessioni remote possono permettere ad alcuni hacker di attraversare il firewall.

6.1.3 FIREWALL HARDWARE

I firewall hardware sono implementati con la tecnica del packet filtering in quanto lavorano a livello Internet del protocollo TCP/IP. Possono anche essere di tipo Stateful Packet Inspection.
Ogni singolo pacchetto viene ricostruito e viene controllato in una tabella di stato dinamica, e se il pacchetto viene riconosciuto viene fatto passare direttamente, altrimenti viene inviato al security server di competenza che lo lascia passare solo se lo ritiene idoneo. Questo tecnica è quella che viene utilizzata maggiormente sui Firewall hardware anche perché garantisce degli ottimi risultati.

Dopo aver descritto i vari tipi di firewall, va fatta una considerazione sulle differenze che queste tipologie garantiscono, queste sono:

- Hardware

Viene utilizzato un sistema operativo specializzato, quindi con un set di istruzioni limitato e una bassa probabilità di buchi del sistema. Ma garantisce una maggiore efficienza sia nell'utilizzo che nei componenti che vengono utilizzati.

- Software

Un firewall di questo genere ha un numero maggiore di funzionalità ed è più semplice implementare, in quanto è portabile su tutti i sistemi operativi.

6.2 PROXY SERVER

La protezione a livello applicativo può essere eseguita anche con altri strumenti, ad esempio proxy server. Un dispositivo di questo genere viene utilizzato sia per ragioni di sicurezza che di performance, inoltre da alcuni analisti il proxy viene considerato come l'unico sistema di sicurezza oltre il livello 4.
I sistemi proxy si collocano, più o meno trasparentemente, tra una rete di client interni ed i server esterni esempio internet. Uno dei benefici che viene garantito dal proxy: l'utente utilizza la rete senza percepirne la presenza. Il proxy consente operazioni di caching è può registrare tutte le richieste all'interno di una memoria, inoltre, svolge anche tecniche di filtering e identifica tutti gli utenti che entrano nel sistema. Come è stato già detto un vantaggio del proxy server e nascondere gli indirizzi IP presenti nella rete interna attraverso il protocollo NAT. Un server proxy utilizza un sistema di tipo *DUAL-HOMED HOST* che sta ad indicare che quella macchina ha almeno due interfacce.

6.2.1 NAT (NETWORK ADDRESS TRANSLATION)

L'idea del NAT (*Network Address Translation)* è una tecnica descritta nel. L'utilizzo del NAT è basato sul fatto che, i computer presenti all'interno di una rete locale vengono interfacciati su internet mediante l'utilizzo di un server proxy a cui viene assegnato un indirizzo statico. Per svolgere questa operazione il server utilizza come protocollo il NAT, le funzionalità principali di questo protocollo sono: rendere trasparente all'esterno la topologia ed il numero di computer utilizzati. Utilizzando un sistema di questo genere si crea uno strato di protezione per la rete privata, rendendo la rete interna non accessibile dall'esterno.
Un router NAT gestisce un numero ridotto di indirizzi IP univoci, ma riesce a mascherare una grande quantità di computer presenti all'interno di una rete. Un router che utilizza un protocollo di questo genere può risultare estremamente utile quando si vuole implementare una VPN aziendale.

6.2.2 PAT (PORT ADDRESS TRANSLATION)

Mentre un router NAT può solo mascherare all'esterno una rete LAN, un router NAT/PAT è in grado di assegnare un a port. Un router di questo genere, viene utilizzato per dirigere le connessioni originate dall'esterno a connessioni che

sono dirette a nodi presenti nella rete locale. Per svolgere queste operazioni, il router PAT assegna un indirizzo statico a più computer presenti nella rete locale, pertanto la comunicazione essendo dedicata può avvenire tra più computer contemporaneamente, con sessioni e indirizzi diversi. Questa comunicazione avviene solo su determinate macchine, mentre per tutti gli altri computer collegati al router la comunicazione verso l'esterno avviene come se il router fose di tipo NAT.

6.3 BASTION HOST

Con il termine Bastion Host (computer bastione) si identifica un host connesso a un firewall di una rete nella quale la sicurezza riveste un'importanza strategica. Il Bastion Host generalmente si interpone tra la rete esterna (Internet) e il firewall presente nella rete locale, in questo modo è spesso soggetto ad attacchi essendo il primo dispositivo interfacciato sulla rete. Pertanto questo dispositivo viene configurato in modo da essere il primo e unico contatto tra rete privata e rete pubblica. Le caratteristiche di questo computer sono:

- Unico computer della rete raggiungibile da Internet;
- Numero minimo di servizi:
- Nessun account utente;
- Salvataggio e controllo dei log;
- Protezione dei file;

Queste sono le caratteristiche che rendono un bastion host il primo di una rete locale. Questo computer quando riceve attacchi da parte di utenti estranei risponde con dati fasulli
Esempio Se gli viene chiesto il tipo di sistema operativo, risponde con il nome di un sistema operativo differente da quello presente sulla macchina.

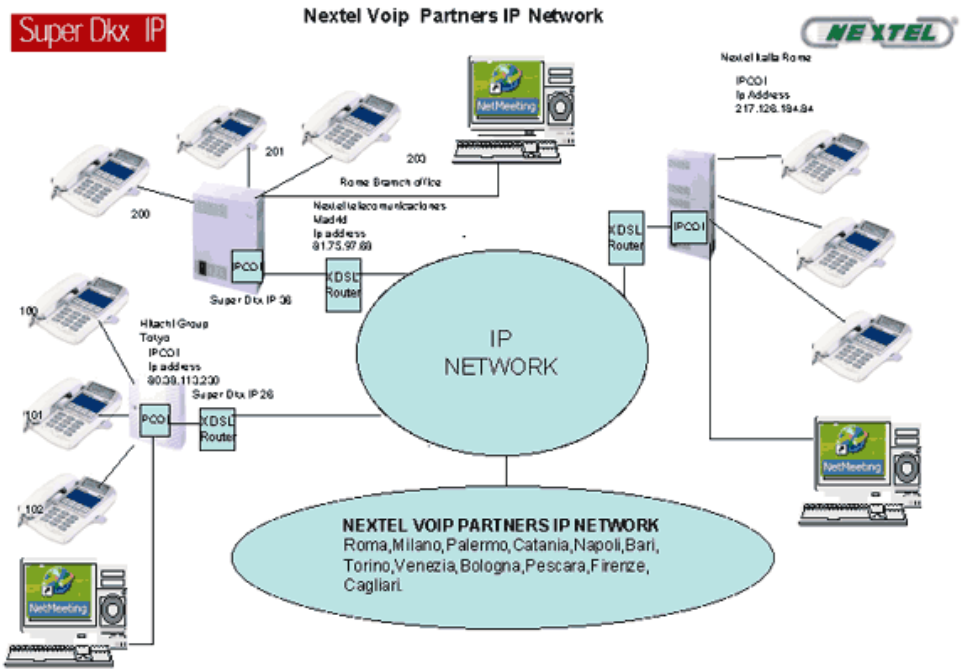
6.4 DMZ (DE-MILITARIZED ZONE)

Il termine DMZ che in italiano significa terra di nessuno indica una parte di rete locale destinata a fornire servizi all'esterno ad esempio: un web server o un server di posta presenti all'interno dell'azienda.
Pertanto essendo servizi che devono essere utilizzati anche da utenti esterni devono essere sottoposti a meno sicurezza, a differenza di come invece accade in una LAN. I nodi di rete della "Intranet" sono protetti da un firewall che impedisce l'accesso dall'esterno per motivi di sicurezza. I due server che invece devono consentire l'accesso esterno vengono collocati in un'area non protetta dal firewall o, più frequentemente, anch'essa protetta, ma con criteri diversi. Utilizzando un'architettura di questo genere, si aggiunge un ulteriore livello di sicurezza alla rete LAN.
Le regole del filtraggio dei pacchetti, realizzate grazie al pacchetto **iptables**, dovranno fare in modo che i pacchetti destinati alla porta TCP/80 del router siano indirizzati alla DMZ dove si trova Apache, andando a modificare le regole della tabella **NAT.**

7 SICUREZZA RETI VOIP

Negli ultimi anni una nuova tipologia di rete ha avuto larga diffusione nelle rete Internet, questo tipo di rete è chiamato VoIP (Voice over Internet Protocol) cioè "*Voce attraverso Internet*". Pertanto anche in queste reti bisogna implementare alcuni sistemi di sicurezza, ma prima di analizzare attentamente come queste strutture vengono rese sicure bisogna prima capirne il funzionamento e gli ambienti dove questi sistemi vengono usati.

FUNZIONAMENTO VoIP:
(Immagine scaricata da Internet)



7.1 VoIP (Voice over Internet Protocol)

La nuova tecnologia del networking ha reso le infrastrutture delle reti aziendali sempre più veloci, sicure ed affidabili. Questo sviluppo verso la fine degli anni 90 ha portato la diffusione a livello mondiale di una rete che oltre a veicolare i dati tra computer, potesse anche trasferire la voce delle normale telefonate.
L'impatto delle VoIP ha causato un vero e proprio crollo delle tariffe della telefonia di rete fissa, infatti la rete internet permette di chiamare solo con il costo di una connessione. Anche se il trasferimento della voce su IP avviene con una qualità di segnale più bassa di quella che avviene normalmente nelle rete tradizionale, il vantaggio che viene offerto da una rete di questo genere è: effettuare una telefonata in qualsiasi parte del mondo al costo molto basso.
Ovviamente la voce non può essere indirizzata come avviene normalmente nelle linee telefoniche, che trasportano il segnale in maniera completamente diversa, ma utilizzando dei pacchetti che viaggiano in rete mediante un indirizzo univoco. Quindi, bisogna trasformare il segnale analogico tipico di una normale telefonata in una serie di pacchetti che siano facilmente trasportabili in rete, la struttura di questi pacchetti deve essere particolarmente affidabile e molto veloce in quanto la telefonata non deve essere spezzettata. Per garantire una telefonata di questo genere bisogna fissare una priorità molto alta sul contenuto del pacchetto e questo avviene mediante politiche di Quality Of Service.La trasformazione da segnale telefonico a flusso di pacchetti dati può avvenire in diverse maniere.
Una soluzione per questo problema è utilizzare un centralino telefonico. All'interno di un'azienda che utilizza un servizio di tipo VoIP è utile installare un centralino telefonico, in quanto un dispositivo di questo genere di nuova generazione è dotato di schede IP che permettono ai centralini stessi di convogliare le chiamate sulla rete, evitando in questa maniera di utilizzare un altro dispositivo presente nella rete. Ma bisogna garantire che la struttura di rete sulla quale verrà instradato il traffico IP generato dai centralini garantisca una qualità di collegamento sufficiente ad ottenere una buona comunicazione.
Un secondo modo per trasformare il segnale in pacchetti è di utilizzare un router. Per svolgere operazioni di questo genere il router deve essere dotato di un collegamento al vecchio centralino, realizzato con le normali linee telefoniche e di un dispositivo di conversione analogico-digitale.
Le chiamate VoIP possono avvenire in diversi modi sia da PC collegati in rete, che da telefoni tradizionali collegati con PC. Sotto vengono proposte le tipologie di chiamate che si possono effettuare.

7.2 TELEFONATA TRA PC E TELEFONO TRADIZIONALE

Il servizio di VoIP non viene solo utilizzato per effettuare chiamate tra due PC collegati in rete (vedremo in seguito), ma anche tra un computer e un telefono tradizionale, utilizzando la rete internet per veicolare i dati.
Per permettere un collegamento di questo tipo, bisogna utilizzare i dispositivi che abbiamo elencato precedentemente cioè un router e un centralino per permettere la conversione del segnale e dei pacchetti dati. Pertanto i due apparati devono essere collegati in modo che il centralino passi al router le telefonate destinate alla sede remota, collegata via

link dati, e viceversa il router passi al centralino le chiamate in arrivo dalla linea dati e dirette verso un'interna. Il collegamento tra questi due dispositivi può avvenire in diversi modi, che vanno dal normale collegamento analogico che può supportare una sola chiamate per volta, fino a collegamenti di tipo "E1" in grado di gestire 32 chiamate contemporaneamente. Con una configurazione di questo genere il centralino deve preoccuparsi di gestire le chiamate fra i vari telefoni interni e passare il resto delle chiamate verso il router per inoltrarle verso l'esterno. Generalmente una configurazione di questo genere viene utilizzata all'interno di una rete locale dove tutti i telefoni vengono prima collegati al centralino, e poi successivamente con un link, le chiamate vengono instradate verso l'esterno mediante il router. Ma tale configurazione la si può anche immaginare nella rete Internet dove un utente può fare una chiamata da un computer ad un telefono fisso. Quindi attraverso la rete viene instradata la chiamata dati fino alla centrale più vicina (se presente) alla persona che vogliamo chiamare, pagando poco più di una chiamata urbana raggiungendo qualsiasi parte del mondo.

7.3 TELEFONATA TRA TELEFONO FISSO E TELEFONO FISSO

In Italia da Maggio, è attivo anche il servizio di effettuare le chiamate via Internet utilizzando solamente telefoni fissi. La chiamata avviene da un telefono tradizionale, dove il suo segnale viene convertito con un adattatore telefonico (ATA) che sostituisce il PC e instrada la chiamata su Internet, dove verrà ricevuto da un altro adattatore (ATA) o da un pc che avrà il compito di riconvertire il segnale. Ovviamente i costi per utilizzare un servizio di questo genere sono ancora da definire anche perché bisogna considerare il costo dell'hardware da utilizzare.

7.4 TELEFONATA TRA PC E PC

Come è stato già accennato nel paragrafo precedente, il VoIP viene principalmente utilizzato per effettuare chiamate via Internet tra PC, al solo costo di una connessione. Tutto questo, avviene grazie a l'utilizzo di un software gratuito installato sulle macchine che vogliono effettuare le chiamate. Una delle più famose compagnie al mondo a realizzare comunicazioni VoIP è Skype, quest'azienda utilizza un software peer-to-peer, che diventa attivo solo dopo un' iscrizione al sito, per indicare ad altri utenti che abbiamo installato questo software (ovviamente la macchina su cui viene installato il software deve essere dotata di casse e microfono).
In futuro si prevede di eliminare totalmente la componente di telefonia tradizionale dalla struttura del sistema telefonico. Utilizzando una struttura di questo genere non si effettuerà più una conversione di segnale analogico in pacchetti dati, ma si genereranno automaticamente i pacchetti. Utilizzando un sistema di questo genere i dati verranno instradati non più con i centralini, ma utilizzando strutture di routing. Con l'utilizzo di un sistema simile sarà possibile garantire anche servizi di video chiamata, segreteria e altre funzioni che vengono offerte dai telefoni tradizionali. Sempre in futuro sarà possibile chiamare ad un altro computer selezionando il nome dell'utente presente all'interno della rubrica di Outlook. Utilizzando un palmare connesso ad un servizio wi-fi, l'internet senza fili; possiamo telefonare come se avessimo in mano un cellulare, ma con i vantaggi del VoIP.

7.5 SICUREZZA RETI VOIP

Come accade nelle nuove tecnologie, la VoIP introduce sia dei vantaggi che dei rischi legati alla sicurezza della rete. Ma, a volte implementare sistemi di sicurezza all'interno di queste reti possono causare un marcato deterioramento della QoS, per effetto dei ritardi o dei blocchi prodotti dai firewall o dai messaggi cifrati.
I protocolli che gestiscono il flusso dei dati nelle reti VoIP sono H.323 e il SIP (ci sono standard che vengono aggiunti al SIP come MGCP, IAX2). Questi standard possono essere utilizzati anche per velocizzare la trasmissione dei messaggi tra i gateway e altri dispositivi nel caso in cui ci sono componenti che rallentano la comunicazione. La sicurezza delle VoIP nelle reti LAN è essenziale, in quanto qualsiasi utente con opportuni tools può ascoltare le conversazioni che avvengono all'interno della rete stessa. Per evitare un inconveniente di questo genere è opportuno cifrare le chiamate che avvengono sia all'interno della LAN che quelle sulla rete Internet.
Mentre nelle reti internet l'utilizzo dei firewall è indispensabile questo non avviene per le reti VoIP, infatti l'utilizzo di un firewall all'interno di una rete di questo genere complica notevolmente le cose, soprattutto nelle procedure di setup delle chiamate. Pertanto è opportuno utilizzare firewall SIP-aware in grado di tracciare lo stato delle connessioni e di respingere i pacchetti che non fanno parte della chiamata originaria. Come i firewall anche il NAT rappresenta un ostacolo per le reti di tipo VoIP, infatti per coloro che vogliono effettuare più chiamate contemporaneamente all'interno di una rete locale verso l'esterno, non possono farlo, perché tutti gli utenti vengono interfacciati all'esterno con lo stesso numero. Delle soluzioni per risolvere gli inconvenienti presenti all'interno delle reti possono essere:

- ✓ Separare i pacchetti che vengono generati dalla chiamate a quelli che invece vengono semplicemente inviati dai computer;

- ✓ Usare IPSec o Secure Shell (SSH) per tutta la gestione remota, e utilizzare firewall che garantiscono migliori risultati nelle reti VoIP;

Comunque i sistemi di sicurezza che vengono implementati nelle reti, dipendono sempre da come la rete è strutturata. Nel prossimo futuro tutti i sistemi telefonici baseranno il proprio funzionamento su tecniche di questo genere, rendendo sempre maggiore l'integrazione tra telefono e computer.

8 ASPETTI LEGALI

- Violenza sulle cose (art. 1.1 - aggiunge il seguente comma dopo il secondo comma art. 392 C.P.): Si ha, altresì, violenza sulle cose allorchè un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.

- Attentato a impianti di pubblica utilità (art. 2.1 - sostituisce art. 420 C.P.): Chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.
  Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni.

- Accesso abusivo ad un sistema informatico o telematico (art. 4.1 - aggiunge articoli dopo art. 615-bis C.P.):
  [art. 615-ter] Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

  La pena è della reclusione da uno a cinque anni:

  1. Se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema. Qualora i fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Si procede a querela della persona offesa.

  2. Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato. Qualora i fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Si procede d'ufficio.

  3. Se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Si procede d'ufficio.

- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico:
  [art. 615-quinquies] Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.Da notare che il DPR 318 del 28 Luglio 1999 prevede:

  "Art. 4 - Codici identificativi e protezione degli elaboratori

  c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale."

  Ma non è tutto visto che, in base all'art. 2050 cc: "chi cagiona danno ad altri per effetto del trattamento dei dati

personali è tenuto al risarcimento del danno se non prova di avere adottato tutte le misure idonee a evitare il danno".

- Corrispondenza (art. 5.1 - sostituisce quarto comma art. 616 C.P.): per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 6.1 - inserisce dopo l'articolo 617-ter C.P.):
  [art. 617-quater] Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

  Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

  I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

  Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

  1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
  2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
  3. da chi esercita anche abusivamente la professione di investigatore privato.

- Danneggiamento di sistemi informatici e telematici (art. 9.1 - aggiunge articolo dopo l'art. 635 C.P.):
  [art. 635 bis] Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, é punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

  Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

- Frode informatica (art. 10.1 - aggiunge articolo dopo l'art. 640-bis del C.P.):
  [art. 640-ter] Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.
  La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante .

- Intercettazioni di comunicazioni informatiche o telematiche (art. 11.1 - aggiunge articolo dopo l'art. 266 C.P.):
  [art. 266-bis] 1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonchè a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.

SITOGRAFIA

WWW.AMAGRI.IT