VPN

e Sicurezza:

IPSec

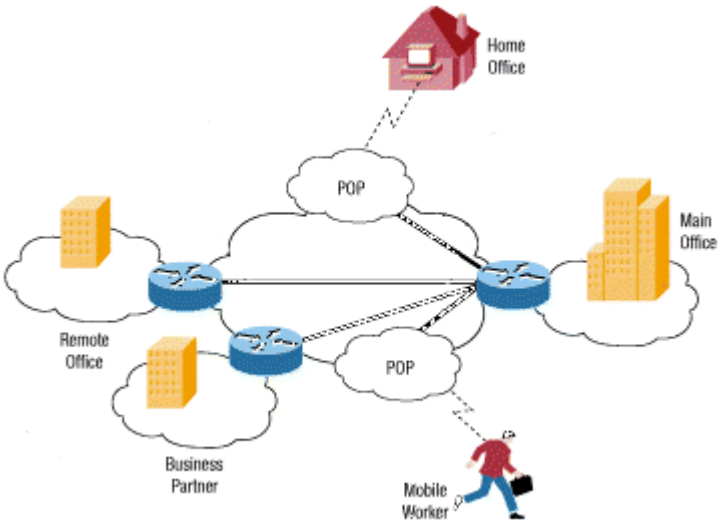
Tesina di:

Claudio Alberto Pisapia

Emanuel Weitschek

Indice

Molte compagnie hanno il bisogno di espandersi sia nel proprio paese che nel resto del mondo. Quello che le accomuna è la necessità di mantenere una veloce e sicura comunicazione tra i loro uffici. Questo fino a poco tempo fa voleva dire usare linee telefoniche dedicate per mantenere in contatto una vasta rete (WAN). Sicuramente una rete WAN ha dei vantaggi rispetto a una rete come Internet, sia a livello di prestazioni che a livello di sicurezza. Ma mantenere una WAN, specialmente quando si usano linee dedicate, significa anche una costo di mantenimento notevole e incrementale man mano che l'azienda si espande con i propri uffici all'estero. Ma con la crescita e lo sviluppo di Internet, il business delle aziende si è orientato insieme a lui. Prima con l'avvento di intranet, siti progettati solamente per gli impiegati dell'azienda e protetti da password che risiedevano su server locale. Ora, molte compagnie si sono orientate e stanno creando le proprie VPN (virtual private network), ovvero reti virtuali private per poter collegare le varie sedi e i vari impiegati situati in tutto il mondo.

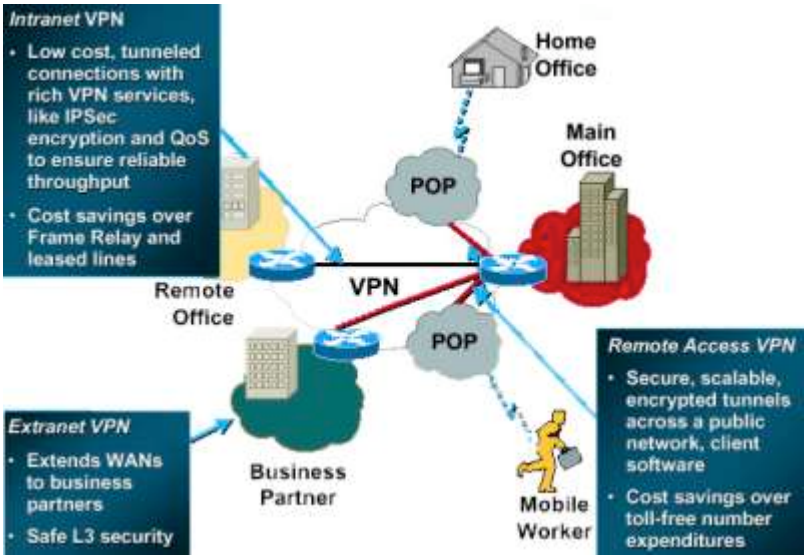


Alla base una VPN è una rete riservata che usa una rete pubblica (solitamente Internet) per collegare insieme i luoghi o gli utenti a distanza. Invece di usare un collegamento dedicato, una VPN usa i collegamenti “virtuali” attraverso Internet, dalla rete riservata dell’azienda al luogo o all’impiegato a distanza.

Che caratteristiche sono necessarie in un VPN ben progettato? Dovrebbe incorporare:

- Sicurezza
- Affidabilità
- Amministrazione di rete
- Amministrazione di politica

Esistono due tipi di VPN. Quella ad accesso remoto, chiamata anche VPDN(**virtual private dial-up network**), del tipo user-to-LAN, ovvero l’impiegato si connette tramite una postazione remota alla rete private aziendale. Comunque un’azienda che desidera installare un accesso remoto in larga scala si può appoggiare ad un fornitore di questo tipo di servizio (ESP: enterprise service provider). L’ESP installa un assistente di accesso di rete (NAS) e fornisce agli utenti a distanza un software per poter collegare i propri calcolatori,chiamando un numero gratuito, al NAS per poi collegarsi alla VPN aziendale.



VPN Security:

Una VPN ben progettata usa parecchi metodi per mantenere i collegamenti e i dati sicuri:

- Firewall
- AAA Server
- Crittografia
- IPSec

Rapida considerazione sul Firewall:

Il firewall è una forte barriera tra la rete privata e Internet. Un firewall serve a restringere il numero delle porte aperte (causa di possibili attacchi esterni), il tipo di pacchetti e i protocolli permessi.

VPN Security: AAA Server

AAA (autehntication, authorization and accounting) server sono utilizzate per una maggiore sicurezza durante una sessione di accesso remoto ad una VPN. Quando viene effettuata una richiesta da parte di un cliente per stabilire una sessione via linea telefonica (dial-up), la richiesta è passata all'AAA server. L'AAA controlla:

- Chi è l'utente (authentication)
- Quali sono i permessi dell'utente (authorizaton)
- Cosa realmente fa l'utente (accounting)

L'AAA Server utilizza come protocollo di sicurezza l'SSL (Secure Socket Layer protocol), il quale provvede a garantire tre funzionalità fondamentali:

1) Privatezza del collegamento: La crittografia è usata dopo un handshake iniziale per definire una chiave segreta. Per crittografare i dati è usata la crittografia simmetrica.

2) Autenticazione: Durante la fase di autenticazione l'identità nelle connessioni può essere autenticata usando la crittografia asimmetrica, o a chiave pubblica, in modo che i clienti sono sicuri di comunicare con il corretto server.

3) Affidabilità: il livello di trasporto include un check dell'integrità del messaggio basato su un apposito MAC (Message Authentication Code) che utilizza funzioni hash sicure (es. SHA,MD5). In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

SSL:

L'SSL procede sui messaggi da trasmettere nel modo seguente: li frammenta in blocchi adeguati, eventualmente comprime i dati, applica un MAC (Message Authentication Code), crittografa e infine trasmette il risultato. I dati ricevuti, viceversa, sono messi in chiaro, verificati, compattati e riassemblati e, quindi, consegnati ai client.

VPN Security: Encryption

I dati inviati da un calcolatore ad un altro vengono inviati in una forma che soltanto l'altro calcolatore potrà decodificare. La maggior parte dei sistemi di crittografia del calcolatore appartengono a due categorie:

- Crittografia a chiave simmetrica
- Crittografia a chiave pubblica

Nella crittografia a chiave simmetrica, ogni calcolatore ha una chiave segreta (codice) che usa per crittare un pacchetto di informazioni prima che sia trasmesso sulla rete ad un altro calcolatore. Nella crittografia a chiave simmetrica è essenziale che la stessa chiave sia conosciuta su ogni computer per decodificare il messaggio. L'uso della chiave simmetrica richiede di sapere quali calcolatori comunicano in modo da poter istallare la chiave su ogni calcolatore. Viene creato un messaggio codificato con la chiave simmetrica, poi viene

crittata la chiave simmetrica con la chiave pubblica del computer destinatario. Il destinatario userà la chiave privata per decodificare la chiave simmetrica, poi userà la chiave simmetrica per decodificare il messaggio.

Nella crittografia a chiave pubblica viene utilizzata una combinazione di chiavi pubbliche e private. La chiave privata è conosciuta solo dal computer destinatario, mentre la chiave pubblica viene resa nota a tutti gli altri computer che vogliono comunicare in sicurezza con il computer destinatario. Per decodificare un messaggio, bisogna usare la chiave pubblica del computer a cui volgiamo mandare il nostro messaggio. Quando riceverà il messaggio, il destinatario userà la propria chiave privata per decodificarlo. Per fare questo viene utilizzato il PGP (Pretty Good Privacy).

IPsec

Cos'è l'IPsec?

IPsec è l'abbreviazione per IP Security una collezione di protocolli implementati da IETF (Internet Engineering Task Force), l'organizzazione principale che crea gli standard su Internet, per supportare scambi di informazioni sicuri al livello IP (Internet Protocol). IPsec è stato sviluppato ampiamente per implementare reti private virtuali (VPN), reti che sono costruite usando infrastrutture pubbliche per connettere nodi privati, per esempio esistono tanti sistemi che permettono di creare una rete geografica servendosi di Internet per il trasporto dei dati. Questi sistemi usano meccanismi di crittografia e di sicurezza per assicurare l'accesso ai soli utenti autorizzati e per evitare l'intercettazione dei dati.

L'IPsec supporta due metodi di crittografia: Transport e Tunnel. Il metodo Transport cifra solo la porzione dei dati (payload) di ogni pacchetto e lascia intatta l'intestazione (header).

Il metodo più sicuro Tunnel cifra entrambi l'header e la payload. Dalla parte del ricevente, un apparecchio compatibile con Ipsec decifra ogni pacchetto.

Per permettere il funzionamento di Ipsec, gli apparati di trasmissione e ricezione devono condividere una chiave pubblica. Ciò è portato a termine da un protocollo conosciuto come Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), che permette al ricevitore di ottenere una chiave pubblica e di autenticarsi al trasmettitore usando un certificato digitale.

Com'è nato l'IPsec?

IETF sapeva che in Internet la sicurezza lasciava a desiderare, renderla sicura non era semplice: non si sapeva dove aggiungere sicurezza. Si riteneva che la soluzione migliore fosse stata l'aggiunta della cifratura e dei controlli di integrità da capo a capo. In questo modo la sorgente di trasmissione cifra e protegge l'integrità dei dati e il processo di ricezione effettua la decifrazione e la verifica d'integrità. Ogni manipolazione dei dati fra i due comunicanti può essere rilevata. Il problema di questo approccio è che richiede la modifica di tutte le applicazioni correnti per poterle usare. Per questo si è preferito mettere la sicurezza allo strato di trasporto o in un nuovo strato intermedio fra lo strato applicativo e quello di trasporto. Anche così si ottiene una sicurezza da capo a capo, ma senza cambiare le applicazioni. Autenticare e/o cifrare i pacchetti è compito dello strato network. Questa filosofia ha raggiunto consensi fino alla definizione di un vero e proprio standard, IPsec. IPsec è descritto principalmente negli RFC (request for comments, i rapporti tecnici dell'IETF) 2401, 2402, 2406. La cifratura può anche essere evitata (per alleggerire i calcoli computazionali) utilizzando un algoritmo nullo che è descritto nell'RFC 2410.

Cosa offre l'IPsec?

IPsec definisce un'infrastruttura per fornire molteplici servizi, algoritmi e granularità. Caratteristica dell'IPsec è che molti servizi sono resi disponibili su richiesta, ciò per evitare di rendere disponibili funzionalità non necessarie a tutti che appesantirebbero soltanto i calcoli computazionali. I servizi principali sono: la segretezza, l'integrità dei dati e la protezione dagli attacchi di tipo ripetizione (dove il crittoanalista invia di nuovo un vecchio messaggio). Tutti questi servizi sono basati sulla crittografia a chiave simmetrica, in quanto la velocità è cruciale (si pensi soltanto alla trasmissione di flussi multimediali, telefonia ip...).

IPsec è aperto a molteplici algoritmi, questa possibilità è data dal fatto che un algoritmo che oggi crediamo sicuro potrebbe essere forzato in futuro. IPsec è indipendente dall'algoritmo, così l'infrastruttura può sopravvivere anche se un particolare algoritmo viene forzato. L'algoritmo di cifratura attuale usato per la maggiore è il DES. Sono previste varie granularità per proteggere una singola connessione, come tutto il traffico fra due host, oppure il traffico fra due router sicuri.

Come funziona l'IPsec?

IPsec è orientato alla connessione, anche se si trova allo strato Ip. Per avere una qualche forma di sicurezza bisogna stabilire una chiave da usare per un certo periodo di tempo. Questa chiave è essenzialmente una sorta di connessione. Le connessione distribuiscono i costi dell'inizializzazione su una serie di pacchetti. Nel contesto dell'IPsec una connessione è chiamata SA (Security Association). Una SA è una connessione simplex (solo invio o solo ricezione) fra due estremi e ha un identificatore di sicurezza associato. Per effettuare un traffico sicuro nelle due direzioni (invio – ricezione) sono necessarie due SA. Gli identificatori di sicurezza sono trasportati da pacchetti che viaggiano su queste connessioni sicure e vengono usati per la ricerca delle chiavi e di altre informazioni

rilevanti (come la dimensione della chiave, l'algoritmo usato...). Le specifiche tecniche di IPsec contengono due parti principali. La prima parte descrive due intestazioni che possono essere aggiunte ai pacchetti per contenere l'identificatore di sicurezza, i dati di controllo dell'integrità e altre informazioni. L'altra parte, ISAKMP (Internet Security Association and Key Management Protocol) riguarda lo scambio delle chiavi. ISAKMP è estremamente complesso e contiene degli errori molto gravi nel suo protocollo principale IKE e quindi deve essere rimpiazzato.

IPsec può essere usato in due modalità.

Modalità trasporto:

Nella **modalità trasporto (Transport)** l'intestazione IPsec viene inserita subito dopo quella dell'IP. Il campo *Protocol* nell'intestazione IP viene cambiato in modo da indicare che un'intestazione IPsec segue quella solita dell'IP. L'intestazione IPsec contiene le informazioni di sicurezza: l'identificatore SA, un nuovo numero di sequenza, eventualmente un controllo di integrità del campo payload.

La modalità trasporto non cambia di molto la lunghezza del pacchetto. Aggiunge un intestazione al pacchetto IP detta AH (Authentication Header). AH garantisce il controllo dell'integrità e la sicurezza contro gli attacchi di ricezione, ma non la segretezza (cioè la cifratura).

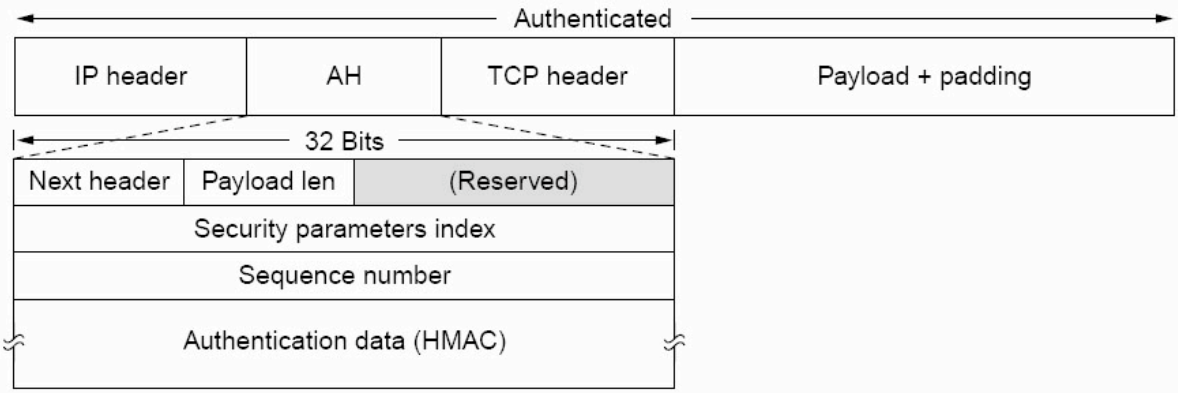


Fig. 8-27. The IPsec authentication header in transport mode for IPv4.

AH viene messo fra l'intestazione IP e l'intestazione TCP. Il campo *payload* può essere riempito fino a raggiungere una particolare lunghezza per facilitare l'algoritmo di autenticazione. Il campo *Next header field* serve per memorizzare il valore originale che aveva il campo IP *Protocol* prima di essere rimpiazzato con il valore 51. Quest'ultimo è usato per indicare che segue un'intestazione AH. Il campo *Payload length* contiene il numero di word a 32 bit nell'intestazione AH meno 2. Il *Security parameter index* è l'identificatore della connessione, inserito dal mittente per indicare un particolare record nel database del ricevente. Questo record contiene la chiave condivisa usata per questa connessione e altre informazioni sulla connessione. *Sequence number* viene usato per attribuire un numero a tutti i pacchetti inviati in un SA. A ogni pacchetto viene attribuito un numero univoco, incluse le ritrasmissioni (ciò per evitare attacchi di tipo ripetizione). Questi numeri di sequenza non vengono utilizzati in circolo: se vengono usate tutte le 2^{32} possibili combinazioni, si dovrà instaurare un nuovo SA. *Authentication data*, è un campo a lunghezza variabile che contiene la firma digitale del payload. L'algoritmo di firma elettronica da utilizzare è negoziato quando viene stabilito l'SA. Questo stadio non usa la crittografia a chiave pubblica, perché i pacchetti devono essere elaborati in modo rapido, mentre tutti gli algoritmi a chiave pubblica sono troppo lenti. Per questo IPsec è basato

sulla crittografia a chiave simmetrica. Il mittente e il destinatario stabiliscono una chiave comune prima d'instaurare la SA, che viene usata nel calcolo della firma. Ovviamente la chiave condivisa non viene trasmessa.

L'intestazione AH non permette la cifratura dei dati, quindi è utile solo quando è necessario un controllo di integrità dei dati. Ciò è particolarmente efficace per evitare ad un intruso di falsificare l'origine del pacchetto, in quanto AH controlla anche alcuni campi dell'intestazione IP, come l'indirizzo della sorgente.

Modalità tunnel:

Nella **modalità tunnel** l'intero pacchetto IP, compresa l'intestazione, viene incapsulato nel corpo di un nuovo pacchetto IP con un'intestazione IP completamente diversa. La modalità tunnel è utile quando il tunnel arriva in un posto diverso dalla sua destinazione finale. Il tunnel di solito arriva a una macchina con un gateway sicuro, per esempio il firewall dell'azienda. Facendo terminare il tunnel su questa macchina sicura, il pacchetto viene mandato in chiaro al destinatario sulla LAN dell'azienda. Il firewall si occupa di decifrare il messaggio. La modalità tunnel è utile anche nella situazione in cui si vuole aggregare un'insieme di connessioni TCP, per poi gestirle come un unico flusso cifrato. In questo modo si evita che un intruso possa avere informazioni sul traffico: per esempio chi sta mandando dei pacchetti, a chi li sta mandando e quanti ne sta inviando. (Analisi del traffico).

Caso di esempio:

- ci troviamo durante una crisi militare
- il traffico fra il Pentagono e la Casa Bianca diminuisce di colpo
- allo stesso tempo il traffico fra il Pentagono e alcune basi militari nelle Montagne Rocciose aumenta
- un intruso potrebbe trarre delle informazioni utili da questi dati (analisi del traffico)

La modalità tunnel aggira parzialmente questo tipo di analisi. Lo svantaggio è dato dal fatto che, aggiungendo ulteriori intestazioni IP, aumenta la dimensione del pacchetto in modo sostanziale.

L'intestazione IPsec più utilizzata sia nella modalità trasporto che nella modalità tunnel è **ESP** (Encapsulating Security Payload).

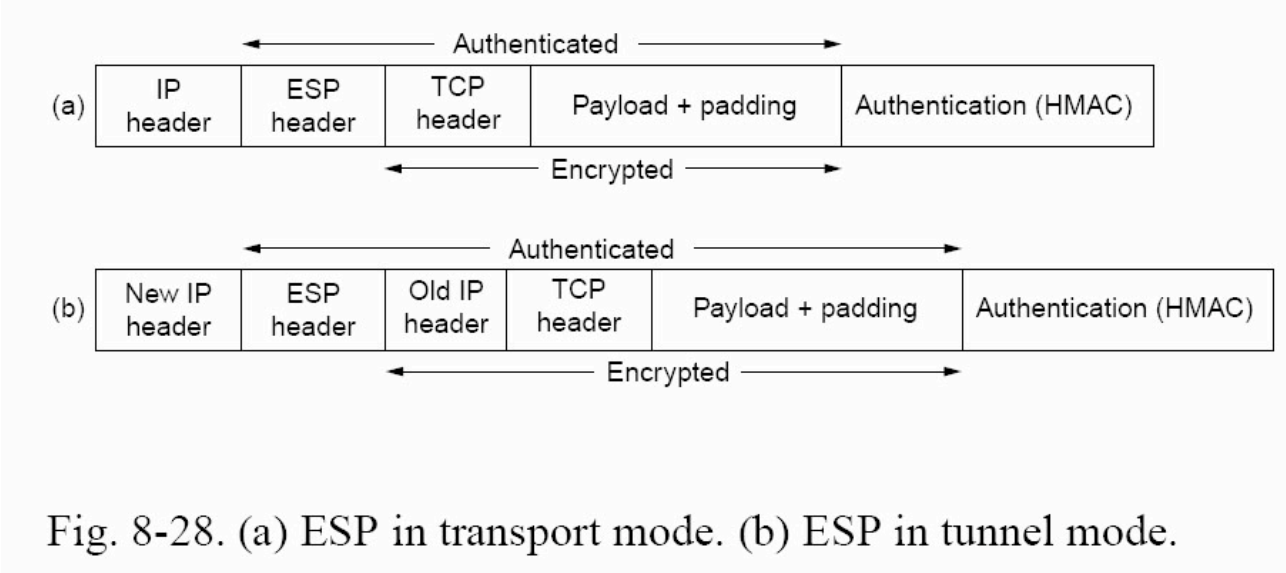


Fig. 8-28. (a) ESP in transport mode. (b) ESP in tunnel mode.

L'intestazione ESP consiste di due word a 32 bit, che costituiscono i campi *security parameters index* e *sequence number*, con funzioni analoghe a quanto abbiamo discusso per AH (identificatore della connessione, numerazione univoca di tutti i pacchetti). L'*initialization vector* è un terza word, usata per la cifratura dei dati. ESP fornisce un controllo d'integrità dei dati come AH, ma non lo include nell'intestazione, lo aggiunge in coda al campo payload (ciò ha vantaggi a livello hardware). ESP ha delle funzioni aggiuntive rispetto a AH ed è anche più efficiente. L'unico svantaggio di ESP è che non controlla l'intestazione IP. Ma vantaggi come l'efficienza e la cifratura ne hanno avvantaggiato la sua diffusione. AH verrà probabilmente eliminato in futuro.

L'inizializzazione di IPSEC e lo scambio delle chiavi sono detti **IKE** (Internet Key Exchange). IKE si basa sull'ISAKMP (Internet Security Association and Key Management Protocol). Gli scopi di IKE sono autenticare i due interlocutori e stabilire i protocolli e le

chiavi segrete da utilizzare per trasferire i dati. I due interlocutori si scambiano per prima cosa la lista degli algoritmi crittografici da usare. Se le due liste coincidono l'iniziatore manda i parametri di Diffie-Hellman. Il ricevente risponde con i propri parametri di DiffieHellman. Sostanzialmente l'iniziatore manda la chiave simmetrica usata per il vero scambio dei dati cifrata con la chiave pubblica del destinatario e con la propria chiave privata. Il ricevente decifra la chiave con la propria chiave privata e ne verifica la provenienza con la chiave pubblica del mittente. D'ora in avanti i due possono quindi comunicare scambiandosi i dati cifrati.

Quali sono i suoi vantaggi/svantaggi?

IPsec è il miglior protocollo di sicurezza IP disponibile al momento. Il suo punto debole è però la sua complessità. IPsec contiene troppe opzioni e lascia troppa flessibilità al suo utilizzatore, mette a disposizione vari metodi per ottenere lo stesso risultato. Questa complessità addizionale ha un effetto devastante sugli standard di sicurezza.

La trappola della complessità

Il nemico peggiore della sicurezza è la complessità. Fallimenti semplici sono semplici da evitare e spesso anche semplici da gestire. Con la complessità invece non si sa come comportarsi. Sistemi complessi mostrano di solito più fallimenti. La complessità non solo rende impossibile la creazione di un sistema sicuro, ma rende il sistema difficile da gestire. IPsec è troppo complesso per essere sicuro. Il progetto chiaramente cerca di supportare differenti situazioni con opzioni diverse. Ciò lo rende estremamente complicato. Anche la documentazione è difficile da capire. IPsec ha due modi operativi: AH e ESP. AH offre l'autenticazione, ESP l'autenticazione, la cifratura o entrambi. Quindi esistono 4 diversi modi per due macchine che vogliono comunicare tra loro usando l'IPsec: transport/AH,

tunnel/AH, transport/ESP, tunnel/ESP. Principalmente le funzionalità della modalità tunnel sono un sovrainsieme delle funzionalità della modalità transport. L'unico vantaggio di transport è la dimensione minore del pacchetto. Con l'attuale sviluppo della banda larga si potrebbe eliminare del tutto la modalità transport. Lo stesso discorso vale per ESP ed AH. Con una leggera modifica ad ESP, includendo il controllo dell'intestazione IP, si potrebbe eliminare anche AH, alleggerendo la complessità del progetto.

Un'altra debolezza di IPsec è l'ordine in cui effettua l'autenticazione e la cifratura. IPsec esegue prima la cifratura e poi autentica il testo cifrato.

Tipico attacco ad IPsec

- supponiamo che due interlocutori abbiano stabilito una SA (che chiameremo SA1) e la usino per trasferire informazioni cifrate con il protocollo ESP (che chiameremo ESP1)
- finita la trasmissione, SA1 viene cancellata
- supponiamo ora che qualche ora dopo i due interlocutori abbiano di nuovo la necessità di scambiare dati sensibili
- se il ricevente usa lo stesso *Security Parameter Index* (l'identificatore della connessione) della ricezione precedente un crittoanalista potrebbe introdurre un pacchetto prelevato dalla trasmissione precedente
- il ricevente controlla l'autenticazione e la trova valida, procede alla decriptazione del messaggio, presumibilmente con una chiave diversa da quella precedente, e si trova con dei dati spazzatura che potrebbero influire sulla stabilità del sistema

Questo attacco si potrebbe evitare introducendo l'autenticazione di tutto ciò che è usato per determinare il significato del messaggio.

Ciononostante, utilizzando un algoritmo di cifratura dei dati robusto e stando attenti ai dettagli, si riesce a trasmettere i dati in modo abbastanza sicuro. Non esiste un'alternativa valida che rimpiazza IPsec utilizzando IPv4, l'attuale protocollo standard per le trasmissioni su Internet. Nello sviluppo di Ipv6, il nuovo protocollo per le trasmissioni

Internet, si sta dando maggiore importanza alla sicurezza e quindi ci sarà da aspettarsi un supporto nativo alle funzioni di crittografia e di autenticazione sicura.

Bibliografia

A.S. Tanenbaum “Reti di calcolatori”, Pearson Education Italia pp.772-776

Niel Ferguson, Bruce Schneier “A cryptographic evaluation of IPsec”, http://www.counterpane.com

http://www.webopedia.com

“Una Introduzione a IPsec”, ICT Security n.16 e 17, Ottobre/Novembre 2003

http://telemat.die.unifi.it/book/Internet/Security/elab3.htm

http://www.infosyssec.net/infosyssec/secvpn1.htm

Claudio Alberto Pisapia 229332

Emanuel Weitschek 224140