

POLITECNICO DI TORINO

III Facoltà di Ingegneria
Corso di Laurea Specialistica in Ingegneria Informatica

Tesina del corso di sicurezza dei sistemi informatici

IPsec in ambienti Broadcast e Multicast



LUCA ARDITO

Dicembre 2009

Indice

I	Nozioni teoriche	1
1	Soluzioni di sicurezza a livello IP: IPSEC	2
1.1	Obiettivi	2
1.2	Architettura	2
1.2.1	Protocollo AH	4
1.2.2	Protocollo ESP	4
1.2.3	Protocollo IKE	6
1.3	Funzionalità	8
1.4	Estensioni multicast/broadcast	8
1.4.1	Group Security Policy Database - GSPD	9
1.4.2	Group Controller Key Server - GCKS	9
1.4.3	Security Association Database - SAD	9
1.4.4	Peer Authorization Database - PAD	9
1.4.5	Modalità tunnel con protezione di indirizzo	10
1.5	Problemi di sicurezza IPsec	11
1.5.1	Problematiche di sicurezza risolte dalle estensioni IPsec di tipo multicast	11
1.5.2	Problematiche di sicurezza non risolte dalle estensioni IPsec di tipo multicast	11
1.5.3	Problematiche di implementazione o installazione che impattano la sicurezza	13
2	Implementazioni opensource per Linux	14
2.1	Storia	14
2.2	Implementazioni disponibili	14
2.2.1	Racoon	14
2.2.2	FreeSWAN	14
2.2.3	OpenSWAN	14
2.2.4	StrongSWAN	15
2.3	Confronto funzionale	15

II	Applicazioni in ambiente Linux	16
3	OpenSWAN	17
3.1	Descrizione architettura	17
3.2	Descrizione funzionalità	17
3.3	Installazione	17
3.3.1	Setup	17
3.3.2	Configurazione di base	17
4	Piattaforma di test	18
4.1	Descrizione	18
4.2	Configurazione	18
4.3	Strumenti di misura	18
4.3.1	Tcpdump	18
4.3.2	Wireshark	18
4.4	Misura diretta di tempi di trasferimento di file	18
4.4.1	Wget	18
4.4.2	Curl	18
5	Test	19
5.1	Formati IPSEC	20
5.1.1	AH	20
5.1.2	ESP	20
5.1.3	Combinazioni AH ed ESP	20
5.1.4	Transport	20
5.1.5	Tunnel	20
5.2	Algoritmi supportati	20
5.3	IKE con chiavi statiche	20
5.4	IKE con certificati	20
5.5	Broadcast IPV4	20
5.6	Misura di prestazioni	20
5.7	Interoperabilità OpenSWAN / Windows XP	20
	Bibliografia	21

Parte I

Nozioni teoriche

Capitolo 1

Soluzioni di sicurezza a livello IP: IPSEC

1.1 Obiettivi

IPsec nasce dall'esigenza di proteggere l'informazione trasmessa nella rete e risulta essere il protocollo crittografico maggiormente utilizzato: si colloca a livello IP, è parte integrante di IPv6, ma è utilizzabile anche con IPv4. IPsec può proteggere direttamente il mittente e il destinatario della comunicazione, oppure può intervenire tra due sistemi intermedi, come nel caso delle VPN. IPsec è una soluzione trasparente rispetto alle applicazioni e può proteggere tutto il traffico IP. IPsec offre autenticazione (ovvero la garanzia dell'identità del mittente del pacchetto), l'integrità (cioè la garanzia che il pacchetto non sia stato modificato durante il suo percorso) e la riservatezza (cioè la garanzia che le informazioni non siano leggibili da terzi, ottenuta mediante cifratura del pacchetto).

1.2 Architettura

L'architettura IPsec è composta da vari protocolli e da altri elementi. I protocolli più significativi che costituiscono IPsec sono tre:

- AH (Authentication Header) si occupa di autenticazione e integrità
- ESP (Encapsulating Security Payload) fornisce servizi di riservatezza, autenticazione ed integrità
- IKE (Internet Key Exchange) gestisce lo scambio delle chiavi

AH ed ESP non gestiscono lo scambio delle chiavi in quanto viene assodato che le due parti abbiano già creato tra loro una Security Association (SA). Per Security

Association si intende una connessione tra le due parti e specifica quali meccanismi di sicurezza e quali chiavi utilizzare affinché si possa proteggere il traffico che vi fluisce al suo interno. Questa operazione di negoziazione e gestione della SA è demandata ad IKE. Le SA sono unidirezionali; perciò si rendono necessarie due SA per permettere a due host di comunicare tra di loro. Una SA può essere associata ad AH o ad ESP, ma non ad entrambi. Tutte le SA attive su di un host sono contenute in un database chiamato Security Association Database (SAD) mentre le politiche di sicurezza sono contenute in un altro database chiamato Security Policy Database (SPD).

Sono disponibili due modalità di funzionamento:

- Modalità Trasporto (Transport Mode): quando, tra due sistemi terminali di una connessione IPsec, viene ad essere garantita la sicurezza dei protocolli di livello superiore ad IP. Si aggiungono gli header dei protocolli utilizzati (AH e/o ESP) tra l'header IP e l'header del protocollo di trasporto (TCP o UDP)

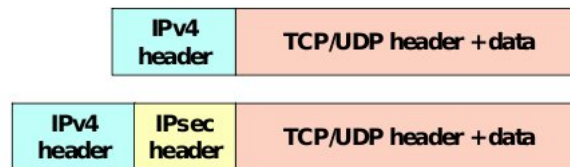


Figura 1.1. Transport Mode

- Modalità Tunnel (Tunnel Mode): quando gli attori vengono ad essere i security gateway e la sicurezza è data a tutto il pacchetto IP. Il pacchetto IP originario viene interamente incapsulato in un nuovo pacchetto IP.

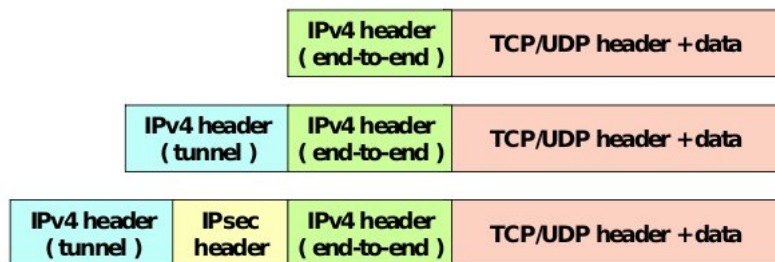


Figura 1.2. Tunnel Mode

1.2.1 Protocollo AH

Il protocollo AH (Authentication Header) fornisce servizi di autenticazione, integrità e protezione da attacchi di tipo replay. AH autentica l'intero pacchetto IP ad eccezione dei campi variabili dell'header IP. Questi campi possono essere modificati dai nodi intermedi e non possono quindi essere autenticati.

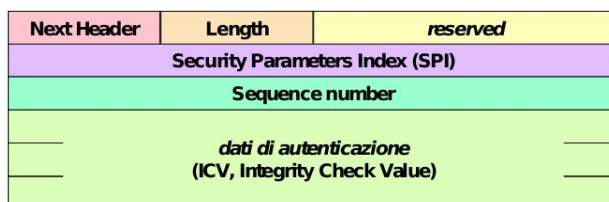


Figura 1.3. Protocollo AH

Next header contiene il codice identificativo del protocollo dell'header successivo, per esempio TCP o ESP.

Length contiene la lunghezza dell'header AH, espressa in parole di 32 bit, meno 2.

Reserved riservato per usi futuri, deve essere posto a zero.

Security Parameters Index (SPI) contiene un valore numerico che, insieme con l'indirizzo IP di destinazione e il protocollo (ovvero AH, in questo caso) identifica la security association utilizzata. Viene stabilito dal destinatario quando la SA viene negoziata.

Sequence number specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza (se il servizio anti-replay è abilitato) tramite un meccanismo a finestra.

Authentication data contiene il valore per il controllo dell'integrità (Integrity Check Value – ICV) del pacchetto. La lunghezza di questo campo è variabile ma deve essere un multiplo di 32 bit, per cui è possibile inserire un padding.

1.2.2 Protocollo ESP

Il protocollo ESP (Encapsulating Security Payload) fornisce servizi di riservatezza, autenticazione ed integrità. È possibile utilizzare uno solo di questi servizi o una combinazione di essi o tutti contemporaneamente. Per quanto riguarda l'autenticazione, questa differisce da quella fornita dal protocollo AH in quanto non copre l'header IP esterno.

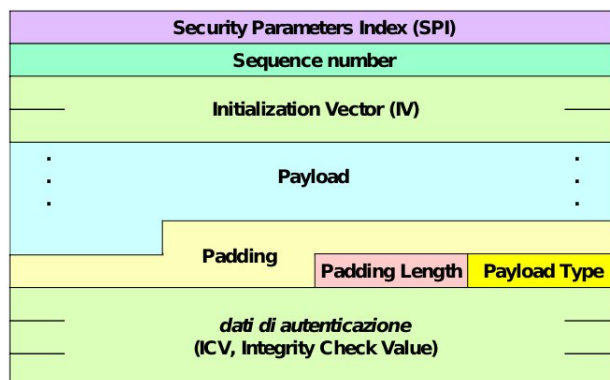


Figura 1.4. Protocollo ESP

Security Parameters Index (SPI) contiene un valore numerico che, insieme con l'indirizzo IP di destinazione e il protocollo (in questo caso ESP), permette di identificare la security association utilizzata. È analogo all'omonimo campo presente in AH.

Sequence number contiene il numero di sequenza del pacchetto nell'ambito della security association, come in AH.

Payload data contiene il payload del pacchetto IP originale (se in modalità trasporto) oppure l'intero pacchetto IP originale (se in modalità tunnel), cifrato se si utilizza il servizio di riservatezza. Nel caso l'algoritmo di cifratura utilizzato necessiti di un vettore di inizializzazione (Initialization Vector – IV), questo viene inserito all'inizio del payload.

Padding il padding (variabile tra 0 e 255 byte) può essere necessario sia perché l'algoritmo di cifratura può richiedere che il testo in chiaro abbia una dimensione multipla di un certo valore, sia per assicurare il corretto allineamento dei campi successivi. È anche possibile aggiungere un padding per limitare gli effetti di un'analisi del traffico basata sulla dimensione dei pacchetti.

Pad length contiene la lunghezza del padding.

Next header contiene il codice identificativo del protocollo per i dati contenuti nel payload, per esempio TCP o UDP. Qualora si utilizzasse il servizio di riservatezza, questo campo è cifrato.

Authentication data contiene il valore di controllo integrità (ICV), calcolato sull'intero pacchetto ESP escluso questo campo. È presente solo se si utilizza il servizio di autenticazione/integrità.

L'ESP in transport mode è solitamente usato dagli host e non dai gateway eccezion fatta nel caso del traffico destinato al gateway (es. SNMP, ICMP). Presenta uno svantaggio notevole: non nasconde l'header

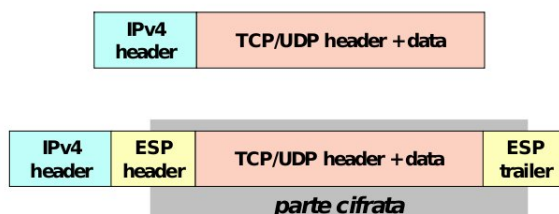


Figura 1.5. Protocollo ESP in transport mode

L'ESP in tunnel mode viene usato solitamente dai gateway e ha il seguente vantaggio: nasconde anche gli header

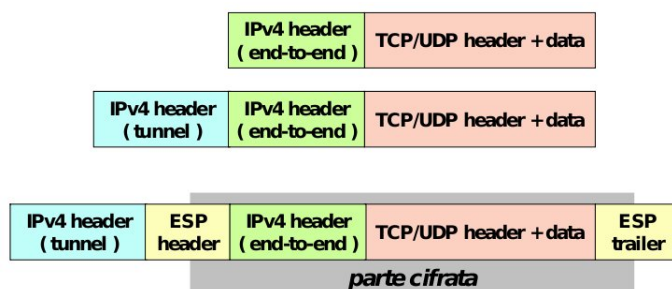


Figura 1.6. Protocollo ESP in tunnel mode

1.2.3 Protocollo IKE

Nell'architettura IPsec è fondamentale il concetto di security association. IKE è un protocollo di tipo generico e si occupa di creare le SA e di gestire gli archivi ad esse dedicati. Il protocollo ISAKMP (Internet Security Association and Key Management Protocol) definisce le procedure e il formato dei pacchetti per la gestione (creazione, modifica, cancellazione) delle security association e per lo scambio e l'autenticazione delle chiavi, in maniera totalmente indipendente dalla tecnica di generazione dagli algoritmi di cifratura, delle chiavi stesse e dai meccanismi di autenticazione. IKE è un protocollo ibrido, che integra ISAKMP con parte dei protocolli Oakley e SKEME. Oakley risulta essere un protocollo per mezzo del quale le due

parti autenticate si accordano per definire il materiale chiave da utilizzare e di cui IKE si servirà per effettuare lo scambio delle chiavi. SKEME è un protocollo di scambio chiave, ma verranno utilizzati il meccanismo crittografico a chiave pubblica e quello del rinnovo veloce della chiave.

IKE ha due fasi: nella prima i due nodi creano una security association per IKE stesso (detta ISAKMP SA), ovvero un canale sicuro da utilizzare per i messaggi di IKE (Negozia i parametri di sicurezza, Genera un segreto condiviso, Autentica le parti), nella seconda fase utilizzano la ISAKMP SA per negoziare security association per altri protocolli. Nella prima fase si può usare il main mode oppure l'aggressive mode, mentre nella seconda fase si utilizza il quick mode.

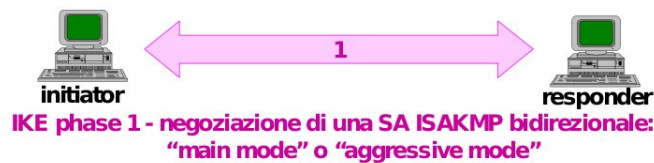


Figura 1.7. Protocollo IKE fase 1

Main Mode: 6 messaggi, 3 dall'origine alla destinazione e 3 in senso opposto (protegge l'identità delle parti)

Aggressive Mode: 3 messaggi, 2 dall'origine alla destinazione e 1 in senso opposto (ma non protegge l'identità delle parti)



Figura 1.8. Protocollo IKE fase 2

Quick Mode: 3 messaggi (negoziatura solo della SA IPsec)
New Group Mode: 2 messaggi

1.3 Funzionalità

Come introdotto nel paragrafo precedente l'architettura ipsec offre:

- Controllo degli accessi
- Integrità dei datagrammi
- Autenticazione dell'origine dei dati
- Rifiuto dei pacchetti introdotti nuovamente in rete (una forma parziale di verifica dell'integrità di sequenza)
- Riservatezza mediante l'uso della crittografia
- Limitata riservatezza del flusso del traffico

IPsec può inoltre essere utilizzato per creare VPN (Virtual Private Network) in entrambe le modalità. Questo uso è di fatto il più ricorrente.

1.4 Estensioni multicast/broadcast

Sono in atto delle estensioni al protocollo IPsec atte a consentire a gruppi di dispositivi IPsec di avere le stesse security association con selettori di traffico dotati di un indirizzo di tipo multicast nel campo di destinazione IP. Queste estensioni supportano anche security association con indirizzi broadcast IPv4 risultanti in un pacchetto broadcast di livello link IPv4 e con indirizzi anycast IPv6 risultanti in un pacchetto anycast IPv6. Potendo esserci molteplici potenziali destinatari di un pacchetto con protezione IPsec, questi tipi di indirizzi di destinazione hanno molte caratteristiche in comune con gli indirizzi di tipo multicast.

Il multicasting IP serve a mandare un unico pacchetto ad un gruppo di host, ovvero ad una serie di zero o più host identificati da un unico indirizzo di destinazione IP. I pacchetti IP di tipo multicast sono pacchetti dati UDP consegnati a tutti i membri del gruppo con l'indicazione best-effort. Il mittente che invia ad un gruppo IP di tipo multicast fissa la destinazione del pacchetto ad un indirizzo IP assegnato per le trasmissioni multicast IP. I potenziali destinatari del pacchetto si uniscono al gruppo IP di tipo multicast registrandosi ad un dispositivo di instradamento di rete che segnala l'intento di ricevere pacchetti inoltrati ad un particolare gruppo IP di tipo multicast. I dispositivi di instradamento di rete, correttamente configurati per trasmettere pacchetti IP multicast, aderiscono ai protocolli di instradamento multicast che mantengono lo stato riguardante quali dispositivi sono registrati per ricevere pacchetti per conto di un particolare gruppo IP di tipo multicast. Nel ricevere un pacchetto IP di tipo multicast, il router ne manda copia fuori da ogni interfaccia con

destinatari noti. Un'implementazione host di IPsec con utilizzo di estensioni di tipo multicast può valersi della modalità di trasporto o tunnel al fine di incapsulare un pacchetto multicast IP. L'indirizzo di destinazione per il pacchetto IPsec è, quindi, un indirizzo multicast IP e non un indirizzo host unicast.

1.4.1 Group Security Policy Database - GSPD

La GSPD è una banca dati del programma di sicurezza in grado di implementare le associazioni di sicurezza unicast e le estensioni multicast definite da questa specifica. Viene quindi introdotto un nuovo attributo della GSPD, ovvero la direzionalità d'ingresso GSPD che può essere di tre tipi. Ogni entry GSPD può, infatti, riportare l'indicazione sender only, receiver only oppure symmetric.

1.4.2 Group Controller Key Server - GCKS

Server di protocollo della Gestione Chiavi di Gruppo (Group Key Management - GKM) che gestisce lo stato IPsec di un gruppo. Un GCKS autentica il programma e il materiale di digitatura della SA IPsec per poi fornirli ai membri di un gruppo GKM.

1.4.3 Security Association Database - SAD

Il security association database è in grado di supportare SA multicast in caso di configurazione manuale. Una SA multicast in partenza ha una struttura uguale a quella di una SA unicast. L'indirizzo sorgente è quello del Mittente di Gruppo mentre l'indirizzo di destinazione è l'indirizzo di gruppo multicast. Una SA multicast in arrivo deve configurarsi con gli indirizzi sorgente di ciascun pari Mittente di Gruppo autorizzato a trasmettere alla SA multicast in questione. Il valore SPI di una SA multicast viene fornito da un GCKS e non dal destinatario come accade invece nel caso di SA unicast.

1.4.4 Peer Authorization Database - PAD

La PAD viene messa a disposizione per avvantaggiare i membri pari che, all'interno del gruppo, possono assumere specifici ruoli come, ad esempio, i ruoli di GCKS, Mittente di Gruppo o Destinatario di Gruppo. Un pari può rivestire ruoli molteplici. La PAD può anche contenere certificati radice per i PKI usati dal gruppo.

1.4.5 Modalità tunnel con protezione di indirizzo

Nell'usare la modalità tunnel per incapsulare pacchetti multicast IP che devono rimanere pacchetti multicast IP, si rendono necessarie nuove semantche di costruzione dell'intestazione dovute alle particolari necessità dei protocolli di instradamento multicast IP. I protocolli di instradamento multicast IP mettono a confronto l'indirizzo di destinazione su un pacchetto e lo stato di instradamento di tipo multicast. Se cambiata, la destinazione di un pacchetto multicast IP non sarà più instradata correttamente. Un gateway di sicurezza IPsec deve, quindi, proteggere l'indirizzo di destinazione di tipo multicast IP dopo l'incapsulamento del tunnel. Il Sottosistema GKM (Group Key Management) su un gateway di sicurezza con implementazione delle estensioni IPsec di tipo multicast protegge l'indirizzo multicast IP nel seguente modo: in primo luogo il Sottosistema GKM imposta l'indicatore PFP dell'indirizzo remoto all'ingresso del GSPD (multicast-capable security policy database) per i selettori di traffico. L'indicatore fa in modo che l'indirizzo remoto del pacchetto corrispondente ai selettori di traffico della SA IPsec si propagano verso il punto d'incapsulamento del tunnel IPsec; in secondo luogo il Sottosistema GKM deve avvertire che la protezione dell'indirizzo di destinazione è in atto per una determinata SA IPsec. Il protocollo della GKM deve definire un attributo che segnali la protezione dell'indirizzo di destinazione al Sottosistema GKM su un gateway di sicurezza IPsec. In genere i protocolli di instradamento multicast IP creano anche alberi di distribuzione multicast a partire dall'indirizzo di sorgente. Qualora un gateway di sicurezza IPsec cambiasse l'indirizzo di sorgente di un pacchetto multicast IP (per esempio lo trasformasse nel proprio indirizzo IP), il pacchetto con protezione IPsec che ne risulta potrebbe non superare i controlli degli invii a percorso inverso (Reverse Path Forwarding - RPF) su altri router. Il pacchetto può essere abbandonato a seguito di un controllo RPF non riuscito. Per agevolare i controlli RPF del protocollo di instradamento, il Sottosistema GKM sull'implementazione di un gateway di sicurezza che mette in atto le estensioni IPsec di tipo multicast deve proteggere l'indirizzo sorgente del pacchetto IP in questo modo: in primo luogo imposta all'ingresso del GSPD per i selettori di traffico l'indicatore PFP dell'indirizzo sorgente che induce l'indirizzo remoto a propagarsi verso la SA IPsec; in secondo luogo il Sottosistema GKM deve segnalare che è in atto per una particolare SA IPsec la protezione dell'indirizzo di sorgente. Il Sottosistema GKM deve definire un attributo di protocollo che segnali la protezione dell'indirizzo di sorgente al Sottosistema GKM su un gateway di sicurezza IPsec.

1.5 Problemi di sicurezza IPsec

Il protocollo IPsec presenta alcuni problemi di sicurezza noti. L'estensione multicast di IPsec ne risolve alcuni e rimangono tuttavia aperte alcune problematiche di sicurezza.

1.5.1 Problematiche di sicurezza risolte dalle estensioni IPsec di tipo multicast

Forniti dal servizio di estensioni multicast di sicurezza IP, i seguenti meccanismi sullo strato di rete consentono comunicazioni di gruppo sicure:

- confidenzialità mediante l'uso di un'unica chiave di cifratura di gruppo
- autenticazione della sorgente e protezione dell'integrità di gruppo mediante l'uso di un'unica chiave di autenticazione di gruppo
- autenticazione dell'origine dei dati del Mittente di Gruppo mediante l'uso di una firma digitale, TESLA, o altro meccanismo
- protezione anti-replay per un numero ristretto di Mittenti di Gruppo mediante l'uso del sistema di numeri in sequenza ESP (o AH)
- filtraggio delle trasmissioni multicast da parte di quei membri che il programma di gruppo non autorizza ad essere Mittenti. Questa è una caratteristica che contraddistingue il servizio di protezione IPsec detto stateless. A supporto dei suddetti servizi questa specifica arricchisce la definizione delle banche dati SPD, PAD e SAD al fine di facilitare la gestione automatica chiavi di gruppo dei gruppi crittografici di grossa portata.

1.5.2 Problematiche di sicurezza non risolte dalle estensioni IPsec di tipo multicast

Non rientra a far parte delle competenze di questa architettura proteggere le chiavi del gruppo o i suoi dati di applicazione dagli attacchi a molti aspetti dell'ambiente operativo in cui si svolge l'implementazione IPsec. Andrebbe comunque notato che il rischio di attacchi provocati da un avversario in rete è ingigantito a tal punto che le chiavi di gruppo vengono condivise da molti sistemi. I problemi di sicurezza lasciati irrisolti dal servizio di estensioni IPsec di tipo multicast si dividono in due grandi categorie: attacchi esterni e attacchi interni. Nel caso di attacchi esterni: il servizio di estensione IPsec multicast non offre protezione contro un avversario esterno al gruppo che ha:

- la capacità di lanciare contro il gruppo un attacco flooding di deny of service di tipo multicast prodotto da un sistema il cui sottosistema IPsec non filtra le trasmissioni multicast abusive
- compromesso un router multicast potendo così corrompere o cancellare tutti i pacchetti multicast destinati alle estremità di gruppo che si trovano a valle del router
- catturato copia di una precedente trasmissione di pacchetto multicast per poi ripresentarla ad un gruppo il cui servizio anti-replay non è attivato. Si osservi che, nel caso di un grosso gruppo multicast proveniente da sorgente qualunque, non è fattibile per i Destinatari di Gruppo conservare uno stato anti-replay per ogni potenziale Mittente di gruppo. I programmi di gruppo che richiedono la protezione anti-replay per un grosso gruppo multicast proveniente da sorgente qualunque dovrebbero considerare un protocollo multicastordine totale dello strato di applicazione.

Nel caso di attacchi interni: per i gruppi di grossa portata le estensioni multicast di sicurezza IP dipendono da un protocollo automatico di Gestione Chiavi di Gruppo che autentica ed autorizza correttamente i membri fidati in conformità ai programmi di gruppo. Inerente al concetto di gruppo crittografico è un segreto o una serie di segreti in comune svelati a tutti i membri del gruppo. Di conseguenza le garanzie di sicurezza del servizio non sono più forti del più debole membro ammesso al gruppo dal sistema GKM. Il sistema GKM ha la responsabilità di rispondere al rilevamento di un membro di gruppo compromesso mettendo in atto una procedura di recupero chiavi di gruppo. Il protocollo di ridigitatura GKM dovrà espellere i membri di gruppo compromessi e distribuirà un nuovo materiale di digitatura di gruppo ai membri fidati. Alternativamente il programma di gruppo può richiedere che il sistema GKM ponga fine al gruppo.

Nel caso in cui il sistema GKM ammettesse nel gruppo un avversario, si possono verificare i seguenti attacchi non risolvibili dal servizio di estensione multicast IPsec:

- l'avversario può svelare la chiave segreta o le informazioni di gruppo ad una parte abusiva al di fuori del gruppo
- l'avversario interno può contraffare le trasmissioni del pacchetto che sembrano provenire da un membro di gruppo pari. Per difendere da questo attacco le trasmissioni di Mittente di Gruppo di particolare importanza, il programma di gruppo può chiedere al Mittente di trasmettere pacchetti multicast utilizzando il servizio di autenticazione dell'origine dei dati. Â

- se il servizio del gruppo di autenticazione dell'origine dei dati utilizza firme digitali, l'avversario interno può lanciare un attacco di deny of service delle risorse computerizzate trasmettendo pacchetti con firme false.

1.5.3 Problematiche di implementazione o installazione che impattano la sicurezza

Verranno ora elencate alcune problematiche di implementazione o installazione che possono impattare sulla sicurezza

- gruppi che abbracciano due o più domini del programma di sicurezza: questa estensione prevede un unico programma per gruppo
- NAT: le applicazioni multicast IPsec devono superare varie barriere architetturali per poter essere installate con successo
- i gateways NAT possono riavviarsi e perdere le informazioni pertinenti alla traduzione del loro indirizzo
- il gateway NAT può rimuovere lo stato di traduzione del proprio indirizzo al termine del periodo di inattività. La traduzione d'indirizzo utilizzata dal gateway NAT dopo la ripresa del flusso di dati può essere diversa da quella nota ai selettori GSPD alle estremità di gruppo
- L'ESP nasconde i propri carichi utili dal gateway NAT
- Impossibile utilizzo di una AH (Authentication Header) con un gateway NAT
- sincronizzazione delle perdite GSPD con layer internet: il meccanismo di programma di sicurezza di gruppo del protocollo GKM può inavvertitamente configurare i selettori di traffico GSPD del gruppo con transitori indirizzi IP inattendibili
- Il GCKS potrebbe non possedere una conoscenza globale delle mappature degli aggiornati indirizzi pubblici e privati dell'estremità di un gruppo a causa di errori di rete o condizioni di percorso. Per esempio l'indirizzo di un Membro di Gruppo potrebbe cambiare a seguito della scadenza del lease dell'indirizzo DHCP assegnato
- Dipendenza delle checksum UDP dall'indirizzo di sorgente IP

Capitolo 2

Implementazioni opensource per Linux

2.1 Storia

Che gran rottura di cazzo

2.2 Implementazioni disponibili

Ce ne sono un fottio tra cui:

2.2.1 Racoon

Gran troiata

2.2.2 FreeSWAN

Vecchio come le palle dell'orso

2.2.3 OpenSWAN

Largamente diffuso

2.2.4 StrongSWAN

Niente di che... meglio l'altro.

2.3 Confronto funzionale

Alla fine fanno cagarissimo tutti equattro!

Temperatura °C	Densità t/m ³
0	13,8
10	13,6
50	13,5
100	13,3

Tabella 2.1. Confronto implementazioni IPSEC

Osservazione 1 Alla fine vaffanculo.

E comunque sto ipsec mi fa cagare

Parte II

Applicazioni in ambiente Linux

Capitolo 3

OpenSWAN

3.1 Descrizione architettura

Si l'han fatto ma...

3.2 Descrizione funzionalità

...na cagata

3.3 Installazione

che due coglioni fai partire il deb o l'rpm e fa tutto lui

3.3.1 Setup

controlla che sia tutto aposto

3.3.2 Configurazione di base

fai un file di configurazione e non scaramellarmi la funcia di minchia

Capitolo 4

Piattaforma di test

4.1 Descrizione

4.2 Configurazione

4.3 Strumenti di misura

4.3.1 Tcpcdump

4.3.2 Wireshark

4.4 Misura diretta di tempi di trasferimento di file

4.4.1 Wget

4.4.2 Curl

Capitolo 5

Test

5.1 Formati IPSEC

5.1.1 AH

5.1.2 ESP

5.1.3 Combinazioni AH ed ESP

5.1.4 Transport

5.1.5 Tunnel

5.2 Algoritmi supportati

5.3 IKE con chiavi statiche

5.4 IKE con certificati

5.5 Broadcast IPV4

5.6 Misura di prestazioni

5.7 Interoperabilità OpenSWAN / Windows XP

Bibliografia

- [1] Prof. A. Liroy, *Dispense del corso di sicurezza dei sistemi informatici*
- [2] <http://www.ipsec-howto.org/italian/x151.html>
- [3] <http://tools.ietf.org/html/draft-ietf-msec-ipsec-extensions-07>
- [4] <http://tools.ietf.org/html/rfc4945>
- [5] <http://eprint.iacr.org/2007/125>