Azzolini Riccardo 2021-05-17

IPSec

1 Servizio anti-replay

Quando si ha un flusso di traffico autenticato tra due nodi di una rete, un accattante potrebbe effettuare un attacco a replay ottenendo una copia di un pacchetto autenticato e successivamente ritrasmettendolo al destinatario, riuscendo così a falsare una successiva esecuzione del protocollo, causare problemi al funzionamento del servizio/protocollo di livello superiore e/o ritrasmettere lo stesso pacchetto molte volte al fine di un attacco DoS. Degli attacchi analoghi sono possibili anche quando la comunicazione è riservata (cifrata) invece (o oltre) che autenticata.

Per evitare attacchi a replay, il destinatario deve accorgersi quando un messaggio ricevuto è un precedente messaggio che è stato ritrasmesso, e in tal caso deve evitare di processarlo. A tale scopo si associa a ogni pacchetto un **sequence number**, e il destinatario scarta ogni messaggio ricevuto che ha un sequence number uguale a un messaggio precedente.

Il sequence number è un contatore a 32 bit che il mittente inizializza a 0 quando si crea una nuova SA. Ogni volta che un pacchetto viene processato in accordo con una SA, aggiungendo un header *AH o ESP* (entrambi forniscono il servizio anti-replay, implementato allo stesso modo), si inserisce nel campo Sequence Number di tale header il valore del contatore, dopodiché il contatore viene incrementato. Quando il contatore raggiunge il suo valore massimo, $2^{32} - 1$, l'SA "scade" e bisogna generarne una nuova, con un nuovo SPI, perché altrimenti se venissero trasmessi pacchetti diversi processati con la stessa SA e aventi lo stesso sequence number il destinatario penserebbe che siano pacchetti ripetuti.

Il destinatario segna i sequence number dei pacchetti che riceve e scarta (non ritiene validi) ulteriori pacchetti ricevuti con gli stessi sequence number. Tenere traccia dei sequence number ricevuti non è però banale:

- un semplice elenco di quali sequence number siano stati ricevuti potrebbe diventare troppo grande, dato che il sequence number può assumere 2^{32} possibili valori;
- siccome IP non garantisce l'ordine di consegna dei pacchetti, né che tutti i pacchetti siano consegnati, non è sufficiente memorizzare l'ultimo sequence number ricevuto e aspettarsi di ricevere solo i valori successivi.

La soluzione è che il destinatario mantenga una finestra di W elementi (tipicamente si pone $W = 64$), i quali rappresentano W sequence number consecutivi, indicando per ciascuno di essi se un pacchetto con tale numero è già stato ricevuto o no. Tale finestra avanza man mano che arrivano nuovi pacchetti, ovvero è una "sliding window".

Quando si riceve un pacchetto, il suo sequence number può essere compreso nella finestra, maggiore di tutti quelli compresi nella finestra ("a destra" della finestra) oppure minore di quelli compresi nella finestra ("a sinistra" della finestra).

- Se il sequence number è compreso nella finestra e non è già segnato come ricevuto, si verifica il MAC del pacchetto per controllare se è autentico, e in caso positivo si contrassegna l'elemento della finestra corrispondente a questo sequence number per indicare che tale numero è stato ricevuto. Se invece il MAC non è corretto o il sequence number è già stato ricevuto, il pacchetto viene scartato, non viene preso in considerazione.
- Se il sequence number ricade a destra della finestra allora si verifica il MAC, e se il pacchetto è autentico:

  1. si sposta in avanti la finestra fino a includere il sequence number di questo pacchetto;
  2. si segna il sequence number come ricevuto.

  Se invece il pacchetto non è autentico esso viene scartato senza far avanzare la finestra.
- Se infine il sequence number ricade a sinistra della finestra, il pacchetto viene scartato. Potrebbe essere che così facendo si scartino dei pacchetti con sequence number non ricevuti in precedenza, ma ciò non è particolarmente problematico perché appunto IP non garantisce la consegna dei pacchetti, dunque i protocolli di livello superiore sono già in grado di gestire la perdita dei pacchetti se necessario.

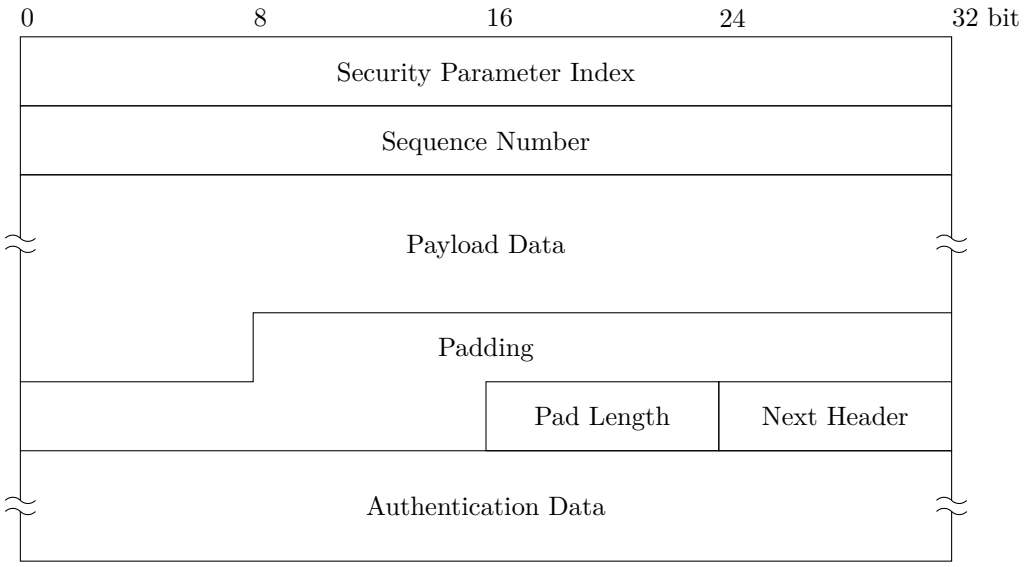
2 Encapsulating Security Payload

L'intestazione ESP (Encapsulating Security Payload) fornisce servizi di

- riservatezza (cifratura) del contenuto del pacchetto (la parte cifrata varia a seconda che ESP sia usato in modalità trasporto o tunnel),
- riservatezza (limitata) del flusso del traffico,

e può opzionalmente fornire anche un servizio di autenticazione del payload e dei campi dell'intestazione ESP, ma non dell'intestazione IP (a differenza di AH). Esso supporta diversi schemi crittografici, tra cui il più usato è AES-CBC, dunque si impiega il padding per raggiungere la dimensione del blocco richiesta.

L'header è composto dai seguenti campi:



- SPI, Sequence Number e Next Header hanno la stessa funzione degli analoghi campi presenti in AH.
- **Payload Data**: contiene la cifratura del payload del pacchetto IP (che nel caso della modalità tunnel è l'intero pacchetto IP originale).
- **Padding**: usato per garantire che la lunghezza totale dei campi Payload Data, Padding, Pad Length e Next Header sia un multiplo di 32 bit e un multiplo della dimensione del blocco richiesta dall'algoritmo di cifratura.
- **Pad Length**: indica la lunghezza del padding.
- **Authentication Data**: contiene l'ICV (codice MAC) che autentica tutta la struttura ESP tranne il campo Authentication Data stesso. Questo campo è opzionale: la SA che specifica il servizio ESP determina se si deve fornire autenticazione, ovvero se il campo Authentication Data deve essere presente.

I campi Payload Data, Padding, Pad Length e Next Header sono cifrati. L'autenticazione è opzionale perché può non servire quando si applicano a uno stesso pacchetto sia AH che ESP (a seconda delle garanzie di sicurezza che si vogliono ottenere e della combinazione di modalità trasporto/tunnel delle SA), ma quando viene usata essa protegge, oltre ai quattro campi cifrati, anche l'SPI e il Sequence Number, poiché (come nel caso di AH) è importante che questi non siano modificabili da un attaccante. Si noti che i campi cifrati vengono dati in input alla funzione MAC in forma appunto cifrata, non in chiaro.

Il termine "encapsulating" nel nome della struttura ESP si riferisce al fatto che essa incapsula al suo interno il payload, compreso tra:

- una "vera e propria" intestazione, composta dai campi SPI e Sequence Number;

- una *coda* ("ESP trailer"), composta dai campi Padding, Pad Length e Next Header e opzionalmente seguita dai dati di autenticazione.

2.1 ESP in modalità trasporto

In modalità trasporto l'intestazione ESP viene inserita dopo l'header IP del pacchetto originale. La posizione precisa dell'intestazione, e quindi i dati che essa protegge, variano in base alla versione di IP:

- Nel caso di IPv4 l'intestazione ESP è seguita solo dalla cifratura di payload e coda, e opzionalmente dai dati di autenticazione. Di conseguenza, i servizi forniti sono:
  - la cifratura del payload del pacchetto originale e della coda ESP;
  - opzionalmente, l'autenticazione dell'header ESP e di tutta la parte cifrata (payload e coda), ma non dell'header IP.
- Nel caso di IPv6 possono in più esserci:
  - degli header di estensione prima dell'header ESP, che non vengono né cifrati né autenticati;
  - degli header di estensione tra dopo l'header ESP, che sono considerati parte del payload, quindi vengono cifrati ed eventualmente autenticati.

  Di conseguenza, come con AH, si mettono prima dell'header ESP le intestazioni che servono per il routing (le quali devono rimanere leggibili e modificabili) e dopo l'header ESP le intestazioni per il destinatario (che devono essere protette).

2.2 ESP in modalità tunnel

Quando si applica ESP in modalità tunnel l'intero pacchetto originale è protetto, in quanto inserito come payload (cifrato ed eventualmente autenticato) di un nuovo pacchetto dotato di intestazione ESP. Ciò significa, in particolare, che vengono nascoste le informazioni relative al mittente e al destinatario del pacchetto originale (purché esse non siano uguali a quelle del nuovo pacchetto). La versione di IP e la posizione dell'header ESP determinano invece quali parti del nuovo pacchetto sono protette:

- Nel caso di IPv4 sono cifrati solo il pacchetto originale e la coda ESP, che opzionalmente vengono anche autenticati insieme all'intestazione ESP, mentre l'header del nuovo pacchetto IP non è protetto in alcun modo.
- Anche nel caso di IPv6 il nuovo header IP non è protetto, e in più non sono protetti gli eventuali extension header inseriti tra l'header IP e l'header ESP, ma come al solito gli extension header inseriti dopo l'header ESP sono considerati parte del payload e dunque protetti.

3 Combinazione di SA

Come già detto, una singola SA può fornire il servizio AH o ESP, ma non entrambi, dunque se un flusso di traffico richiede sia la riservatezza che l'autenticazione è necessario applicare a ciascun pacchetto più SA, una dopo l'altra. Una sequenza di SA applicate a un pacchetto si chiama **bundle di SA**, e ci sono due modi di utilizzarla:

- **Transport adjacency**: si applicano allo stesso pacchetto IP più SA in modalità trasporto. Ogni volta che si applica una SA successiva si considerano parte del payload gli header di tutte le precedenti, dunque il nuovo header viene inserito prima di essi e la protezione che esso fornisce si applica anche a essi. Complessivamente, alla fine, gli header delle SA risultano uno adiacente all'altro, nell'ordine ordine inverso rispetto a quello in cui le SA sono state applicate.
- **Iterated tunneling**: si applicano più SA in modalità tunnel, aggiungendo per ciascuna di esse un nuovo header IP e l'header della SA.

Ci sono allora vari modi di combinare la riservatezza e l'autenticazione; le combinazioni più significative sono:

- **ESP con opzione di autenticazione**;
- **bundle transport adjacency**;
- **bundle transport-tunnel**.

3.1 ESP con opzione di autenticazione

In modalità trasporto, ESP con l'opzione di autenticazione cifra e autentica il payload IP, mentre non protegge l'intestazione IP. In modalità tunnel invece si cifra e autentica l'intero pacchetto IP originale, ma ancora non il nuovo header IP (in ogni caso, l'header IP esterno non può mai essere cifrato, dovendo essere leggibile ai fini dell'instradamento, ma i suoi campi immutabili possono essere autenticati usando AH).

In entrambe le modalità, l'autenticazione viene applicata al testo cifrato, quando invece, come detto in precedenza, sarebbe preferibile applicarla al testo in chiaro, il che permetterebbe ad esempio di memorizzare il messaggio autenticato e verificarne facilmente l'autenticità quando serve, senza doverlo decifrare ogni volta.

3.2 Bundle transport adjacency

Il bundle transport adjacency consiste nell'applicare due SA in modalità trasporto:

1. Per prima cosa si applica al pacchetto IP originale *ESP senza autenticazione in modalità trasporto.*

2. Al pacchetto così ottenuto si applica poi *AH in modalità trasporto* (considerando come payload l'header ESP e la cifratura del payload originale e della coda ESP.

Il vantaggio rispetto a ESP con l'opzione di autenticazione è che qui l'autenticazione include anche i campi immutabili dell'intestazione IP (tra cui in particolare gli indirizzi IP di sorgente e destinazione), ma essa si applica ancora al testo cifrato e non al testo in chiaro.

3.3 Bundle transport-tunnel

Il bundle transport-tunnel consiste nell'applicare un'SA in modalità trasporto e una in modalità tunnel:

1. Si applica *AH in modalità trasporto* al pacchetto IP originale.
2. Al pacchetto così ottenuto si applica *ESP con l'opzione di autenticazione in modalità tunnel*.

L'opzione di autenticazione ESP serve perché in questa configurazione AH autentica solo il pacchetto originale, essendo applicato prima di ESP, dunque i campi importanti di ESP (l'SPI e il Sequence Number) devono essere autenticati separatamente, anche se ciò comporta una seconda autenticazione (ridondante) del pacchetto originale.

Come con il bundle transport ajdacency, con questa soluzione l'autenticazione comprende i campi immutabili dell'intestazione IP originale (però qui si aggiunge un nuovo header IP esterno che non viene autenticato), ma in più si ha il vantaggio che l'autenticazione si applica al testo in chiaro, prima della cifratura.

4 IPSec Architecture

Il documento IPSec Architecture (RFC 2401) specifica quattro combinazioni di associazioni di sicurezza che costituiscono sostanzialmente delle architetture di riferimento, le quali devono essere supportate dagli host e dai security gateway che implementano IPSec.

- Nella prima architettura, *end-to-end*, la sicurezza è garantita tra gli host terminali tramite una o più associazioni di sicurezza di tipo qualsiasi.
- La seconda architettura realizza una *VPN semplice*, in cui la sicurezza è garantita solo tra i gateway di sicurezza, mediante SA di tipo tunnel.
- La terza architettura descrive una *VPN con sicurezza end-to-end tra host*, cioè estende il caso precedente aggiungendo delle SA per garantire anche la sicurezza tra gli host terminali.

- La quarta architettura fornisce il supporto per un host remoto che utilizza Internet per raggiungere il gateway di una rete locale, e poi comunica con un host all'interno della rete locale. In questo caso si usano una o più SA di tipo qualsiasi per garantire la sicurezza tra gli host terminali e una o più SA di tipo tunnel per garantire la sicurezza tra l'host remoto e il gateway.