Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

Lezione VI: IPsec

La suite TCP/IP

La suite TCP/IP non è progettata con particolari misure di difesa per la confidenzialità o integrità dei dati dalle manomissioni.

- Lo scenario di riferimento: nodi per lo piú cooperativi (accademici)
- e qualcuno sostiene che NSA fu contraria all'inserimento di tecniche crittografiche in una rete pubblica

IPsec

IPsec specifica come crittare, autenticare e scambiare chiavi con IP.

- Basato su IP (in maniera differente IPv4 e IPv6)
- Obbligatorio supportarlo per gli stack IPv6, facoltativo in IPv4

Servizi di sicurezza offerti

- Controllo dell'accesso alla comunicazione
- Autenticazione dell'origine dei dati
- Integrità dei dati
- Confidenzialità dei dati
- Protezione da *replay*

Protocolli IPsec

Si tratta in realtà di piú specifiche protocollari

- Authentication Header (AH) per l'autenticazione e integrità del datagramma
- Encapsulating Security Payload (ESP) per la confidenzialità

Entrambi presuppongono una Security Association (SA), per lo scambio di credenziali.

AH

- Serve per autenticare l'origine del pacchetto e l'integrità dei campi immutabili.
- Un security parameter index identifica la SA
- Identifica replay di pacchetti con una tecnica "sliding window" e un contatore che per essere inizializzato necessita una nuova SA

Sliding window

Il nodo destinazione tiene un array di $SW[1:w] = 0$ elementi per ogni SA

1. Primo datagramma contatore n: $SW[w] = n$
2. Datagramma contatore i

   $n - w + 1 \leq i \leq n \wedge OK(sig)$ controlla se $SW[i + w - n] > 0$ (replay!), altrimenti $SW[i + w - n] = i$

   $i \leq n - w$ vecchio

   $i > n \wedge OK(sig)$ sposta la finestra

ESP

- Serve per crittare il contenuto dei pacchetti
- Un security parameter index identifica la security association
- Due modalità
  1. transport protocolli superiori vengono crittati end-to-end
  2. tunnel i pacchetti IPsec contengono (crittati) pacchetti IP

Security association

Ogni conversazione IPsec è abbinata ad una Security association (SA) frutto di una negoziazione dei parametri di sicurezza e delle credenziali.

- IP destinazione
- Una SA per AH e una per ESP
- Statiche o dinamiche (ISAKMP: Internet Security Association Key Management Protocol, IKE: Internet Key Exchange)

problemi IPsec

- La configurazione dei firewall per permettere i protocolli IPsec non è banale
- Ogni volta che una comunicazione comporta la manipolazione dei pacchetti IP (proxy e NAT) occorre adottare misure speciali, con successive security association.

Riassumendo

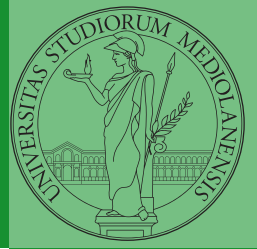
- IPsec introduce autenticazione, integrità e confidenzialità
- Protezione da *replay*
- Necessita di un certo overhead amministrativo e computazionale

TLS/SSL

Un'altra possibilità è introdurre misure di sicurezza sopra il livello di trasporto TCP.

- 1993–1995, Netscape rilascia un Secure Socket Layer SSL (2.0) pensato per proteggere la navigazione web.
- SSL 3.0, standardizzato da IETF come TLS Transport Layer Security

Obiettivi di sicurezza



- cifratura end-to-end
- protezione dell'integrità
- autenticazione del server (il client rimane anonimo)
- efficienza adeguata alle connessioni HTTP, brevi e stateless

sessione TLS

I nodi mantengono lo stato della sessione per gestire la cifratura del traffico.

- TLS handshake protocol
- TLS record layer
- una sessione può gestire piú connessioni per ridurre l'overhead

TLS handshake

1. C richiede la connessione, elencando quali cipher suite (CS) conosce
2. S sceglie CS compatibile e spedisce un digital certificate (DC) firmato da una CA
3. C controlla DC e manda criptata una chiave di sessione (K) random

Integrazione con le applicazioni

Tre strategie:

1. Creare un nuovo servizio (es. SSH2)
2. Aggiungere TLS ad un servizio noto (es. HTTPS)
3. Estendere un servizio noto affinché usi TLS (es. ESMTP)

Riassumendo

- TLS permette cifratura e autenticazione dei server (tramite CA) a livello di trasporto
- La gestione delle sessioni è progettata per essere efficiente in presenza di connessioni ripetute
- Molto diffuso perché facile da integrare nelle applicazioni

Livello di trasporto

IPsec e TLS possono essere piuttosto penalizzanti dal punto di vista delle prestazioni (Dal punto di vista delle performance del server, TLS può arrivare ad essere fino a 82 volte piú lento di una connessione TCP).
tcpcrypt è una proposta recente (2010) piú efficiente (3 volte piú lento di TCP)

Altri limiti di TLS

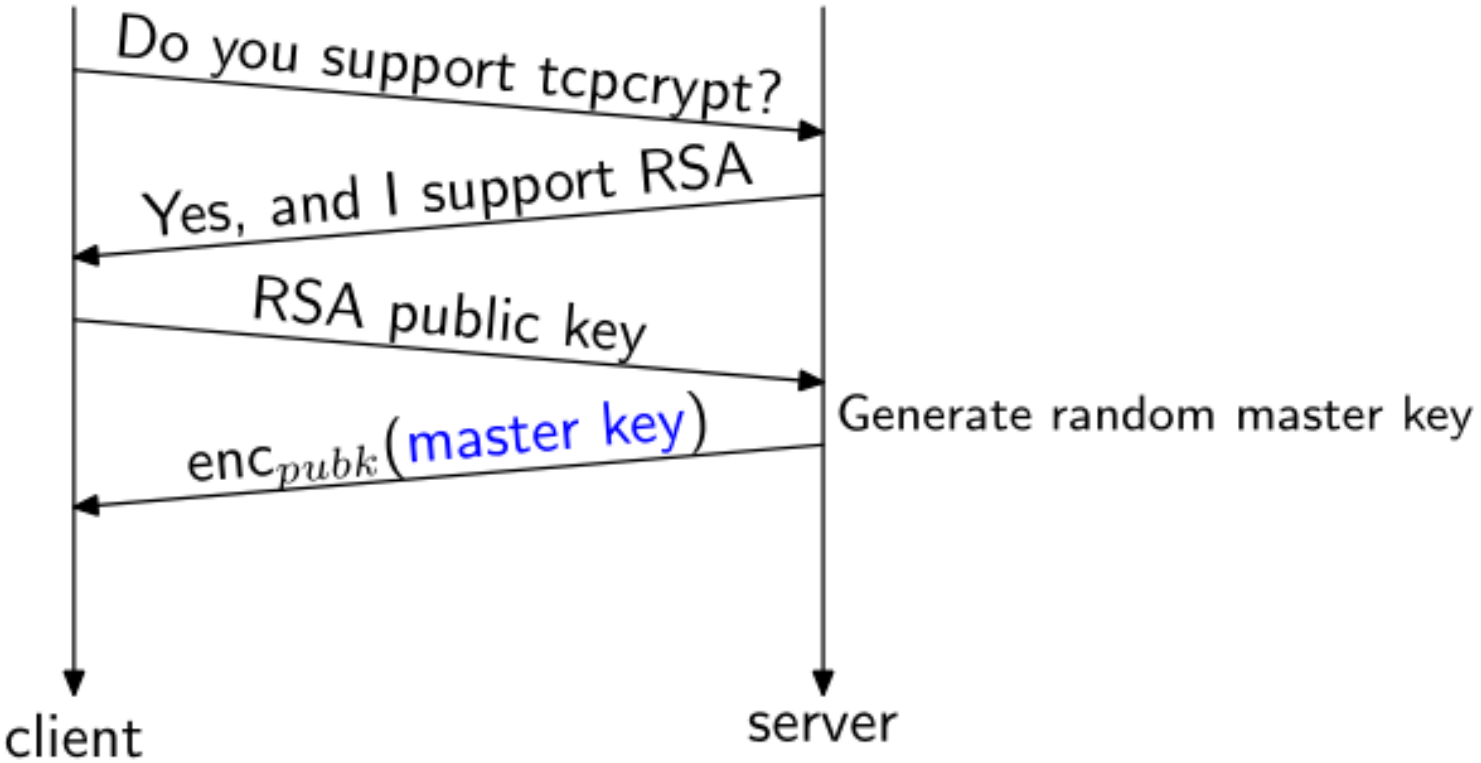
La cifratura dipende dall'autenticazione del server, a sua volta garantita dall'autorità certificatrice.

- Se l'autenticazione è falsa, la cifratura non è molto utile (ma l'overhead rimane)

tcpcrypt

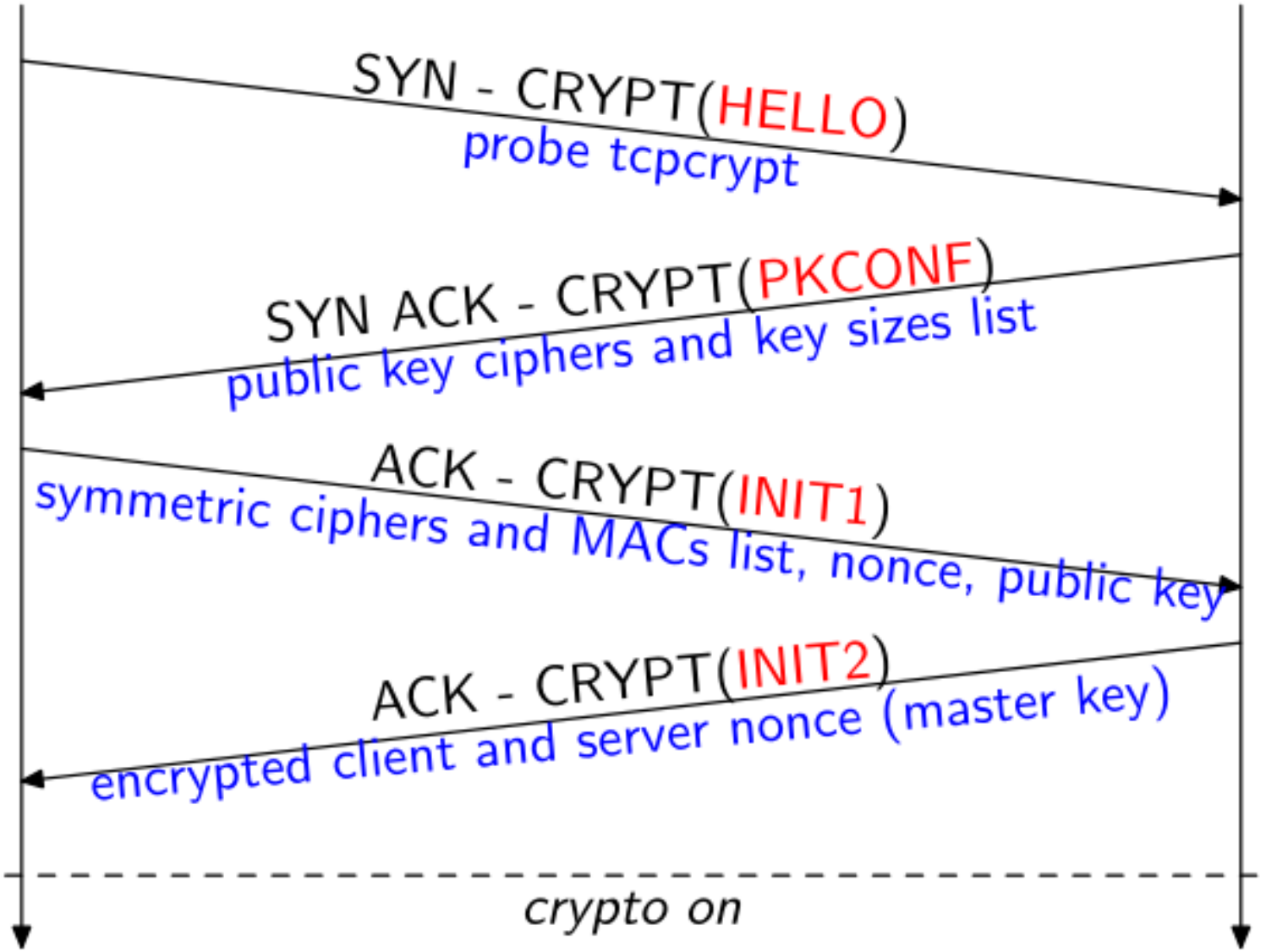
- Estensione di TCP
- Il carico computazionale crittografico è per lo piú spostato sui client
- Opportunistic encryption: attiva solo se supportata da entrambi (attenzione agli attacchi attivi!)

tcpcrypt handshake



36 volte piú veloce di TLS

tcpcrypt handshake



Autenticazione

Non c'è autenticazione del server con CA come nel caso di TLS, ma un session ID probabilisticamente unico (anche quando uno dei nodi è malevolo).
Un segreto condiviso k può essere usato cosí

1. $C \rightarrow S : HASH(k, C|SessionID)$
2. $S \rightarrow C : HASH(k, S|SessionID)$

Se anche S è malevolo (e k non generabile da un dizionario), non potrà riusare k (non estraibile da $HASH(k, C|SessionID)$) né $HASH(k, C|SessionID)$ perché il $SessionID$ sarà diverso.

Riassumendo

- tcpcrypt è un'estensione di TCP, che permette di cifrare il livello di trasporti
- è molto piú efficiente di TLS perché il carico crittografico è per lo piú spostato sui client
- Il Session ID permette di costruire protocolli di autenticazione a livello applicativo