Alberto Ferrante

Security Association caching of a dedicated IPSec crypto-processor: dimensioning the cache and software interface

Relatore: Prof. Roberto Negrini

Correlatore: Dott. Jefferson Owen (STM)

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

IPSec

- Fornisce servizi relativi alla sicurezza a livello del protocollo IP:
  - Protegge i dati provenienti dai livelli superiori dello stack
  - Protegge gli header dei datagrammi IP
- È altamente configurabile/flessibile

1 2 3 4 5 6

IPSec – SA

- Il funzionamento di IPSec è basato sulle *Security Association* (SA):
  - Sono dei “canali di comunicazione” protetti
  - Sono monodirezionali

1
2
3
4
5
6

IPSec - IKE

- La creazione delle SA è eseguita tramite il protocollo *Internet Key Exchange*
- IKE permette di:
  - Negoziare le SA
    - Algoritmi da utilizzare e loro impostazioni
    - Protocolli da utilizzare
  - Scambiare le chiavi da usare negli algoritmi crittografici a chiave simmetrica

1 2 3 4 5 6

IPSec – AH ed ESP

- Implementano la sicurezza delle comunicazioni
- Possono essere combinati o usati singolarmente per ottenere il livello di sicurezza desiderato
- Possono essere usati sia in Tunnel sia in Transport Mode

1
2
3
4
5
6

IPSec–Transport e Tunnell Mode

- Il Transport Mode:
  - Mantiene la struttura del datagramma iniziale
  - Aggiunge informazioni e/o modifica i dati
- Il Tunnell Mode:
  - Crea un nuovo datagramma
  - Tratta il vecchio datragramma (header+payload) come un pacchetto di dati da proteggere

1 2 3 4 5 6

ESP - Transport e Tunnell Mode

- Transport mode: protegge i dati provenienti dai livelli superiori criptandoli

- Tunnel mode: protegge sia i dati che lo header IP tramite la crittografia

1 2 3 4 5 6

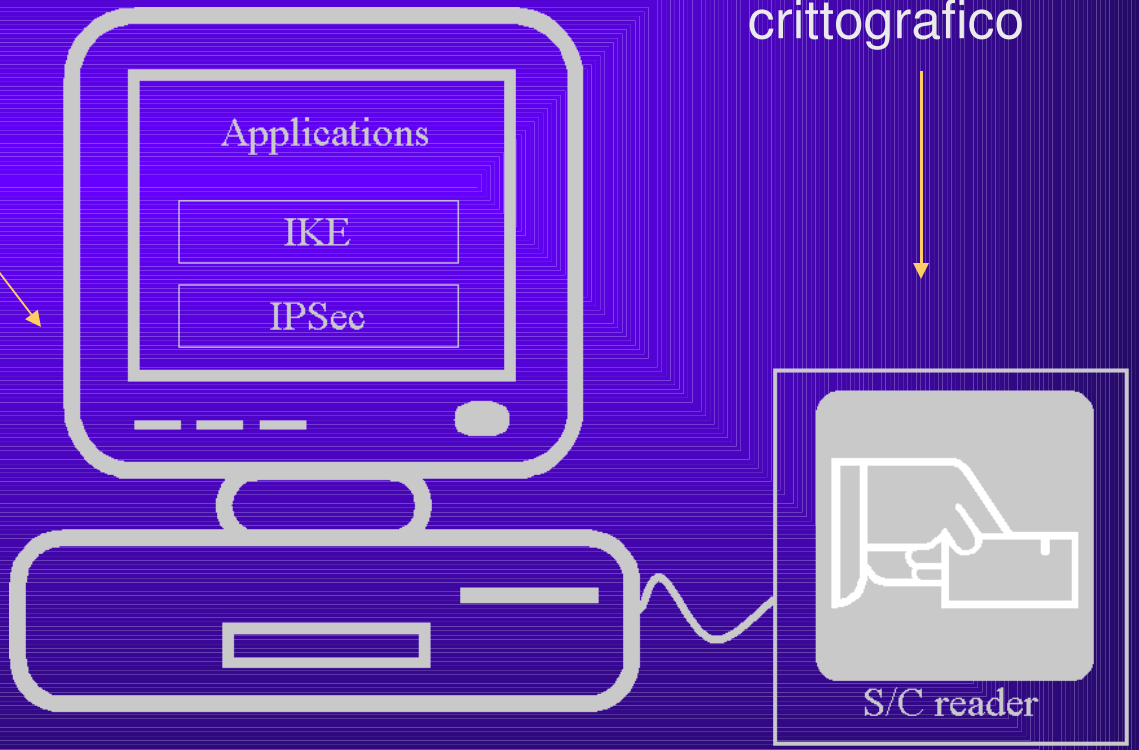
Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

Descrizione del sistema

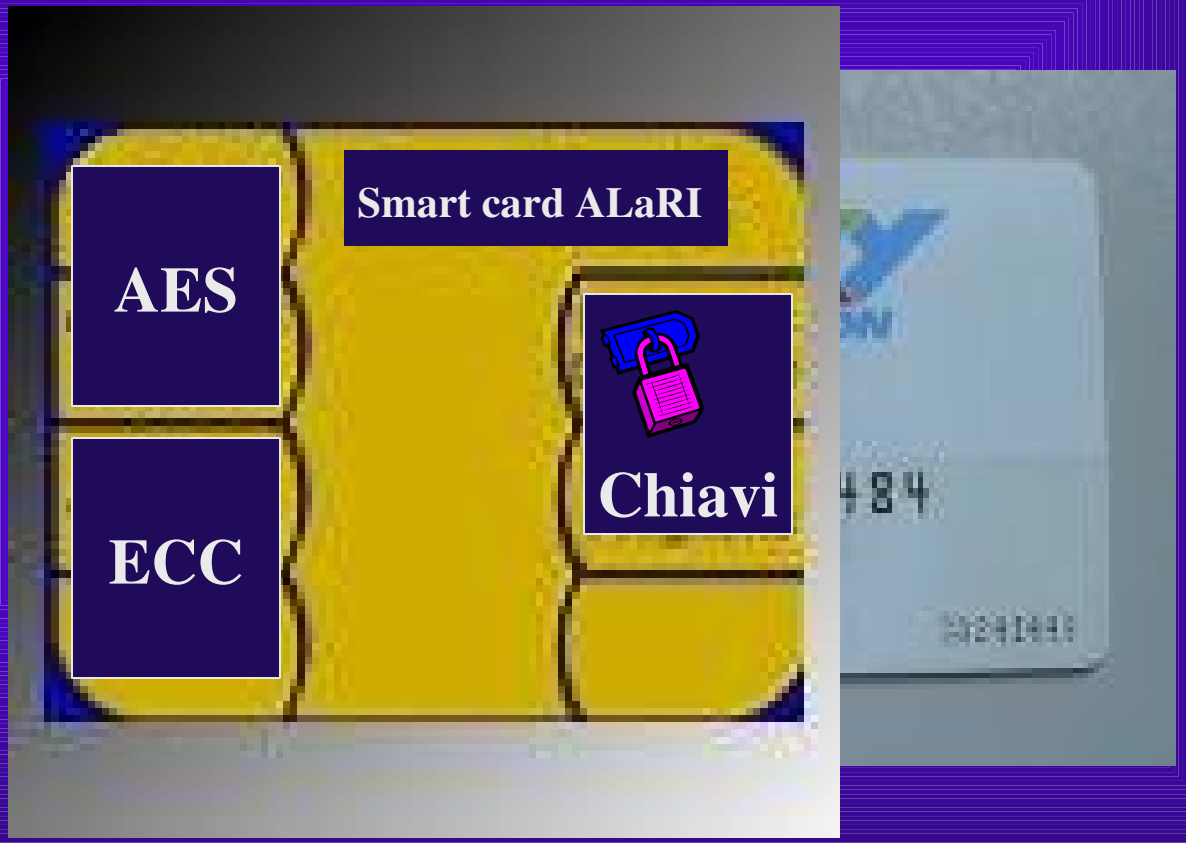
Host sul quale è installato lo stack contenente IPSec

crypto-smart card/ processore crittografico



1
2
3
4
5
6

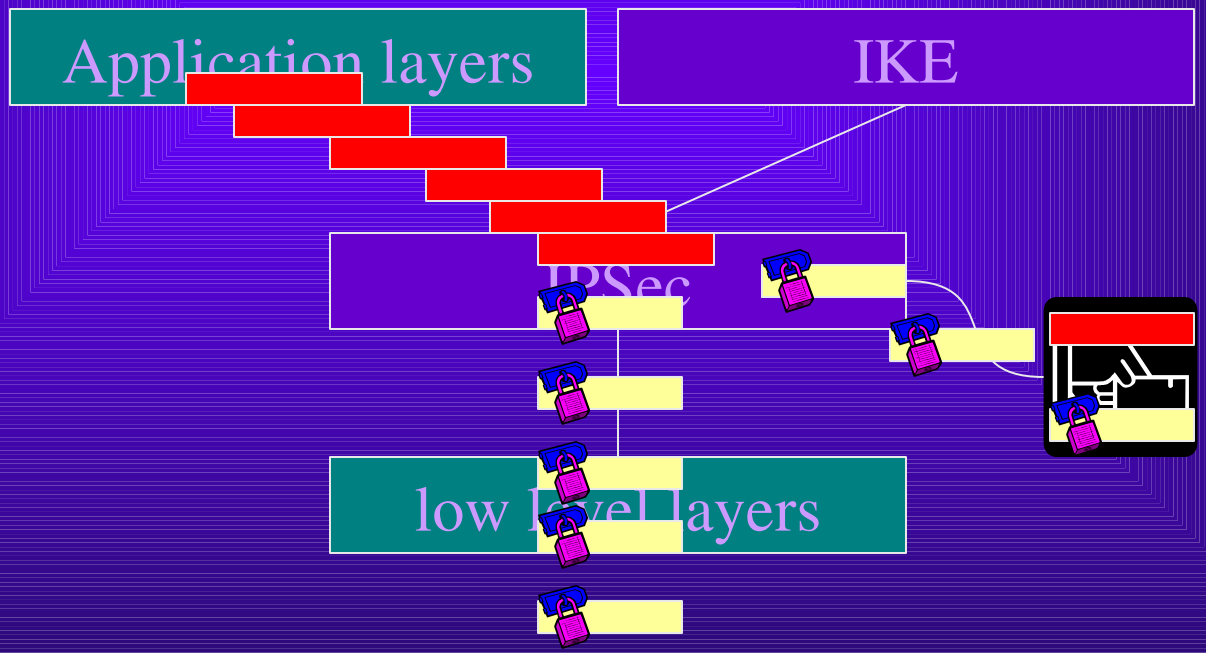
Caratteristiche della smart card



1
2
3
4
5
6

Come funziona il sistema

IPSec usa i servizi di crittografia forniti dalla smart card



1
2
3
4
5
6

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

Obiettivi del progetto

- Progettare l'interfaccia software tra il processore crittografico ed IPSec
- Studiare la dimensione ottima della cache delle SA

1
2
3
4
5
6

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

La security policy

- Specifica tutte le considerazioni legate alla sicurezza ed alle performance del sistema nel suo complesso
- Definisce i servizi che il processore crittografico deve fornire
- Mette in evidenza alcuni problemi e propone le soluzioni da adottare

1 2 3 4 5 6

Il problema della chiavi

- Le chiavi non devono essere rivelate all'esterno del processore crittografico:
  - Devono essere tenute nella memoria del processore stesso
  - Il processore ha una memoria limitata

Solo un numero limitato di SA potrebbe essere aperto in ogni istante

1 2 3 4 5 6

Il problema delle chiavi - soluzione

- Usare un meccanismo di caching delle chiavi tra processore crittografico e host:
  - Le chiavi vengono criptate con AES prima di essere salvate sull'host.
- Il meccanismo di caching si può usare anche per altri dati relativi alle SA: l'insieme di queste informazioni e delle chiavi forma la *cache delle SA*.

1 2 3 4 5 6

L'interfaccia software

- E' stato definito l'insieme di comandi che il processore crittografico deve supportare per permettere il corretto funzionamento di IPSec
- E' stato definito il protocollo software di comunicazione
- E' stata scritta un'implementazione di riferimento dell'interfaccia in C++

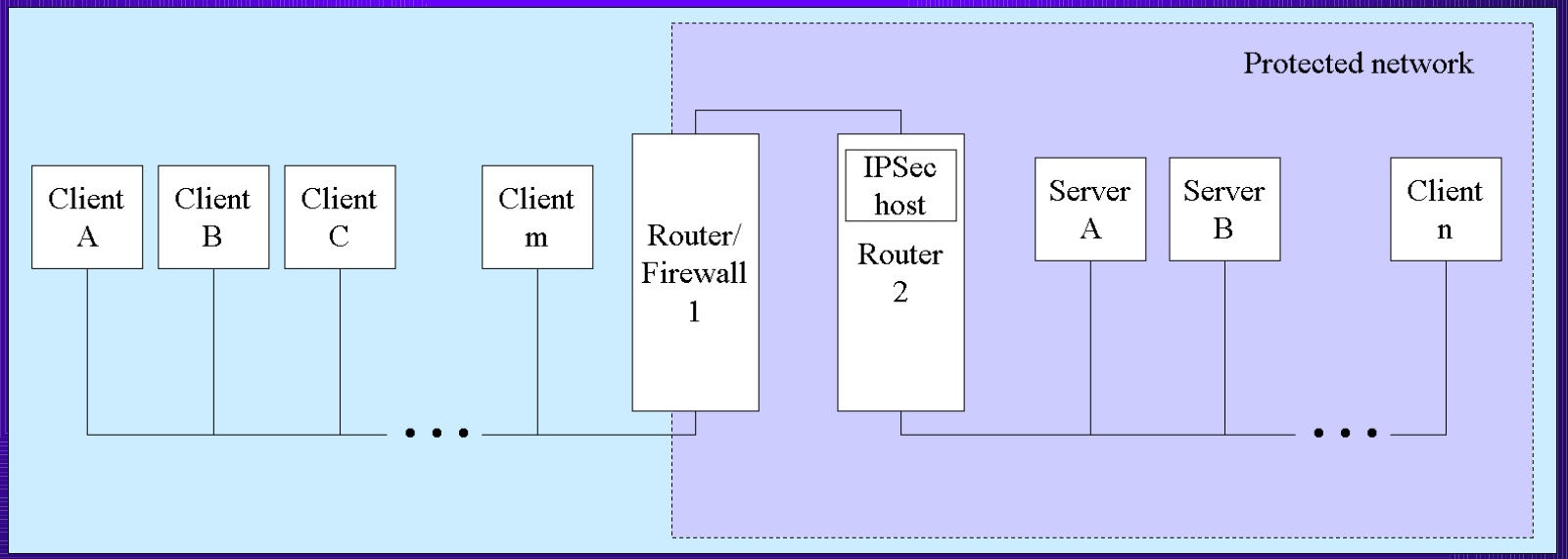
1 2 3 4 5 6

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

Caching delle SA (1)

- Consideriamo il processore crittografico impiegato in un sistema ad alto bitrate (200Mbit/s)



Caching delle SA (2)

- Lo studio è stato condotto tramite due tipi di simulazioni:
  - Considerando solo il numero di cache miss
  - Considerando anche i ritardi introdotti dal sistema crittografico
    - Questo permette di valutare il bitrate supportato dal sistema

1 2 3 4 5 6

Caching delle SA – dati

- forniti dallo “Internet Traffic Archive”
- riguardano un sistema con bitrate di circa 300kbit/s
- Riguardano 1,8 milioni di pacchetti IP
- Contengono:
  - timestamp
  - Indirizzi IP so
  - Porte TCP sor
  - Dimensione del pacchetto (header esclusi)

```
0.010445 2 1 2436 23 2
0.023775 1 2 23 2436 2
0.026558 2 1 2436 23 1
0.029002 3 4 3930 119 42
0.032439 4 3 119 3930 15
0.049618 1 2 23 2436 1
0.052431 5 2 14037 23 2
```

1 2 3 4 5 6

Simulazione cache miss

- Simula il comportamento del sistema ogni volta che una SA deve essere utilizzata:
  - Legge una riga del file di dati
  - Controlla se la corrispondente SA è già nella cache:
    - Se lo è (cache found), prosegue
    - Se non lo è (cache miss), la SA viene caricata in cache, eventualmente effettuando un replace

1 2 3 4 5 6

Cache miss - risultati

Dim. cache (#elementi)	Cache miss totali	Cache miss evitabili	Riuso elementi
16	798593 (44,61%)	794888 (44,41%)	2,24
32	382498 (21,37%)	378793 (21,16%)	4,68
64	124369 (6,95%)	120664 (6,74%)	14,39
128	25122 (1,40%)	21417 (1,20%)	71,25
256	11892 (0,66%)	8187 (0,46%)	150,52
512	8056 (0,45%)	4351 (0,24%)	222,19

Cache miss non evitabili: 3705

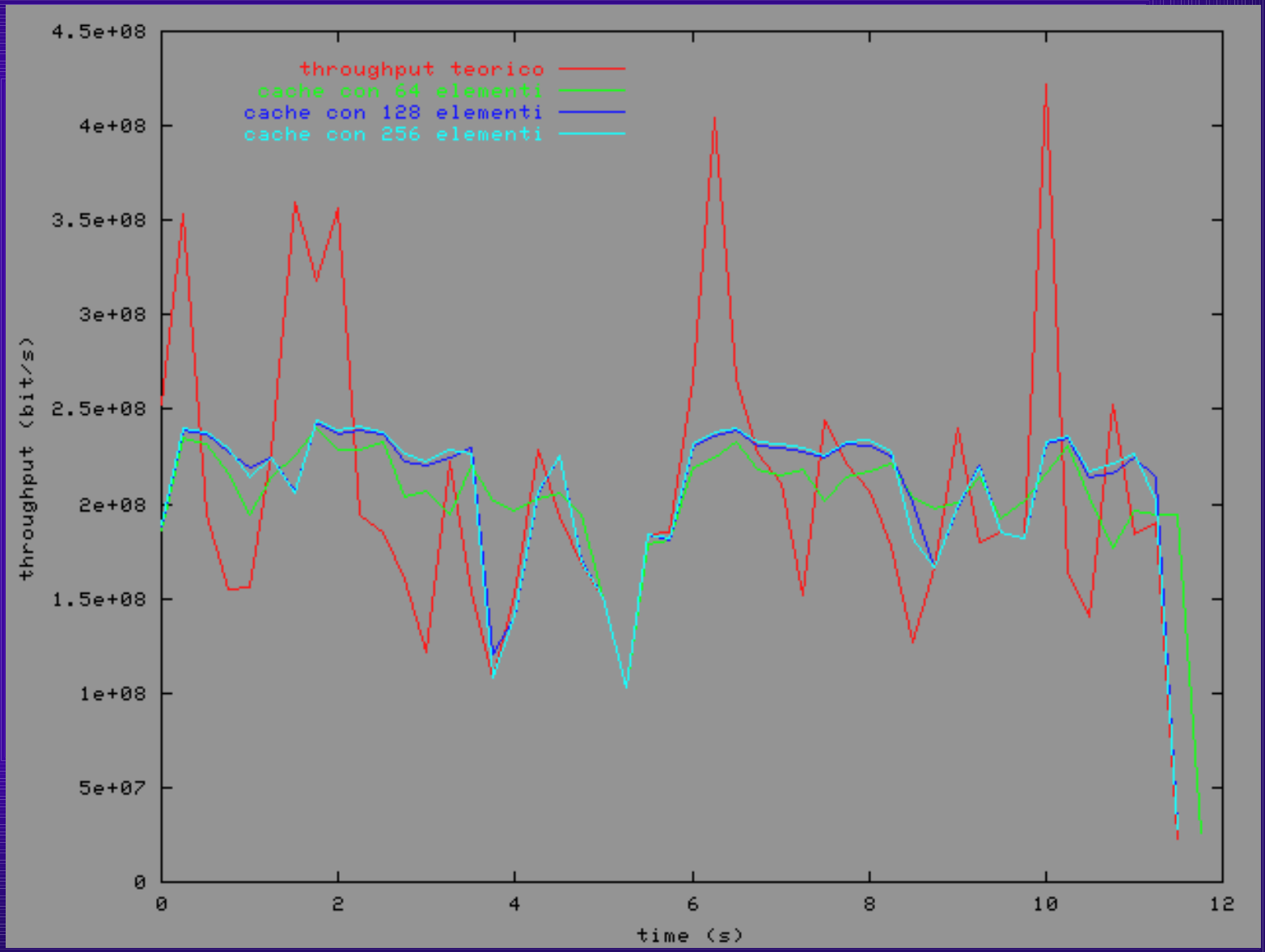
Riuso medio SA: 483

Simulazione – throughput

- E’ basata sulla precedente
- Tiene in considerazione il tempo necessario a trattare i pacchetti:
  - Trasferimento dati dall’host al processore crittografico e viceversa
  - Tempo per l’esecuzione degli algoritmi crittografici
  - Tempo introdotto nel caso di cache miss/found

1 2 3 4 5 6

Throughput – (AES@60MHz)



1 2 3 4 5 6

Throughput - conclusioni

- La soluzione migliore è quella di utilizzare una cache di 128 elementi (8kb), unita a un hardware AES funzionante a 60MHz

1
2
3
4
5
6

Approssimazioni introdotte

- I timestamp sono stati moltiplicati per un fattore
- Non si è tenuto conto della fase di creazione delle SA: si suppone che queste siano già state precedentemente create

1 2 3 4 5 6

Tener conto di IKE fase 1 e 2

- Si sono valutati i ritardi da introdurre
- Si è studiata la simulazione
- Si è concluso che con i dati a disposizione non è possibile scrivere una simulazione di questo tipo che sia di una qualche utilità

1 2 3 4 5 6

Sommario

1. La suite di protocolli IPSec
2. Descrizione del sistema
3. Obiettivi del progetto
4. Il progetto dell'interfaccia
5. Caching delle SA
6. Conclusioni

Conclusioni

- E’ stata scritta l’interfaccia software tra il processore crittografico ed il calcolatore host
- E’ stata valutata la dimensione ottima della cache delle SA da utilizzare nel caso di processore crittografico usato su un router

1 2 3 4 5 6