

A Query Unit for the IPSec Databases

Alberto Ferrante, Satish Chandra

ALaRI, University of Lugano E-mail: {ferrante, kaverips}@alari.ch Vincenzo Piuri

DTI, University of Milano E-mail: piuri@dti.unimi.it



Outline

IPSec

The Database Query Unit

Multithreaded Unit

Simulations

Conclusions and Future Work

IPSec

The Database Query Unit

Multithreaded Unit

Simulations

Conclusions and Future Work



IPSec

IPSec

IPSec

- AH, ESP
- Databases
- Security
- Associations
- Main IPSec
- Processing Steps
- Database Query
- The Database Query Unit
- Multithreaded Unit
- Simulations
- Conclusions and Future Work

- Is a suite of protocols
 - ★ adding security at IP (network) level;
 - makes extensive use of cryptographic functions.



AH, ESP

IPSec

IPSec

AH, ESP

- Databases Security Associations Main IPSec Processing Steps
- Database Query
- The Database Query Unit
- Multithreaded Unit

Simulations

Conclusions and Future Work

- ✓ IPSec is mainly composed of two protocols:
 - ✗ Authentication Header (AH);
 - **×** Encapsulating Security Payload (ESP);
 - both protocols can be used in:
 - **x** transport mode;
 - **×** tunnel mode.



Databases

IPSec

IPSec

AH, ESP

Databases

Security

Associations

Main IPSec

Processing Steps Database Query

The Database Query

Unit

Multithreaded Unit

Simulations

Conclusions and Future Work ✓ IPSec uses two databases:

x the Security Policy Database (SPD); **x** the Security Association Database (SAD):

✓ the records are the Security Associations (SAs).

Advanced Learning and Research Institute ALaRI

Security Associations

IPSec

Università

della Svizzera

italiana

IPSec

AH, ESP

Databases

Security

Associations

Main IPSec

Processing Steps

Database Query

The Database Query Unit

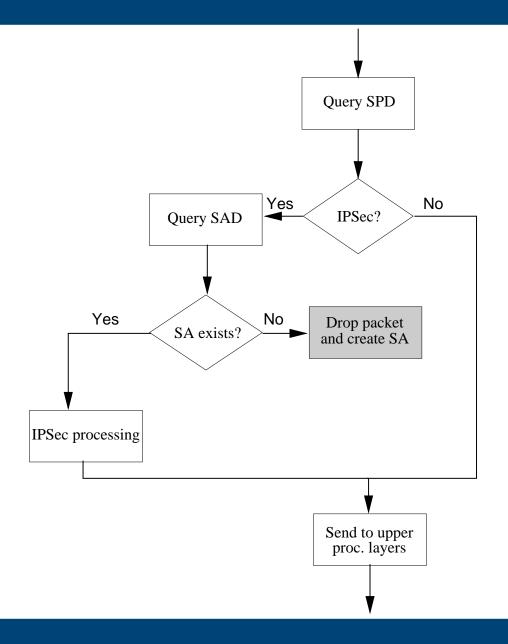
Multithreaded Unit

Simulations

Conclusions and Future Work Each SA contains:

- x protocol/algorithms settings;
- **x** keys for cryptographic algorithms;
- ✓ SAs are mono-directional:
 - two SAs need to be created for normal bidirectional communications.

Main IPSec Processing Steps



SECRYPT 2007 - July 30, 2007

Università

della Svizzera italiana Advanced 👘

Learning and Research Institute ALaRI



Database Query

IPSec

IPSec

AH, ESP

Databases

Security

Associations

Main IPSec

Processing Steps

Database Query

The Database Query Unit

Multithreaded Unit

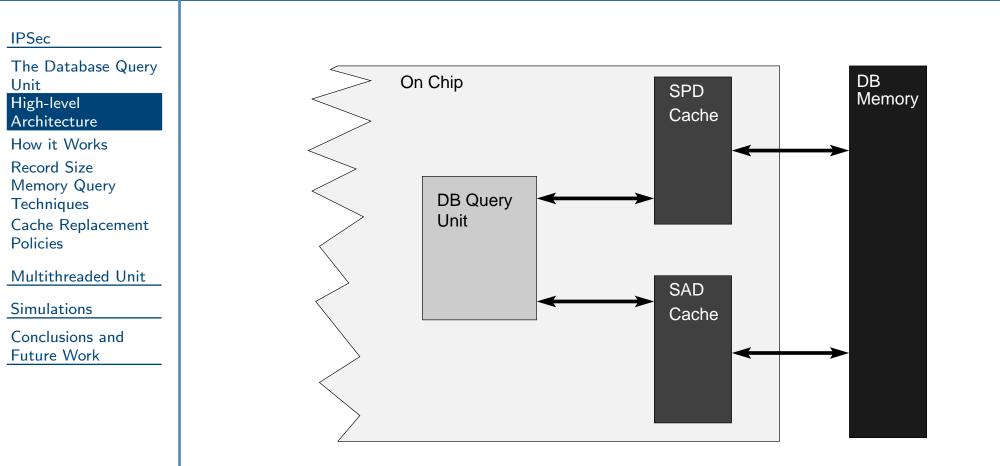
Simulations

Conclusions and Future Work More than 3 million queries/s in a 1Gbit/s system (worst case);
 may be a bottleneck;
 may become a weak point (DoS).

SECRYPT 2007 – July 30, 2007



High-level Architecture



Caches are Content Addressable Memories.

SECRYPT 2007 – July 30, 2007

A. Ferrante, A Query unit for the IPSec Databases – 9 / 20



How it Works

IPSec

- The Database Query Unit High-level Architecture
- How it Works
- Record Size Memory Query Techniques Cache Replacement Policies
- Multithreaded Unit
- Simulations
- Conclusions and Future Work

SPD query:

- **x** cache query;
- **x** main DB query if not in cache;

SAD query:

- **x** cache query;
- **x** main DB query if not in cache:
 - ✓ SPD-provided pointer.



Record Size

IPSec

- The Database Query Unit
- High-level
- Architecture
- How it Works

Record Size

- Memory Query Techniques Cache Replacement Policies
- Multithreaded Unit

Simulations

Conclusions and Future Work

SPD:

- two parts:
 - x repeatedly used information
 (IP, SA pointers, ...);
 - x rarely used information (proposals);
- repeatedly used information (232 bits) are cached.

SAD:✓ all fields are repeatedly used (792 bits).

Memory Query Techniques

IPSec

Università

della Svizzera

italiana

The Database Query Unit

Advanced

and Resear

Learning

Institute ALaRI

- High-level
- Architecture
- How it Works
- Record Size
- Memory Query Techniques
- Cache Replacement Policies

- Multithreaded Unit
- Simulations
- Conclusions and Future Work

- Linear LookUp Technique (LLUT);
 - **x** memory queried in a linear fashion;
 - Partitioned LookUp Technique (PLUT).
 - **x** memory divided into pages;
 - **×** IP address is used
 - to associate a record to a page;
 - **×** linear search inside the pages;
 - **×** "fragmentation" problem.



Cache Replacement Policies

IPSec

The Database Query Unit

High-level

Architecture

How it Works

Record Size

Memory Query

Techniques

Cache Replacement Policies

Multithreaded Unit

Simulations

Conclusions and Future Work

First In First Out;Least Recently Used.

SECRYPT 2007 – July 30, 2007

A. Ferrante, A Query unit for the IPSec Databases – 13 / 20



Parallelizing Queries

IPSec

The Database Query Unit

Multithreaded Unit Parallelizing Queries

Simulations

Conclusions and Future Work Queries in memory take a long time;
 other queries in cache can be done during this time;

✓ parallel queries related to the same SA are not allowed.

SECRYPT 2007 – July 30, 2007

A. Ferrante, A Query unit for the IPSec Databases – 14 / 20



Simulation Description

IPSec

The Database Query Unit

Multithreaded Unit

Simulations Simulation Description

Design Space Queries/second Sequential System: SAD and SPD Query Times Multithreaded System: SAD and SPD Query Times

Conclusions and Future Work SystemC functional model;
 simulates behavior and delays of the blocks;

✓ input: ITA tracefiles.

SECRYPT 2007 – July 30, 2007

A. Ferrante, A Query unit for the IPSec Databases – 15 / 20

Design Space

IPSec

Università

della

Svizzera

italiana

The Database Query Unit

Advanced

and Researc

Learning

Institute ALaRI

Multithreaded Unit

Simulations Simulation

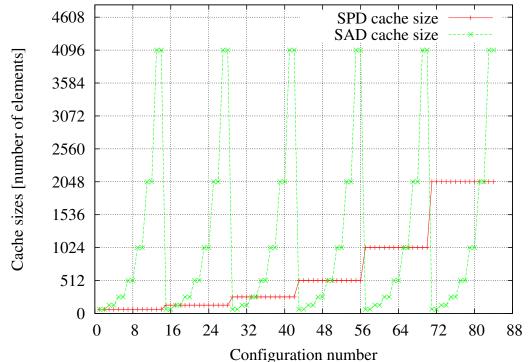
Description

Design Space

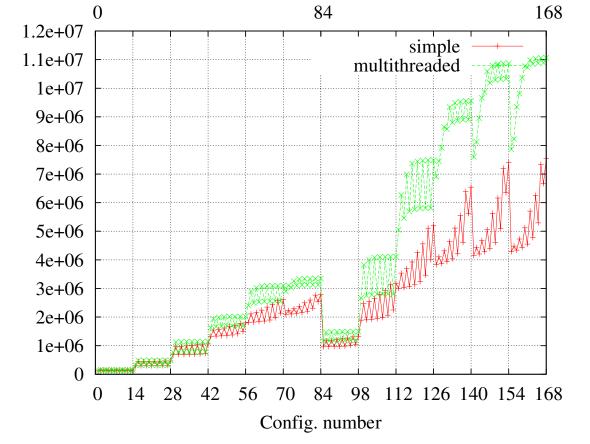
Queries/second Sequential System: SAD and SPD Query Times Multithreaded System: SAD and SPD Query Times

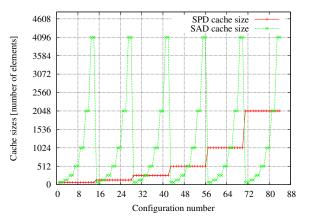
Conclusions and Future Work 168 different configurations;
 LLUT for the first 84 configurations, PLUT for the others;

✓ FIFO for odd configurations, LRU for even ones.



Queries/second





Università

della Svizzera

italiana

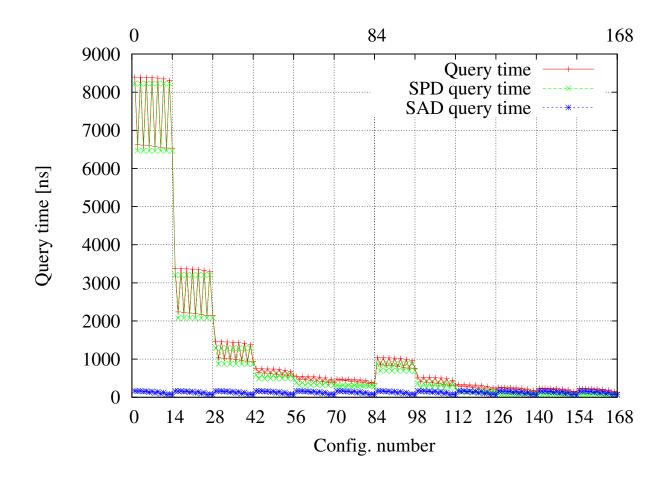
Advanced

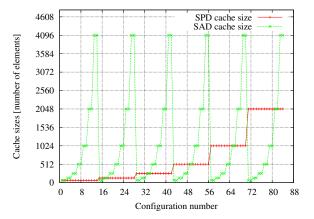
Learning and Resea

Institute ALaRI



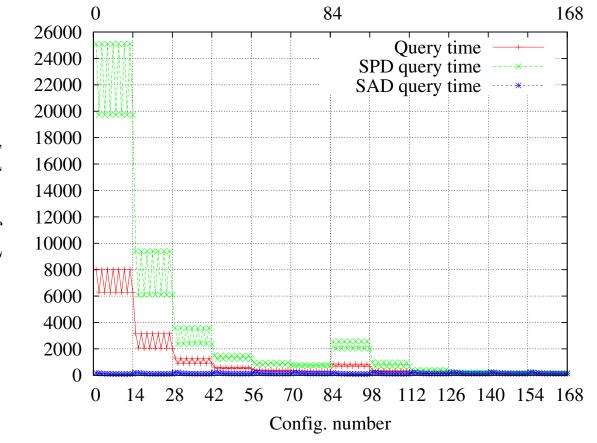
Sequential System: SAD and SPD Query Times

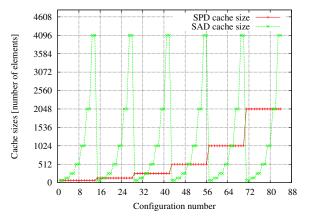






Multithreaded System: SAD and SPD Query Times





Query time [ns]



Conclusions and Future Work

IPSec

The Database Query Unit

Multithreaded Unit

Simulations

Conclusions and Future Work Conclusions and Future Work We designed a DB query unit:

- ✓ able to exceed
- 11 million queries per second;✓ efficient.

Future Work:

- more accurate simulations;
- ✓ out of order queries.