Université Libre de Bruxelles

Implementation of High-Level Cryptographic Protocols using a SoC platform

June 24th, 2015

Quentin Delhaye

Contents

1. Context
2. Cryptographic protocols
3. Platform
4. Implementation
5. Results
6. Conclusion

- Internet of things
- Work done with Barco Silex

Objectives

- Real life use cases.
- Decrease CPU load.
- Improve performance.

Cryptographic protocols

VPN

- TLS
- IPsec

Schemes

- AES
- SHA-2
- Diffie-Hellman
- RSA

Contents

1 Context

2 Cryptographic protocols

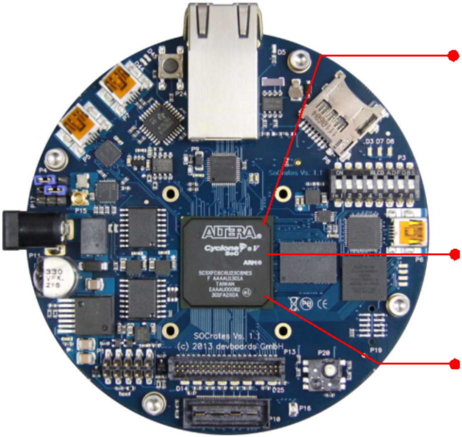
3 Platform
- Hardware
- Operating System

4 Implementation

5 Results

6 Conclusion

SoCrates

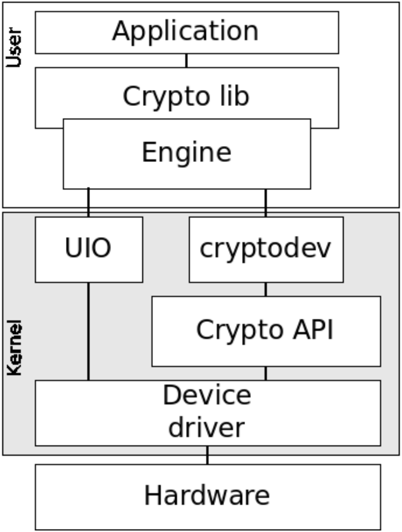


ARM Cortex A9
dual core
800MHz

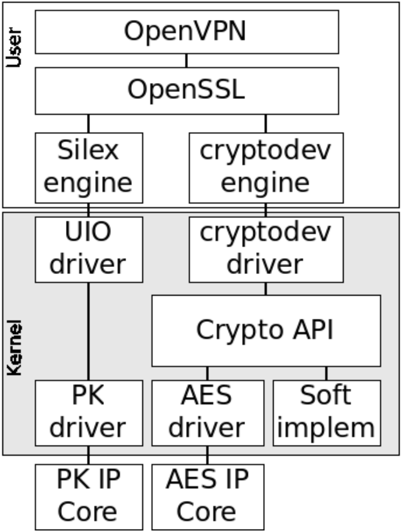
Altera Cyclone V

Barco Silex IP Cores
PK
AES

Linux structure



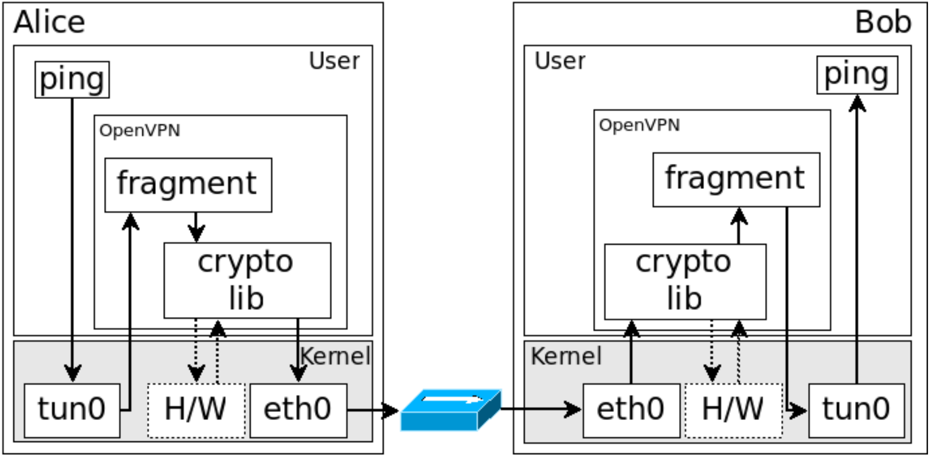
Linux structure (Cont'd)



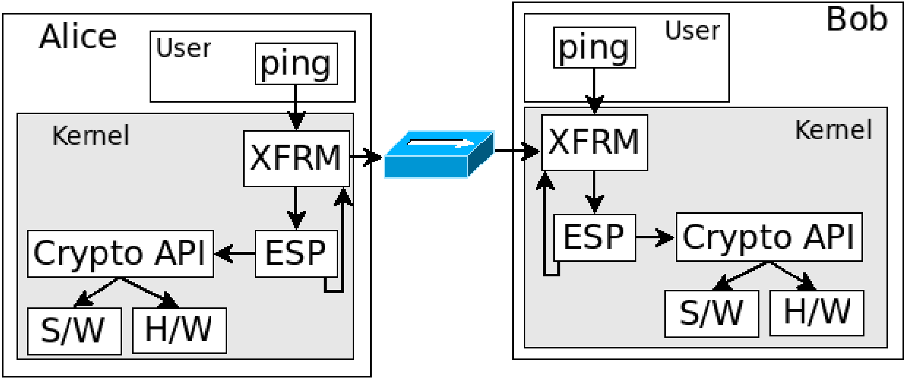
Contents

1. Context
2. Cryptographic protocols
3. Platform
4. Implementation
   - OpenVPN
   - IPsec
5. Results
6. Conclusion

OpenVPN


Alice
User
ping
OpenVPN
fragment
crypto lib
Kernel
tun0
H/W
eth0
Bob
User
ping
OpenVPN
fragment
crypto lib
Kernel
eth0
H/W
tun0

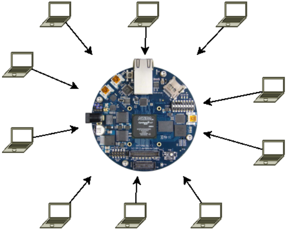
IPsec


Alice
User
ping
Kernel
XFRM
Crypto API
ESP
S/W
H/W
Bob
ping
User
XFRM
Kernel
ESP
Crypto API
S/W
H/W

Contents

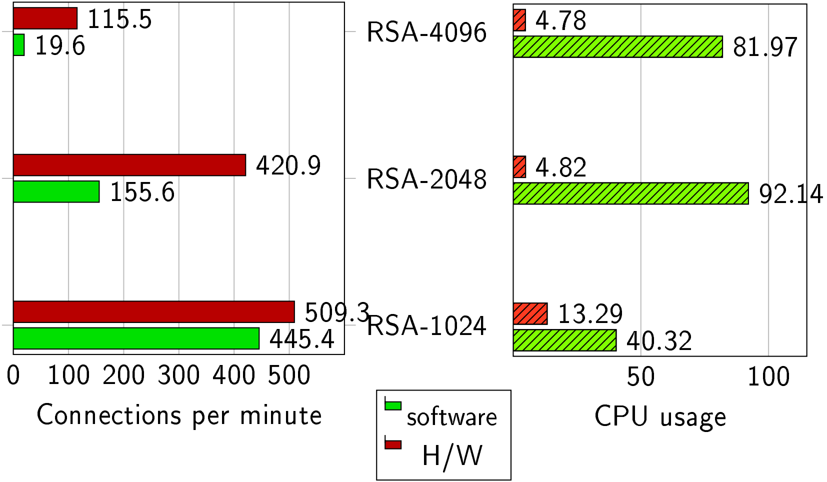
1. Context
2. Cryptographic protocols
3. Platform
4. Implementation
5. Results
   - TLS connections
   - File transfer
   - Interpretation
6. Conclusion

TLS connections – Context

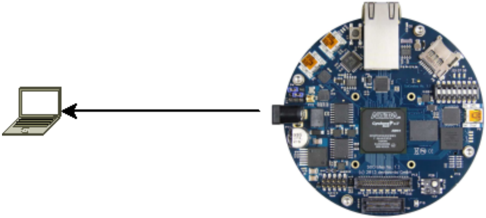


- 1 server, 10 clients
- 1-second connections
- RSA-1024/2048/4096
- OpenVPN

TLS connections – OpenVPN

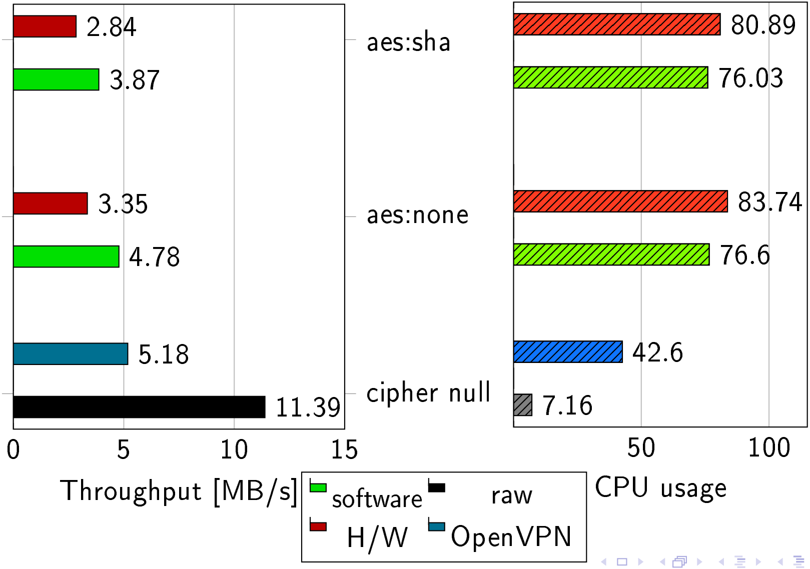


File transfer – Context

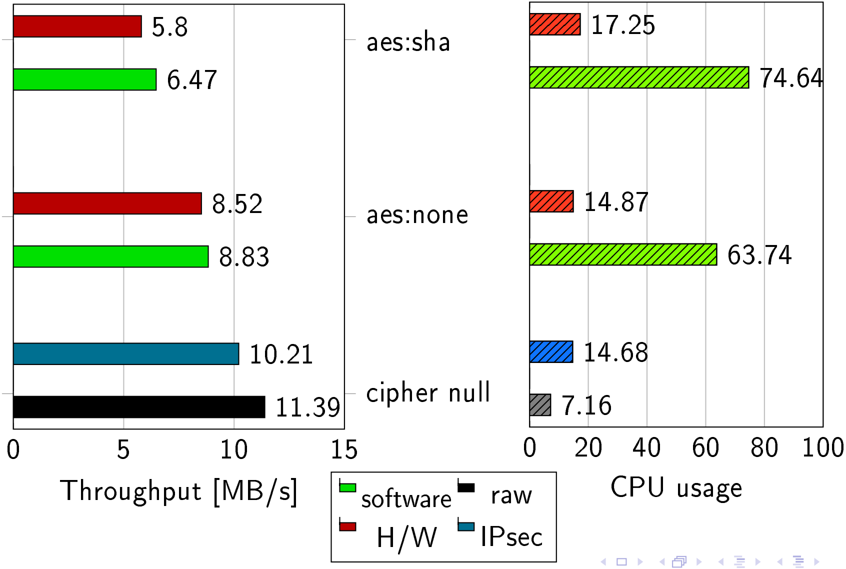


- 128MB file
- AES-256-CBC/SHA-256
- OpenVPN/IPsec

File transfer – OpenVPN



File transfer – IPsec



Results interpretation

- OpenVPN is single-threaded
- OpenVPN software overhead

Conclusion

TLS connections

- connections ×6
- CPU usage ÷20

File transfer

- Drop OpenVPN
- Performance −10%
- CPU usage ÷4

Conclusion

- Ongoing development
    - Test better hardware
    - Improve the drivers
- GCM is comming

Software GCM

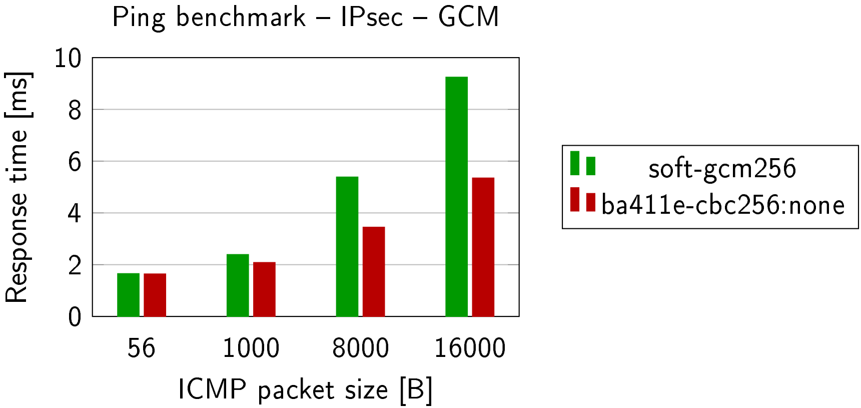


Figure: Software: asm kernel module mode GCM
Hardware: AES IP core mode CBC