



Université Libre de Bruxelles

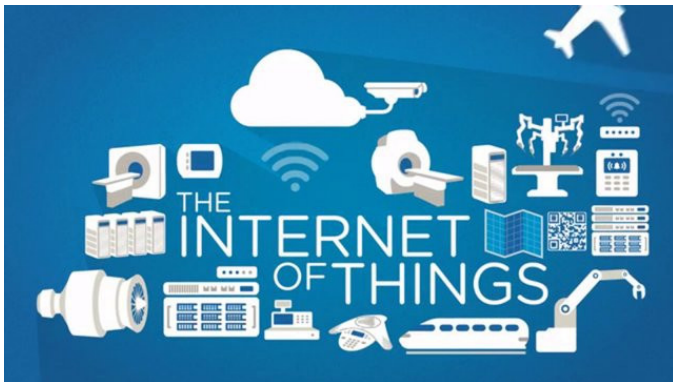
Implementation of High-Level Cryptographic Protocols using a SoC platform

June 24th, 2015

Quentin Delhay

Contents

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



- More connections, less power, same security
- Work done with Barco Silex

Objectives

- Use a dedicated hardware.
 - Real life use cases.
- Decrease CPU load.
- Improve performance.

Contents

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

Cryptographic protocols

VPN

- TLS
- IPsec

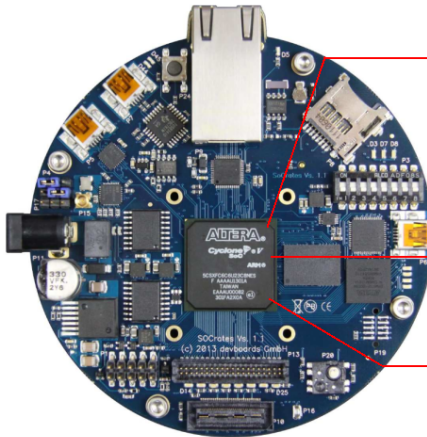
Schemes

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

Contents

- 1 Context
- 2 Cryptographic protocols
- 3 Platform**
 - Hardware
 - Operating System
- 4 Implementation
- 5 Results
- 6 Conclusion

SoCrates

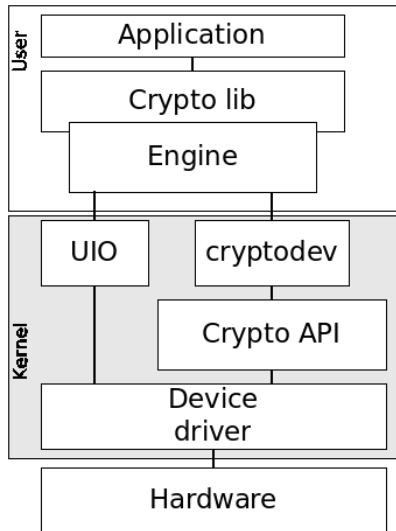


ARM Cortex A9
dual core
800MHz

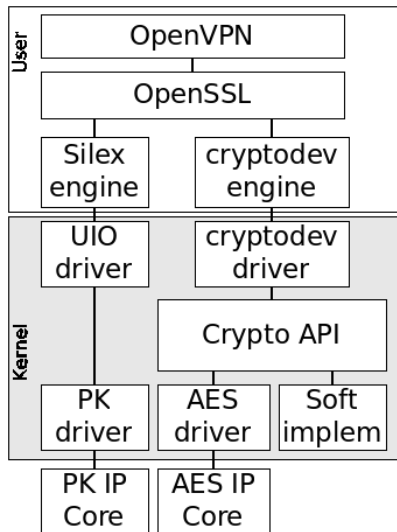
Altera Cyclone V

Barco Silex IP Cores
PK
AES

Linux structure



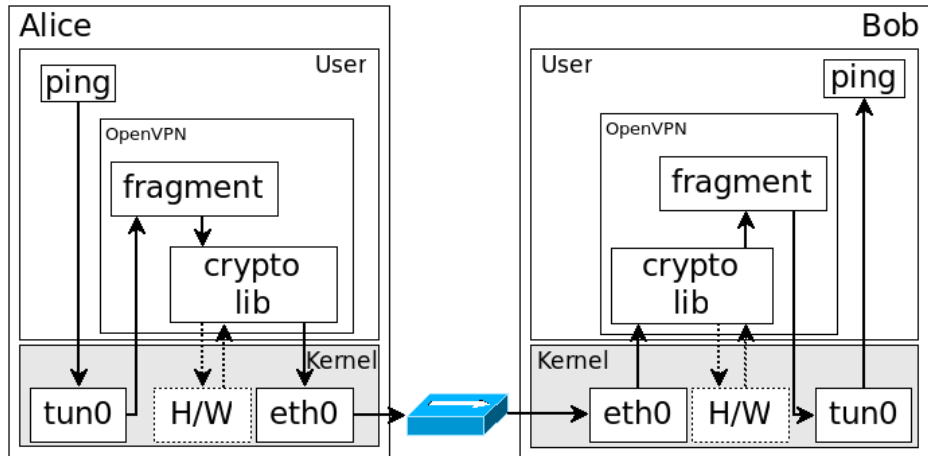
Linux structure (Cont'd)



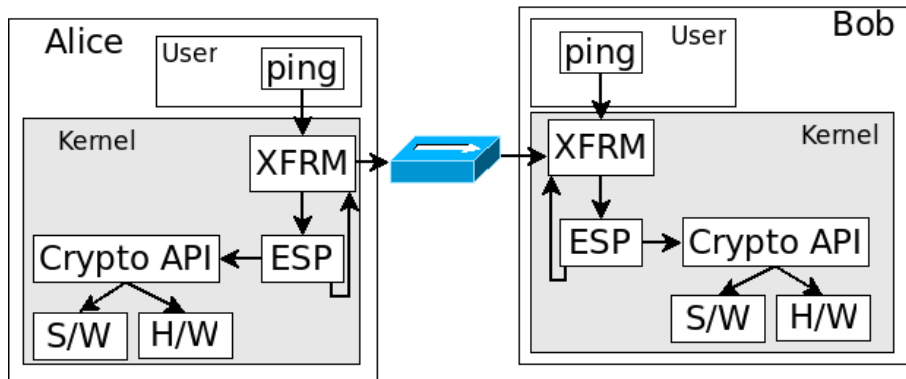
Contents

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

OpenVPN



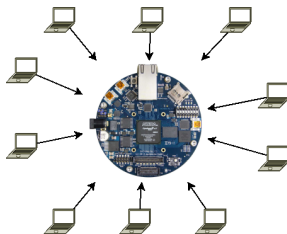
IPsec



Contents

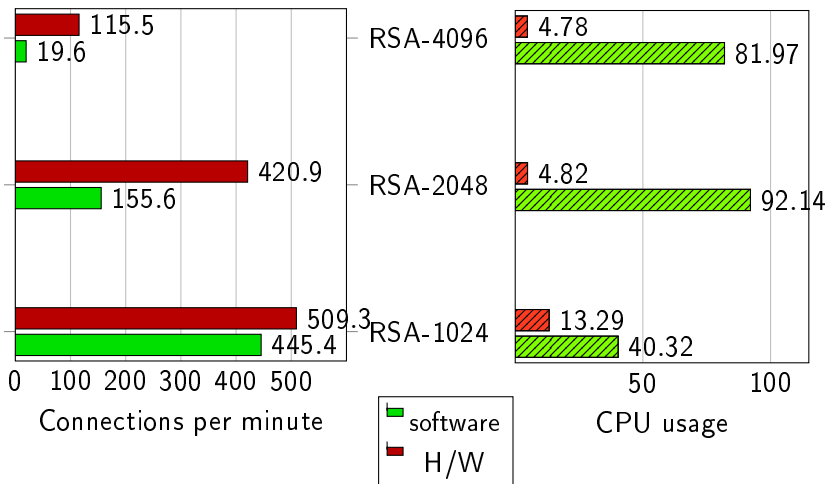
- 1 Context
- 2 Cryptographic protocols
- 3 Platform
- 4 Implementation
- 5 Results**
 - TLS connections
 - File transfer
 - Interpretation
- 6 Conclusion

TLS connections – Context

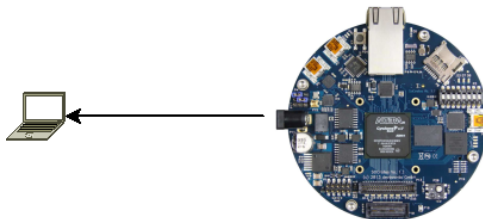


- 1 server, 10 clients
- 1-second connections
- RSA-1024/2048/4096
- OpenVPN

TLS connections – OpenVPN

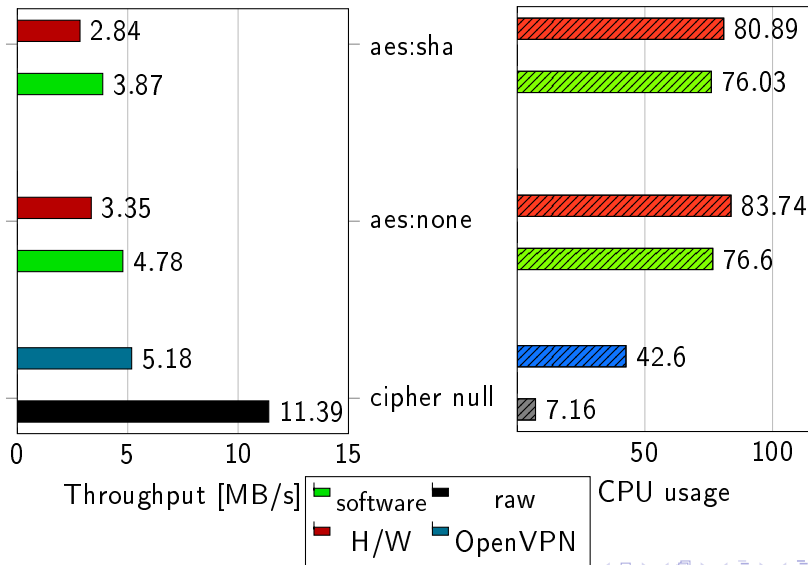


File transfer – Context

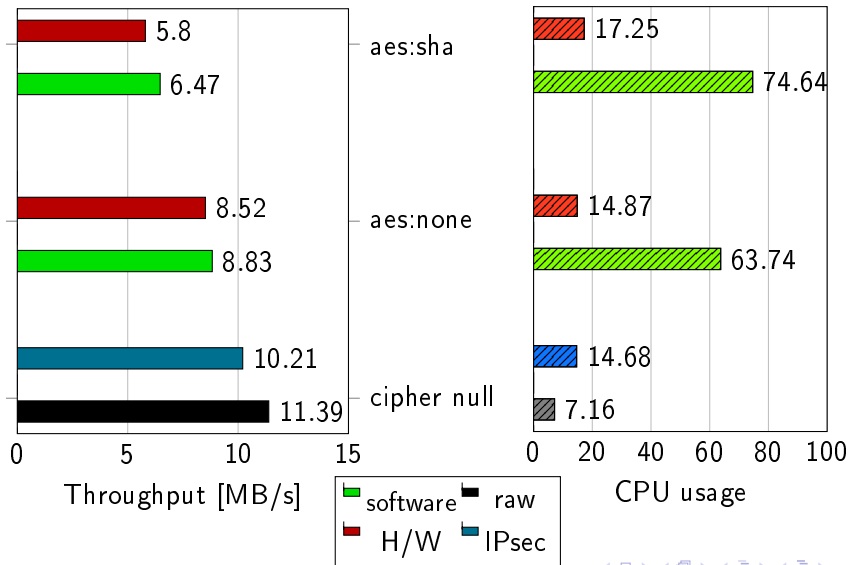


- 128MB file
- AES-256-CBC/SHA-256
- OpenVPN/IPsec

File transfer – OpenVPN



File transfer – IPsec



Results interpretation

TLS connections

- connections $\times 6$
- CPU usage $\div 17$

File transfer

- Drop OpenVPN
 - Performance -10%
 - CPU usage $\div 4$
-
- OpenVPN is single-threaded
 - OpenVPN software overhead
 - IPsec works in kernel

Conclusion

- Match implementation and application
- Interesting for low energy devices
- GCM mode is coming
- Ongoing development
 - Other platforms tested
 - Driver improvement

Software GCM

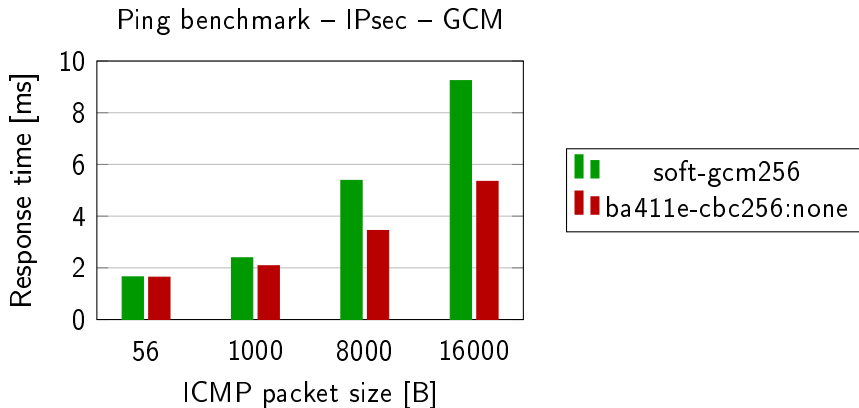
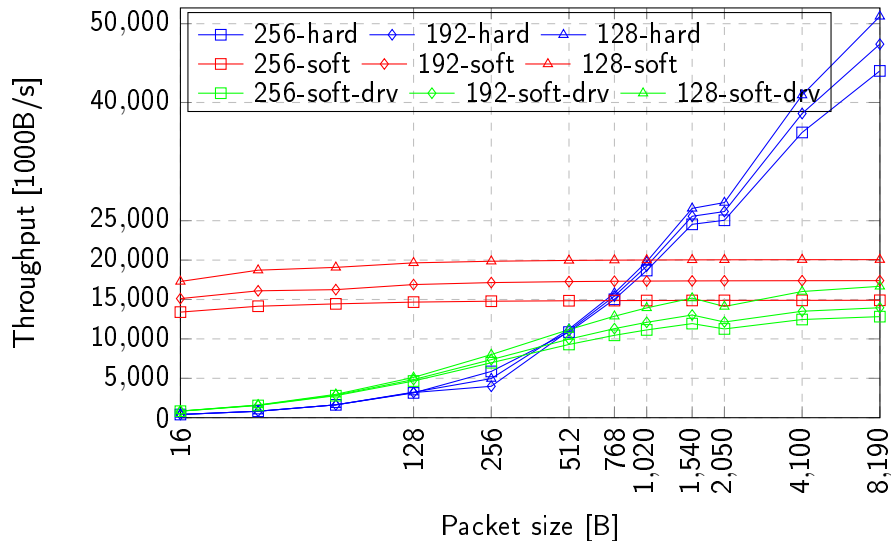


Figure: Software: asm kernel module mode GCM
Hardware: AES IP core mode CBC

OpenVPN file transfer – AES-256-CBC – MAC none

- Hardware top 3:
 - 1 Kernel memory handling
 - 2 Context switch
 - 3 IRQ restore
- Software top 3:
 - 1 AES encryption
 - 2 IRQ restore
 - 3 OpenVPN encryption routine

OpenSSL benchmark



TLS connection latency

		Connection time [s]	
RSA-1024	soft	0.041921	÷2
	BA411E	0.020312	
RSA-2048	soft	0.202945	÷5
	BA411E	0.039965	
RSA-4096	soft	1.436743	÷7.8
	BA411E	0.183533	

Table: OpenVPN connection time necessary to establish an aes-256-cbc connection with DHE.