Université Libre de Bruxelles

Implementation of High-Level Cryptographic Protocols using a SoC platform

June 24th, 2015

Quentin Delhaye

Contents

Objectives

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

Cryptographic protocols

VPN

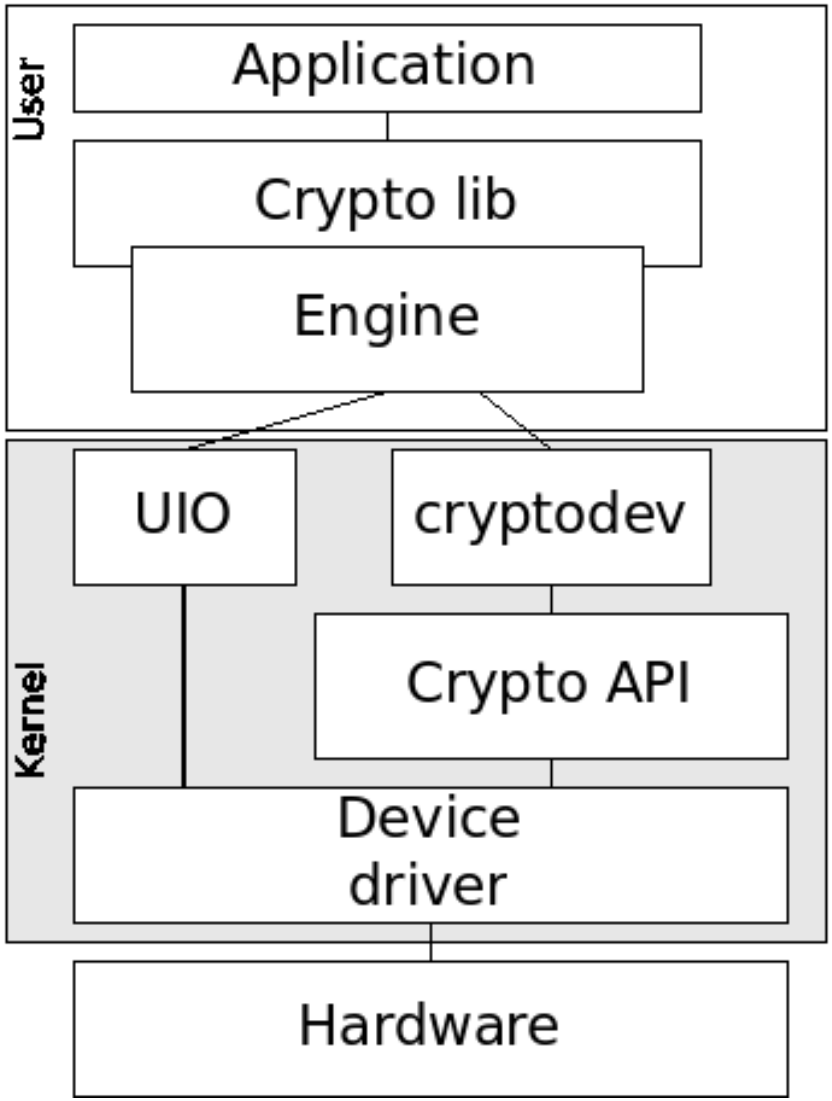
- TLS
- IPsec

Schemes

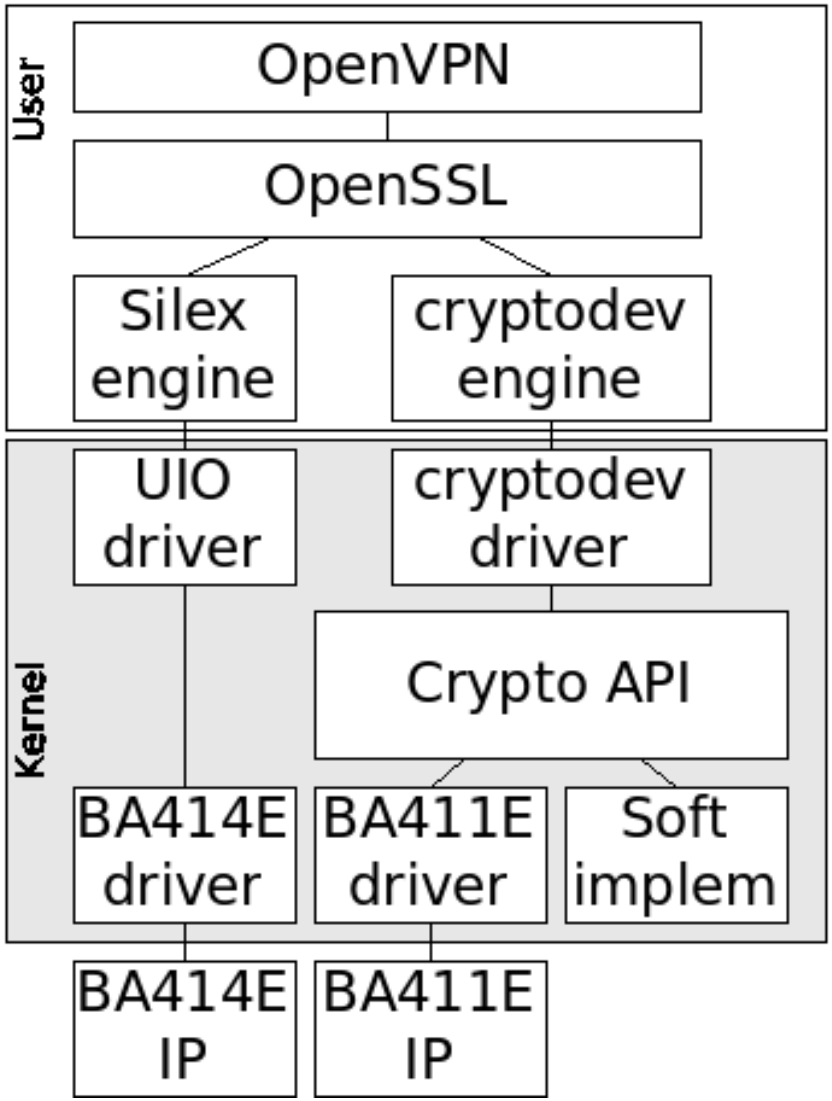
- AES
- SHA-2
- Diffie-Hellman
- RSA

Contents

Linux structure

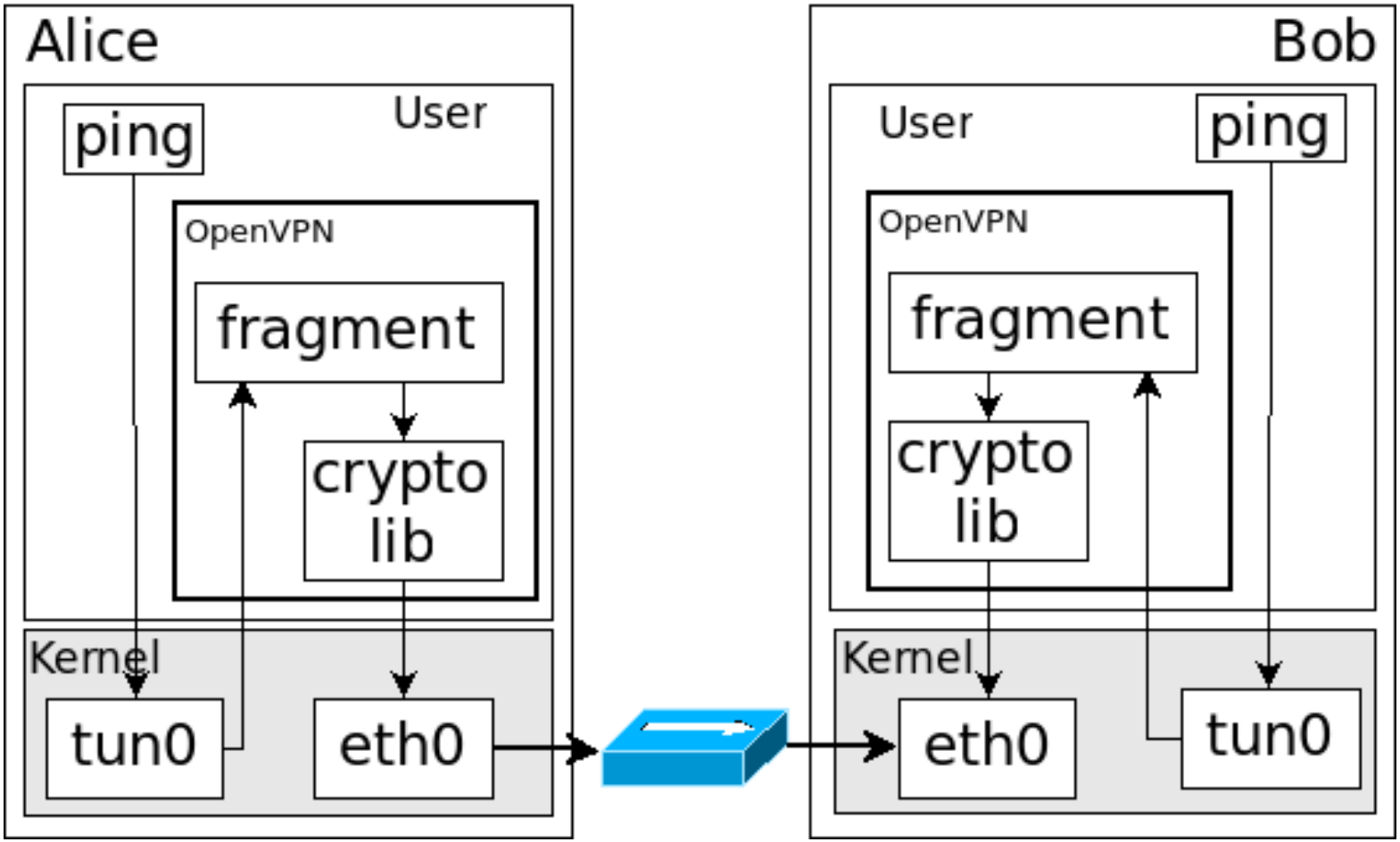


Linux structure (Cont'd)

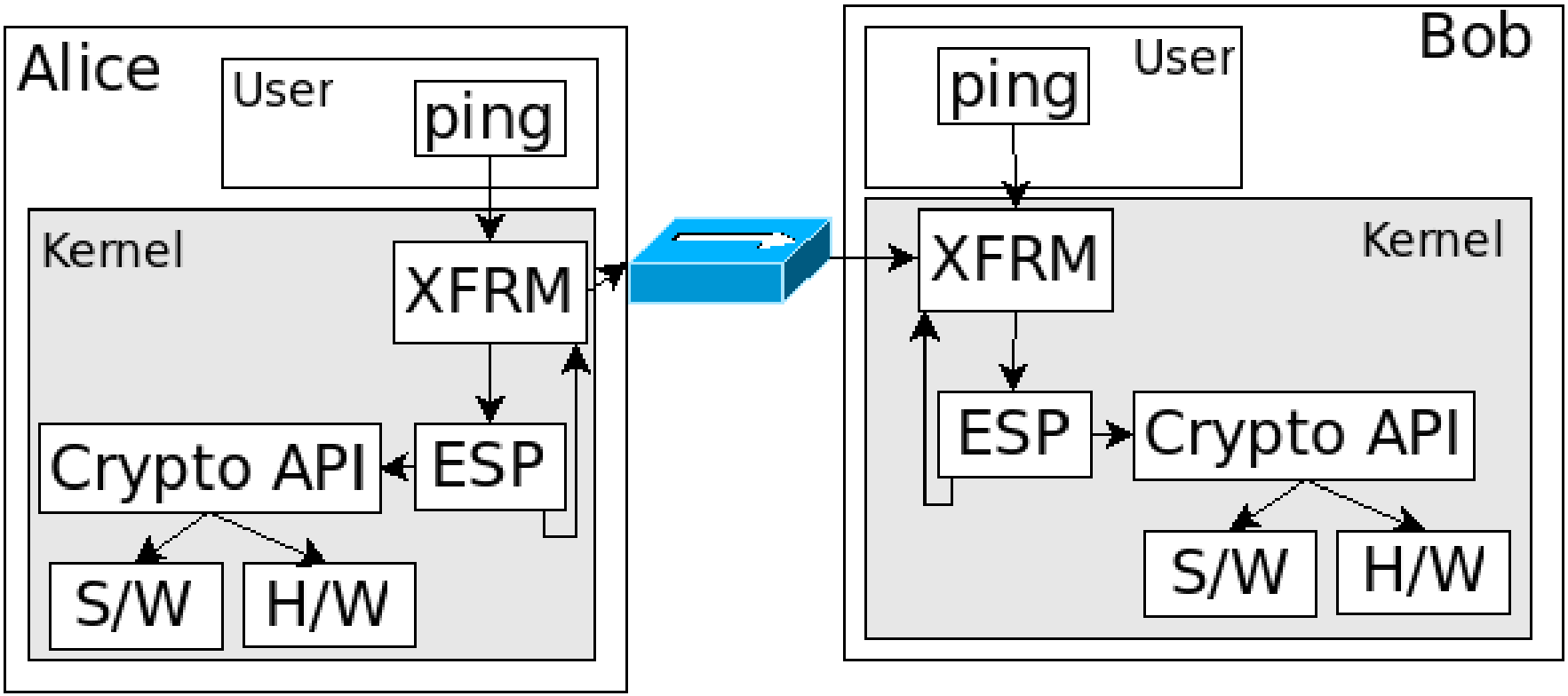


Contents

OpenVPN

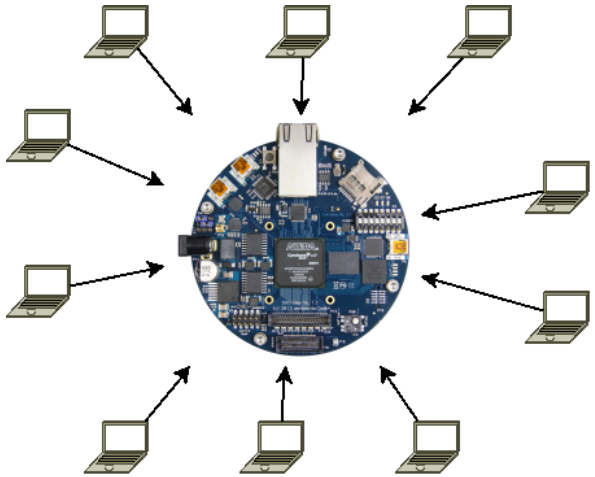

Alice
ping
User
OpenVPN
fragment
crypto
lib
Kernel
tun0
eth0
Bob
User
ping
OpenVPN
fragment
crypto
lib
Kernel
eth0
tun0

IPsec


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

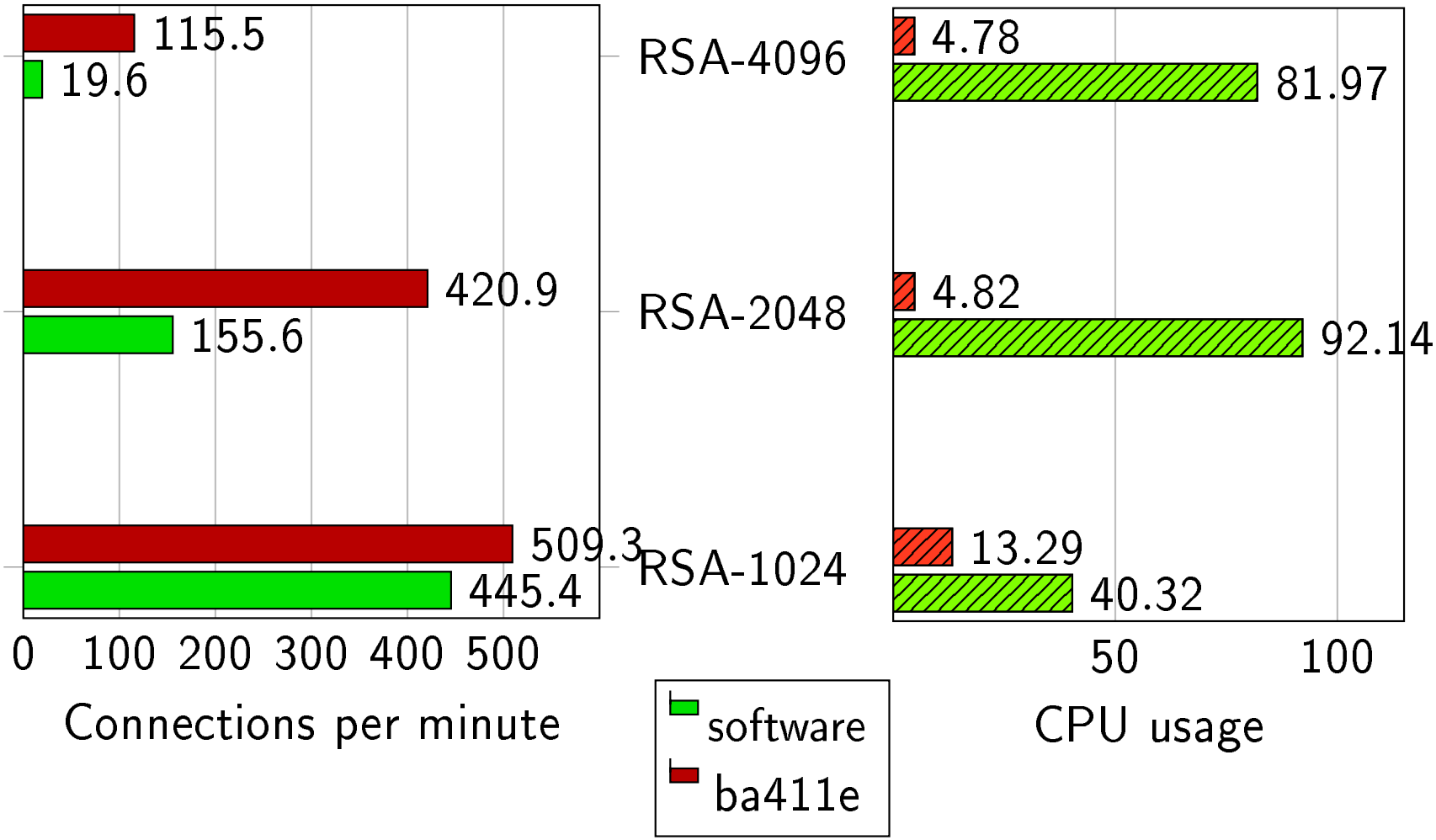
Contents

TLS connections – Context

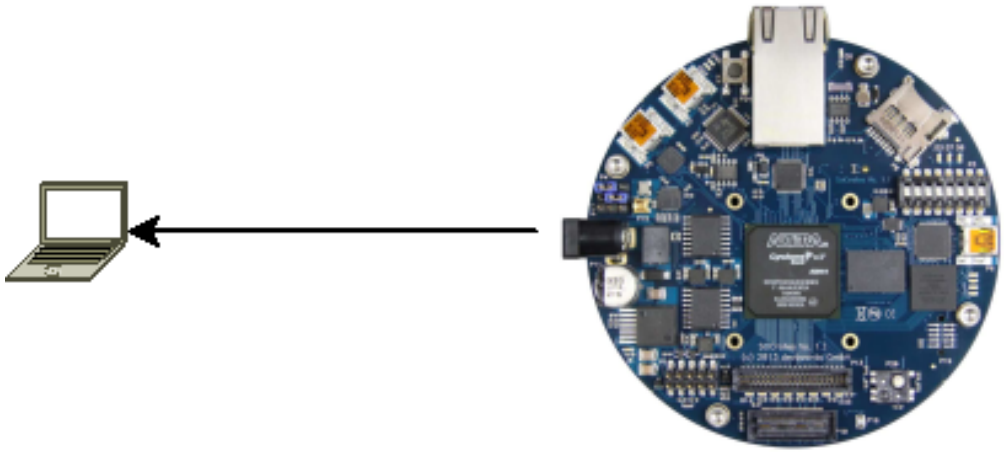


- 1 server, 10 clients
- 1-second connections
- RSA-1024/2048/4096
- OpenVPN

TLS connections – OpenVPN

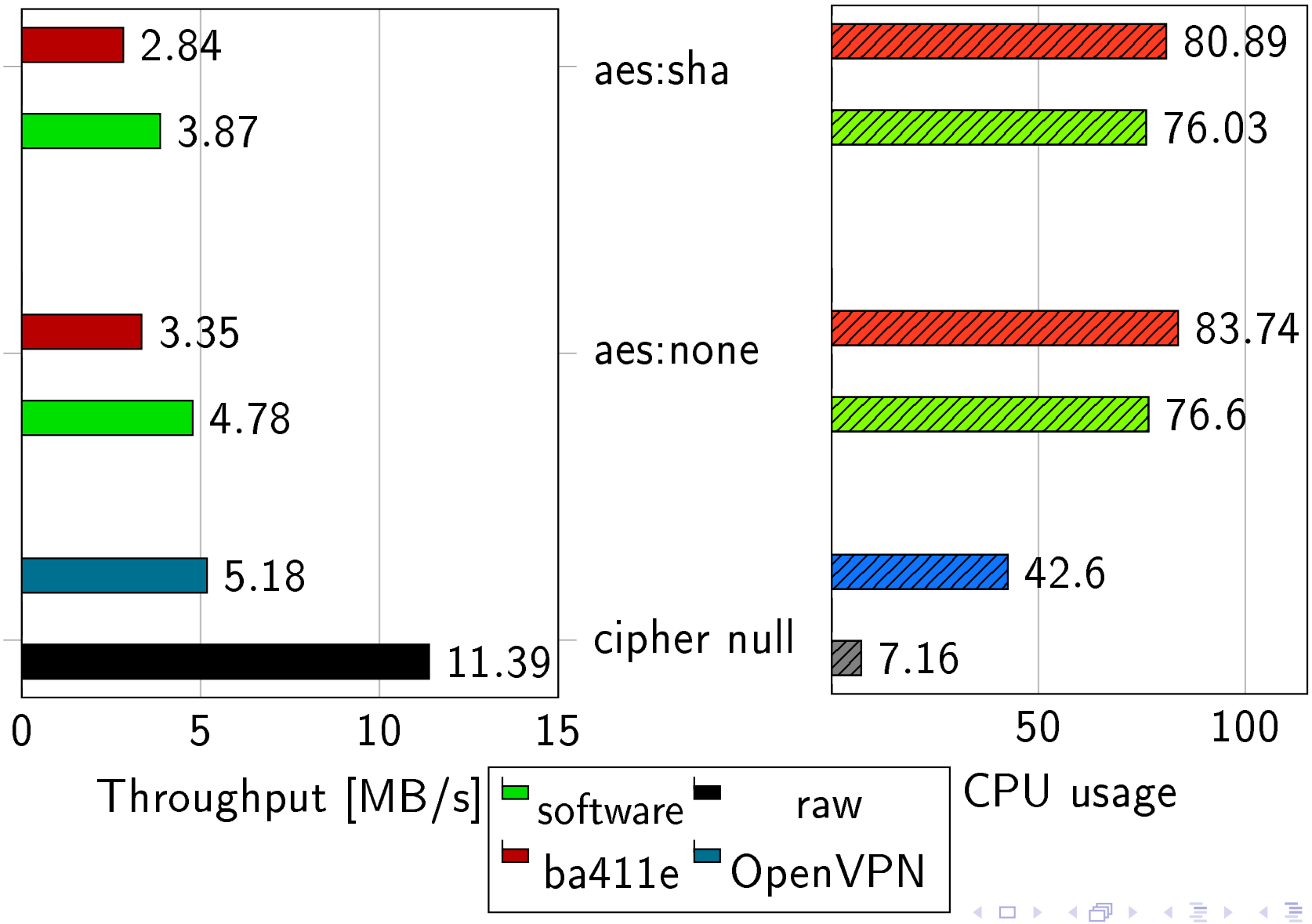


File transfer – Context

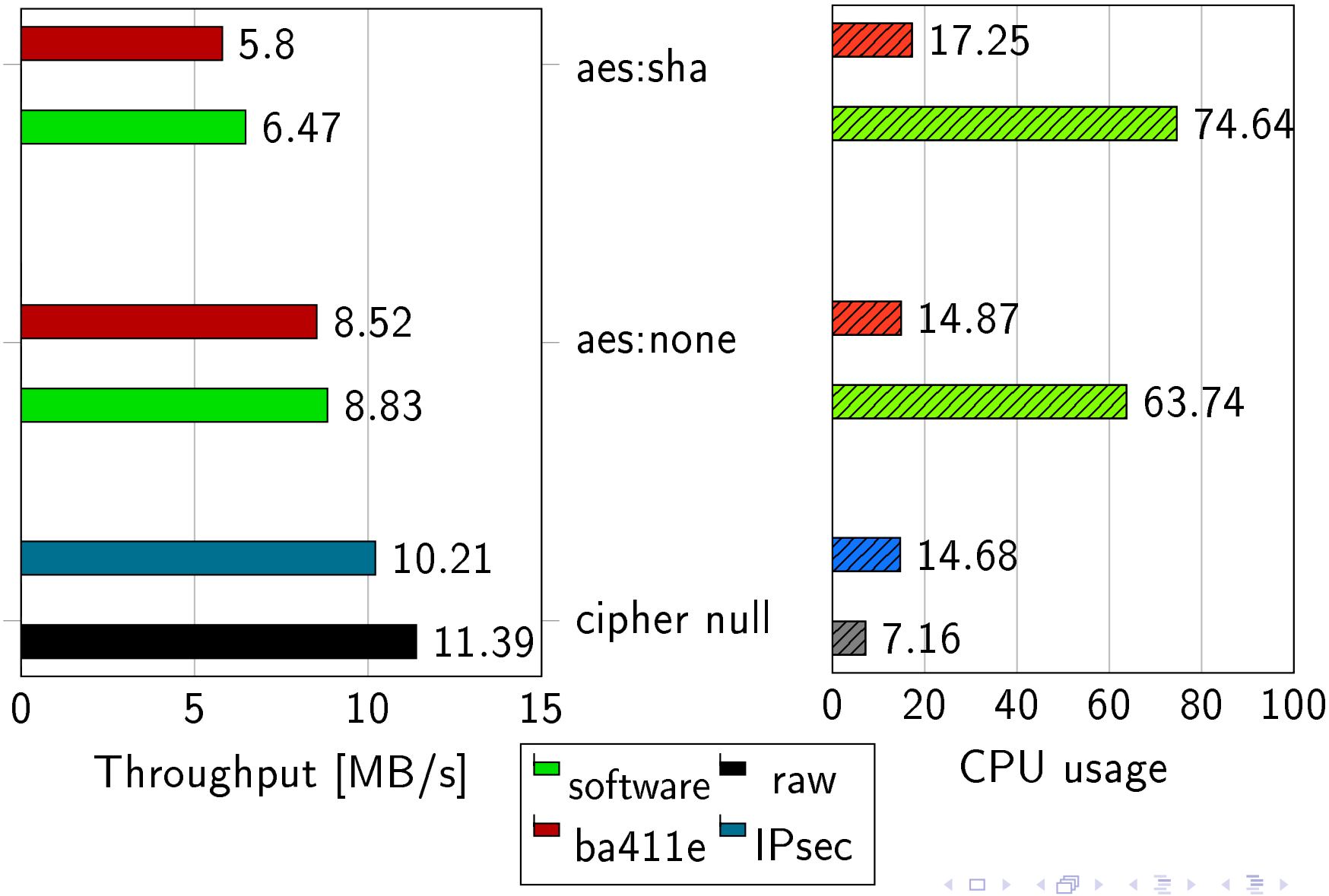


- 128MB file
- AES-256-CBC/SHA-256
- OpenVPN/IPsec

File transfer – OpenVPN



File transfer – IPsec



Conclusion

TLS connections

- 589% connections
- 5% the CPU usage

File transfer

- Drop OpenVPN
- 89% performance
- 23% the CPU usage

Conclusion

- Ongoing development