

Security Protocols in ATCA Systems *Addressing Software Challenges using QuickSec IPsec Toolkit*

Presented by Steve Singer
Worldwide Systems Engineer Manager

Agenda

1. Security Protocols in ATCA systems
 - IP Security and the ATCA platforms
 - IPsec and IKE basics
 - Protocol Architecture

2. Real life requirements for Security Protocols
 - Challenges on the Data Plane
 - Challenges on the Control planes
 - Solutions

3. Conclusions

1. Security Protocols in ATCA Systems

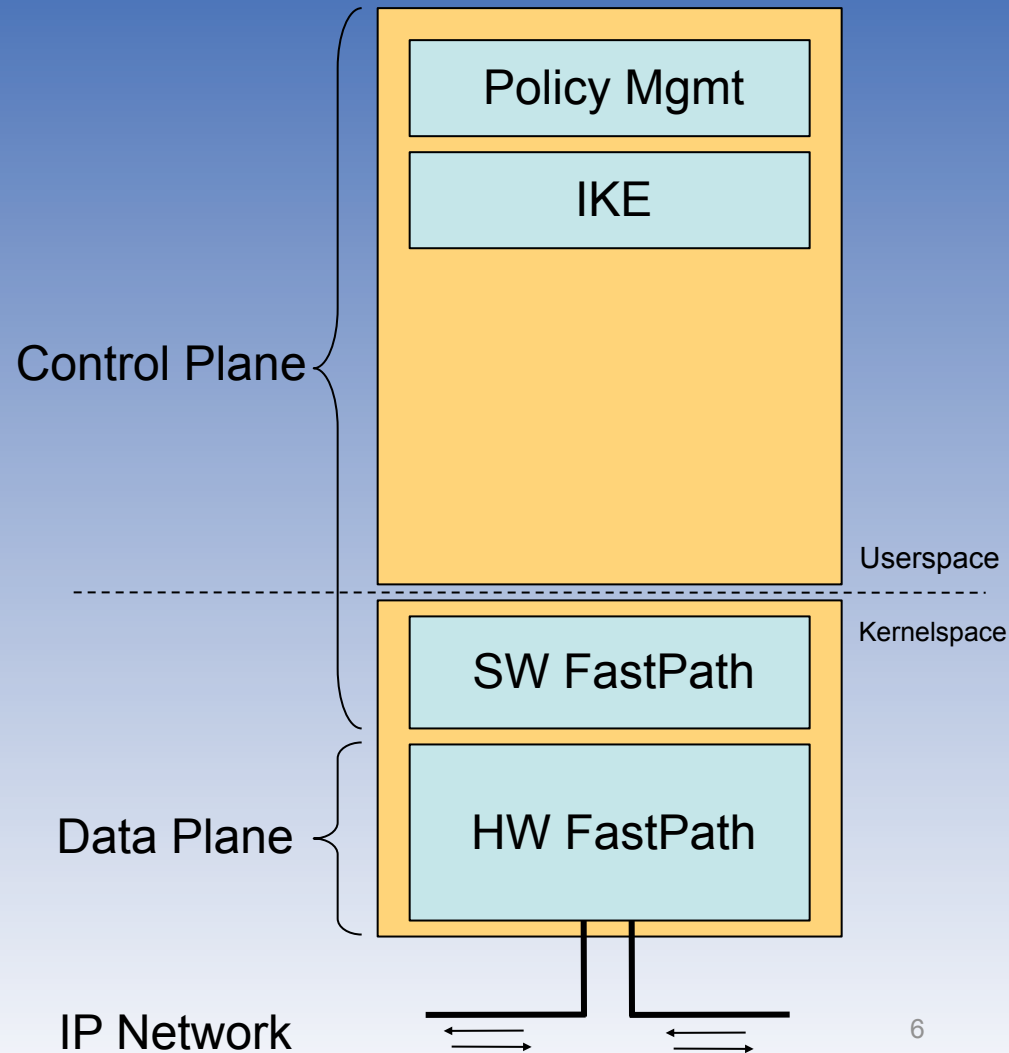
- IP Datagram Security Examples:
 - Packet Data Gateways (PDGs)
 - SecGWs for I-WLAN
 - Sec GWs for Femtocell
 - Unlicensed Mobile Access (UMA)
 - Network Interconnect Gateways
 - Enterprise Remote Access and Site-to-Site VPNs

IPsec and IKEv2 Protocols

- Basic network level security protocols
 - Offer “packet by packet” protection of IP datagrams
- Building blocks of security in IP networks
 - Strong mutual *Authentication* of communicating peers
 - Protection of information *Confidentiality*
 - Assurance of packet *Integrity* in transit
- Mature standards
 - First standard versions from late 90’s, updated constantly
 - IETF as the standardizing body
 - Widely referred to in 3GPP/2 documentation

General IPsec and IKE Architecture

- **Control Plane**
 - Authentication
 - Session set-up
 - Rekeying
 - “Security intelligence”
 - Mostly software
- **Data plane**
 - Packet by packet operations
 - HW utilization required



SafeNet QuickSec 5.0 Client & Server Source Code Toolkits



- Complete IPsec & IKEv1 & IKEv2 toolkit for:
 - Robust IPsec protocol support
 - Dual mode IKE, MobIKE, EAP
- Broad Server OS support :
 - Linux, VxWorks, BSD, Solaris
- Broad Client OS support :
 - Windows XP, Vista
 - Windows Mobile 6, 6.2, 6.5
 - Linux (MontaVista Mobilinux and kernel.org)
 - Symbian, Andriod
- High performance with multi-core hardware
- Multi-core support with linear scaling
- Standards-compliant interoperability (IETF, VPNC, ICSA, TAHI)
- Easy integration with developer-level integration support

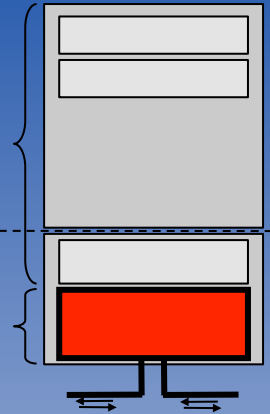


2. Real-life Requirements for Security Protocols

IPsec and IKE Deployments

- Requirements in actual deployments:
 - Very high performance:
 - Data rates (protected Mbit/second)
 - Packet rates (protected packets/second)
 - Session set-up rates (IKE negotiations/second)
 - Wide authentication support
 - Methods: PKI, EAP, Legacy
 - Flexibility - dataplane exception handling
 - What to do when the HW dataplane encounters exceptions?

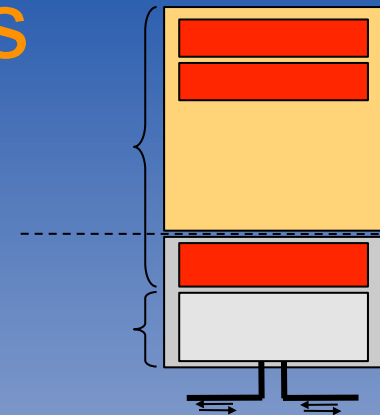
Data Plane Challenges



- Most deployment scenarios require:
 - High scalability for encrypted data throughputs
 - Interoperability and standards compliance
 - Performance independent of packet size
 - the smaller the packets, the larger the overhead
- Performance addressed with hardware
 - Modern (inline/multicore) hardware offers (near) constant packet processing time...
 - ...but requires optimized software to perform well
 - “Backup” software dataplane (“SW Fastpath”) important
 - to cover cases not implemented in hardware (exceptions)

Control Plane Challenges

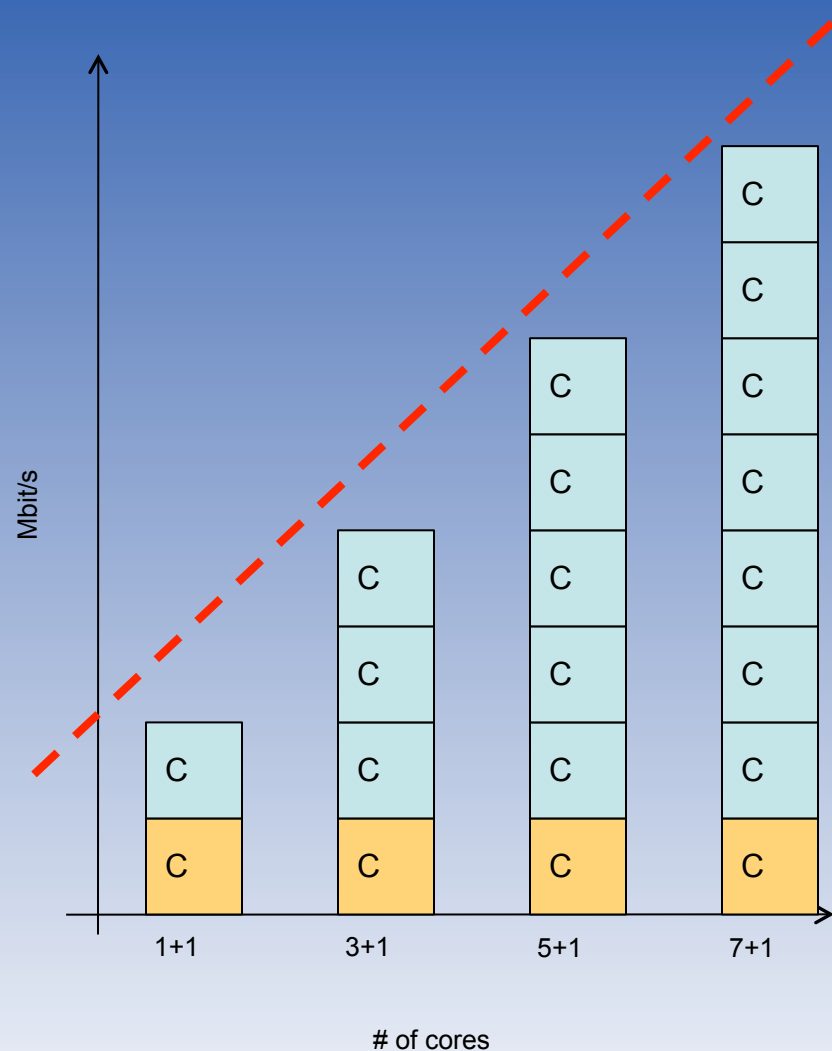
- Performance
 - Sessions set up per second
 - Re-keying performance
- Functional Complexity
 - Comparison of Control Plane vs Dataplane
 - *SafeNet QuickSec* software code
 - ~80% is control plane
 - ~20% is (software) data plane
- Standards Compliance
 - Literally dozens of complex RFC's to implement
- Interoperability
 - Proper interpretation of RFC intended functionality



- Session set up of an IPsec tunnel involves:
 - Mutual Authentication
 - Tunnel parameter negotiation and installation
 - Authentication of messages
- High performance requires:
 - Optimized Security Association Database (SADB) management from control plane
 - Use of hardware cryptography for
 - Diffie-Hellman operations (symmetric key exchange)
 - RSA, DSA, ECC for asymmetric based authentication
- Multicore systems can profit from assigning multiple cores for control plane processing

Linear Performance Scaling with Multi-Core

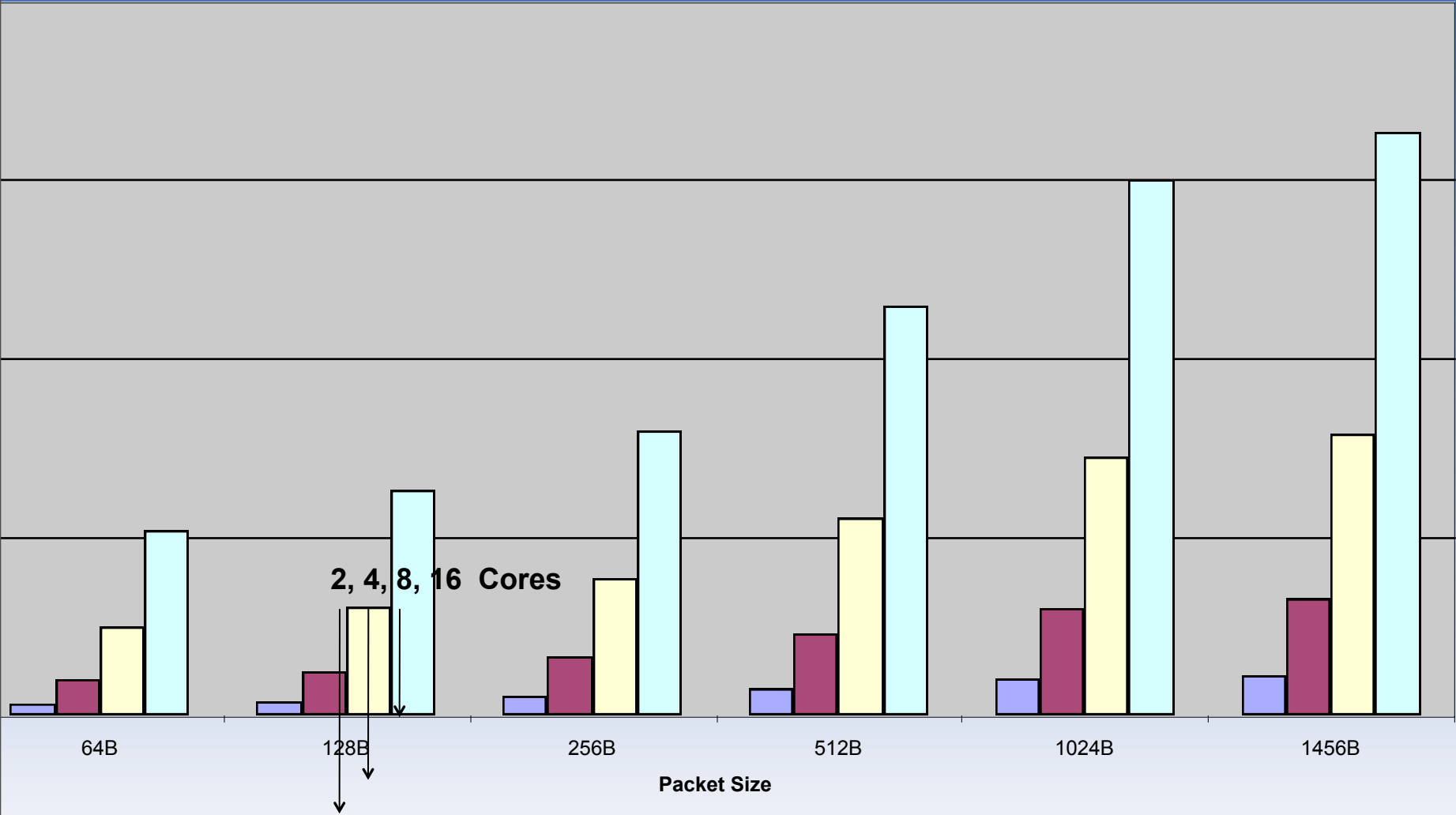
- Adding CPU power (cores) to the HW fastpath increases performance
- An efficient IPsec implementation scales up *linearly* as the number of cores increases
- Adding cores can also be used to boost the control plane performance



Multi-Core Performance (2 to 16 cores)

→ Cavium Octeon using QuickSec Toolkit

QuickSec Performance on Octeon CN58XX@700 MHz (AES-SHA1 IPsec encryption and decryption total throughput)



3. Conclusions



- Security Protocols
 - Typically divided into Control and Data plane
 - Control plane
 - Mainly software
 - Complex logic
 - Data plane
 - Mainly hardware, emphasis on packet-by-packet performance
 - Quality software implementation a key to meeting market requirements

- Using best-of-breed SW offers:
 - High quality
 - Improved TCO
 - Better interoperability
 - Reduced development risk and time-to-market
 - Future proof solution that scales with the product requirements
 - Reduced maintenance load