Topics

Introductions

Threats and challenges to data center security

Security considerations at Oracle

A review of encryption options: TLS vs. IPSec

IPSec implementation options

Extensions and opportunities
Presenters

Avneesh Pant
avneesh.pant@oracle.com
Director, Database Development
Virtual Operation System Group

Kumaran Siva
kumaran.siva@intel.com
Director, Data Center
Programmable Solutions Group

Nicola Tan
nicola.tan@intel.com
Senior Manager, Data Center Marketing
Programmable Solutions Group
- **NFV Node**: high-performance networking functions
- **Compute Node**: compute and infrastructure acceleration
- **Storage Node**: provides physical I/F and stack offload
- **Acceleration Node**: high compute throughput
Forces **Impacting** Data Center Security

More data, moving faster, with greater security needs

---

**NEWS**

- Hacked data on millions of US gov't workers was unencrypted
- Health Insurer Anthem Didn’t Encrypt Data in Theft
- Companies Aren’t Required by Law to Scramble Records, and Often Don’t

- Yahoo: 500 million accounts have been stolen

**2+ ZB GLOBAL DATA TRAFFIC**

ANNUALLY BY 2020¹

**50B CONNECTED DEVICES** BY 2020²

---

[Image 865x8 to 903x33]

[Image 369x24 to 629x416]

[Image 675x144 to 938x350]

[Image 55x79 to 358x385]
Intel Data Center Security Strategy

Effective security is built on a foundation of trust

- Trust
- Resilience
- Visibility/Control

Secure the platform

Protect the data

Without compromise

AT-REST
IN-FLIGHT
IN-USE
The NSA Hacked Google and Yahoo's Private Networks

More documents from the Edward Snowden leak show that the National Security Agency has tapped Google and Yahoo's cloud networks to access massive amounts of data, including from Americans.

Performance issues have been a chief inhibitor to encryption adoption

- Longer keys
- Complex algorithms
- Exponential data growth
Why security?

Oracle RAC (Real Applications Cluster) traffic currently requires a private network, so traffic goes in the clear today.

As we scale to multi-tenant Cloud environments, we have multiple tenants sharing the same physical infrastructure.

Attack vectors that need to be considered:

- Protecting tenant payload from identity theft, providing privacy (encryption) of tenant/application data, protection from replay attacks, integrity protection.

- Protecting the tunneling protocol header itself (TCP, UDP headers, tunneling protocol headers).
Networking protocol considerations for Oracle traffic

Oracle application transactions are typically massive numbers of request-response exchanges that expect reliable, ordered delivery of data.

Why not use TCP for these transactions (and TLS from user space)?

- Large number of peers, so using a TCP socket for each pair of communicating peers would result in a connection explosion.

TCP sockets provide stream semantics (no message boundaries). Oracle application complexity is significantly reduced with datagram semantics (message boundaries managed by the transport).
Why not UDP?

UDP provides datagram semantics. A single UDP socket can be used to send/receive packets to/from multiple peers. DTLS provides AAA (Authentication, Authorization, Accounting) and privacy for UDP sockets.

Drawbacks to using UDP:

- UDP does not have intrinsic congestion management, so application is burdened with complex congestion management logic
- Oracle application data tends to be 8K or larger packets so that we have to choose between:
  - performance impact of IP Fragmentation, or,
  - track MTU on in user space and manage a layer that can reliably send/receive MTU sized records

What we ideally want is “Reliable UDP socket”
RDS-TCP: A Reliable Datagram Socket over TCP
Security considerations for kernel managed TCP and UDP sockets

TCP socket in the RDS-TCP architecture is a kernel managed socket, and we do not currently have a standards-compliant TLS implementation in the kernel.

TLS is a complex protocol, kernel implementations of TLS have steep challenges.

Lack of security for the tunneling protocol header also exists for other data-center protocols like VXLAN, RoCEv2 etc.

We do have mature, standards-compliant implementations for IPsec in the kernel that provide AAA and privacy at the IP layer of the network stack.
Encrypting User Data With TLS/DTLS

North South use-case with TLS/DTLS
- Implements DTLS/TLS in user space using open source implementation
- Uses TCP or UDP sockets in Kernel
- Allows Large Segment Offload in NIC

Challenges With TLS
- DTLS/TLS control and data plane are complex and tightly coupled
- Does not protect against TCP attacks
- Does not support RDS, KCM today → need to bring into Kernel for RDS, KCM support
Encrypting User Data With IPSEC

IPSEC Provides Kernel Encryption
- Works across broad socket types

Separable Control & Data
- Standard interface for key management

IPSEC Processing After NIC limits offloads
- Large Segment Offload cannot be used
IPSec Background

Internet Protocol Security (IPSec) architecture is a set of protocols that ensures data security of an IP network.

IPSec ensures:

• **Integrity** – data has not been changed
• **Confidentiality** – data is not readable by third parties
• **Authentication** – data comes from intended source

Works at the network level, not application specific.
Intel Products for Encryption & Compression

**Standard**
For standard algorithms that do not require further acceleration or CPU offload

**Compute Intensive Crypto & Compression**
For lookaside offload acceleration on standard algorithms
symmetric crypto, public key encryption, de/compression

**Custom Algorithms or Inline Processing**
For desired flexibility in crypto/compression algorithms or for inline processing capability

Intel® Xeon® Processor E5 and E7 Families

Intel® QuickAssist Technology

Intel FPGAs

**Example:** AES-256 bit encryption using Intel® AES-NI

**Example:** Bulk operations

**Example:** Customer or Geo Specific algorithm
Three Models for IPSec Implementation

**Standard**
- CPU: Xeon E5 or E7
- Fortville NIC: XL710
- IPSec on CPU
- No LSO with IPSec

**Look-aside**
- CPU: Xeon E5 or E7
- Fortville NIC: XL710
- No LSO with IPSec
- IPSec offload on QAT

**In-line**
- CPU: Xeon E5 or E7
- Fortville NIC: XL710
- Intel MAP Card
- FPGA: Arria 10
- LSO on Fortville NIC
- IPSec on FPGA

**Host terminated:**
- IPSec protocols initiated in host
- Flexible functionality
- FPGA does encrypt/decrypt

**Device terminated:**
- Full IPSec protocol in FPGA
- IPSec invisible to host
- Targeted functionality
In-line IPSec Acceleration

Key benefits:

- Minimizes CPU overhead
- Minimizes latency
  - Less PCIe passes
- Exploits order of operations limitations
  - Encryption occurs after passing through NIC
  - NIC offloads (checksum, LSO, tunneling) not permitted in other IPSec implementations

In-line

CPU
Xeon E5 or E7

Host terminated:
IPSec protocols initiated in host
Flexible functionality
FPGA does encrypt/decrypt

Fortville NIC
XL710

Device terminated:
Full IPSec protocol in FPGA
IPSec invisible to host
Targeted functionality

FPGA
Arria 10

Intel MAP Card

Host terminated:
LSO on Fortville NIC
IPSec on FPGA

Device terminated:
Full IPSec protocol in FPGA
IPSec invisible to host
Targeted functionality
Inline IPSec Implementations

**Device Terminated**

- Terminates IPSEC headers in hardware
- Bump the wire, transparent to host
- Main challenge is control plane

**Host Terminated**

- Software terminates IPSEC headers
- Leverages IPSEC control plane infrastructure
- Interface to applications is simplified
Kernel support

What needed to happen to software to enable this?

Upstream Linux kernel stack infrastructure - a series of patches, that started with https://lwn.net/Articles/710591/ with several follow-ons.

Contributors: Steffen Klassert, Ilan Tayari, Sowmini Varadhan (Oracle)
System Architecture

Key Functions

**Arria 10 FPGA**
- IPSec encryption and authentication

**Fortville NIC**
- DMA Ring Interface
- Queue management
- MAC, VEB, VLAN

**Host**
- Fortville driver
- IPSec driver
- Host termination of IPSec protocol
- Security association configurations
Intel® Arria 10 FPGA-based SmartNIC

- **Arria 10 (FPGA)**
  - Intel Arria 10 1150 GT, 20nm
  - Accelerated function IP and gearbox

- **QSFP-A**
  - 4x 10G or 4x 25G QSFP28

- **QSFP-B**
  - 4x 10G

- **XL710**
  - Intel Fortville Ethernet NIC
  - 10/40 GbE
Pervasive FPGA Use Throughout Datacenter

- **NFV Node**: high-performance networking functions
- **Compute Node**: compute and infrastructure acceleration
- **Storage Node**: provides physical I/F and stack offload
- **Acceleration Node**: high compute throughput
Takeaways

**Securing East/West traffic** is vital to an overall data center security strategy

**Inline IPSec acceleration** offers high throughput, low latency encryption

**Intel FPGAs** offer flexibility for multiple uses across the data center

For more information: IPSec Workshop at Netdev 2.2 (Nov 8-10, Seoul)
BACKUP
FPGA Technology Introduction

**Logic Elements**
- Main programmable component
- Millions of logic elements
- Simple logic, adders, and registers
- Interconnect with configurable fabric

**PCIe Host Interface**
- Hardened + Soft host interface
- Hardened PCIe controller
- Soft interface allows different use models and drivers

**Partial Reconfiguration**
- Allows separate regions

**Memory Interfaces**
- Configurable high performance memory interfaces
- Hardened controllers

**Network Interface**
- Configurable network interfaces
- Hard/soft interfaces

**Memory Blocks**
- Thousands of 20Kb memory blocks
- Allows processing to stay on-chip

**Variable Precision DSP Blocks**
- Allows FPGA to perform compute intensive functions
Where FPGAs Fit In?

- **Balanced architecture:**
  - Good enough most workloads
  - Good single thread & throughput perf.
  - Fastest cadence

- **Focused on compute throughput**
  - Many low performance threads
  - High memory throughput
  - Purpose made programming tools

- **Full custom pipeline**
  - Capable of networking and compute
  - High memory throughput
  - Change cadence in months → rapidly changing needs
  - Requires sophistication

- **Fixed function**
  - High efficiency – only blocks that are needed
  - Change cadence in years → needs stable standards
  - Expensive: minimum volume for viability
  - Requires sophistication
Application Level Comparison – Skylake vs. Broadwell

![Graph showing comparison between Skylake and Broadwell]

*Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/performance/datacenter. Configurations: see backup*
Intel® QuickAssist technology

Optimize the platform beyond processor ISA algorithm performance with hardware for additional scale and workload efficiency

- Cryptography (cipher and authentication operations)
- Public key (RSA, Diffie-Hellman, and elliptic curve cryptography)
- Compression and decompression (DEFLATE and LZS)

Technology available in form factors and packages to meet multiple market requirements for cost, form factor, power, flexibility, etc)

- PCIe Card – Intel and 3rd party (e.g. Intel® QuickAssist Adapter)
- Chipset Option (e.g. Intel® Communications Chipsets 89xx)
- Integration with CPU as SoC (e.g. Intel® Atom™ Processor C2000, Intel® Atom™ Processor C3338)

* Ideal choices for solutions targeting crypto and compression heavy workloads

FD.io VPP IPSec Encrypted Throughput (single core)*
AES128-CBC HMAC-SHA1 1024B (Encrypt only) (Gbps)

- Default OpenSSL 1.767
- OpenSSL + Intel® AES 7.525
- OpenSSL + Intel® QAT 25.814

* See backup slide “VPP IPSec Performance Configuration” for details