Protecting EPC User plane & Charging with Intel® Software Guard Extensions (Intel® SGX)

Somnath Chakrabarti - Security & Privacy Research/Intel Labs

ONF Connect 2019
Background - Network Functions Evolving For NFV Cloud

Physical Appliance
- Built into Telco HW Function
- In-Building Access
- Protection from Insiders

Distributed SW Infra-
- Automated instantiation w/ VNFs
- + Secured Remote Access
- + Protection from Outsiders
Virtual Network Function – Software Building Blocks

Fixed network functions on proprietary hardware

- Router
- EPC
- VPN
- Firewall
- Load Balancer
- Deep Packet Inspection/IDS

Virtual network functions on commodity hardware

- Router
- EPC
- VPN
- Firewall
- Load Balancer
- DPI/IDS

Software Building Blocks

- N-tuple Lookup
- State Machines
- Policy Manager
- Key Manager
- Hash Table
- Filters
- ...
Reducing the “Attack Surface” with Software Guard Extensions (SGX)

Application gains ability to defend its own secrets
- Smallest attack surface (App Memory + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug
- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model
- Platform integration not a bottleneck to deployment of trusted apps

Scalable security within mainstream environment
### Security sensitive VNF Hardening with Intel® SGX – Use cases

<table>
<thead>
<tr>
<th>NFV/SDN Building Blocks</th>
<th>SGX Value Add*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software Isolation</td>
</tr>
<tr>
<td>N-tuple lookup</td>
<td>Y</td>
</tr>
<tr>
<td>Filter Packets, State Machines</td>
<td>Y</td>
</tr>
<tr>
<td>MEC/Cloudlets/Edge cloud/5G VNFs</td>
<td>Y</td>
</tr>
<tr>
<td>Protection of Keys (Encryption keys, Certificates, IPSec keys)</td>
<td>Y</td>
</tr>
<tr>
<td>IP Protection of Algorithms, Data (SIG Files, Policies, Hash Tables, Analytics Meta Data)</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Potential Security-Performance Trade-offs

- **Software Isolation**: Encrypted & protected pages, OS/VMM not in TCB, contained impact of leaky VNFs
- **Runtime Physical Attacks**: System administrators, operators not in TCB
- **Other SGX Cloud usages applicable to NFV**: Keys Protection, DB protection, SSL termination
Design choices: Packet processing inside SGX enclave

- Enclave packet access mechanisms
  - 1 core - Calling into enclave to transfer every packet or burst of packets (bad idea)
  - 1 core - Calling into enclave everytime to transfer pointers to packets (still bad)
  - 2 cores – I/O core outside the enclave. Packet processing core inside the enclave
    - call into enclave just once to initialize Rx and Tx ring pointers (current Prototype)
  - 1 core – setup the NIC/DMA outside the enclave.
    - call into enclave and run I/O engine inside enclave (new prototype)
Goal of OMEC - Open Mobile Evolved Core

Can we securely run Telco core infrastructure on high volume servers to deliver operational capacity?
OMEC 1.0 – Fully Featured & Intel® SGX Hardened Charging

E2E Comprehensive EPC Infrastructure:

- [https://github.com/omec-project](https://github.com/omec-project)
- Fully protected & distributed Xeon E3 based SGX enabled billing system, automated, real time billing data collection and storage.
- SGX based auditable mutual attestation. Provides confidentiality and integrity of Charge Data Records (CDRs)
- Cross platform deployment orchestration, provisioning and network configuration tools ready- KVM, AWS, Docker, K8, …
OMEC – Charge Data Security

Service Gateway User Data (SGW-U) → Intel SGX Billing Dealer In

**TLS**
Client Auth + SGX Attestation

Intel IAS Cert
Dealer Enclave measurements

Sprint Server Cert
Intel IAS Cert
Sprint CA Cert
KeyGen Enclave measurements

**Intel SGX KeyGen**

**Intel SGX**

**Message Queue**

**AES-GCM 128**
Protected messages

**TLS**

RSA 3072 + SHA256 With SGX Mutual Attestation

RSA 3072 + SHA256 With SGX Mutual Attestation

**TLS**
Client Auth + SGX Attestation

**Intel SGX**

**Message Queue**

**AES-GCM 128**
Protected messages

**Intel SGX Billing Dealer In**

**TLS**
Client Auth + SGX Attestation

Sprint Server Cert
Intel IAS Cert
Sprint CA Cert
KeyGen Enclave measurements

**SGX SDK ProtectFS**

**CDR**

**sgx rijndael128GCM_encrypt()**

**AES**
GCM 128 Protected messages

**AES**
GCM 128 Protected messages

**SGX SDK ProtectFS**
OMEC – Charge Data Security contd.

- Provides Confidentiality and Integrity of CDR Records
- Telco out of trust boundary provides ease of auditability
- Scalable
Mobile Infra Core Control/Data plane configuration – With Intel® SGX Dataplane and Billing

- Requires minimum 1+1 SGX server per dataplane frame of capacity
- n+1 SGX servers required for up to n dataplane frames of capacity
Current prototype performance numbers with hash table lookup

Application: L2FWD
Lookup type: Hash table (1M 5-tuple entries, ~13MB)

- Additional SGX threads can enhance performance.
- Queuing/de-queuing adds additional overhead (queuing theory)

* Lab research data. Potential Security-Performance Trade-offs.
Future OMEC Mobile Infra Core Control/Data plane – WIP

Protecting
- SPGW-U and SPGW-C
- Subscriber databases
- Transient databases
- MME
- GTP-C/U links
Thank You

Questions ?