# Innovative Usages for Intel® Software Guard Extensions

Platform Security Summit 2019

Vinnie Scarlata
Security and Privacy Lab, Intel Labs

October 1, 2019

# Legal Disclaimers and Notices

This presentation contains the general insights and opinions of Intel Corporation (“Intel”). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

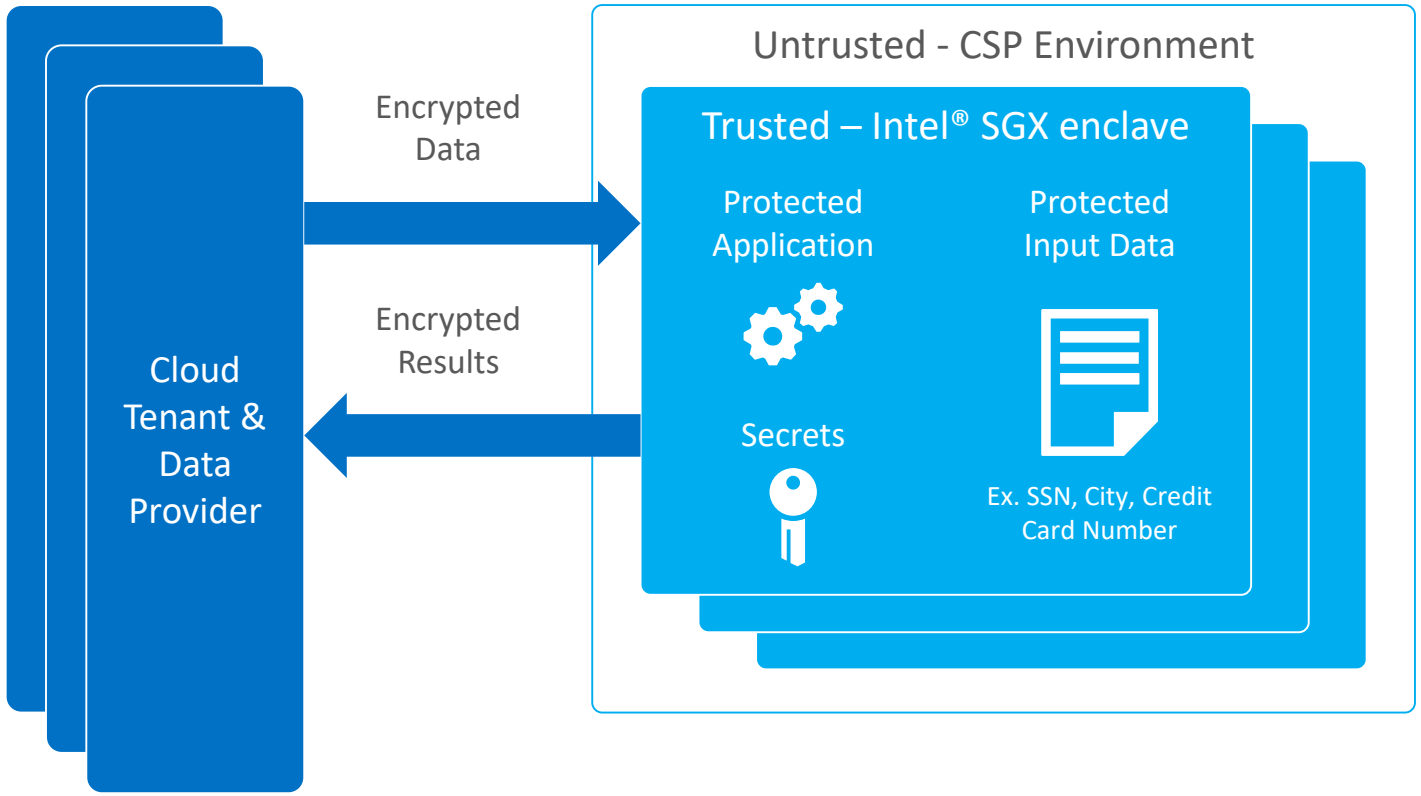
No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

# INTEL® SOFTWARE GUARD EXTENSIONS

## APPLICATION ISOLATION AT THE MOST GRANULAR LEVEL, ENABLING FINE-GRAINED DATA PROTECTION WITHIN A HYPER-FOCUSED TRUST BOUNDARY



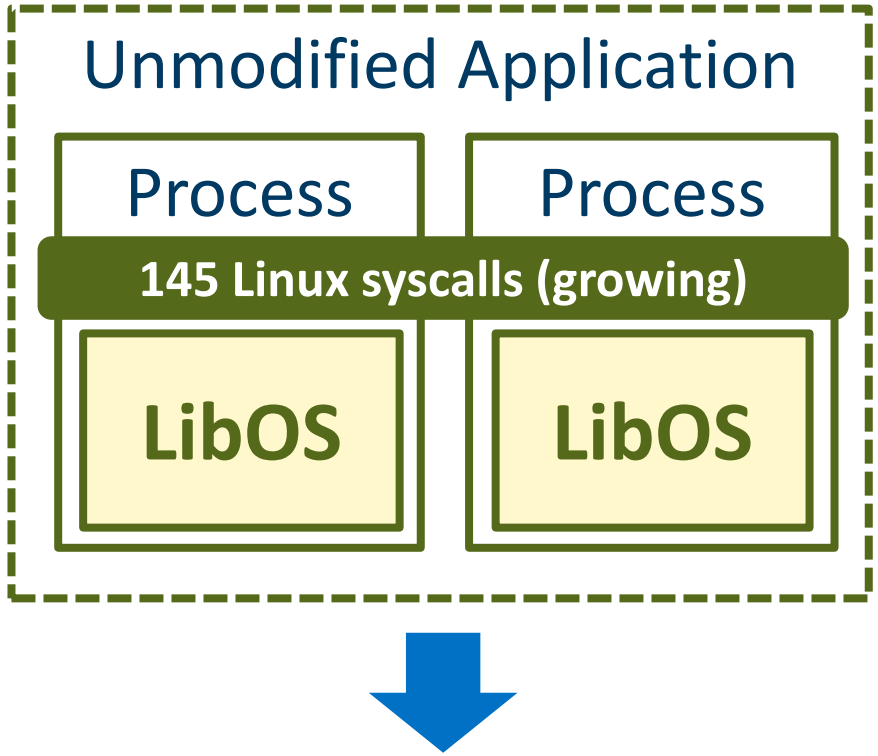

- Increases protection against SW attacks even if OS/drivers/BIOS/VMM/SMM are compromised
  - Smallest possible TCB
- Increased protection applies even when attacker has full control of platform
  - Other technologies allow some privileged sw in their boundary
- Increases protection against memory bus snooping, memory tampering, and “cold boot” attacks against memory images in RAM
  - Protection in unprotected spaces
- Provides hardware-based attestation capabilities to measure and verify valid code and data signatures
  - Increasing Transparency and accountability
- In-band execution utilizing the full power of the Intel® processor

# Reducing Enabling Costs

# The Graphene LibOS Project [Eurosys14]

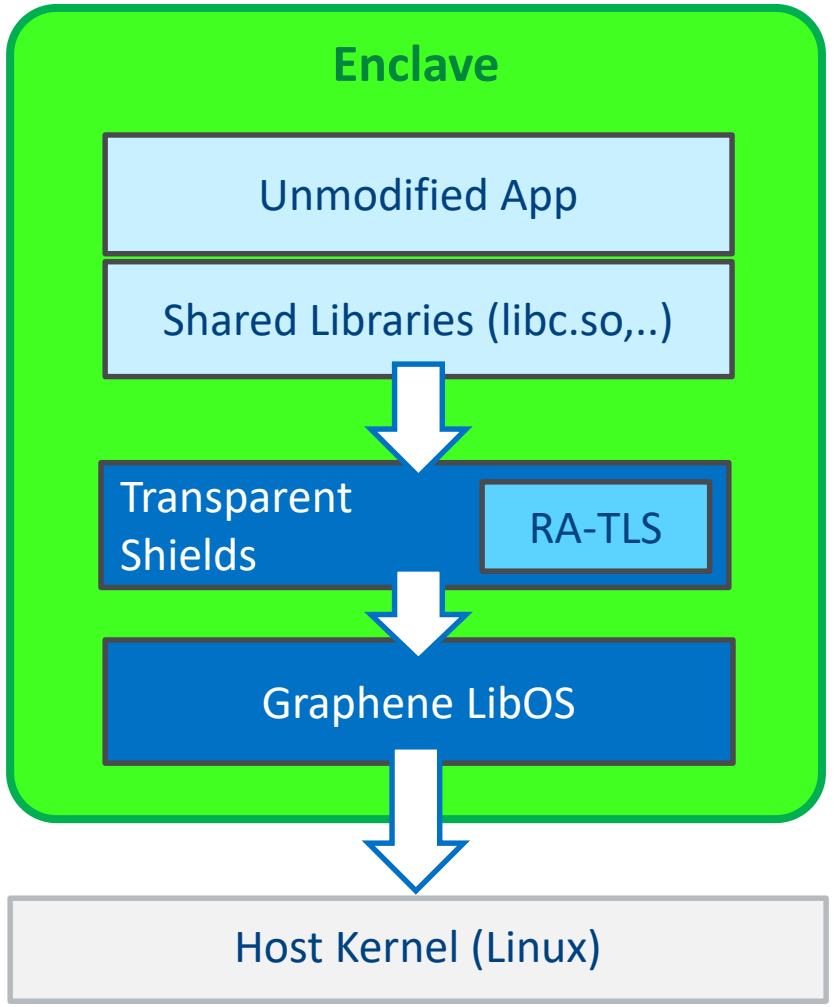
## An open libOS for running unmodified multi-process Linux applications (**github.com/oscarlab/graphene**)

- Inspired by Drawbridge[ASPLOS11] and Haven [OSDI14 Best Paper]
- Continues to be a university open source project
- Very active use of SGX port [ATC'17]
  - Productized by a couple of startups
    - Fortanix, Anjuna
  - In use by many academic research projects
- Docker Integration




**Easy to port to new OS/platform**

# Graphene Library OS




https://grapheneproject.io/

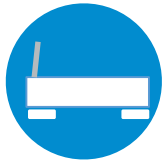
- Graphene Library OS runs Unmodified Linux Application within an Intel® SGX enclave.
- Supports dynamic loading of libraries
- Supports a variety of languages like C, Python, R …
- Transparent Encryption with Network and File System shields
- Transparent Intel® SGX Remote Attestation with RA-TLS
- Docker Integration

# Intel® SGX Usages

# USE CASES – DATA CENTER, CLOUD & INTERNET OF THINGS

## Key Protection

Helping protect keys on local file system; hardening disk protection, building scalable cloud KMS

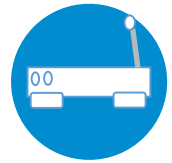


## HSM
Hardware Security Module

Customers and ISVs use enclaves to increase protection of encryption keys and/or HSM replacement

## Encrypted Databases

Encrypted database operations



## Internet of Things

Enhanced security for IoT edge devices and cloud communications

## Enhanced Privacy Analytics
& Workloads

Enables multi-party joint computation on sensitive data in a privacy-preserving manner

## NFV
Network Function Virtualization

Enhanced trust to help protect & virtualize network functions

## Blockchain

Enhanced security transaction processing for Cryptocurrency, Secure Contracts, and Hyperledger protection

## Machine Learning

Enhanced security for machine learning algorithms, models, and data during inferencing.

# Machine Learning

# Machine Learning as a Service

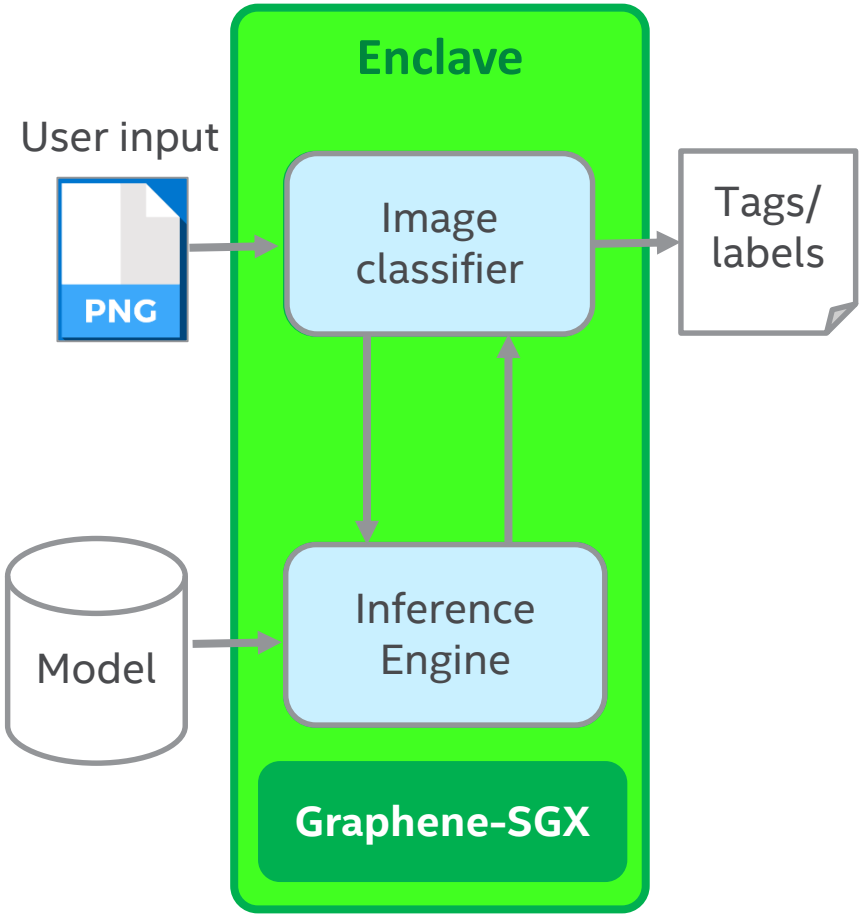
## Deployed on Cloud as ML-as-a-Service

- Models can be provided by the users or by service
- Users provides the data
- Users desired high confidentiality of their models and input data, which is hard in public clouds.

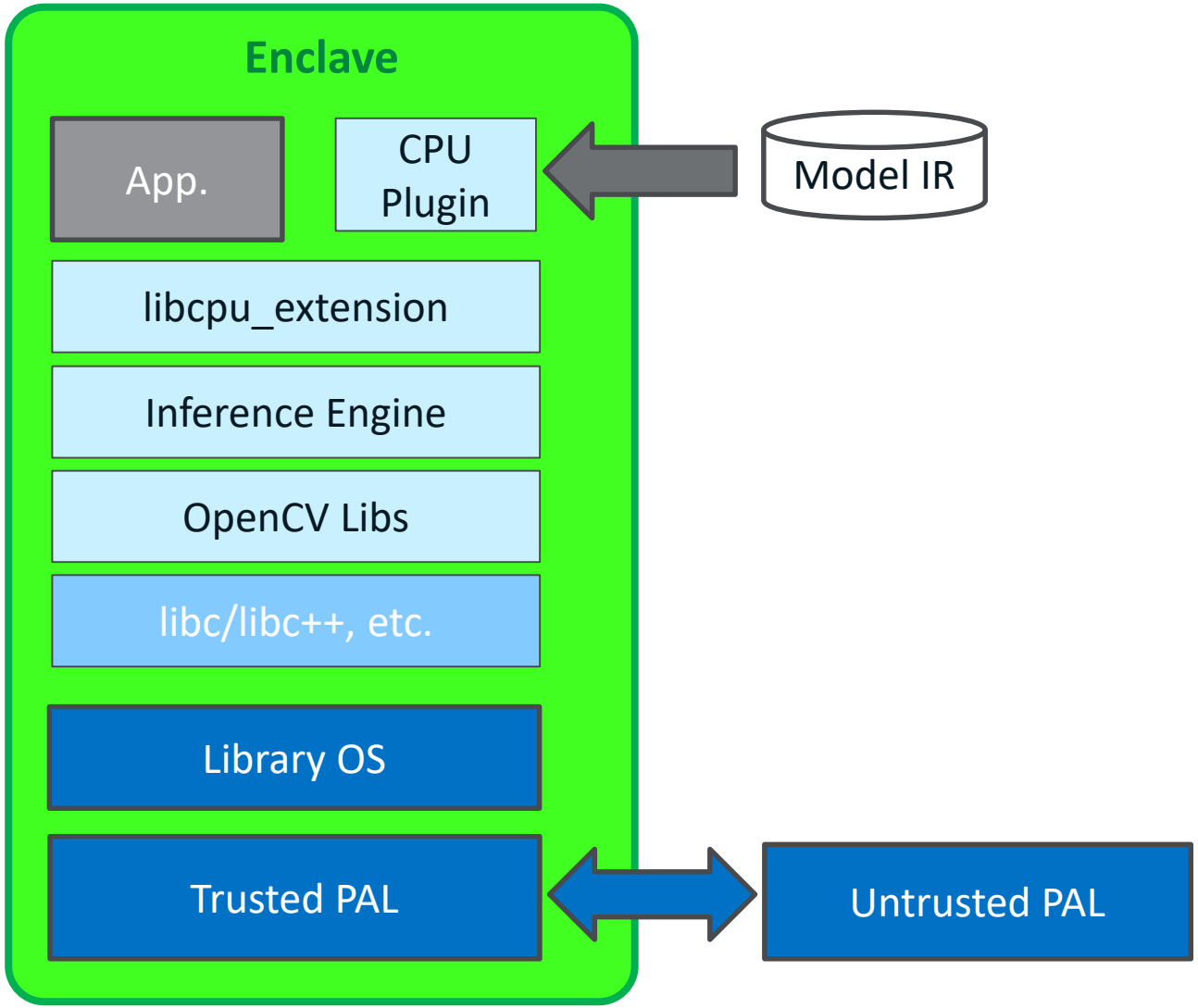
## Deployed on Edge Devices

- ML models can be provided by device vendor
- Vendor desired high confidentiality of their models, which his hard in many edge environments.

## Intel® SGX can provide enhanced security for the ML model and user data.



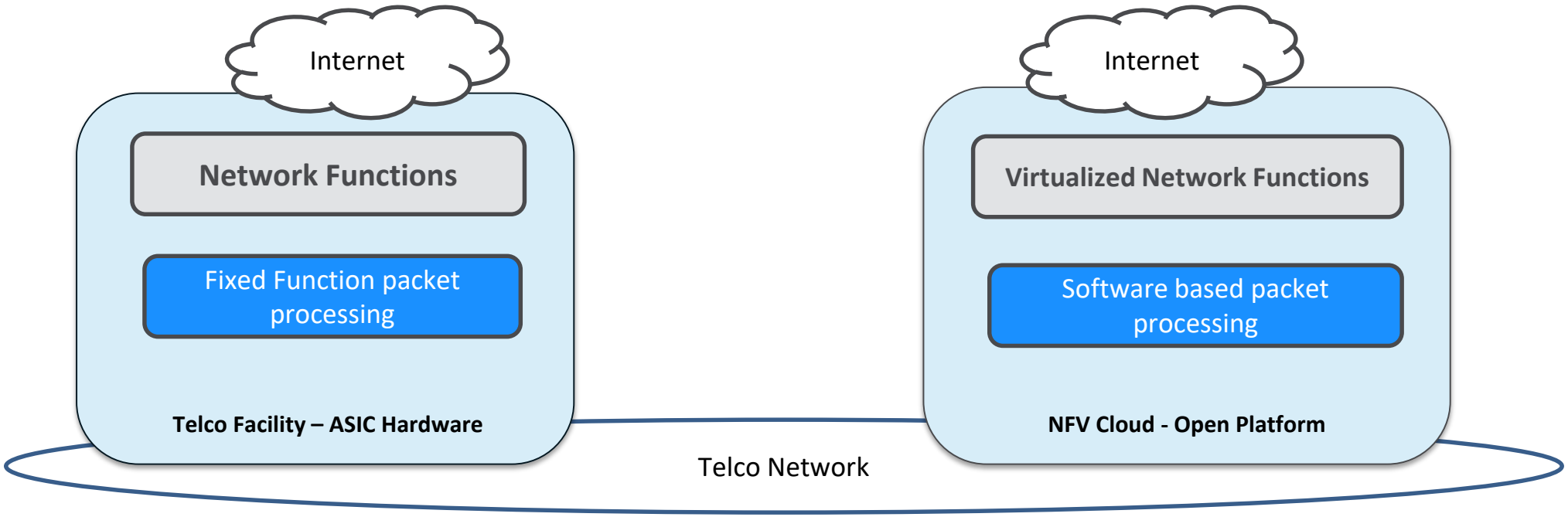
# Graphene-SGX with OpenVINO®




- Graphene-SGX enables SGX use by unmodified OpenVINO ® inferencing stack.
- SGX's provides enhanced isolation on shared cloud servers.
- Using SGX attestation, data owners can remotely detect that the desired ML stack is running in the enclave before delivering sensitive data.
- With additional software enhancements, model owners could also use attestation to detect the OpenVINO® stack is running in an enclave before delivering sensitive model information.

# Network Function Virtualization & 5G

# Network Functions Evolving For NFV Cloud




Physical Appliance

Built into Telco HW Function

In-Building Access

Protection from Insiders

Distributed SW Infrastructure

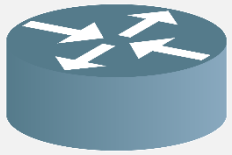
Automated instantiation w/ VNFs

+ 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

VS

## Virtual network functions on commodity hardware

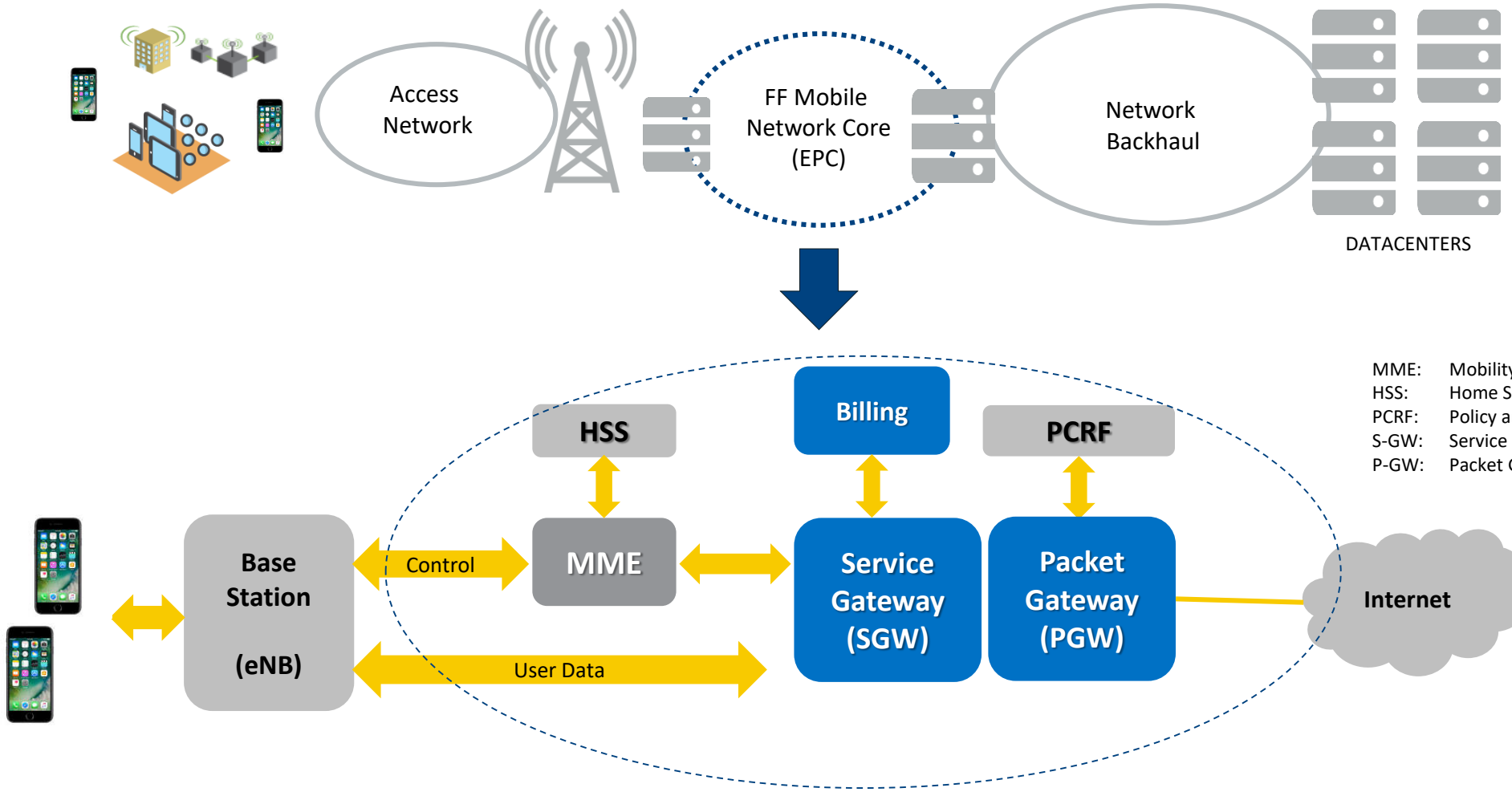
Router | EPC | VPN | Firewall | Load Balancer | DPI/IDS

### Software Building Blocks

N-tuple Lookup | State Machines | Policy Manager | …

Filters | Key Manager | Hash Table | …

# Open Mobile Evolved Core (OMEC)

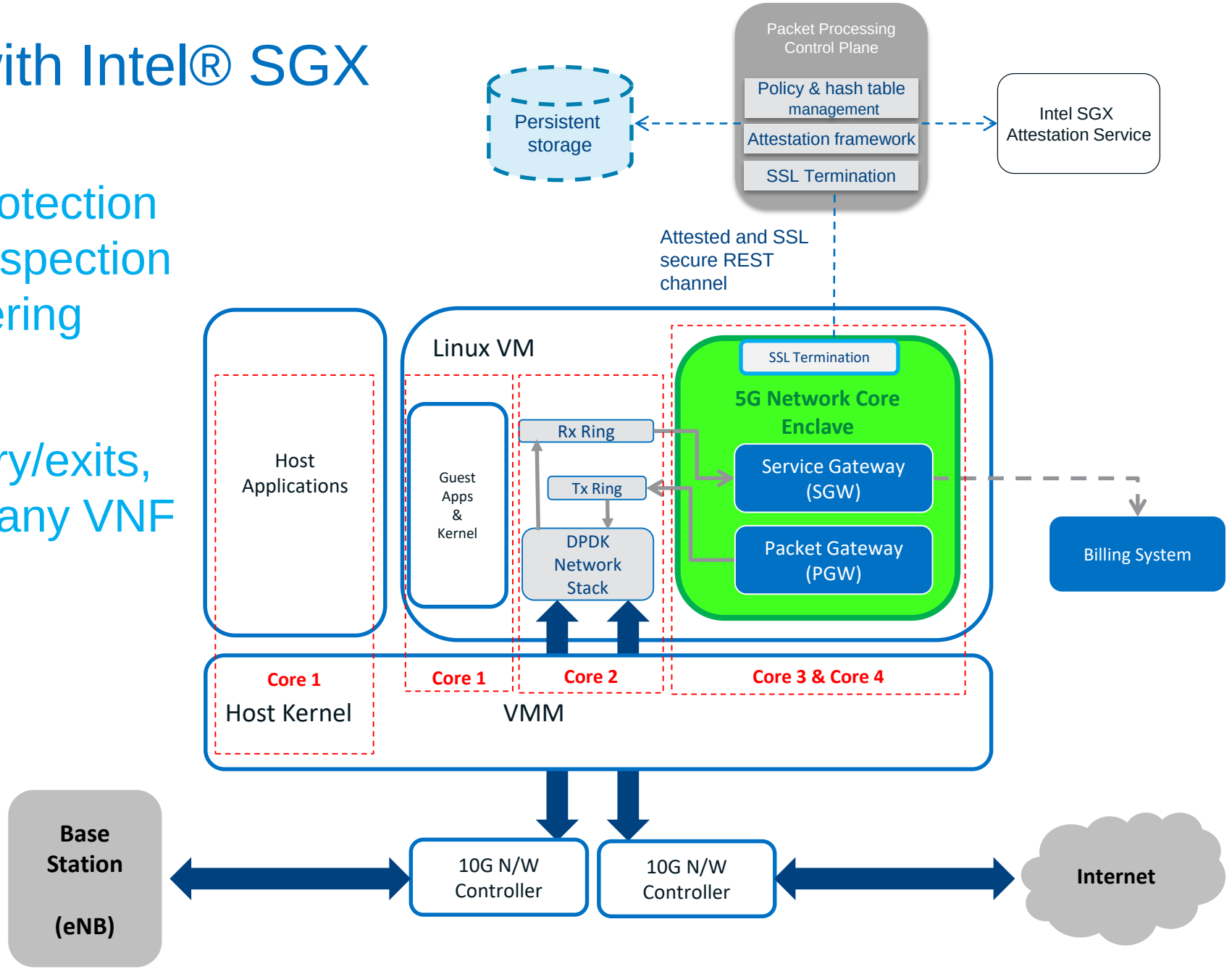



Opensource project with Telco partners to implement 5G Network Core using VNF.

# 5G Network Core with Intel® SGX

Intel® SGX increases protection of the VNF from traffic inspection (confidentiality) or tampering (integrity).

By reducing enclave entry/exits, enclaves can process many VNF at line rate.



# Blockchain

# Intel® SGX Opportunity for Blockchain

Blockchain offers fully decentralized coordination for a variety of uses.

- Examples: cryptocurrency, supply chain tracking, data provenance, IOT enabling.

Consensus algorithms are the core of the blockchain model.

Many consensus algorithms achieve their security using very expensive techniques.

Intel® SGX's enhanced runtime isolation and attestation create opportunities for new, inexpensive, consensus algorithms.

# Example Blockchain Leader Election: Bitcoin

- Proof Of Work:

```
while TRUE:
    nonce = random()
    if (hash(nonce + block) <
difficulty)
                return (nonce)
```

- Leader: First to Complete
  - Fully decentralized—no coordination is required between the participants
  - Easy to prove correct execution—the nonce is trivial to validate
  - Completely fair—anyone can be elected leader for any block
- And…
  - Incredibly high power requirements

# The Key Insight About Bitcoin Leader Election


Observation: Interval between blocks is random and exponentially distributed

It is the distribution (in time) of leader election that is critical to the protocol not the hashing

# Leader Election With Intel® SGX

- Proof Of Elapsed Time (PoET):
  - wait(random(difficulty))
  - return sign(block)

- Leader: First to Complete
  - Fully decentralized—no coordination is required between the participants
  - Easy to prove correct execution—SGX provides verifiable attestation
  - Completely fair—anyone can be elected leader for any block
- And…
  - Very little compute/power required

# Power Efficiency of Consensus

**Proof of Work**

Transaction Validation

Communication

**Hashing**

50 TWh/year

(small country)

**Proof of Elapsed Time**

Transaction Validation

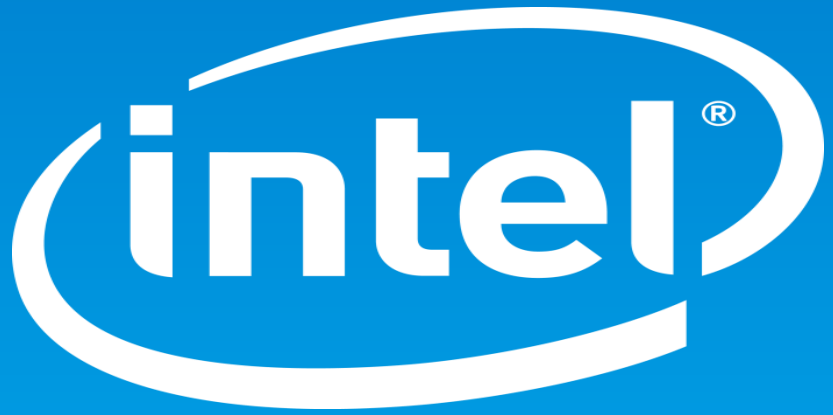
Communication

**Enclave Entry/Exit**

5 GWh/year

(500K servers, 1W estimate)

Leverage enclave's strengths to deliver significant power savings for some usages.


intel