Using TDISP to Extend Attestation Devices Connected to a TEE

Alec Fernandez

Azure Confidential Computing

Microsoft

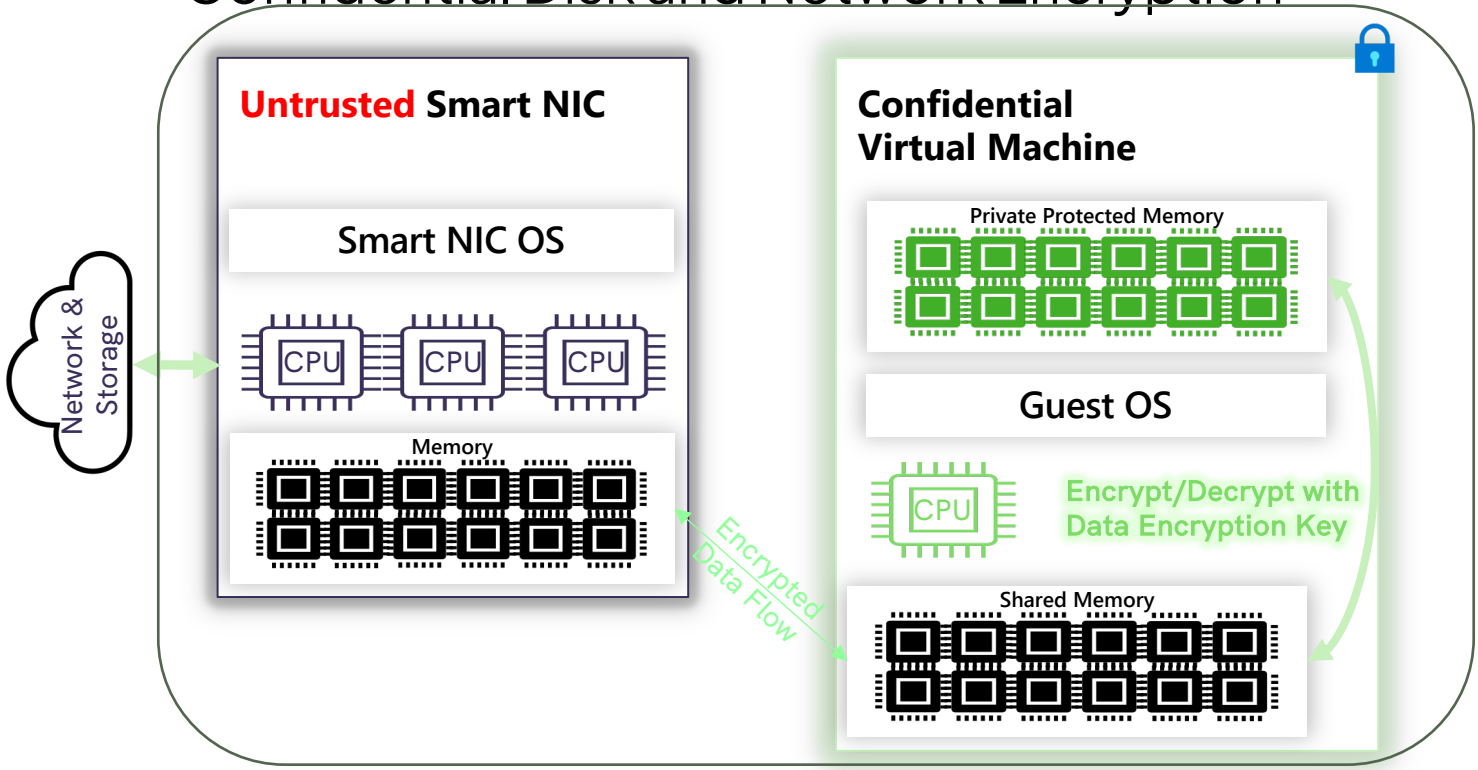
Agenda – Smart NICS

- TEEs can maintain confidentiality of the file and network I/O streams by encrypting data within the TEE boundary (Confidential Disk Encryption). This uses the CPU in the TEE to do the crypto which consumes CPU cycles
- Cloud Service Providers (CSPs) use hardware/software running on the Smart NICs to perform encryption for Network and File System I/O
    - Increases Performance - designed for CSP infrastructure
    - Reduces Cost-of-Goods-Sold – designed and built by the CSPs
- Customers who desire higher performance/cost can choose to trust the Smart NIC to do encryption. This frees cycles on the TEE CPU and adds the Smart NIC to the TCB.
- CCC requirements for Remote Attestation involve using SPDM and TDISP
- **NorthStar question**: How to measure the trustworthiness of a CSP's Smart NIC

Evolution of CC and TCB Boundaries

- Enclave
- Entire VM - Guest OS, File System, Network
    - CPU plus other devices (Smart NIC)

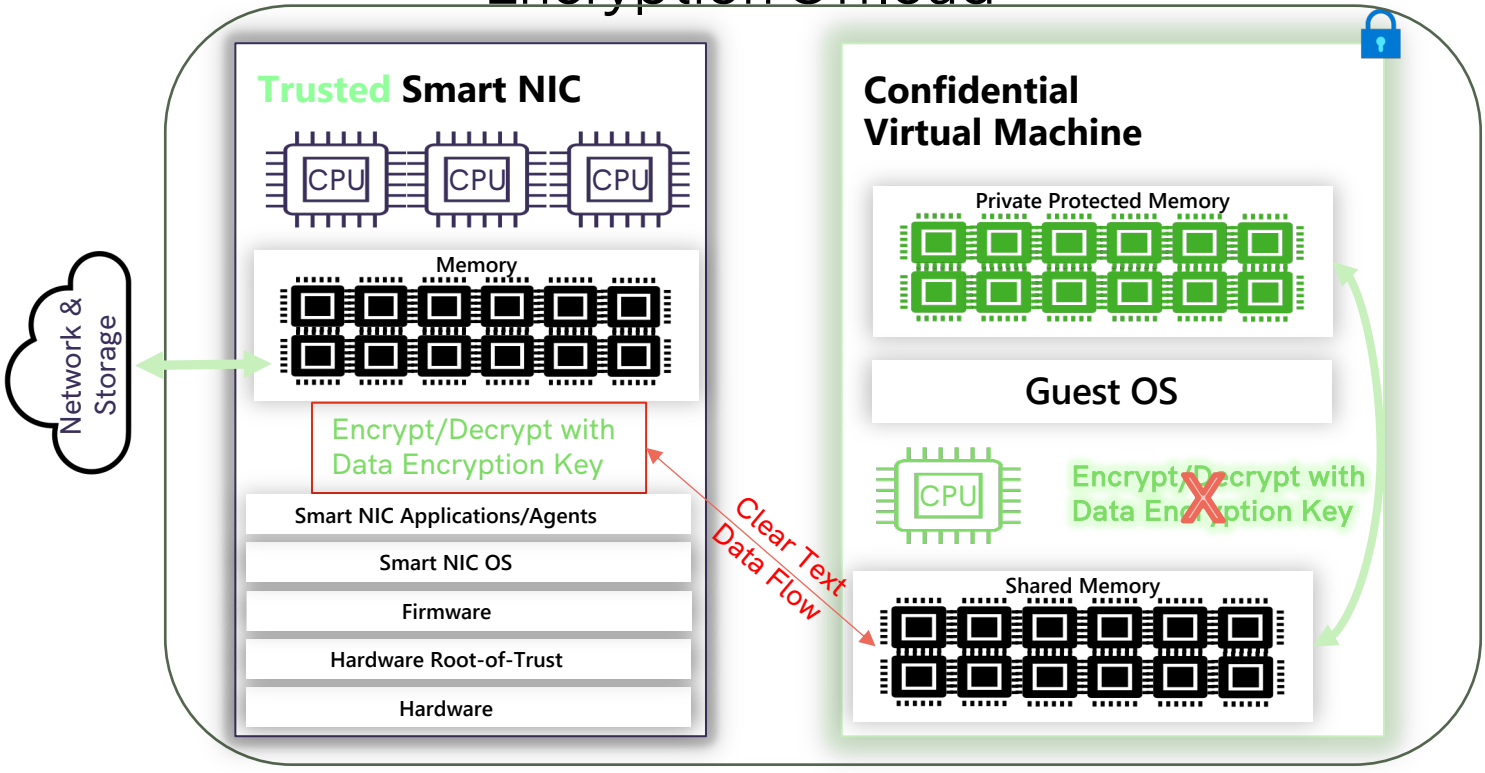
Confidential Disk and Network Encryption



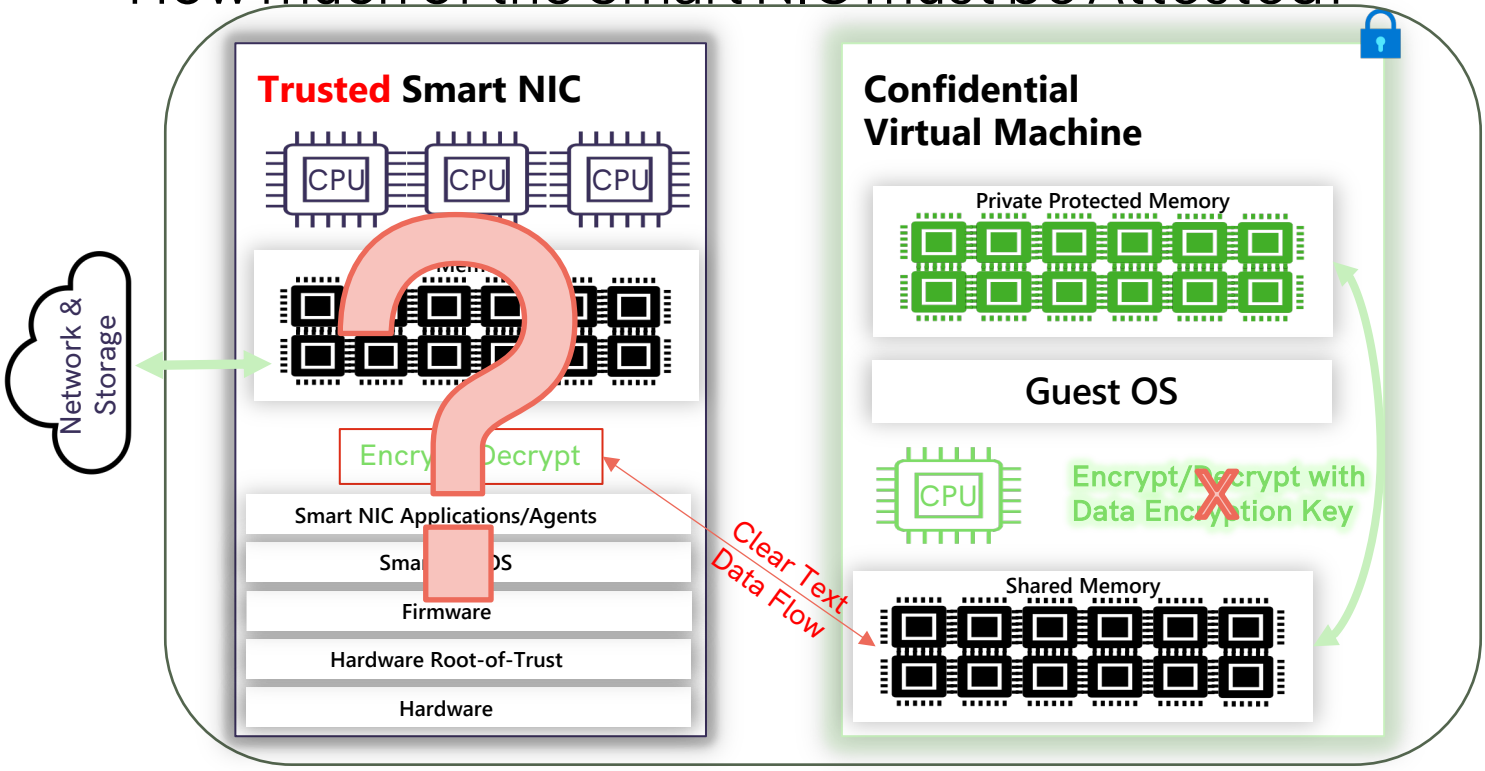
Encryption Performance Overhead

- The CPU
  - encrypts all data enter/exiting the TEE
  - In addition to what it's "supposed" to be doing
- Can Impact IOPS and reduce performance
- Can increase cost

Encryption Offload



How much of the Smart NIC must be Attested?



How is Attestation Accomplished?

- Security Protocol and Data Model (SPDM)
  - Creates a secure connection between the TEE the attached device. Negotiates PCIe Integrity and Data Encryption (IDE) keys to secure traffic over the PCIe.
  - Allows the TEE to query the attached HW device and get signed attestation reports

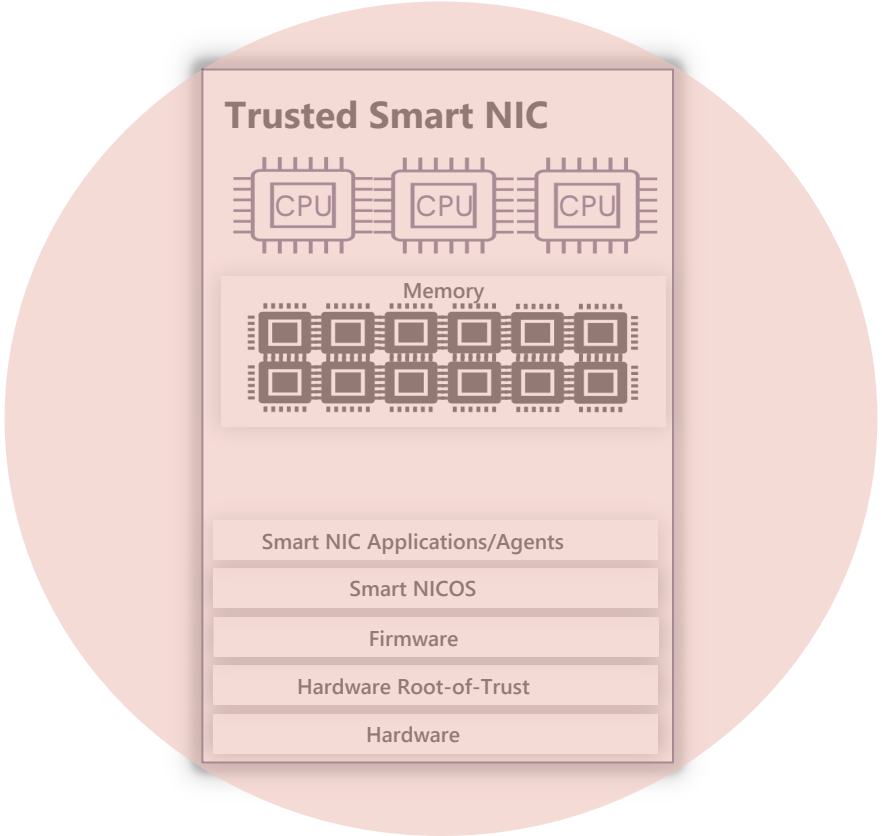
How is Attestation Accomplished?

- TEE Device Interface Security Protocol (TDISP)
  - Allows the TEE to get configuration data from the HW device and enforce the TEE boundary within that device.

What must be Attested?

- Simple Answer:

  Everything in the Trusted Compute Base (TCB)


Trusted Smart NIC
CPU
CPU
CPU
Memory
Smart NIC Applications/Agents
Smart NICOS
Firmware
Hardware Root-of-Trust
Hardware

Confidential Computing Requirements

- Hardware-Based, Attested TEE
- Hardware Root-of-Trust
- Remote Attestation

For more info: Confidential Computing Consortium: Common Terminology for Confidential Computing

What must be Attested?

- Hardware/Silicon (Chip Suppliers)
- Programmable Logic on Silicon (CSPs et al.)
- Firmware (Chip Suppliers, CSPs et al.)
- Root-of-Trust Platform Management Controller
- Memory Management System
- Possibly, the Smart NIC Operating System/Applications/API

What must be Attested?

- Hardware/Silicon
- Programmable Logic on Silicon
- Firmware
- Root-of-Trust Platform Management Controller
- Memory Management System
- Possibly the Smart NIC Operating System/Applications/API

Independently Patchable

Trust in the Verifier

- Attestation of TCB components ensures the HW/FW and configuration measurements meet CSP requirements, not that the TCB is trustworthy.
- Trustworthiness principles include
  - **Code Publishing**
  - **Code Auditing**
  - **Code Transparency**

Establishing Verifier Trustworthiness

- **Code-Publishing** does not prove that code is safe. Allows the community to inspect code for back-doors and bugs.
- **3rd-party audits** provide proof of whatever claims the audit sponsor paid for. Difficult to keep pace with a production release cadence.
- **Code Transparency Service** (CTS) coupled with a **Reproducible Build System** (RBS). The CTS provides an immutable ledger where production build components and their configuration can be registered. An RBS is an environment to reproduce the production build measurements.

For more info: Why Should I Trust Your Code?

Agenda – Confidential Smart NICS

- Cloud Service Providers (CSPs) offload Network and File I/O to proprietary hardware/software devices (Smart NICs)
    - Increases Performance
    - Reduces Cost-of-Goods-Sold
- TEEs can maintain confidentiality of the file and network I/O streams by encrypting data within the TEE boundary (Confidential Encryption). This consumes TEE CPU cycles which affects workload performance.
- Customers who require higher performance can choose to expand the TCB boundary using SPDM and TDISP to gain better performance and lower cost
- NorthStar question: How to measure the trustworthiness of CSP Smart NIC code and hardware

Thanks! See you at the Q&A!