A Secure Network Stack for the Untrusted Cloud

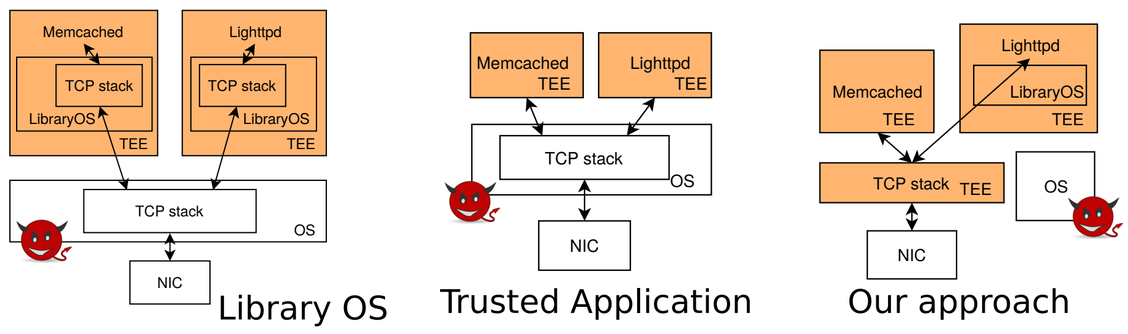
Keita Aihara, Pierre-Louis Aublin and Kenji Kono
k.k.aihara@sslab.ics.keio.ac.jp
Keio University, Japan

Context

- **Trusted Execution Environments** (TEE) provides **integrity** and **confidentiality in untrusted** environments
- **Cloud** not inherently malicious but **subject to bugs** or **data leakage**
- **Cloud** is a prime **target of attacks**
- Example of TEE: Intel SGX, ARM TrustZone, etc.

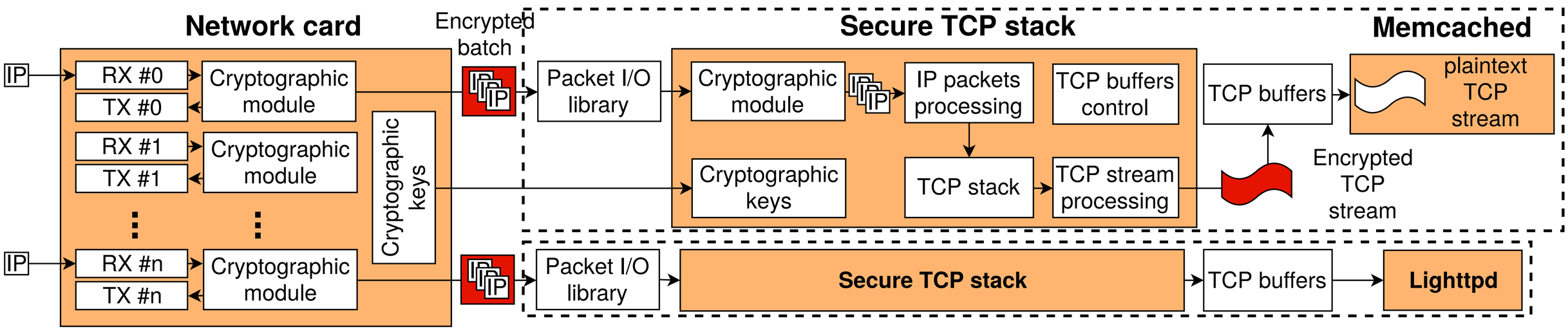
Problem

- Existing TEE-based **applications rely on untrusted** network **stack**
- **No isolation** from other components
- **No** metadata **protection**



Proposal: Shinkansen

1) Network card with encryption 2) User-space packet I/O library 3) User-space secure TCP stack
4) Stream/packet processing API for debugging, logging, etc.

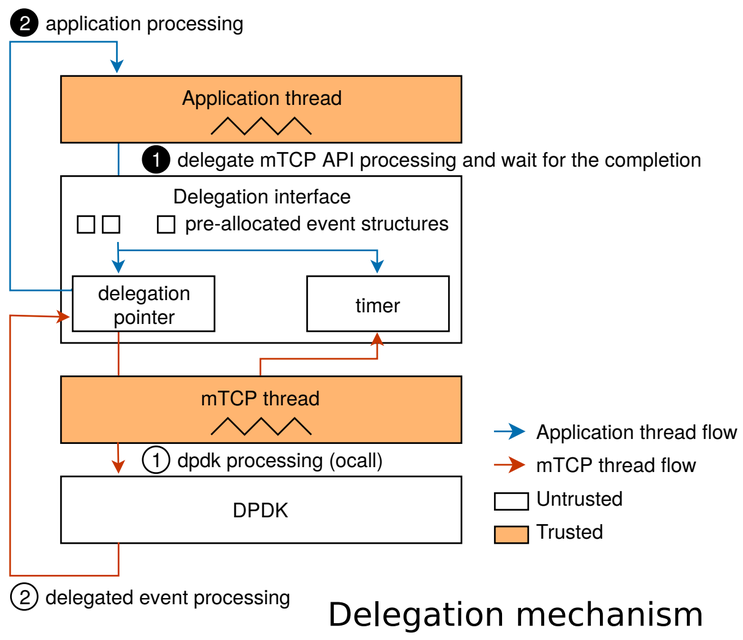


Implementation

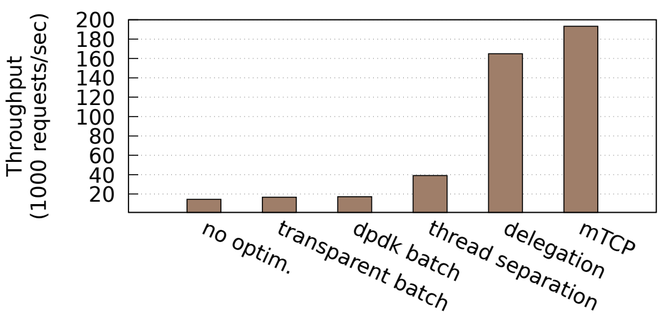
- Network card: Mellanox **SmartNIC**
- Packet I/O library: **DPDK**
- Secure TCP stack: **mTCP**
- TEE: Intel **SGX** enclave

Performance optimisations:

- Batching of network operations
- Delegation mechanism avoids transitions



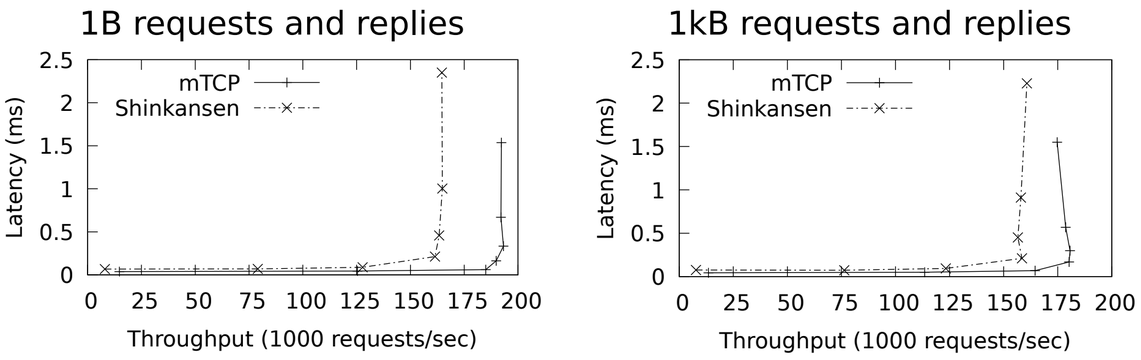
Delegation mechanism



Performance optimisations

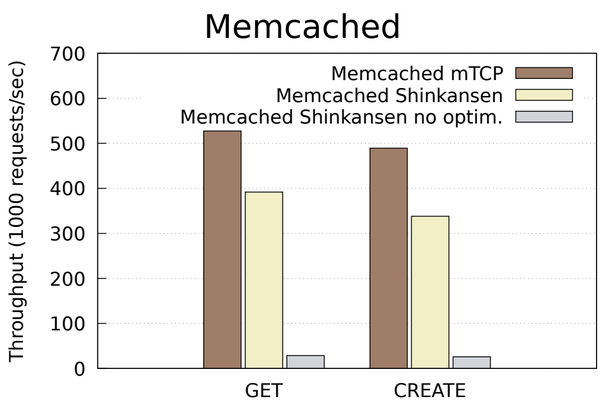
Microbenchmark performance

- Intel SGX capable processor
- 10Gbps standard NIC



- 15% overhead due to enclave transitions w/ DPDK
- SmartNIC AES-GCM encryption: 477Mbps / core

Applications performance



- **9%** performance **overhead**

Application-specific processing: data exfiltration