Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Seminar
Applied Methods in Network and System Security

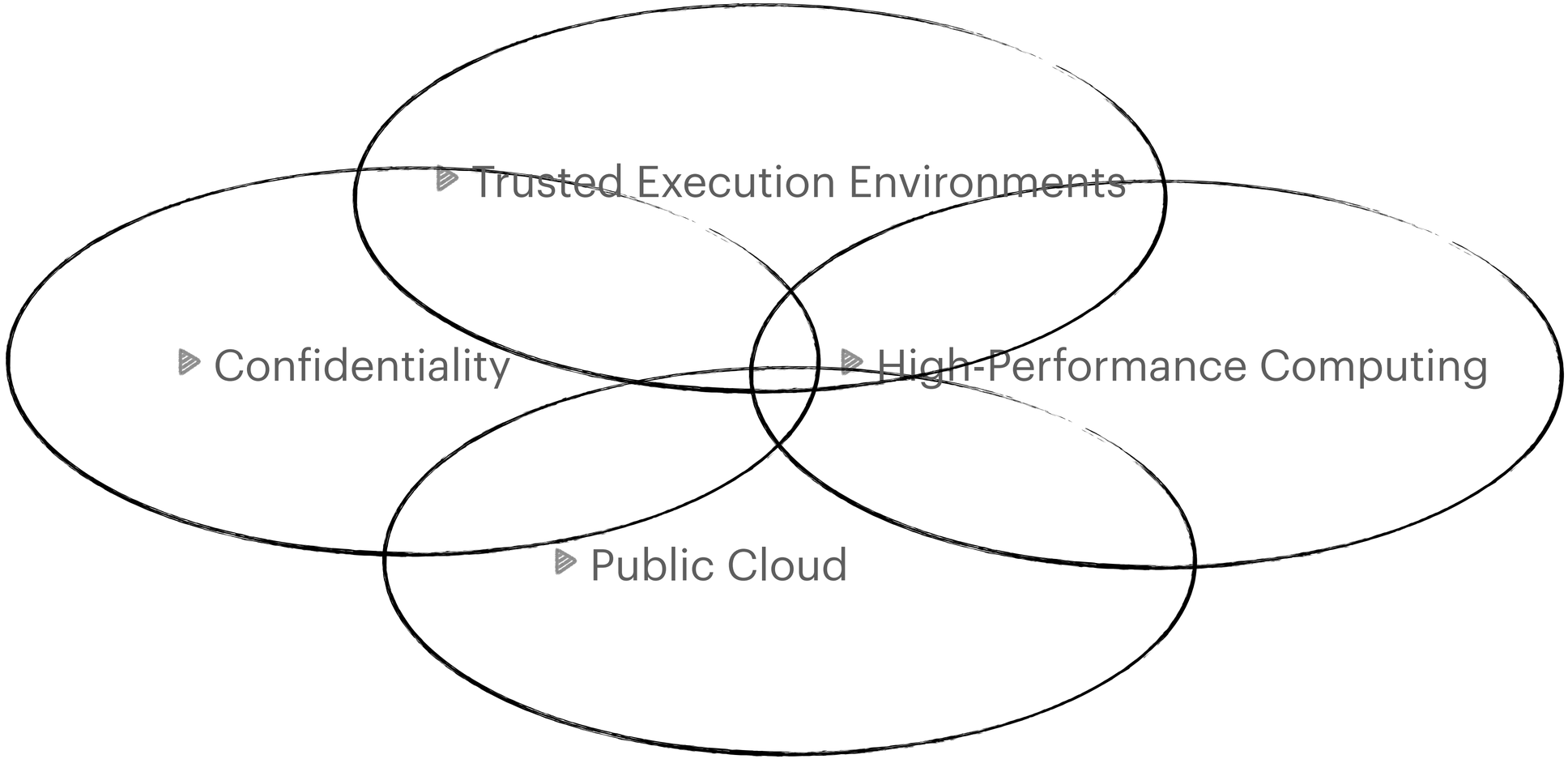
High Performance Computing: Trusted Execution Environments

Second lieutenant, Representative, Valentin Pfeil

Confidential High-Performance Computing in the Public Cloud

Keke Chen

Computer Science Department, Marquette University


Trusted Execution Environments
Confidentiality
High-Performance Computing
Public Cloud

Single-User vs Collaborative-Multiparty Cases

- Problem: Confidential computation tasks on untrusted cloud servers (OS/Hypervisor), Reproducible workflows/logging
- **Approach: Intel SGX (hardware-protected memory area, enclave, RAM/Cache)**
- **Challenges: Mem.-Acc.-Patterns, Interplay between private components and service components**

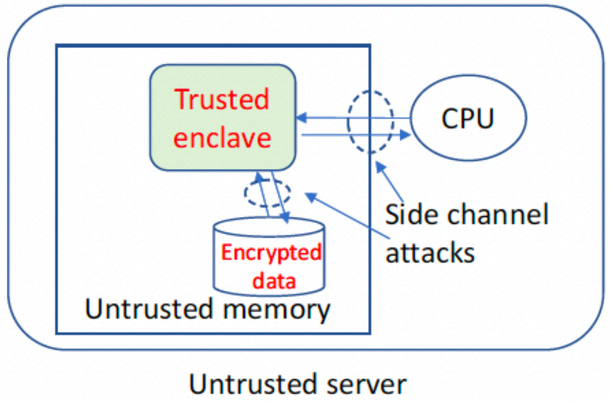


Figure 1. Threat model for TEEs.

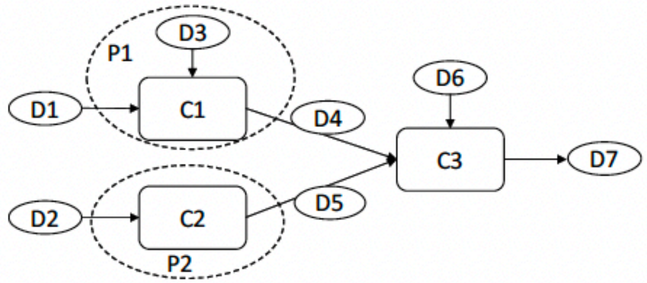


Figure 2. Collaborative workflow with private components. P_i: participants who may own private components, C_i: processing component, D_i: data component. P_1 and P_2 own private components, while all other components are public.

- **Pure Software Approaches vs Hybrid Setups**
  - Homomorphic Encryption
  - Secure Multiparty Computation (MPC)
  - Hybrid Constructions: AHE, SHE, MPC
  - **TEE: Unique CPU features**
    - **Intel Software Guard Extensions (SGX)**
    - **AMD Secure Encrypted Virtualization (SEV)**

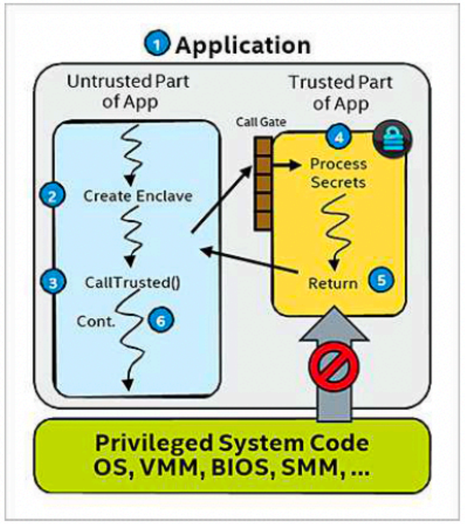


Figure 3. Illustration of SGX runtime execution (from intel.com)

- **Pure Software Approaches vs Hybrid Setups**
  - Homomorphic Encryption
  - Secure Multiparty Computation (MPC)
  - Hybrid Constructions: AHE, SHE, MPC
  - **TEE: Unique CPU features**
    - **Intel Software Guard Extensions (SGX)**
    - **AMD Secure Encrypted Virtualization (SEV)**

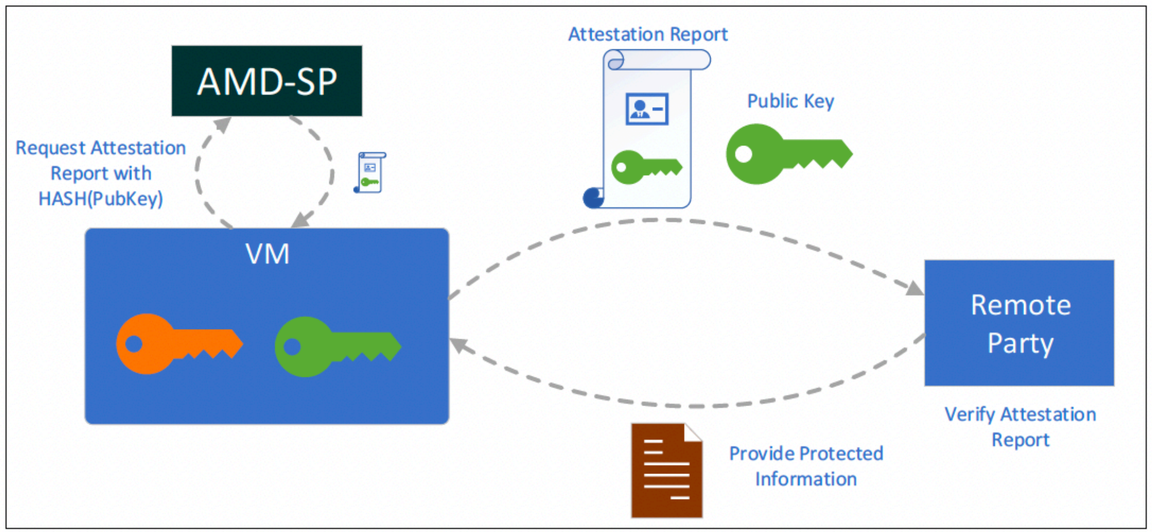


FIGURE 10: SEV-SNP ATTESTATION

Unique Challenges

- **Usability**: Intel SGX - Complex, requires code mod; AMD SEV - more practical; Higher level of confidentiality **requires** code modification
- **Side-Channel Attacks:** Memory and Cache needs different access patterns to be more resilient, requires higher complexity
- **Performance:** Performance penalty included in any implementation
- **Collaborative Workflow:** Owners attack, conflict between confidentiality and provenance analysis, Reproducibility Verification

Possible Solutions

- **Usability**: Intel SGX - Graphene-SGX and SCONE try to build library OS or shim layer allow unmod. Linux Apps in enclaves; Google Asylo and Open Enclave try simplifying SGX programming without using API
- **Side-Channel Attacks:** Protection of Block Access Patterns, ORAM (disguise block I/O accesses), Data flow optimisation, Data Oblivious Approaches (App-Specific), Access Pattern Protection (Framework-Level, SGX-MR), Monitoring and Detection (Intel Transactional Synchronisation Extensions (SGX-TSX)
- **Collaborative Workflow:** Protect from dishonest owners, Control accesses to provenance data, automated secure replay of workflows

- **Insights and benefits for the research paper**
  - Systems in the public cloud are considered as untrusted
    - TEEs contribute significantly to their trustability by adding a hardware-level security layer
  - The developments of TEE address the unique challenges of confidential computing on HPC systems as
    - Usability, Side-Channel attacks, Performance and Collaborative Workflow
- **Benefits:** Provides a decent introduction into TEE and HPC by explaining general concepts and providing insides on current threats and possible measures

References

- Keke Chen. Confidential high-performance computing in the public cloud. IEEE Internet Computing, pages 1–10, 2023. ISSN 1089-7801. doi: 10.1109/MIC.2022.3226757.
- What is hpc? introduction to high-performance computing | ibm, 2/10/2023. URL https://www.ibm.com/topics/hpc.
- confidentiality, 2/13/2023. URL https://dictionary.cambridge.org/dictionary/english/confidentiality.
- What is high performance computing | netapp, 2/13/2023. URL https://www.netapp.com/data-storage/high-performance-computing/what-is-hpc/.
- HPE. Boosting security with trusted execution environments, 2021. URL https://www.hpe.com/us/en/insights/articles/boosting-security-with-trusted-execution-environments-2102.html.
- VMware. What is a public cloud? - definition - how it works? | vmware, 2023. URL https://www.vmware.com/topics/glossary/content/public-cloud.html.

@FI_CODE

http://www.unibw.de/code

Q & A

Valentin Pfeil
Institute for Software Engineering
Research Institute CODE
University of the German Federal Armed Forces in Munich
valentin.pfeil@unibw.de
https://www.unibw.de/code

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München