Secure HPC:
Processing Sensitive Data on Shared HPC Systems

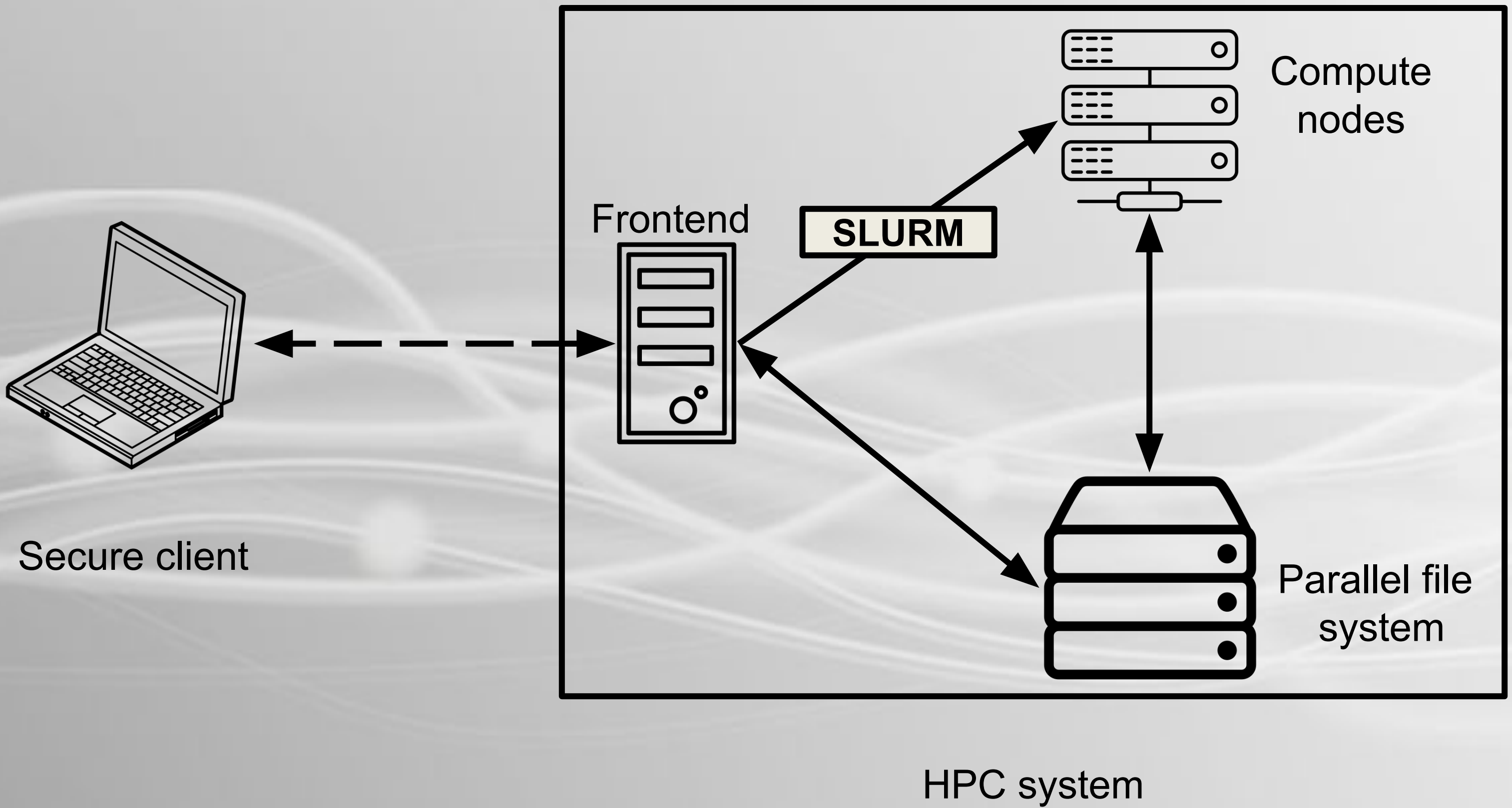
Trevor Khwam Tabougua

Motivation

- Challenge: Security issues on a traditional HPC systems
  - Admins with root access can access all data
  - Attacker that gains root privileges
- Goal: Full data sovereignty of the user

⇒Only the user decides who can access the data

Typical usage



Attack Scenarios

1. Data stored on a shared filesystem
   - Root has immediate access
2. Data stored on a compute node
   - Users can SSH to any node
   - Verification via compromised UID
3. Manipulation of the software
   - System OS or Software in the shared module system
4. Network Manipulations
   - Injection of management packages from compromised nodes

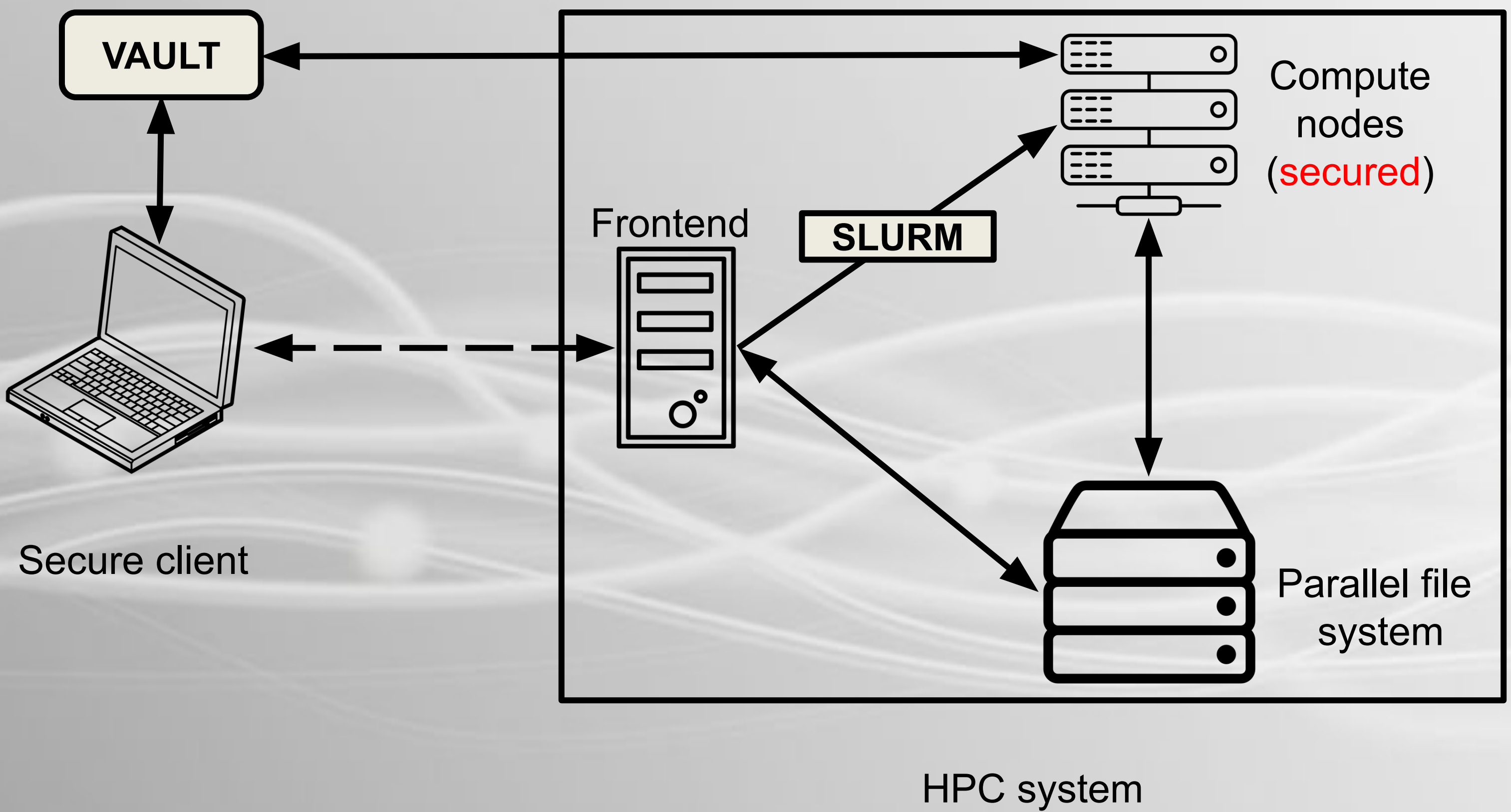
Solution

The **secure workflow**:

● Enables processing of sensitive data on a shared HPC system
 -> Typical use case is with medical data

● Secure workflow minimizes the attack surface
 -> Even legitimate admins would not get access to the data

Overview


VAULT
Compute
nodes
(secured)
Frontend
SLURM
Secure client
Parallel file
system
HPC system

Prerequisites

- **Data**
- **LUKS**
- **Singularity container**
- **Public key**: with the corresponding private key on the HPC system
- **Private key**: with the corresponding public key on the HPC system
- https://github.com/gwdg/secure-hpc

Execution

- Automatic end-to-end workflow
- A shell template **command.sh.template** has to be edited with <uid> , <hpc_uid>, and <container_name>. This is the only file that has to be modified. The rest is executed automatically
- Execute the command (in the client folder)

```
./automatic.sh <uid> <hpc_uid> <container_name>
```

⇒Data encryption, singularity container encryption,
keys upload to Vault, batch script encryption,
batch script signature, batch upload, and get the results

References

- Nolte, Hendrik, Simon Hernan Sarmiento Sabater, Tim Ehlers, and Julian Kunkel. ***"A Secure Workflow for Shared HPC Systems."*** In 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), pp. 965-974. IEEE, 2022.
- Icons are from thenounproject.com, and the authors are: Jamison Wieser, Mentari Pagi, Angelic, Kihosa, Achmed Zaha, and Valeriy

More detailed schema