Secure Disk Scrubbing in a Large-Scale Automated Testbed

Cody Cutler, Eric Eide, Mike Hibler, Robert Ricci
Flux Group, School of Computing
THE UNIVERSITY OF UTAH

Node Booting

The Emulab testbed gives users full access to physical nodes

Must be secure:

- Physical nodes are time-shared
- Users have root access
- Even BIOS is untrusted

Nodes must be scrubbed completely between uses

Must be scalable:

- 500+ physical nodes in constant use
- Automated node allocation/deallocation

Admin interaction is not feasible

Must be flexible

- Node boot paths change frequently
- Boot code is upgraded periodically

Locking down to one particular boot path per node is not acceptable

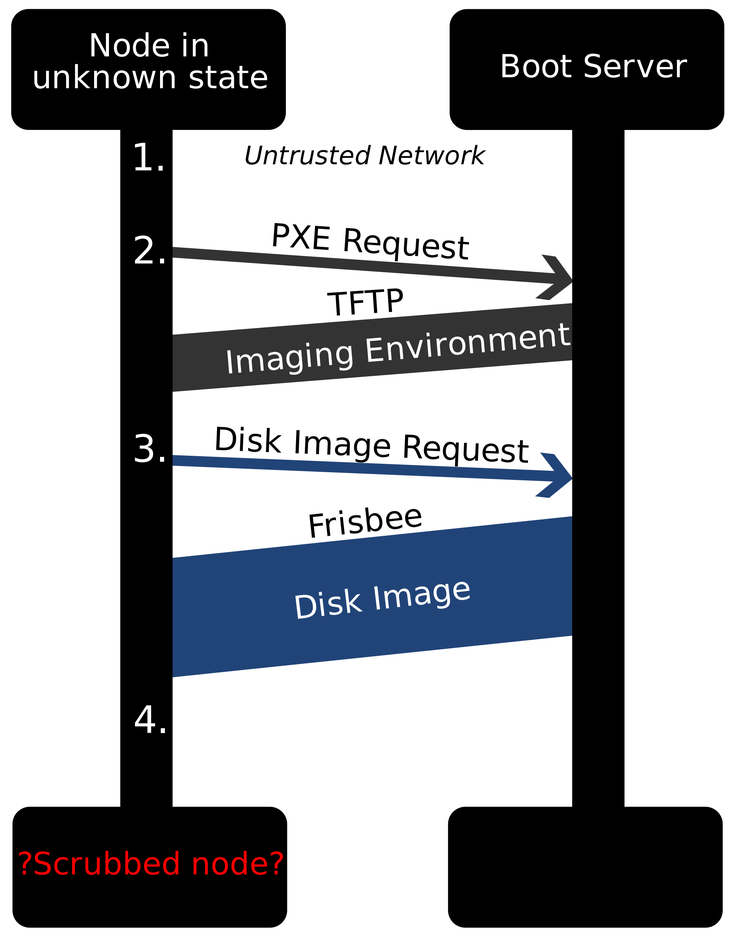
Our approach:

Redesign the boot path to protect the disk-loading process while adhering to the above requirements

Standard Boot Path

1. BIOS POSTs and boots PXE code
2. PXE consults boot server and receives imaging environment
3. Imaging Environment writes new image to disk
4. Node reboots and boots from disk

State not guaranteed

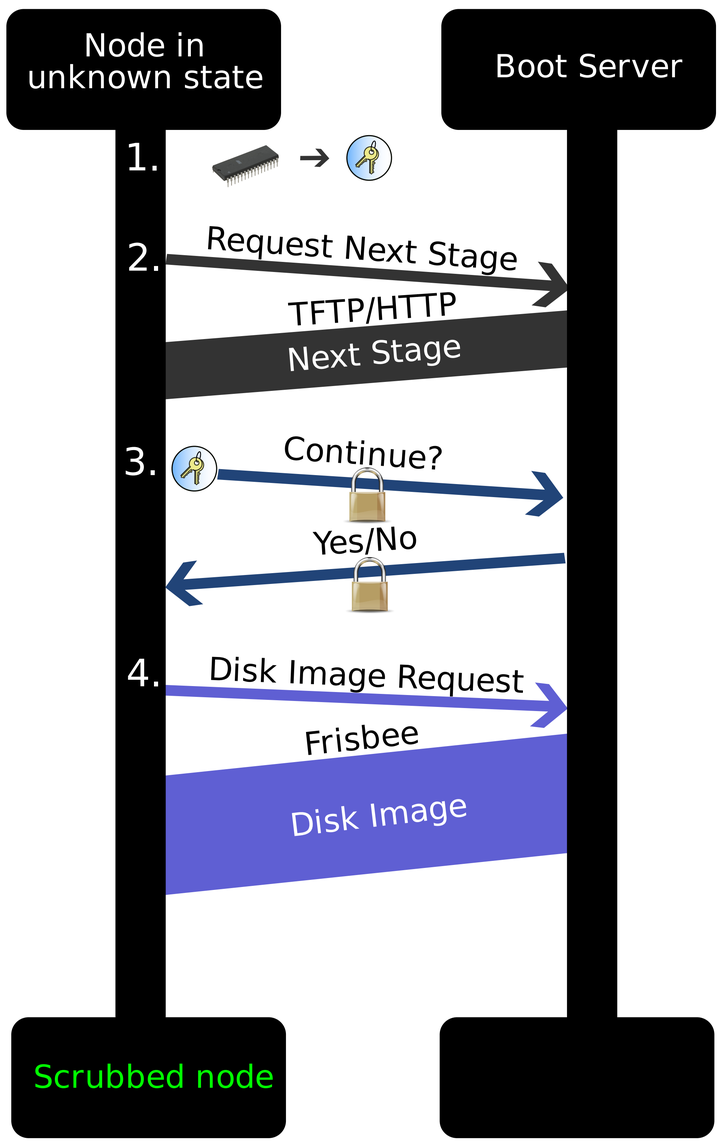


Secure, Flexible Boot Path

1. BIOS and boot loader are measured by TPM - control is passed to the boot loader
2. Current stage receives next stage and measures it in software
3. Current stage creates TLS session with the boot server and asks whether or not to continue

Repeat steps 2 through 3 until the last stage is reached

4. Imaging Environment writes new image to disk
5. Node reboots and boots from disk



Critical Design Points

- Hybrid HW/SW technique for "measuring" (verifying) boot stages
- Immutable hardware trust root (TPM)
- Server verifies dynamic boot stages
- If any stage fails to verify, boot process is aborted
- TPM contains TLS key allowing secure communication channel

Novel Properties

- Add or modify boot paths
- Transparent to node user
- VM-like isolation for physical nodes
- Fully automated
- No local state dependency

This material is based upon work supported by the National Science Foundation under Grant No. 0709427. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation