PECI Power and Energy Conference at Illinois March 10-11, 2022

Open-Source Architecture for Multi-Party Update Verification for Data Acquisition Devices

Benjamin Newberg and Santiago Grijalva

School of Electrical and Computer Engineering

Georgia Institute of Technology

Atlanta, Georgia, USA

bnewberg@gatech.edu, sgrijalva@ece.gatech.edu

Vincent Mooney

School of Electrical and Computer Engineering

School of Computer Science

Georgia Institute of Technology

Atlanta, Georgia, USA

mooney@ece.gatech.edu

This work has been partially supported by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) under Cybersecurity for Energy Delivery Systems (CEDS) Agreement Number DE-CR0000004 to the Georgia Tech Research Corporation

Georgia Tech

Outline

- Introduction
- Background
- Attack Scenario
- Proposed Mitigation: Multi-Party Update
- Prototype System
- Experiment
- Discussion and Conclusion

Introduction

- Cyberattacks on the power grid can be a major problem
- Ukraine suffered such an attack in 2015 that knocked out power for 200k customers
  - Done through insecure firmware
  - US CISA ICSA-16-152-01
- It is difficult to assess the security of proprietary devices
- We propose to use an open-source platform to model different combinations
  - Gentoo, which is a Linux distribution
- Run an air-gapped network

Background

- Rivest-Shamir-Adleman (RSA)
  - Asymmetric cryptography
- Transport Layer Security (TLS)
  - Protocol commonly used to encrypt data traveling over the internet
- Certificate Authority (CA)
  - Way to establish root of trust for connections
- Gentoo
  - Linux variant with USE Flags to control compiling the software packages from source
- Containers to help with ease of administration and scheduling

Software Packages

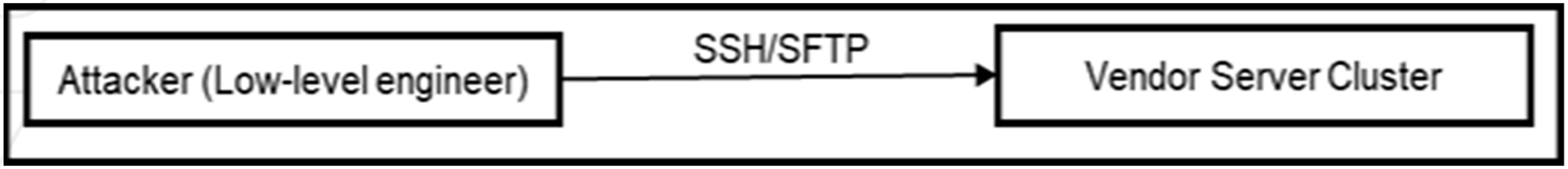
SOFTWARE	Description
Podman	Container Management Software
Moby	Container Management Software
Nomad	Workload orchestrator
Consul	Service mesh communication coordinator
Vault	Management of the certificate authority
Ceph	Storage backend that creates storage clusters

Software Packages

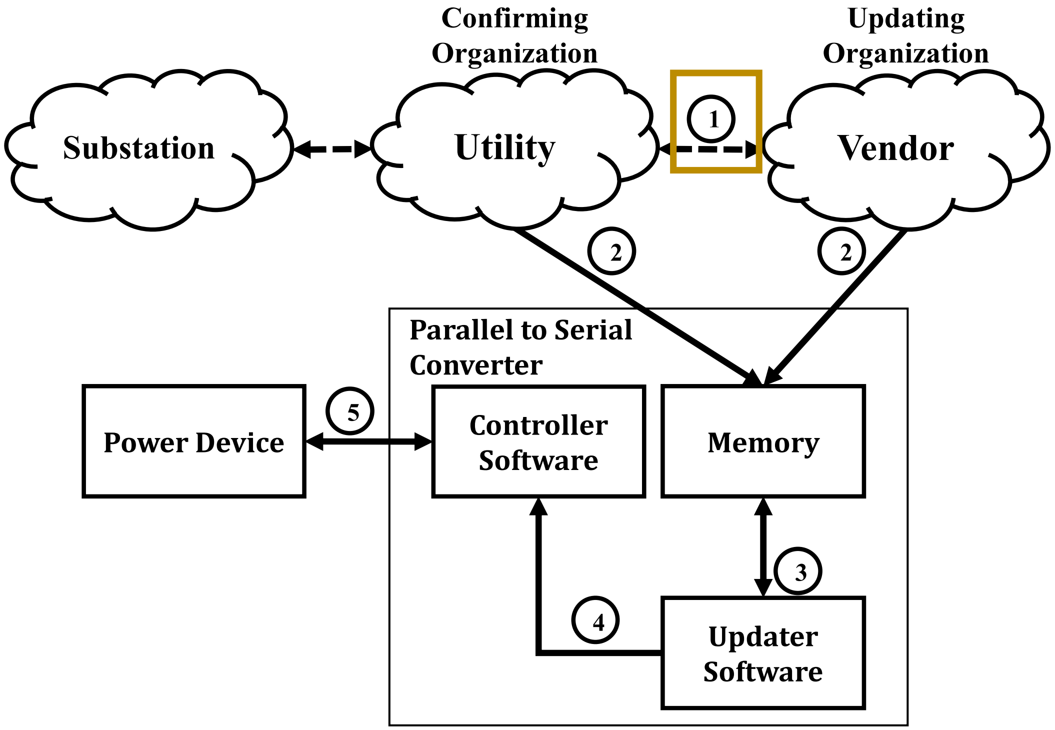
SOFTWARE	Description
Hockeypuck	Key server
GitLab	Git server
Traefik	Reverse proxy
Chrony	Network time protocol server
CoreDNS	DNS Server
Gemato	Gentoo manifest creator/verifier
Portage	Gentoo package manager

Attack Scenario

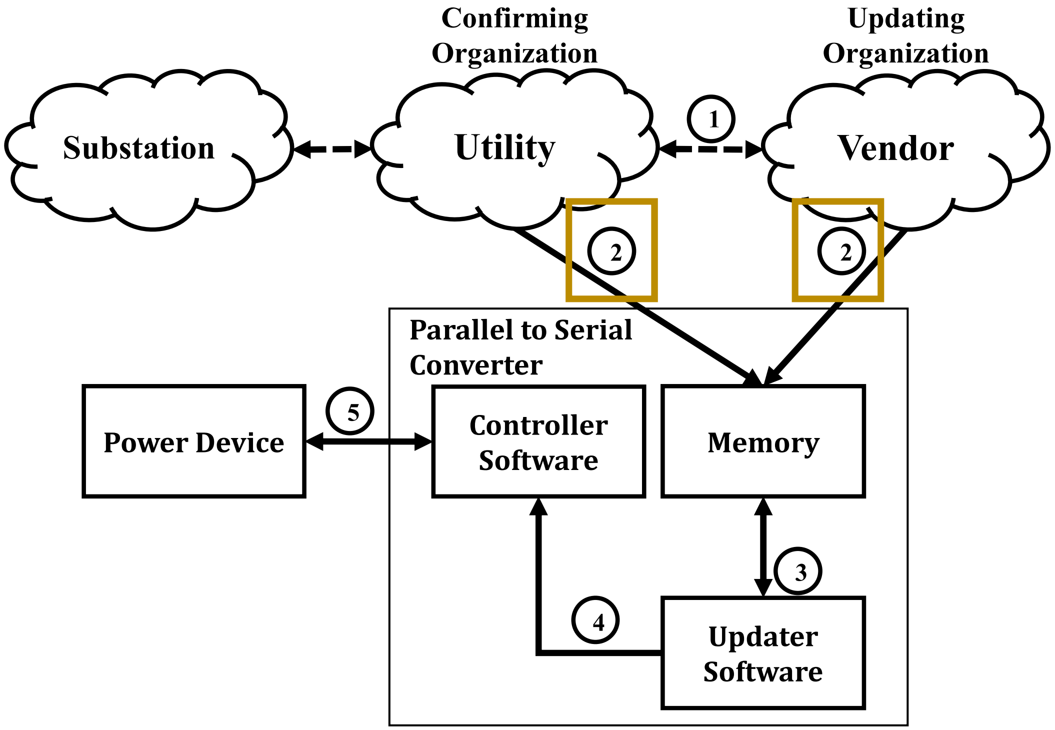
- Low-level engineer inside network



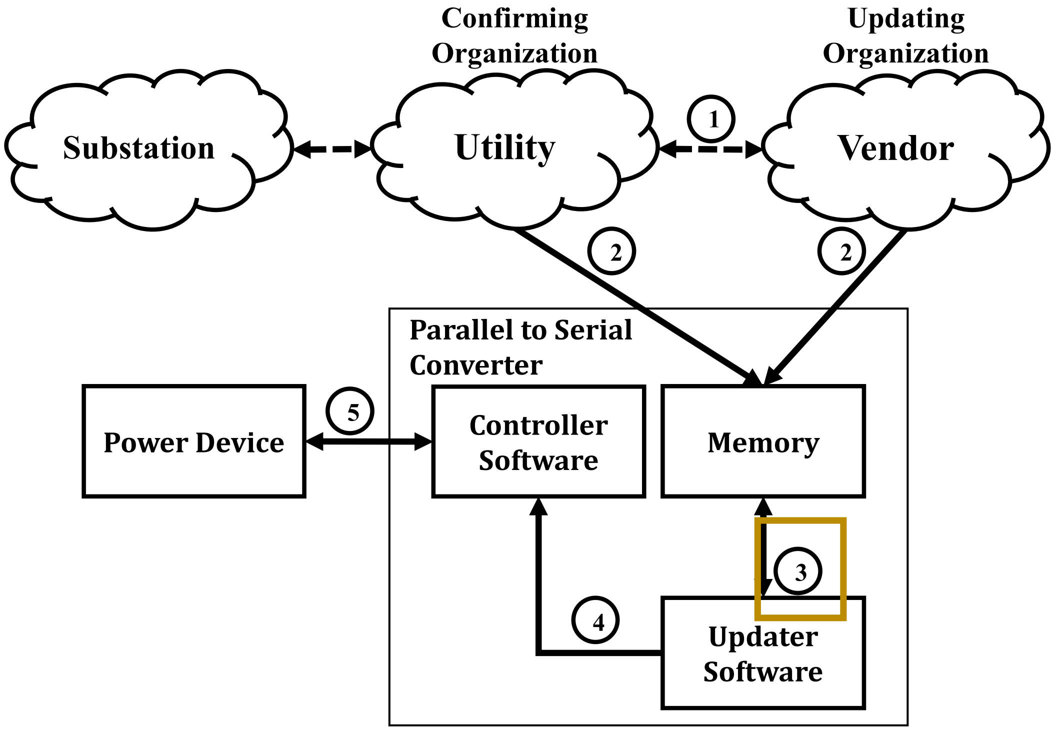
Proposed Mitigation: Multi-Party Update



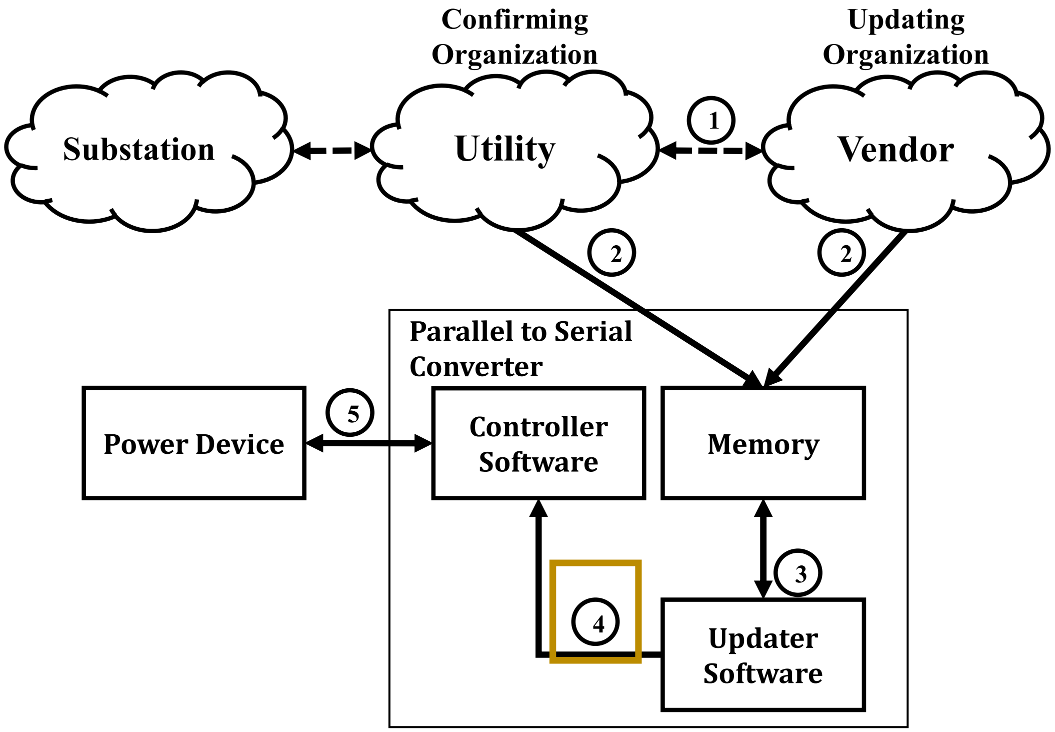
Proposed Mitigation: Multi-Party Update



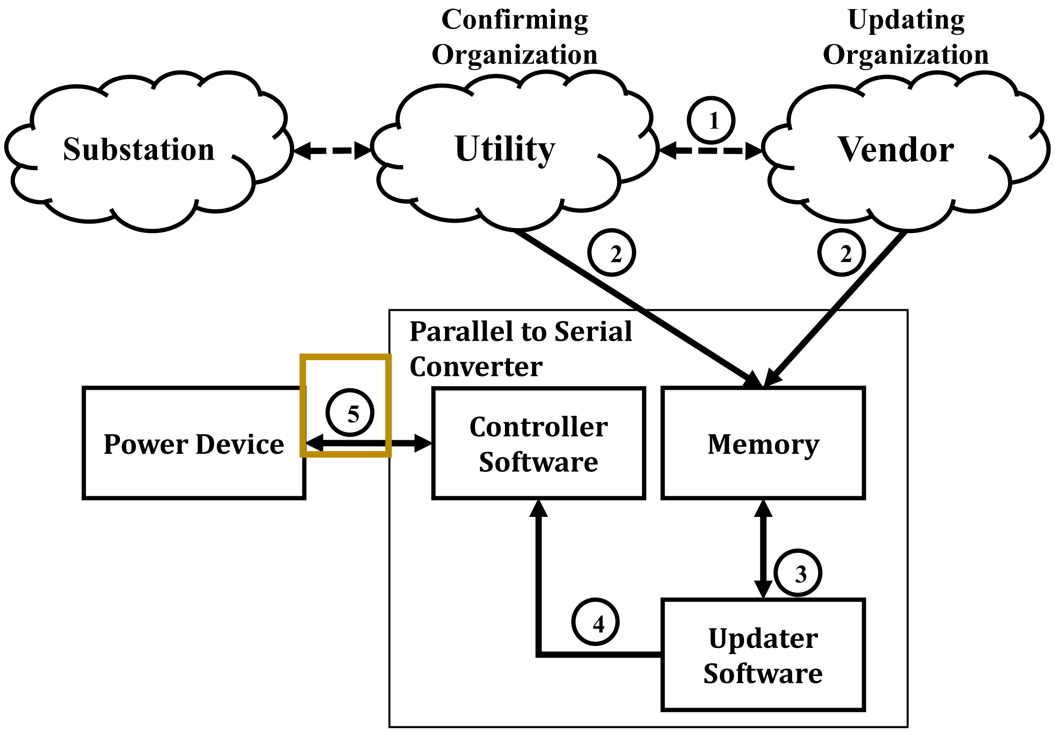
Proposed Mitigation: Multi-Party Update



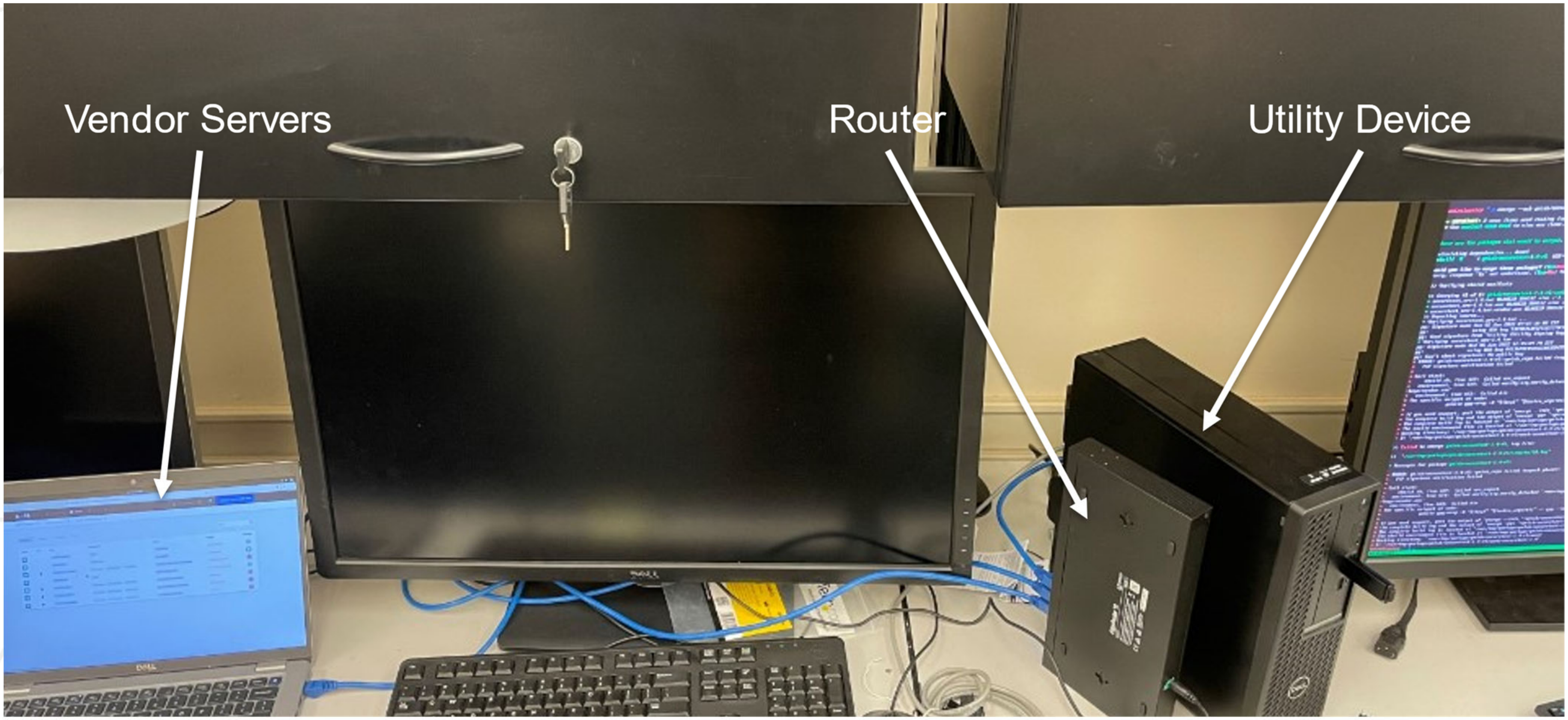
Proposed Mitigation: Multi-Party Update



Proposed Mitigation: Multi-Party Update



Prototype System



Experiment

TABLE II: Experiment Setup and Results

Experiment	Utility Signature	Vendor Signature	Certificate Authority	ebuild Manifest Signature (Vendor)	ebuild Git Signature (Utility)	MITM	Result (at which point did it fail)
1st	Correct	Correct	Correct	Correct	Correct	Not tried	Update installed successfully
2nd	Missing	Correct	Correct	Correct	Correct	Not tried	Fails to download detached signature
3rd	Correct	Missing	Correct	Correct	Correct	Not tried	Fails to download detached signature
4th	Tampered	Tampered	Fake by attacker	Correct	Correct	Tried	Warning of unknown CA so nothing downloaded
5th	Correct	Correct	Correct	Unknown	Correct	Not tried	Warned no signature, and then deleted the downloaded copy
6th	Correct	Correct	Correct	Missing	Correct	Not tried	Warned signature missing, and then deleted the downloaded copy

Experiment

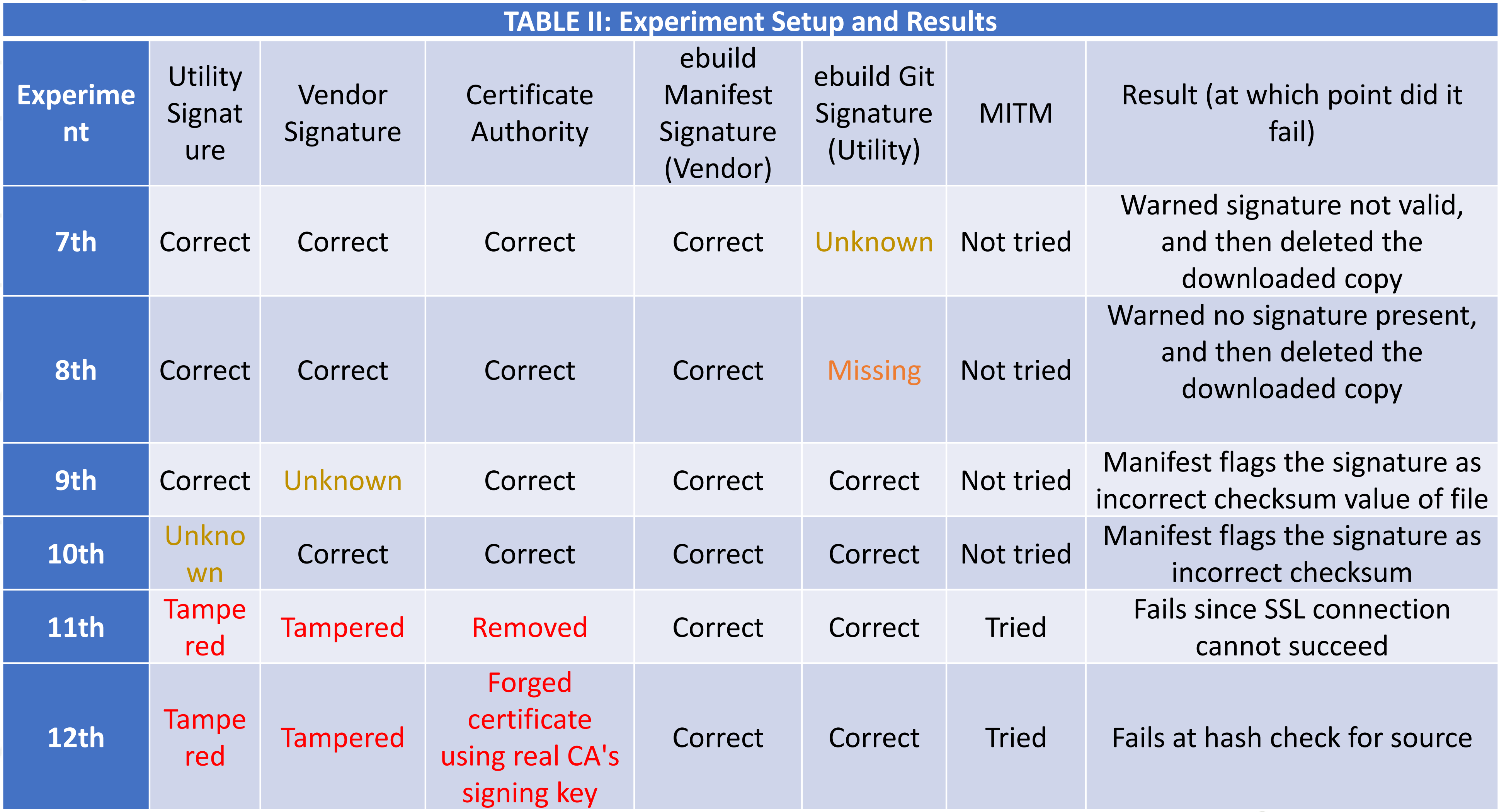


TABLE II: Experiment Setup and Results

Experiment	Utility Signature	Vendor Signature	Certificate Authority	ebuild Manifest Signature (Vendor)	ebuild Git Signature (Utility)	MITM	Result (at which point did it fail)
7th	Correct	Correct	Correct	Correct	Unknown	Not tried	Warned signature not valid, and then deleted the downloaded copy
8th	Correct	Correct	Correct	Correct	Missing	Not tried	Warned no signature present, and then deleted the downloaded copy
9th	Correct	Unknown	Correct	Correct	Correct	Not tried	Manifest flags the signature as incorrect checksum value of file
10th	Unknown	Correct	Correct	Correct	Correct	Not tried	Manifest flags the signature as incorrect checksum
11th	Tampered	Tampered	Removed	Correct	Correct	Tried	Fails since SSL connection cannot succeed
12th	Tampered	Tampered	Forged certificate using real CA's signing key	Correct	Correct	Tried	Fails at hash check for source

Discussion and Conclusion

- Defense in depth
  - Two separate networks increase security by spreading out keys
- New modeling technique allows to look at different devices
- Cloud orchestration technology can be used in power grids to enhance reliability and security
- Open source software can be used to further increase security of the grid