Tamper-Event Detection Using Distributed SCADA Hardware

Jason Reeves and Sean W. Smith

GOALS

- To prevent attackers from accessing a utility's control network by tampering with its remotely deployed embedded devices.
- To determine whether a tamper signal sent from a device represents malicious activity, benign activity (e.g., a technician is servicing the device), or an emergency situation such as a natural disaster.
- To use data from sensors attached to an embedded device, as well as signals from similar devices nearby, to decide whether a tamper signal coming from the device is legitimate or a false positive.

BACKGROUND

- Utilities collect and monitor data from a number of devices, such as reclosers, that are distributed all across their service area. These devices are often mounted on utility poles in both remote and densely populated areas, and have little physical security outside of the cabinet in which they are placed.
- These devices require a connection to the utility's SCADA network. If attackers were to defeat the physical security of the cabinet, they would have direct access to the network.

Image from http://www.gwelec.com/images/products/sel-651r_control.jpg

- The goal of a utility is to shut down access to the control network if one of its devices reports that it has been compromised. However:
  - The utility requires its devices to operate in extreme environments without generating false positives.
  - The utility must also allow for "legitimate" tampering, such as when a technician is sent to service a device.
  - The utility also wants to leave the connection open in the event of a natural disaster, to simplify and expedite recovery effects.

PLAYING DEFENSE IN COMPUTER SCIENCE

- Three categories of physical defenses [9]:
  - **Tamper evidence**: Systems designed to leave obvious evidence if a device is accessed.
    - Tapes, seals, and labels [9].
    - Tamper-evident microprocessors [8].

  - **Tamper resistance**: Systems that resist tampering attempts through either physical properties or design complexity.
    - Special chip coatings [9].
    - Circuit hardware obfuscation [2].

  - **Tamper detection/response**: Systems equipped with sensors that can be monitored for anomalies.
    - SEL-3622 security gateway [6].
    - Integrated microelectric patches [3].
    - Probe attempt detectors [5].

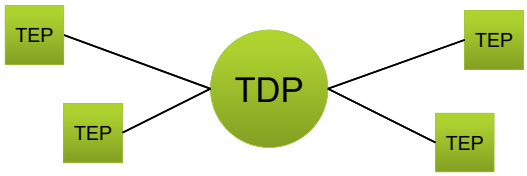
- Security guidelines:
  - **FIPS 140-2** [7]: Federal standard for cryptographic modules used to protect sensitive information.

TODAY'S DEFENSES ARE NOT ENOUGH

- Most tamper protection systems are geared towards protecting data at an individual node, but we wish to protect operations across a multi-node system.
- Tamper-evident systems are often easy to defeat (for example, [1]).
- Tamper-evident systems do not account for non-malicious intrusions, such as when a technician services a device during an emergency.
- Retrofitting of older cabinets with tamper-resistant systems may be too costly.
- Tamper detection/response systems do not always work in extreme environment conditions (for example, the operating conditions of [6] exceed the proper operating temperatures of [4]).
- Tamper detection/response systems may not have enough information to differentiate between a malicious attack and an emergency situation such as a natural disaster.
- Tamper detection/response systems generally have a single course of action to follow, but a system should change its response based on the kind of tampering it detects.
- Standard security levels are not wholly applicable.

OUR APPROACH

- We propose a *distributed* approach to tamper detection, where tamper responses for a single device are based on the status of all the enabled devices in the network.
- *Tamper Enforcement Points* (TEPs) placed in a utility's cabinets use their sensors to monitor the cabinet for intrusions.
  - Sensor possibilities:
    - [6]: Light sensor, accelerometer
    - [9]: Voltage sensor, motion sensor, temperature sensor
    - Cabinet improvements: cover switches, special coatings, etc.
- Abnormal sensor readings trigger a signal to a *Tamper Decision Point* (TDP), which resides in a higher-security area of the network (e.g., inside a substation).
  - Devices will need to be authenticated to the TDP, and tamper signals will need to be secured against replay attacks.



INITIAL IDEAS

- The TDP will maintain a "heartbeat" exchange with each managed device to ensure that they all remain connected to the network. If a TEP becomes disconnected, the TDP must deactivate its port.
- The TDP will also have an interface that allows control center personnel to specify times when tamper signals from particular devices should be ignored.
- When the TDP receives a tamper signal from a TEP:
  - The TDP checks to see whether or not the command is expected (e.g., it has a valid ignore command from the control center).
  - If the command is unexpected, the device gathers tamper status information (either via polling or by reviewing recent signals and pausing a few moments for future ones).
    - If the information received by the TDE fits the profile of a natural disaster, no action is taken. Otherwise, the TDP's tamper signal is considered legitimate, and its network connection is severed.
    - The TDP may also have to take some action as well—for example, deleting some or all of its secret data.

BROADER IMPACT

- To the best of our knowledge, this is the first work to consider making decisions outside the device being attacked, using information from other devices in the area.

NEXT STEPS

- Continue talking to power hardware manufacturers to see how their devices could be used for this project.
- Evaluate the available sensor options for our remote devices.
- Begin profiling the events we are looking for. How do attacks differ from natural disasters in the eyes of a sensor?

WORKS CITED

1. Appel, Andrew W. "Security Seals on Voting Machines: A Case Study." In *ACM Transactions on Information and System Security*, vol. 14, September 2011.
2. Desai, Avinash. "Anti-Counterfeit and Anti-Tamper Implementation Using Hardware Obfuscation." Master's Thesis. Virginia Polytechnic Institute and State University, August/September 2013. http://hdl.handle.net/10919/23756.
3. Dragone, Silvio. "Physical Security Protection Based on Non-deterministic Configuration of Integrated Microelectric Security Features." In *The First International Cryptographic Module Conference*, September 2013.
4. IBM. IBM 4765 PCIe Cryptographic Coprocessor Data Sheet. http://www-03.ibm.com/security/cryptocards/pciecc/pdf/PCIe_Spec_Sheet.pdf.
5. Manich, Salvador, Wamser, Markus, and Sigl, Georg. "Detection of Probing Attempts in Secure ICs." In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, June 2012.
6. Schweitzer Engineering Laboratories. SEL-3622 Security Gateway. https://www.selinc.com/SEL-3622/.
7. United States. National Institute of Standards and Technology. Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
8. Waksman, Adam, and Sethumadhavan, Simha. "Tamper Evident Microprocessors." In *Proceedings of the 31st IEEE Symposium on Security & Privacy*, May 2010.
9. Weingart, Steve. "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses 2008 (Updated from the CHES 2000 version)." Revised and extended version of paper from *Second International Workshop on Cryptographic Hardware and Embedded Systems*, August 2000.

- **Special Thanks To:**
  - **Ryan Bradetich, Jason Dearien, Dennis Gammel, and Rhett Smith of Schweitzer Labs**
  - **Elaine Palmer of IBM Watson**
  - **Steve Weingart of Atsec**

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T