MOSAICS
2020
INDUSTRY
DAY

SRI International

Threat Intelligence for Grid Recovery[1]

Michael E. Locasto and David Balenson
SRI International

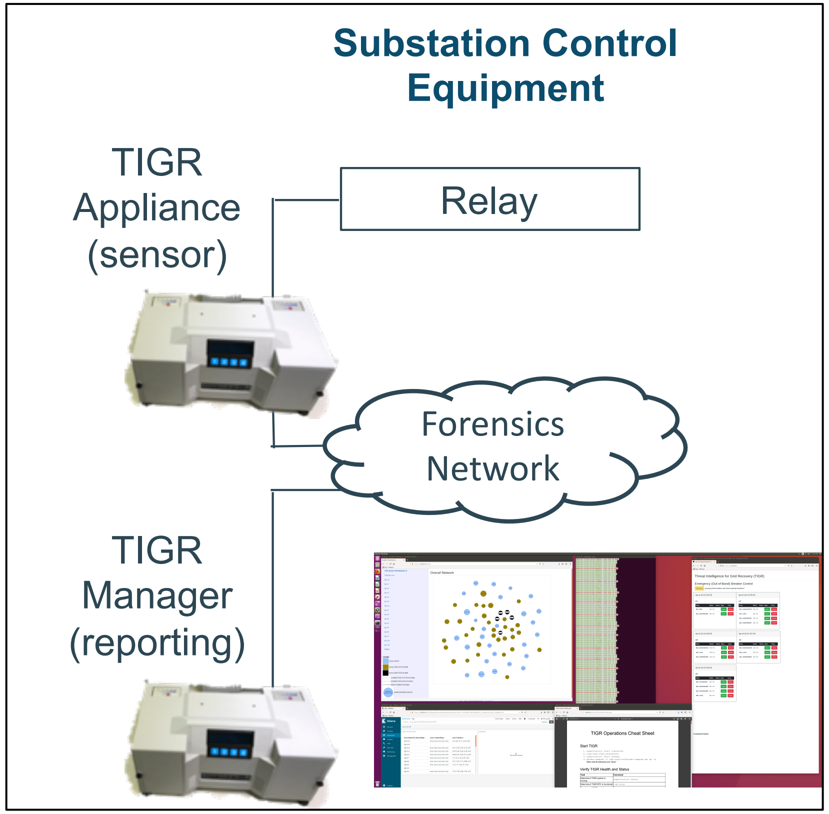
[1] This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the defense advanced research projects agency or the U.S. government.

Bottom Line Up Front: Three Highlights

1. TIGR is a security appliance for protecting critical energy infrastructure that enables utilities and first responders to extract reliable security measurements faster and more safely than traditional IT network and HIDS

2. TIGR identifies presence of non-legitimate software code or configuration modifications with no a priori knowledge of the code or modifications (no signatures required)

3. TIGR completed successful operation in lab tests and in DARPA-sponsored field exercises



Substation Control Equipment

TIGR Appliance (sensor)

Relay

Forensics Network

TIGR Manager (reporting)

Additional Information

4. What synergy does your product bring to MOSAICS?

   TIGR aligns directly with MOSAICS' goal of integrating technologies for enhanced situational awareness and defense of industrial control systems associated with task critical assets

5. What gap does this fill in MOSAICS?
   a) TIGR provides a forensic capability that accelerates human ability to quickly localize cyber faults, flaws, and potential device compromise
   b) TIGR rapidly highlights discrepancies and departures from an inferred specification in ICS equipment and networks

Additional Information (Continued)

6. What is your TRL – which validating agency?
   a) TIGR has not been formally assessed a TRL, but the overall system meets the criteria for TRL 6
   b) TIGR has been implemented as a portable field-ready ruggedized device for diagnosing real substation equipment
   c) The prototype system has been tested at scale in a simulated operational environment

7. What is the contract capability execution path?
   a) TIGR research and development funded under the DARPA RADICS program
   b) SRI is actively seeking commercial licensing partners

Additional Information (Continued)

8. What is novel about your product/capability
   a) The TIGR system performs efficient impact-based detection of unknown malware operation on real ICS devices; its sensors operate by consistency checking against an inferred specification
   b) TIGR can perform threat analysis on uncooperative, closed devices with an adversary present
   c) TIGR explores under-appreciated techniques that are robust enough to operate at the same (presumed) privilege level as an attacker
   d) TIGR performs its threat analysis in a form factor that is compact enough (e.g., handheld or shoebox-sized) and operates without external dependencies, so that it remains field-deployable

Additional Information (Continued)

9. Success Stories
   a) TIGR helped minimize number and specialized expertise of first responders in the DARPA-run field exercises
   b) TIGR enabled National Guard units to independently monitor and remediate realistic substation environments
   c) TIGR has a direct impact on a utility transition partner’s OT forensics knowledge, tools, and procedures

10. POC Contact Information
    a) Michael E. Locasto, michael.locasto@sri.com
    b) Doug Bercow, doug.bercow@sri.com

Technical Operation

11. Leverages latent access and management interfaces as an emergency hatch into ICS devices for deep introspection in contested environments
    a) TIGR uses defensive implants and logic extraction to monitor crucial system properties to create and continuously validate an execution integrity heartbeat
    b) TIGR's novel sensors monitor code behavior (CPU path profiling), file and memory activity (integrity checking of process memory), network communications (using language-theoretic parsing), and model extracted system configurations
    c) TIGR co-opts existing management interfaces, software, and clients as information feed proxies into a scriptable data analytics

Technical Results

12. TIGR provides a forward-deployed bastion host that safely bridges the ICS LAN environment with an analysis network to support remote human operator analysis of ICS devices, collection and exchange of forensic information and files
    a) TIGR operates on real HMI’s, Relays, RTUs, RTACs, and PLCs on x86, x86_64, ARM, and PowerPC platforms
    b) TIGR deduces the operation of non-legitimate software code or configuration modifications without signatures or code
    c) The TIGR software system is installed on a well-provisioned Intel NUC and hosted in a ruggedized metal enclosure with dual automatic failover battery backup and multiple serial, USB, and Ethernet interfaces and connectors