Assessment and Forensics for Large-Scale Smart Grid Networks

Kevin Larson, Mirko Montanari, Roy Campbell

Research Goals

Security monitoring is used in every organization to ensure that its systems are operating correctly. Security policies define how systems should operate (PCI-DSS, NERC CIP, NIST SCAP).

Sophisticated, targeted attacks such as Stuxnet are inevitable, and detecting and developing a deep understanding of what happened is paramount.

We must build monitoring systems that can **tolerate attacks** with limited loss of *integrity* or *confidentiality.* We focus on the security of the information integration.

We must build systems that reliably provide information about compromised SCADA system components and their impact on the power grid, leveraging new and existing forensics tools for better analysis.

Fundamental Questions/Challenges

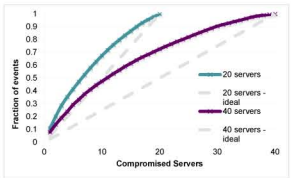
The centralized process used for validating compliance of power systems to policies such as NERC CIP cannot scale in a secure way to the systems that form the "Smart Grid."

An attacker could disrupt electricity networks by obtaining information about vulnerabilities in the system and by injecting false information to the operator.

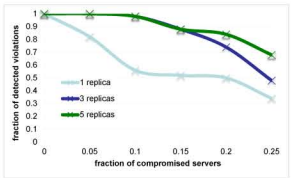
Results

We collected event-traces from lab machines and defined a probabilistic event model.

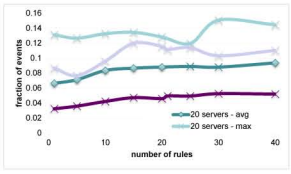
Measurements were performed using Amazon EC2.



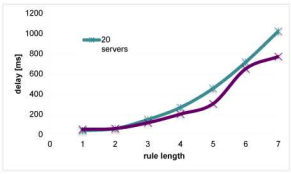
Limited effects of compromises on confidentiality



Limited effects of compromises on integrity



Limited avg and max load on each server

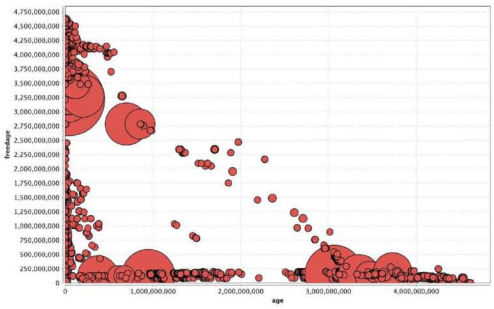


Limited delay in the detection of policy violations

Results

The Forenscope tool is designed to perform trustworthy analysis on machines, even in the presence of malware infections, without shutting them down. It collects information about running processes and open network sockets and detects alterations to critical OS state that may indicate a compromise.

Cafegrind is a survey tool for examining what persists in memory over the duration a program is run. It was designed in tandem with Forenscope in order to understand what a forensics specialist could expect to obtain.



Cafegrind running Konqueror

Broader Impact

Our distributed, secure architecture could be applied to power systems that use distributed computing to transport data like power meter readings, sensor measurements, logs of activity, pressure, and more. Integration of monitoring, policies, and forensics to provide better situational awareness will allow for deeper understanding of compromises and help in responding to them.

Interaction with Other Projects

This research acknowledges contributions and interactions with Boeing and the Assured Cloud Computing Center at Illinois.

Future Efforts

In the area of forensics, our previous research focused mostly on recovering high-quality information to aid in the analysis process.

Future work aims to expand upon that, extrapolating information to learn more about the compromised systems and their impact on the power grid.