Assessment and Forensics for Large-Scale Smart Grid Networks

Overview and Problem Statement

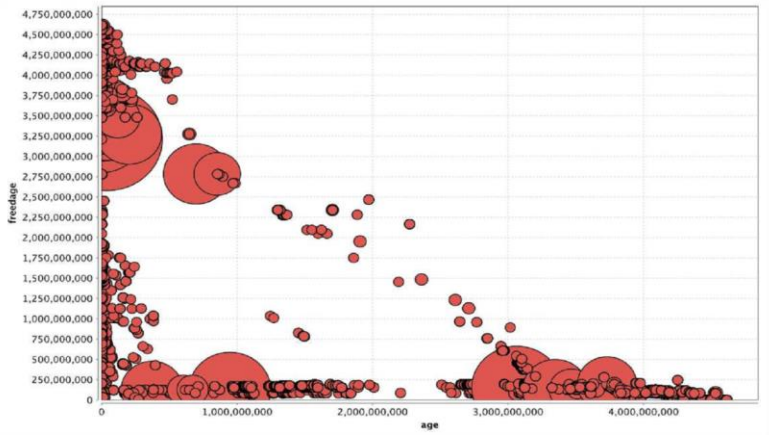
The infrastructure that supports the power grid is vulnerable to attack by intruders who could potentially take control of certain points and cause great damage to systems. The SCADA systems and other components in the smart grid are complex, and many systems rely on information from other sources. An embedded system, such as a breaker, could be compromised and set to report false information. As a result of such a compromise, analyses from monitoring systems and logging would be incorrect, as they would be based on falsified data. Stuxnet and Flame have shown that entities exist that are willing and able to create extremely sophisticated attacks. The Flame malware showed that even an immensely large and complex attack can run undetected for years. The sophisticated rootkits employed by Stuxnet and Flame showed that the current standard of detection software is easily defeated. Sophisticated, targeted attacks such as Stuxnet are inevitable, and both detection of such attacks and development of a deep understanding of what happened are critically important. If machines such as those in SCADA are compromised, we want to know as much about the attacks as possible, and understand what the effects will be on the power grid.

Research Objectives

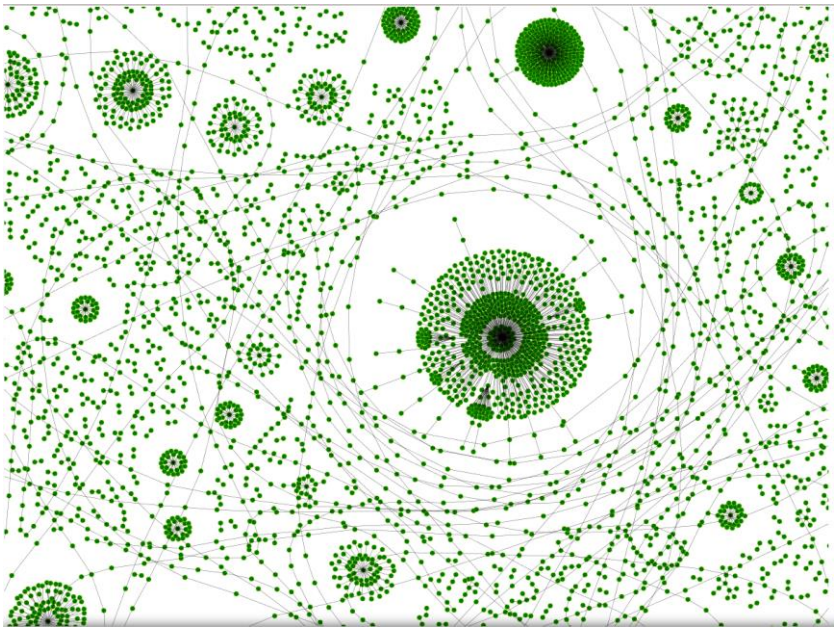
- We will integrate forensics techniques in the monitoring process to ensure the integrity of the applications involved and the information acquired.
- We will communicate with industry to understand what they want to know about compromised hosts and how these compromises will affect the power grid.
- We will leverage new and existing forensics tools for better analysis.
- **Smart Grid Application Area:** Virtual machines, forensics

Technical Description and Solution Approach

- We have continued to develop novel forensic tools and techniques.
- Forenscope collects high-quality information about compromised machines.
- Cafegrind analyzes applications to determine what information is available to forensic investigators.
- Our memory visualization tool provides visual context to assist in creating models to detect attacks from an application's volatile memory.



Cafegrind executed with the Web browser Konqueror. Sizes of circles represent sizes of data structures in Konqueror. The "age" axis represents the number of cycles from when a structure is allocated to when it is freed. The "freedage" axis represents the number of cycles from when a structure is freed until the memory containing the instance of the structure is overwritten.



Memory visualization of the Chromium application. Each green dot represents a pointer, and the lines represent the memory location to which a pointer points.

Results and Benefits

- We have created the Forenscope framework, a memory forensics platform that can perform memory analysis, capture, and sanitization on critical systems outside of the execution context of malware. The platform provided by Forenscope can be extended to perform any number of forensic tasks.
- Additionally, we have created Cafegrind, a memory analysis tool that analyzes applications to determine what information is available in memory for forensic investigation. Cafegrind monitors every instance of every data structure created by an application and monitors all accesses, when the instance is freed, and when the memory in which it was stored was overwritten.
- In order to better understand the structure of an application's memory, we have created visualization tools to provide insight into how we might model memory.
- Partnerships and External Interactions: Information Trust Institute, Assured Cloud Computing Center at UIUC.
- **Technology Readiness Level:** Initial stage.

Researchers

- Kevin Larson, klarson5@illinois.edu
- Karthik Rajashekar Gooli, gooli2@illinois.edu
- Prof. Roy Campbell, rhc@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security