TCIPG

Assessment and Forensics for Large-Scale Smart Grid Networks

Volatile Memory Analysis

Kevin Larson, Karthik Gooli, Roy Campbell

GOALS

- Improve the ability to detect malicious agents and diagnose irregular behavior of SCADA machines in the power grid through the use of live memory forensics techniques.
- Leverage the state of the art in order to create targeted memory forensics tools for the power grid. These tools should be applicable not only to incident response, but also for monitoring operating machines for errors, policy violations, and malicious agents.

FUNDAMENTAL QUESTIONS/CHALLENGES

- 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, analysis 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 these attacks can run undetected for years at a time, even if they are immensely large and complex. The sophisticated rootkits employed by Stuxnet and Flame showed that the current standard is easily defeated.
- Sophisticated, targeted attacks such as Stuxnet are inevitable, and both detecting such attacks and developing a deep understanding of what happened are of paramount importance. If machines, such as those in SCADA, are compromised, we want to know as much about them as possible, and understand what the effects will be on the power grid.

RESEARCH PLAN

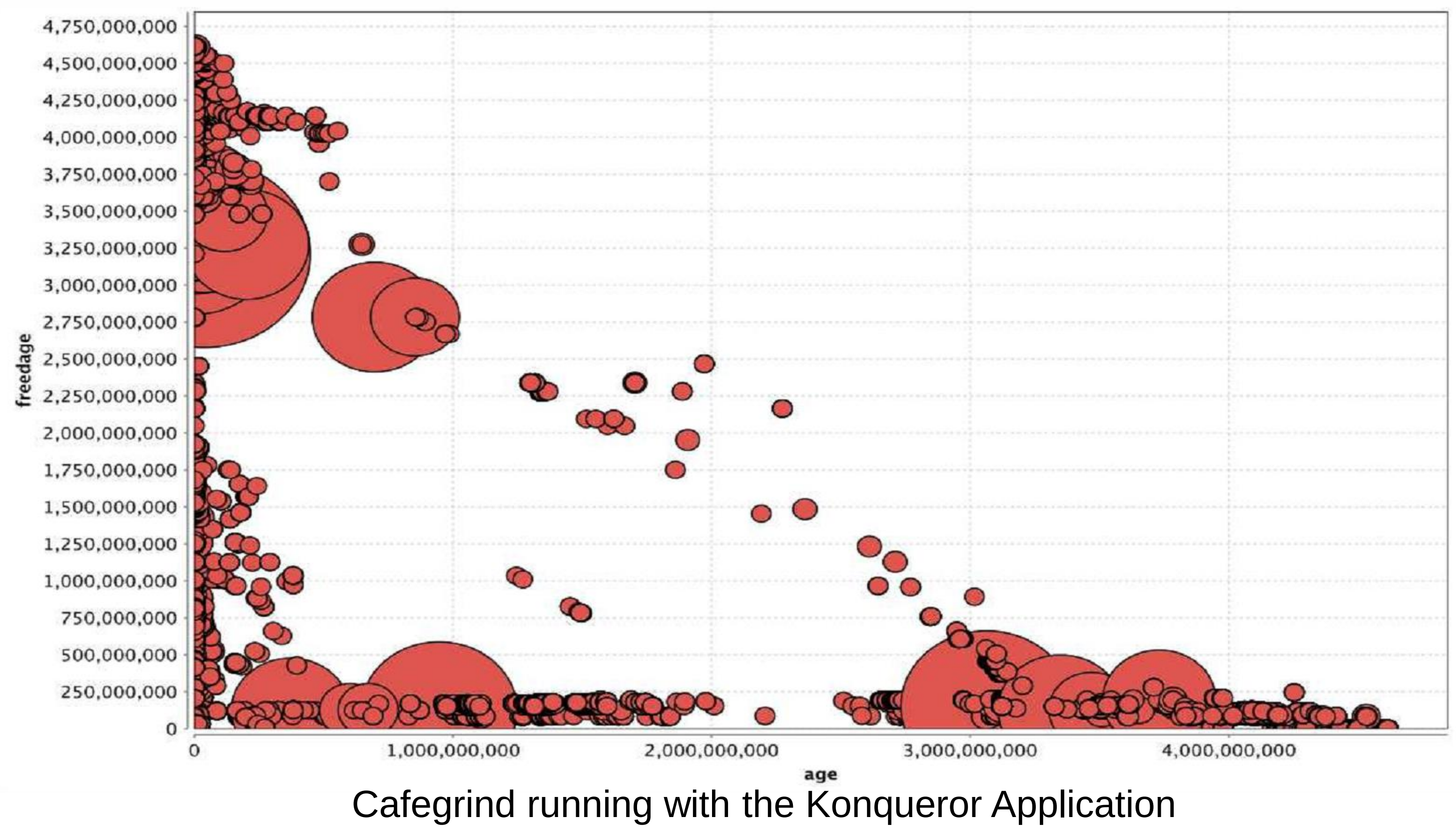
- We have developed Cafegrind, which allows us to see what types of information might be available in a given application when memory is analyzed for forensic analysis.
- Cafegrind could be used to explore the memory contents of reporting, logging, and analysis systems. That information could be leveraged to provide more insight about SCADA protocols and applications.
- The Forenscope tool collects high-quality information about running machines, such as the critical systems running in the power grid.
- Now that Forenscope can produce high-quality memory images of a running system, the next step is to leverage that ability to learn more about a running smart grid system.
- We have a virtual machine environment set up to produce high-quality memory dumps quickly and reliably.
- We are using the Volatility framework to extract an application's heap data in order to model non-malicious behavior.

BROADER IMPACT

- Cafegrind could be used in conjunction with SCADA applications in order to understand those applications' memory structures. Knowledge of what data are available in memory and how the application's memory structures are accessed could be used not only to improve incident response software, but also to aid in the detection of unidentified malicious modifications to SCADA software.
- Forenscope could be adopted for use in both incident response and monitoring in power systems. In incident response scenarios, Forenscope could be used to quickly get high-quality memory images from live systems, such as SCADA machines, that cannot be taken offline. For monitoring, periodic invocation of Forenscope could be used to regularly take images of memory, which could then be used with analysis tools to do some basic checks for errors, policy enforcement, and the presence of malware.

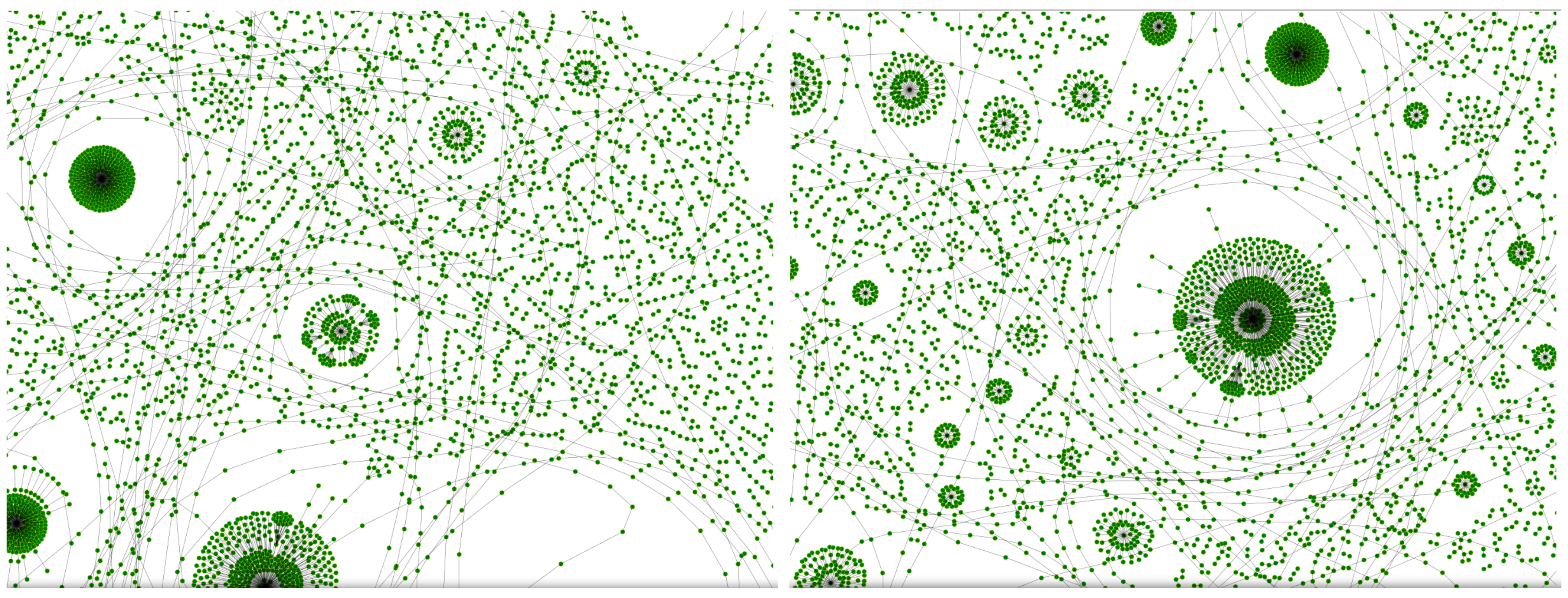
RESEARCH RESULTS

- 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 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.



Cafegrind running with the Konqueror Application

- The above visualization shows the lifespan of various data structures within the Konqueror application (a browser similar to Firefox). The size of each circle represents the size of an object's corresponding data structure. The horizontal (age) axis represents the duration (in cycles) from when an object is allocated to when it is freed. The vertical (freedage) axis represents the duration from when an object is freed and when that data is clobbered (it is recoverable in this stage). Objects shown close to the origin are available only for very short intervals; objects are increasingly available as they are farther from the origin.
- 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.



Visualizations of Chromium with 1 tab (left) and 25 tabs (right)

- The above visualizations show the memory structures from the heap of the Chromium application. They were generated by extracting Chromium's heap pages from each of the two memory dumps. In the left image, Chromium is run with a single open tab, and in the right, 24 additional tabs are opened.

FUTURE EFFORTS

- The primary goal of our research is to create tools and techniques that can be used to detect complex targeted attacks such as Stuxnet and Flame.
- In the short term, we intend to extend our visualization software to better understand how to usefully model application memory. Type inference, inclusion of the stack and code segment data, and temporal analysis (variations across the duration of a running program) are all potential extensions.
- Long-term, those models should be used to train tools to detect modifications to critical system components, such as the modifications to the Step7 software in the Stuxnet attack.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T