Assessment and Forensics for Large-Scale Smart Grid Networks

Kevin Larson, Fangzhou Yao, Karthik Rajashekar Gooli, and 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 to monitoring of 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 relay 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 immensely large and complex attacks 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 paramount. 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 PLAN

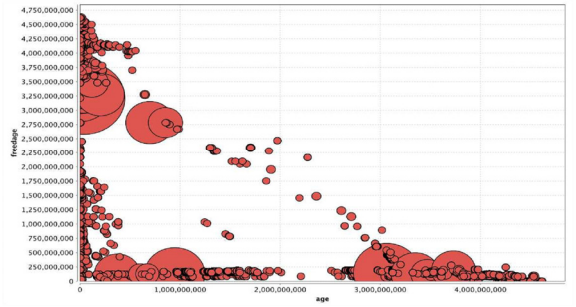
- Cafegrind allows us to see what types of information might be available in a given application when memory is analyzed for forensic analysis.
- Cafegrind could be used to explore the memory contents of reporting, logging, and analysis systems. That information could be leveraged to provide more insight about SCADA protocols.
- Forenscope 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 created a simple virtual SCADA system using the disk images of an SEL 3354 and have begun exploring how the SCADA interfaces appear in memory.
- We are currently working to extend the Forenscope platform to support more directed analysis for SCADA implementations.

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 malware.

RESEARCH RESULTS

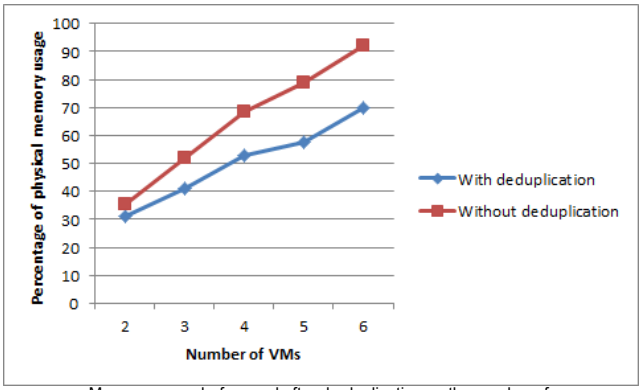
- We have created the Forenscope framework, a memory forensics platform that can perform memory analysis, capture, and sanitization on critical systems outside of the execution context of malware. The platform provided by Forenscope can be extended to perform any number of forensic tasks.
- Additionally, we 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 it was stored in was overwritten.



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

INTERACTION WITH OTHER PROJECTS

- In collaboration with UIUC's Assured Cloud Computing Center, we have explored some of the potential benefits of virtualizing some SCADA applications. As the smart grid grows, increasing monitoring, logging, and computation in SCADA requires a significant increase in computing power. Virtualization in a cloud environment is one of the most cost-effective ways to provide computation, and SCADA applications could benefit from this.
- We developed a system to reduce the memory overhead in virtualized cloud environments. It is built off the idea that many virtual machine images have large quantities of common data stored in memory. Read-only pages containing kernel code, kernel data, application binaries, and application libraries can all be shared across virtual machines, reducing the memory costs of the systems.



Memory usage before and after de-duplication as the number of VM instances per physical host increases.

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. Those attacks both had many components and layers spread across large industrial systems. We suspect that detecting inconsistencies in the interfaces between various HMI (human-machine interface) systems, core SCADA devices, and embedded systems will be key in uncovering such attacks.

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