CSC7575 - Final Exam

Rob Gillen

Question 1

Is the PLC logger presented in the paper useful for volatile memory forensics? If yes, how? If not, why not?[1]

The answer to this question depends on your perspective (in a few ways). As detailed in this paper, the authors state that it is *not*. They cite its failures to adhere completely to the referenced NIST standard as to the characteristics of a proper volatile memory forensics tool. If you have a requirement of strict adherence to this standard, then one cannot but agree with their conclusions.

However, having worked with a number of investigators over my career, this simply doesn't hold water. There *are* some things that are non-negotiables (e.g. ensuring a write-blocker is used or the device prevents tampering). Beyond those items most are somewhat mercenary in their approach. They'll take anything that will give them more insight into what went on. Obviously there are some tools that have legal implications and therefore must provide certain functionality (e.g. adherence to the standards referenced above), but many will use whatever tool (so long as it is non-destructive_) that moves the investigation forward. Often, a non-court-approved tool will give them the hint they need to then go back to a tool-of-record and find (for official records) the same piece of information.

In most of the referenced failed test cases, the tool failed due to a failure to notify the user of a change in state (connected, disconnected, etc.). These are certainly nice features, but may not reach the level of *required* for adding value. One of the failed scenarios points to an uncertainty in whether or not the tool altered the state of the device. Unfortunately, it "failed" not because of confirmed state manipulation, but due to the fact that the researchers were unable to determine either way. While I agree that conclusive evidence is needed, I am uncertain that this should black-ball the tool. Further, if you insist on using a network-connected tool for harvesting this information (thus interacting with the device's local network stack) you may, by definition, be eliminating your tool from consideration due to environment manipulation.

The paper did show the device's ability to successfully retrieve the memory and to provide the investigators with enough information to determine what was going on, and what the attackers were doing (supporting hypothesis #1). This is a clear "adding of value" and demonstration of at least some usefulness.

In the final analysis, the question should be rephrased or dissected into a few. Rather than the authors asking is the PLC logger "useful" (a broad, and somewhat nebulous term), they might ask one or more of the following:

1. Does the PLC logger adhere to the NIST standard?
2. Does the PLC logger provide information that contributes to a forensic investigation?
3. What attributes would disqualify a tool (e.g. the PLC logger) from being used in any fashion in a forensic investigation?
4. At what stage, or in what capacity, might the PLC logger be used in a forensic investigation?

Question 2

What is "betweenness" in a graph? How might unexpectedly disconnecting a link with high betweenness effect the stability of the electric grid?[2]

"Betweeness" is often more completely referred to as "Betweeness Centrality" or sometimes just as "Centrality". While referenced in this paper, it a general graph-theory term/definition and is not unique to these authors. The concept of betweeness centrality is mostly easily understood by executing the following steps:

1. For every pair of vertices in a graph, calculate the shortest path connecting them
2. For each vertex that is traversed by one of these shortest paths, increment a vertex-specific counter totaling how many times it has been crossed
3. Sort the vertices by the vertex-specific counter... this counter is a measure of *betweeness* or *centrality*

It is essentially a measure of how critical a given node is to the optimal (shortest paths) traversal of a graph.

As regards the stability of the electric grid... if a given node has a high betweeness value, that indicates that many other nodes depend on it as a primary route of their power source. If this node were to be taken out, then secondary routes/paths would be utilized. This could have the following effects:

1. The flow of electricity is now on non-optimal paths, potentially increasing the transmission loss and increasing the cost of delivering the service.
2. Like any fault-tolerant system, sometimes the secondary paths are not designed to support the same scale or load as the primary paths. The redirection of load onto secondary paths may inadvertently overload particular paths, causing cascading failures which can ripple/continue until stability is achieved.

Question 3

SCADA network traffic is often considered to be consistent and reliable (in contrast to IT traffic). Do the authors consider this to be true? Why or why not? Do you agree? Why or why not? [3]

The authors are unclear as to their initial position, however the hypothesis (there exists a need to confirm/debunk commonly held opinions as to the characteristics of said traffic) leads a reader to assume they are at least, to some degree, skeptical. Regardless, it is a clear and easy-to-rationalize position and has some basis in historical empirical testing. SCADA systems (historically) were closed networks that operated with fixed protocols often driven by clock-synchronized circuitry. In this case, the traffic is, due to clock cycle-locks, very regular. The traffic on the CANBUS in modern automobiles is another example of a closed-loop system that has very regular traffic patterns.

What the authors show based on their longitudinal study, is that *modern* SCADA systems (e.g. DNP3 over IP) do not exibit this same stability or consistency, even in drastically over-provisioned networks. They show that poll time and inter-packet arrival times have wide distributions rather than the narrow variance one would expect. Similarly, they show that TCP flow durations and flow size are much shorter than would be anticipated in long-connected, lock-step communications.

My agreement (or lack thereof) is essentially a non-issue. Meaning, given a lack of my own empirical evidence, I do not have a position from which to argue. I do agree with the notion that the original assumption (inherent consistency of traffic) is a fair and assumed position by most (myself included). I would further state, however, that their results are intriguing and present opportunities to study other similar networks to establish the broad applicability of their results (e.g. ICS protocols over modern networks such as TCP/IP do not inherit their former regularity).

Question 4

What do the authors identify as the largest source of system instability? Why?[3]

Based on their testing, the authors believe that it is the network controllers in the various embedded ICS devices that introduce the variability. They surmise that these devices had been designed and tested to operate over private networks (e.g. serial) and that later "bolt-ons" such as IP/TCP/DNP3-over-IP have been just that, and that the network stacks are at the bottom of the veritable totem pole when it comes to

time-synchronous operations. An under-powered network controller in these devices would clearly explain the behavior observed.

Of additional note, was that the authors suggested that their initial research showed that the characteristics of these controllers would cluster by manufacturer. This leads them to believe that, with a little effort, such properties could be utilized to identify devices by vendor and possibly even model. This is an interesting area of research that I hope will be explored further.

Question 5

Why is there a challenge to "black start" of nuclear power plants? How do the authors propose to address this challenge?[4]

The sheer scale of these systems (the turbines, etc.) as presently designed and deployed present two (related) issues that prevent them from being strong candidates for bootstrapping in a blackstart scenario. The first is that they require a significant amount of power (> 20 MW) to start. This places their startup requirements well beyond not only onsite generators but also many smaller power plants.

Secondly, the scale of these turbines also means that as they start, the amount of reactive power they introduce to the network is huge. The sources supporting the existing load must be able to handle this level of backpressure which, today, can only be managed by a relatively fully-loaded grid.

One of the core tenants to the author's design is to change the large, monolithic design of today's Nuclear power plants in favor of a modular approach that would be broken into many smaller reactor units. This would enable a finer-grained scale-up/-down based on load as well as allow a single module to be black-started from on-site generators. As that first module comes online, it would be able to start additional modules which would begin a chain that could start the entire plant (as neccessary) to restore full operational capacity.

References

1. Wu, Tina, and Jason Nurse. "Exploring The Use Of PLC Debugging Tools For Digital Forensic Investigations On SCADA Systems." Journal of Digital Forensics, Security and Law10, no. 4 (December 31, 2015): 79–96. http://ojs.jdfsl.org/index.php/jdfsl/article/view/347
2. Cai, Ye, Yong Li, Yijia Cao, Wenguo Li, and Xiangjun Zeng. "Modeling and Impact Analysis of Interdependent Characteristics on Cascading Failures in Smart Grids." International Journal of Electrical Power & Energy Systems 89 (July 1, 2017): 106–14. https://doi.org/10.1016/j.ijepes.2017.01.010
3. Formby, David, Anwar Walid, and Raheem Beyah. "A Case Study in Power Substation Network Dynamics." Proc. ACM Meas. Anal. Comput. Syst. 1, no. 1 (June 2017): 19:1–19:24. https://doi.org/10.1145/3084456
4. Greene, Sherrell R. "Are Current U.S. Nuclear Power Plants Grid Resilience Assets?" Nuclear Technology 202, no. 1 (April 3, 2018): 1–14. https://doi.org/10.1080/00295450.2018.1432966