Human Machine Interface development and vulnerabilities in SCADA systems

Introduction

* Why your topic is important (convince us!)
* Where is it used? Applications
* What you will talk about / do
* Overview of the rest of your paper

Background and related work

* Any relevant and specific info, e.g. software / hardware statistics, equipment used
* What other people had to say on this topic
* What other people did on this topic
* Problems and shortcomings of their work
* How your work is different and better

Proposed methodology

* Your approach to the problem
* What you did
* Code / Algorithms
* What did / didn’t work
* Results – include graphs, equations, pictures, as appropriate

Conclusions

* What was accomplished / learned
* What you would have done differently
* Future work

References

Appendix

* **Main point:** Go over how the interface between human and machines for SCADA processes developed over time and how the web HMI is ignored for security vulnerabilities since the focus is on networks.
* Use GSU, CANDU, and Georgia Nuclear Power plants as examples

Technology Discussion

1. What SCADA is and how does the HMI come into play
   1. Go over SCADA framework (data historian, control, where digital meets analog, RTUs and PLCs). Emphasis on data.
   2. 2 sentences on how everything was old in microcomputer world and then distributed systems came along. It was console then applications with basic GUI.
   3. Now the world is web.
2. Research in Vulnerabilities of HMI
   1. Pretty much tossed aside, people focus on networks [cite from garbage sources].
   2. Talk about NIST and CERT, SANS courses
   3. Talk about ASME, IEEE, standards and specifications
   4. Security through obscurity. Show CVEs, show ICS-CERT alerts, discuss OT/IT. Discuss the scope of problems and what can be reasonable assured with not just updates, but action.
3. Project Purpose
   1. Look at the current SCADA scale and see vulnerabilities that affect it and the systems with it.
   2. Won’t be looking into password/auth hacks. Assume control of external operator laptop with hacked credentials and access.
   3. We should secure in what happens to changes in the data to ensure integrity, not only its transportation and rulesets.

Problem Approach

1. Identify XML, JSON, Excel, Word, possible attacks. Give example of Angular interface in Siemens application. Source siemens slides. (qt and angular qualification needed)
2. Use conpot with an HMI (either built-in or maybe find one). Give example of multiple attacks browser-based with OWASP (must give qualifications like siemens shows windows 10 with wincc, so this is reasonable)
3. If possible, try to do XSS, remove SVG by tree transversal or other attack.
4. Show splunk monitoring, snort monitoring. Compare with monitoring of packaged systems. Maybe Wireshark.

Conclusion

* Focusing on networks, improper organizational reporting and security through obscurity, and dealing with the symptoms is bad.
* Realistically adding more monitoring functions including SNORT and Splunk-like stuff is good.
* Check for external, unknown Javascript, check for symbols that aren’t supposed to be in XSS. SCADA-antivirus needs to check not only for signatures but also polymorphic viruses.
* A web attack is faster and easier to deploy but also detect. If caught, might signal a bigger issue.