Averting Espionage in Distributed Control System Environments through Partial Data Disclosure

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

Technology Discussion

Project description should include: **“…of its scientific objectives, of the methodology that will be used, and of the significance and originality of this research project within the applicants’ field.”**

1. Description of field
   1. Overall systems look
   2. The age of cloud and data
   3. Data protection
2. Frameworks and questions to ask
   1. Many standards: IEEE, IEC, NIST; primary framework: OPC, PLC, TCP
   2. Main question: How to distribute/obfuscate/guard detailed data to protect against intellectual theft/espionage?
      1. Who wants access to the data?
      2. How does data security function in frameworks right now?
      3. What requirements are needed to preserve data security?
   3. Cloud aspect of DCS
      1. How does it work now?
      2. What does it offer in terms of data security?
      3. Is encryption enough?
3. Objective: Research ways of preserving data security in DCS to disclose data within requirements
   1. Possible routes
      1. Differential Privacy
      2. Disclosure of only relevant indexes of data required
      3. Cloud security

Problem Approach

What do business need to do to create detailed data privacy within compatible standards?

How do we protect the detailed data against intellectual theft/espionage?

Can we create a framework to protect data while meeting compatible standards?

If not what changes need to be implemented to current standards to protect detailed data?

* Logically centered control authority in networks control the control plane. When a switch or device wants information they ask the controller.
* SCADA operates the reverse way (assumpiton) where the decision was made at the forward data plane and now we tell the data historian.
* Need to protect data plane at both device level and historian level