

Agenda for “The Gathering”

Note: This agenda is not set in stone. These are the high points we want to make.

This is an open conference including an exchange of ideas. We'll also have a show-and-tell hacking session. After the introductory remarks we'll have both going in parallel. This is an outline of what we'll discuss.

I encourage people to develop policies and standard ethical positions for dealing with the problems we find. I do not expect us all to agree on this, but at least we can know what the views and positions are. We may discuss some of the aspects of these ethics here. It demands a circumspect and a dispassionate view of something that we are all passionate about.

Below is a proposed agenda for what we'll discuss and how we'll proceed on it. This is a brainstorming session. It is a social event as well. We mean for this to be the face to face equivalent of SCADASEC. While we're at it, I hope we can do some real discovery too.

1. Introduction
 1. What we're about
 1. Offline version of SCADASEC
 2. Show and Tell
 3. Socializing (may avoid friction)
 2. Do we want a better name for this gathering?
 3. Any different missions?
2. Background:
 1. This is the first gathering
 1. All of us care; all of us are experts at something; please leave your titles at the door
 2. We have an idea of what we're looking for
 3. We don't know if we're doing the right things
 4. Please tell us how to make this better
 2. We all know industrial cyber security usually isn't
 3. Preventing broad hacks, mistakes, and catching problems
 1. Not just specific attack vectors, but vector classes
 2. Embedded device security/upgrading
 3. System architectures that avoid problems
 4. Developing better forensics
 5. Developing better policies and regulatory mandates
 4. Toward that end, how can we scale this up?
 1. Commercialize it without corrupting the message
 2. Operate openly without jeopardizing users
 3. There isn't enough expertise world wide to limit our audience to any specific country
3. What we're doing today
 1. Pick on a device
 1. Fuzz it
 2. Hack its network
 3. Figure out how to protect it
 4. Document risks
 2. While that's going on:

1. Conceptual discussions on
 1. Forensics
 1. Recovery after an event
 2. Where is it practical to store
 3. Where is it NOT good idea to store?
 4. What kind of format?
 2. Firewalling
 1. Protocol specific topics
 1. Modbus
 2. DNP
 3. EthernetIP
 4. Other industrial protocols
 2. Bandwidth limiting
 1. Concept: Control systems bandwidth is known and controllable
 2. What sort of IDS methods could we institute in HUMAN TIME if we slow down the data transfer in a firewall?
 3. Self Integrity Monitoring
 1. Where does it make sense
 2. Where is it a waste of time
 3. What sorts of things are worth measuring
 4. Do we have specific recommendations for the various types of telcom infrastructure?
2. Policy Discussions
 1. Types of staff
 1. Identifying Critical People (staff and contractors)
 1. Who generates and distributes the keys and passwords
 2. Who has inside knowledge
 3. What sort of checks do we keep on people like this?
 2. Identifying Technical People (staff and contractors)
 1. They use keys and passwords
 2. Know the technology
 3. Need authority to repair broken security gear
 3. Identifying Operational People
 1. Use keys and passwords
 2. Know the routines, but not always the technology
 3. Can identify when things are broken
 2. How should we determine background investigations
 1. For Staff?
 2. For Contractors?
 3. Is there a difference?
 3. What is due diligence and what is overkill?
 4. What does licensing accomplish?
 5. What kind of reporting should we ask for in critical safety processes?
 1. What about strategically necessary processes?
 2. What about environmentally ugly processes?
3. Review of discoveries with training session on the side
 1. What did they test for?
 2. What did they find?
 3. How can we classify this discovery?

4. Make a responsible report
4. Concluding thoughts
 1. How can we make this better?
 2. Can we scale this up?
 3. How should we publicize this?
 4. What impact do we think we'll have?