SCADA security lab/center

Mikael Wedlin
mwe@foi.se
National SCADA security lab/center

- Talks about a SCADA lab for a number of years
- Lots of prestudies

- SEMA/MSB has funded the planning of a National Lab for the last three years
- A longer program has started this year.

- Raising awareness / Courses
- Network of technical resources
- Lab resources that is too large for other groups/organisations.
Fun-fair of IT security

• Have been demonstrating practical IT security for the last 9 years

• A modified version focused on SCADA issues
Courses

- Normal courses in electronic security for a number of years
- A focus on practical elements
- The 2-day course is given for the fourth time now
- Lab system of steam engines and exploding factories
Lab resources

- FOI Linköping lab has started 1999.
- Main asset today is a cluster of 180 PC-nodes
- Every PC-node can emulate 200 virtual noders
- Two separate networks, one admin and one "gamenet"
Baltic cyber shield (CDX II)

• Collaboration between Sweden and Estonia
  • National Defence College, Stockholm and Cooperative Cyber Defence Centre of Excellence (CCD CoE), Tallinn

• Swedish part funded by MSB

• All technical stuff at FOI in Linköping

• Second exercise with this setup

• Held in Linköping, Stockholm and Tallinn May 10-12 2010
Blue Team Systems

Diagram showing various systems and components of the Blue Team's network infrastructure, including DMZ, Blue Team own setup, Ext.FW (Debian 5.0), HMI (Debian 5.0), In-FW HMI: DNS+DHCP (Debian 5.0), and other systems and networks.