Cyber Security Stuff n' Junk

SANS SCADA Summit 2011

Kenneth Rohde
Cyber Security Research & Development

March 1, 2011

Idaho National Laboratory

INL/CON-11-21254

We had nothing to do with the Stuxnet worm, so please don't ask.

"Idaho National Laboratory was not involved in the creation of the STUXNET worm. As a Department of Energy Laboratory, we work with Government Agencies and Industry through mutually agreed upon contractual terms and conduct programs in accordance with those terms and conditions. Industrial programs typically require Nondisclosure of propriety information and, as such, we do not divulge this information."

-- The best our HR department could come up with…

Idaho National Laboratory

Major Program Supporters

- Department of Energy
- Department of Homeland Security
- “Work for Others”

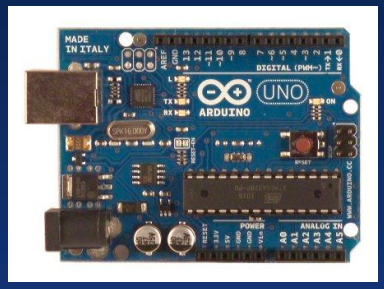
Why this panel discussion?

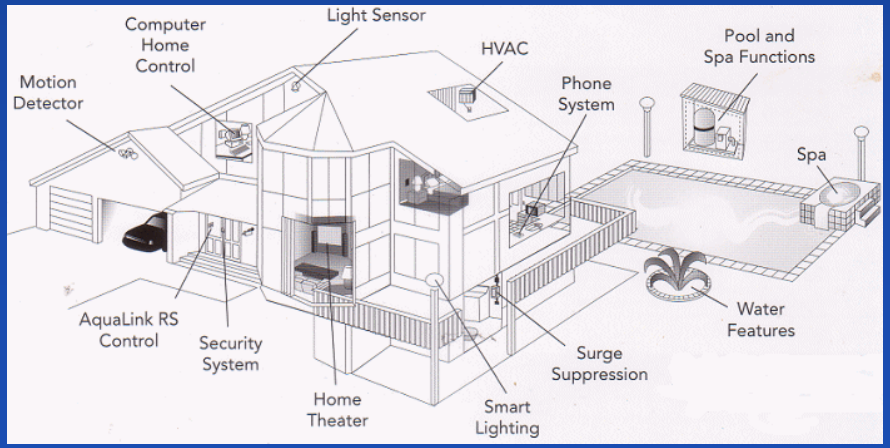
- There are only a few people in the world that can intelligently discuss “the latest trends” in exploitation
  - I’m not one of them ;-)
  - How many of you are in this audience?
- What do you want to hear?
  - Next generation of Stuxnet?
  - Doom and gloom? The sky is still falling…
- What is the true state of the industry?
  - It’s boring to hear the “same old same old,” but that is our reality
- Read the news regarding reputable companies being pwned by “old” rudimentary hacks

What *will* I talk about?

- Our (INL) latest control system hacks
  - The type of folks that work in Cyber Security
- What we are doing to make the world better
  - Industry and Government are starting to believe us

“Control Systems” We’ve Hacked





Saving the World Step #1
Tool Development

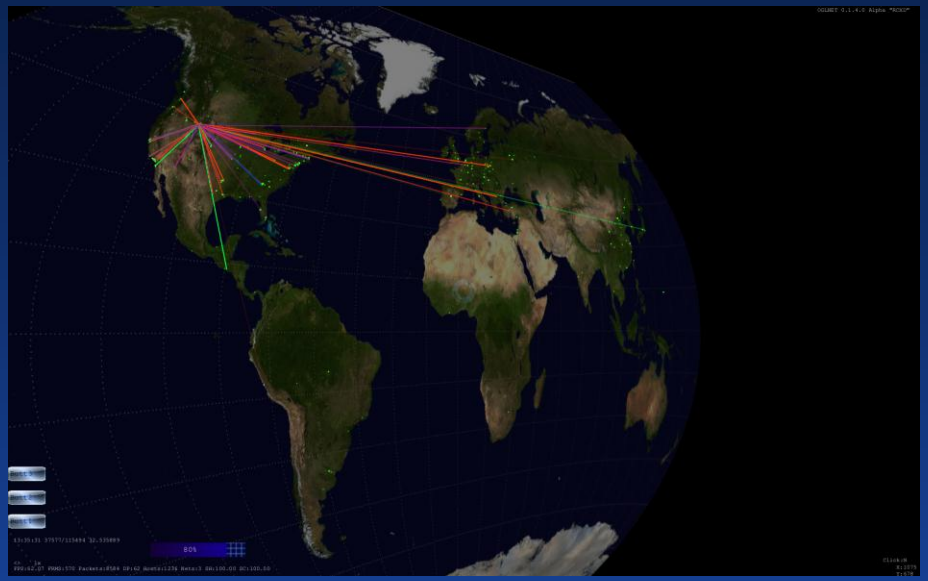
- Years of assessment work has given us insight into the needs of the community
- Traditional IT tools are often lacking the features that the ICS community might need
- Leverage our customer relationships to develop tools that work and meet their needs

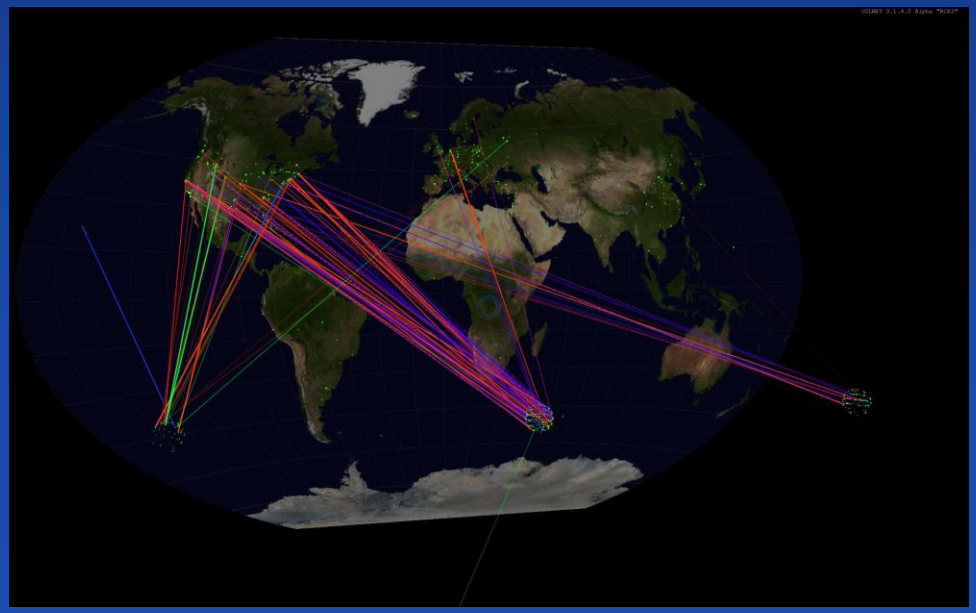
Examples:

- Sophia
- Mesh Mapper

Sophia – Greek God of Knowledge

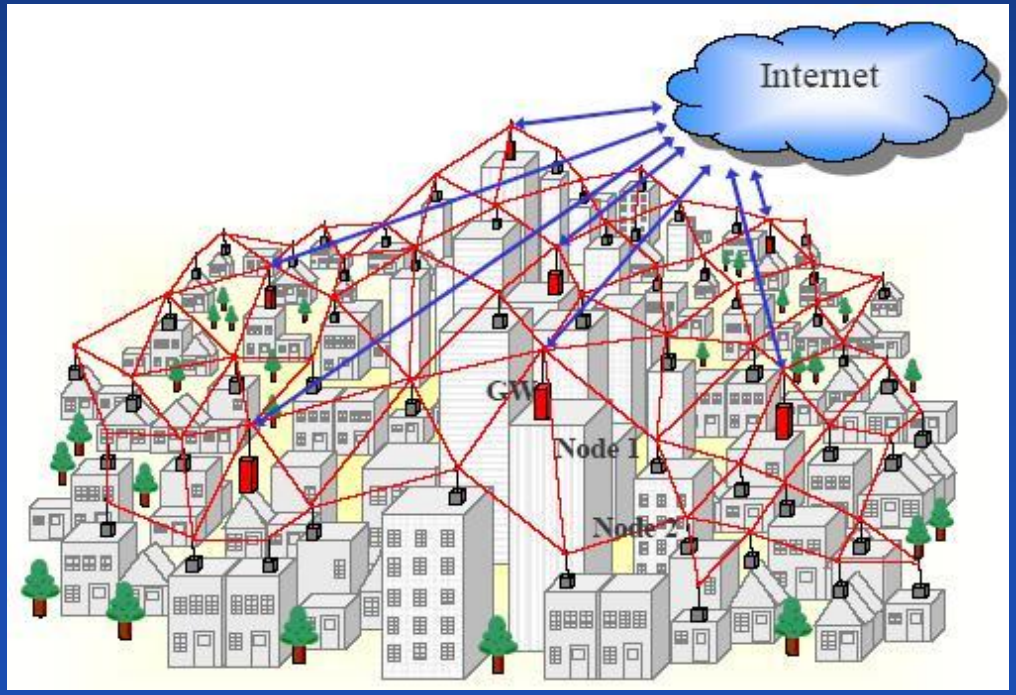
- Alpha Release Date
  - April 2011
- Beta Release Date
  - June/July 2011
- 3rd Party Licensing (TBD)





Mesh Mapper
Making Sense of the Smart Grid

- Proof of Concept
- Alpha and Beta Development (hopefully)
  - FY 2012
- Integration with Sophia
  - FY 2012



Idaho National Laboratory

Saving the World Step #2
Malware Analysis

- INL Malware lab grew exponentially to support the DHS ICS-CERT
- Developing unique skills in analysis and forensics for ICS
- Leverage community relationships to further develop capabilities
  - "Vendor of the Month Club"
    - Partnership to prepare for the next "stuxnet"
  - Automated Forensics
    - Reduce the amount of human effort required

Saving the World Step #3 Assessments

- Vendor Assessments of “Latest Configuration”
- On-site Assessments (Government and Private)
  - Working to keep current with the market
  - Continuing to develop new relationships

Saving the World Step #4 Training

- Started with training specific to DoE
  - Grew into several training scenarios specifically for DHS
- New Customers requesting training specific for their needs
  - Training can be done on-site
  - Everyone from 1337 to managers

Other Fun Stuff We Did…

DEFCON 18

AP
ACME Pharmaceuticals

opentaps

ORACLE
e-businesssuite

SAP®

INL Idaho National Laboratory

Contact Info

Kenneth Rohde

kenneth.rohde@inl.gov

Thomas Anderson

thomas.anderson@inl.gov


INL
Idaho National Laboratory