NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

SCADA Penetration Testing

Why we do things backwards…

Kenneth Rohde
Cyber Security R&D

SANS SCADA Security Summit
February 3, 2009

Program Sponsor:
Department of Energy
National SCADA Test Bed

INL/CON-09-15298

Who we are and what we're good at

- Cyber Security Research & Development Department at the Idaho National Laboratory
  - **About 16 full-time dedicated cyber personnel**
  - **Contributors to many open source projects**
  - **Full range of skills (protocol analysis, code review, reverse engineering, wireless security, firmware, zero-day exploits, IDS research, forensics)**
  - **About 5 years of experience exploiting SCADA software & hardware**
- Vulnerability Discovery and Exploitation
- System Architecture & Security Recommendations
- Vendor & Asset Owner Training

How we do it…

- Not traditional penetration testers
  - **We work closely with vendors and asset owners**
  - **Our "assessment plans" are designed from the inside out**
  - **Vulnerability discovery and exploitation is done to assess the overall potential impact to the system**
  - **The goal is to manipulate the system, not just gain access**
- We help vendors secure their products
- We help asset owners secure their deployments

Our contributions to the community

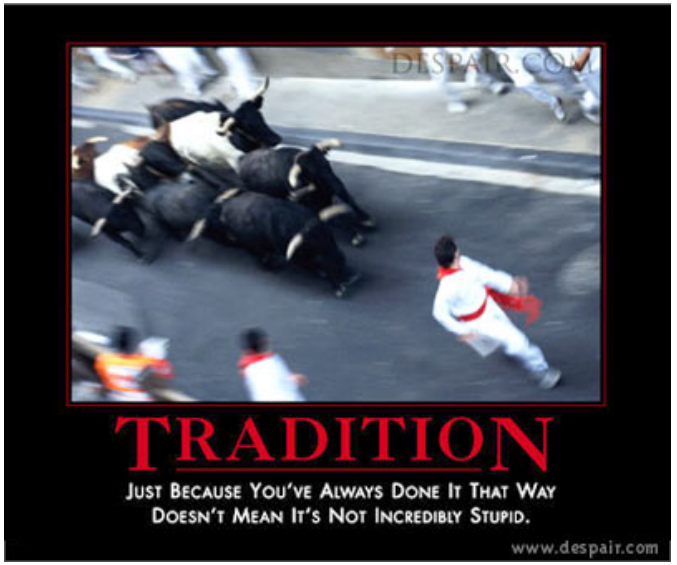
- Long-term relationships with several companies
  - **Testing cycles**
  - **Collaborative work and funding**
- Provide support at the major user-group meetings
- SCADA specific training opportunities
  - **Introductory and Intermediate classes**
  - **“Red vs. Blue” exercises**
- Custom software & tool development

What has changed and what has not

- INL is still giving “common vulnerability” presentations
- Contrast the SCADA common findings with the SANS Top 20 and Top 25
- Vendors and asset owners are getting better, but we’re now finding *different* vulnerabilities
  - **It is difficult to implement security properly**
- Wireless technology is becoming inevitable
- Chicken little is working himself out of a job

How will we continue to make a difference?

- Developing and releasing SCADA specific tools to the community
- Continuing to develop appropriate training classes
- Vendors need to continue to make security a priority
- Asset owners need to “invest” in the security economy



Conclusion

- Cyber Security R&D is only a small part of what the INL does for the critical infrastructure
- Everyone is making good progress, but we're not there yet
- Can't we just all get along?
- Join us in class tomorrow!