Advanced Network Toolkit for Assessments and Remote Mapping

SANS SCADA Summit 2009
Orlando, Florida

Bryan T. Richardson
Senior Member of Technical Staff
Sandia National Laboratories

February 2nd, 2009

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

What is it?

- The result of many conversations about:
  - How to improve and simplify network assessments
  - Tools needed to better understand networked systems and their topology
- A reduction of ‘information process drudgery’
  - Discovery of networks
  - Discovery of hosts
  - Correlation of available information

Why is it needed?

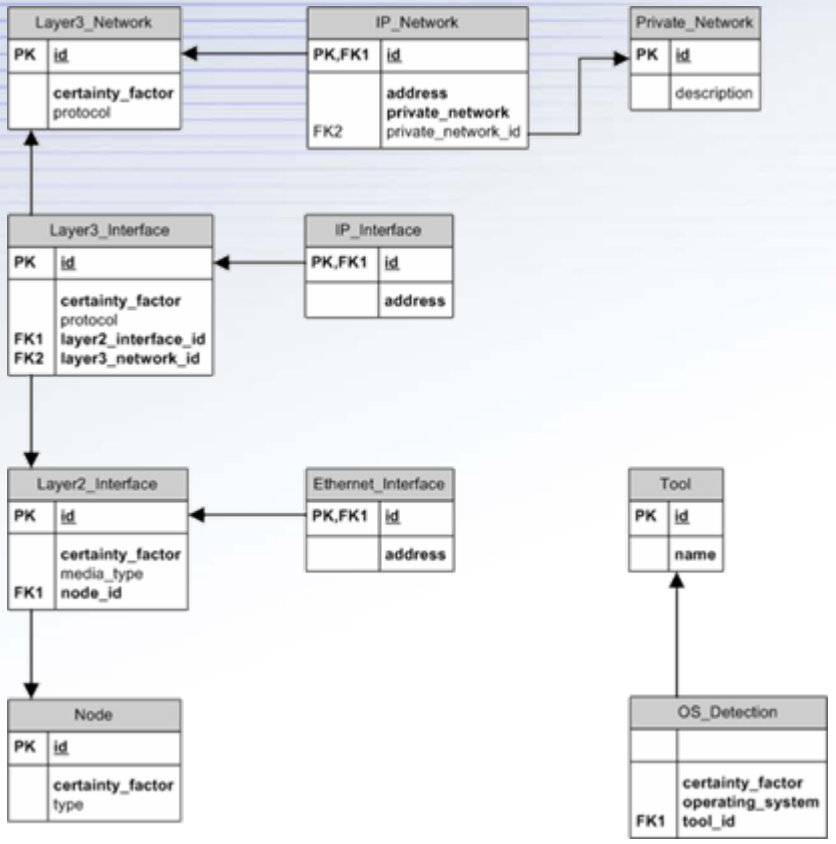
- **There exists a need for automated network discovery**
  - **Policy of documenting new additions to a network doesn't always get followed**
  - **People don't always know exactly what their network(s) look like**
- **There exists a need for the discovery to be passive or out-of-band**
  - **Control system software can sometimes be 'weak-in-the-knees' when it comes to network probing**

How does it work?

- **Existing network tools are used to gather data about networks**
  - **SNMP**
  - **Traceroute and Route Record**
  - **Tcpdump and Wireshark**
  - **Port and vulnerability scanners**
- **Existing network configuration files and logs can also be used to gather data**
  - **Router, firewall, and switch configuration files**
  - **Firewall, DHCP server, IDS, etc. log files**

So… how does it work?

- Database schema maps to OSI network layers
- Active Record is used to provide access to the database
- Unknown/inferred details are added/updated as more information becomes available
- Most information has an associated certainty factor used to resolve conflicting information



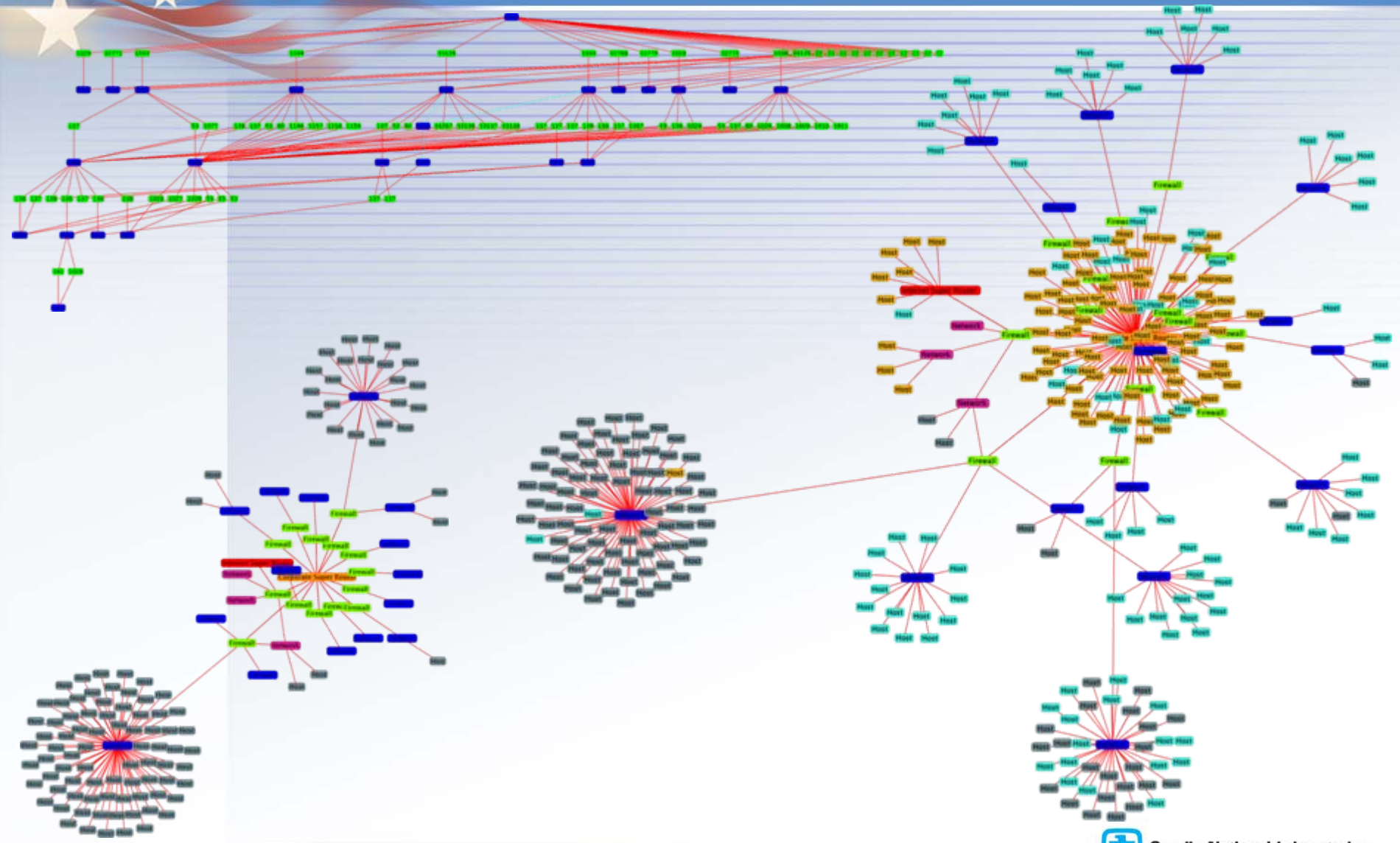
But still… HOW DOES IT WORK?!

- Custom ANTFARM scripts are written as needed to parse output data of network tools and insert it into the ANTFARM database.
  - Many scripts already exist for Cisco equipment configuration files, traffic sniffs, traceroute results, etc.
- Custom scripts are written as needed to parse and display data from the ANTFARM database using visualization tools.
  - Scripts currently exist for Graphviz (DOT language) and Prefuse (GraphML, an extension of XML).
- ANTFARM essentially provides the framework for writing input and output scripts (plugins) and accessing the internal ANTFARM database

What does it provide?

- **Network tools – provide data for further analysis and records of what was done**
- **ANTFARM input – provides a database with network information describing relationships**
- **ANTFARM output – provides visualization of the network relationships for further examination**

Show me results!!!



Sandia National Laboratories

Status?

- Antfarm is now open source software
  - http://antfarm.rubyforge.org
- Scripts development continues as needed by projects
- Documentation exists, but continues to be improved upon
- Users guide exists, but continues to be improved upon
  - http://wikibooks.org/wiki/ANTFARM
- Updates to the core continue as needed