A Universal Instrumentation for the Network

L. Todd Heberlein
Net Squared, Inc.
lth@NetSQ.com

Design a universal instrumentation architecture that can effectively harvest the necessary information to perform a reasonably accurate security assessment and can make a "Saltzer Schroeder class" network infrastructure a reality.

Motivating Anecdotes

- Suspicious outbound traffic
- Transferring files to a Mac
- File sharing for joint proposal
- Conclusion: Security is too hard

Security Audit / Assessment

- TrendCenter and Environment Aware
- Client information is critical
- Dynamic connection information is critical
- Understanding all control surfaces is critical
- Garbage In, Garbage Out

Robust Network

- What is a robust network?
- Prof. Matt Bishop's definition of a vulnerability
- Principle of least privilege
- Principle of fail safe defaults
- Principle of psychologically acceptable

Why a Joint Agenda

- The Internet is International
- Should permeate all elements of the infrastructure
- Built-in from the beginning
- Hard problem; a universal architecture?
- Consensus is hard

Research Goals and Agenda

- Measure the "collection problem"
- Identify collection of "control surfaces"
- Develop "gap metric"
- Design universal instrumentation
  - The next, next generation of SNMP
- Eat our own dog food