



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivet^{technology}labs.iu.edu

Introduction and Welcome Advanced Network Management Lab (ANML) DDoS/Security workshop

Indianapolis, Indiana
June 2-6 2003



Who am I?

- Gregory Travis
 - Assistant Director and Manager, Network Security Initiatives, ANML
 - Came to ANML in 2001 from commercial software background (relational database and airline reservation systems)
 - ~25 years in industry (first program, 1975)
 - Network experience dates to ca. 1984 with UUCP, Berknet, and then TCP/IP



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Presenters (in order of presentations)

- Matt Davey, Chief Network Engineer, ABILENE
- Ed Balas, Network Security Lead Engineer
- David Ripley, Lead Network Security Developer
- Steven Wallace, Director, & Chief Technologist, Advanced Network Management Lab
- Grover Browning & Jon-Paul Herron, ABILENE Network Engineering



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

What is ANML?

- Advanced Network Management Lab, part of Indiana's Pervasive Computing Initiative



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Idea behind Initiative

Advance fundamental research in information technology, specifically in pervasive computing

Leverage investment in IT research for economic development: creation of new businesses, modernization of existing businesses

Build on these investments to improve employment opportunities for citizens of Indiana and thereby retain graduates of Indiana's colleges and universities



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Pervasive Computing

Involves intelligent devices (from scientific instruments to home appliances to digital libraries), interconnected and available anywhere in the world

Represents continuation of three major IT trends -- rapid improvements in size, speed and cost

- Smaller, faster, less expensive microprocessors

- Larger, faster, less expensive telecommunications networks

Results in an increasing impact of IT on education, entertainment, manufacturing, commerce, healthcare

- Enables higher levels of productivity = economic growth



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

The Advanced Network Management Lab (ANML)

- Initial funding through the Lilly Endowment
- Current funding includes Lilly, the US National Science Foundation, and the Department of Defense (\$1.7M in external funding to date)
- Comprised of five researchers, five graduate students
- Focus on applied network research
 - Technologies that have impact within a few years (at most)
 - Leverage opportunities presented through IU's leadership in high performance networking (Abilene, etc.)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML - a range of projects

- Network Security
- High performance file transfer protocols
- Network visualization
- Wireless network management and performance
- The next generation Internet Protocol: IPv6



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML - Network Security

- Abilene NOC presented with an opportunity to partner with Asta Network and Arbor Networks via Internet2
- Distributed Denial of Service (DDoS) detection equipment first installed at Indianapolis core node in 2000
- DDoS detection equipment showed *many* DDoS incidents traversing Abilene each day
- Determined that this was a potential opportunity to provide more focus on security for the research and education network space



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML - Network Security

- Drafted a proposal to establish an applied network security research project homed in ANML
- CIO Michael McRobbie established a contact with Richard Clarke (then Chair of the National Security Console in the office of the President)
- Richard Clarke convened a meeting in the Situation Room of the White House to introduce the proposal to a number of government agencies in an effort to find suitable funding
- Funding comes from Air Force in the form of a two-year contract to provide security services for Abilene



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML - Network Security

- Indiana University leveraged the security services provided to Abilene, along with the existing Policy and Security arms of the the Office of the Vice President for Information Technology, into a proposal to perform the function of the Research and Education Information Sharing and Analysis Center (REN-ISAC)
- February 21st 2003, Indiana University signed an agreement with the National Infrastructure Protection Center to provide the REN-ISAC function
- Mark Bruhn is the acting director of the REN-ISAC (www.ren-isac.edu)



ANML - Network Security

- ANML is engaged in other areas of security research as well:
 - Host Management system for *Honeypots*. Uses virtual host software (VMware) to emulate a number of Honeypots on a single physical machine. Automates the distribution of honeypot instances and the collection of activity to each honeypot
 - Development of a modified Linux root kit known as Sebek to allow honeypot researchers to monitor attacker activity even when the attacker is using encrypted transmissions. ANML works closely with the HoneyNet alliance.
 - Development of Spoofwatch, a SNORT plug-in that detects and locates sources of spoofed IP addresses



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML - Network Security

- Security at Wire Speed - ANML is working on an NSF-funded project, along with the University of Washington and Internet2, to establish best practices and technologies for securing networks
- ANML is collaborating with University of Illinois at Chicago's National Center for Database Mining on a DoD-funded project to evaluate architectures for correlating distributed security alert data



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

ANML Air Force Contract

- Advanced Networking Lab @ IU has a contract with the US Air Force to provide DDoS incident reporting and data
- Scope of DDoS view is limited to Abilene network
- Reporting is sanitized/aggregated according to UCAID and IUPO criteria



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Air Force (cont)

- Contract funds 2.5FTEs (1/2Greg, Ed, David) for two years
- Applications being developed and made available via IU's software license (open-source)
- Doing a series of workshops and “best practices” documents



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Indiana University

- Signed agreement with National Infrastructure Protection Center (NIPC) to act as a Research and Education Network Information Sharing and Analysis Center (REN-ISAC)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

REN-ISAC

- Composed of several resources, including:
 - IU Policy Office
 - IU Security Office
 - Advanced Network Management Lab (ANML)
- All organized under the office of the Vice-President for Information Technology



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

What does REN-ISAC do?

- Coordinates communications and activities related to threats against the US research and education infrastructure
- Work in progress.



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Levels of Coordination

- Policy Offices (IUPO, UCAID)
- Security Offices (IUSO)
- Network Operations (IU GNOC)
- Network Engineering (GNOC engineers)
- Third-parties
 - Commercial (Arbor, Asta, Ixia, etc.)
 - Institutional (SANS, CERT, Honeynet alliance, etc.)
- Government



pervasivet^{technology}labs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Housekeeping

- You are on your own for lunch and breaks. There is a food-court as well as several restaurants within the building. You may want to travel outside for lunch as well, many good restaurants w/in 10 minute drive -- ask us!
- Please do not take any snacks from tables outside the room - those are reserved for other conferences!