



Security at Line Speed: Workshop and Next Steps

2003 Dec

CANARIE, GEANT, Internet2 meeting

Overview



- Context, Background 5 min
- Security at Line Speed Workshop 5 min
- SALSA 5 min
- Conclusion & Questions

total time ~15 mins

Background



- The Educause/Internet2 Security Task Force
 - Primary focus to date has been on user education, management awareness building, policy development
 - Effective practices (Policy, Technical); Advanced technical issues
- REN-ISAC (information security and analysis center)
 - Provides information to DHS and to ISAC's in other sectors; Helps protect Abilene and other research backbones
 - Located at Indiana University, near to Abilene NOC and CS Security Research Institute

Security Relationships



- R&E relationships with the corporate sector
 - R&E members consume security products and produce new security ideas
 - Research/commodity security requirements exist in a number of corporate sectors such as medical, automobile, high tech, etc.
 - The creation of new technologies creates new marketplaces
- R&E relationship with government sector
 - Higher ed campuses hold many of the scientists doing agency research and needing access to agency facilities
 - Public sector policies on security and privacy apply to both

S@LS Workshop 2003



- NSF Sponsored workshop, in conjunction with Indiana University, Internet2, the Massachusetts Institute of Technology and the University of Washington.
- 1.5 day Workshop
- Held in Chicago, Illinois
- 12-13 Aug 2003



“Line Speed” means...

- Requires supporting those activities that our membership are building, inventing and creating
 - High bandwidth (bulk data streams)
 - Exceptionally low latency (remote instrument control)
 - End-to-end clarity (grids)
 - Exceptional low jitter (real time, interactive HDTV)
 - Advanced features (multicast, IPv6)
- Security and High Performance simultaneously
 - Difficulty in realizing end-end high bandwidth connections, deploying and using videoconferencing, deploying grids
 - Limited remote instrument control use
 - Lack of scalable approaches
 - Inability to identify what's broken or incompatible

Workshop Goals



- Effective practices whitepaper- technology oriented, architectural principles and specific recommendations
- Research agenda suggestions- to NSF and any other agencies that might be interested
- Recommendations for mechanisms for maintenance of the above

Workshop Report



Next Slides Cover:

- Current State of Security
- Trends
- Tradeoffs
- SALSA

Table of Contents

- Tradeoffs, Trends, General findings
- Tool matrix
- Architectural frameworks, Local factors
- Case studies
 - Background information; Alternative approaches, pros/cons; Applied research and research computing
- Non-technical issues
- SALSA

Current State of Security

- First, and foremost, this is getting a lot harder
- 2003 seems to mark a couple of turning points
 - New levels of stresses; Necessary but doomed approaches
- High performance security is approached by a set of specific tools that are assembled by applying general architectural principles to local conditions.
- The concept of the network perimeter is changing; desktop software limits security and performance options
- There are interactions with the emerging middleware layer that should be explored
- Tool integration is an overarching problem

Trends



- We are entering diagnostic hell
- More aggressive and frequent attacks result in more isolation
 - Desktop lockdowns and scanning
 - New limits at the perimeter
 - Increased tunneling and VPN's
- Changes in technology
 - Rise of encryption
 - New attack vectors, such as P2P
 - Higher speeds make for more expensive middleboxen
 - Convergence of technology forces
- New policy drivers
 - DHS, RIAA, etc.
 - LCD solutions to hold down costs

Tradeoffs



- Host vs. Border security
- Deny/Allow vs. Allow/Deny
- Unauthenticated vs. Authenticated network access
- Central vs. End-user management
- Server-centric vs. Client-centric
- False positives vs. Zero-day attacks
- Organizational priorities between security and performance

- Technical steering committee composed of senior campus security architects
- Membership includes:
 - Terry Gray (Washington), Jeff Schiller (MIT), Jim Pepin (USC), Steve Wallace (Indiana), Mark Poepping (CMU), Doug Pearson (Indiana) and others
- Starting down a path of prioritizing opportunities and identifying resources
- Likely working groups in net authn/z, advanced security architectures, etc.

Possible Work Areas

- Building on the Security at Line Speed workshop, including more case studies
- Working with the REN-ISAC on both development and deployment of collaborative security measures
- Engaging with network security researchers facilities and services available from the Abilene Observatory
- Initiating organized activities to develop network authentication and authorization architectures and sample implementations, including TERENA TF
- Working with corporate partners in network security on test bed and pilot opportunities
- Involvement with diagnostic developments

From where could we deliver?

- Integration with middleware
 - user AND device authentication/authorization
- Diagnostics
 - Middleware Diagnostics, E2Epi
 - Network security compounds the process
- Vendor interactions and effective practices
 - Educause, STF Corporate Forum, working with Router Vendors

Questions



Contact Information:

T. Charles Yun

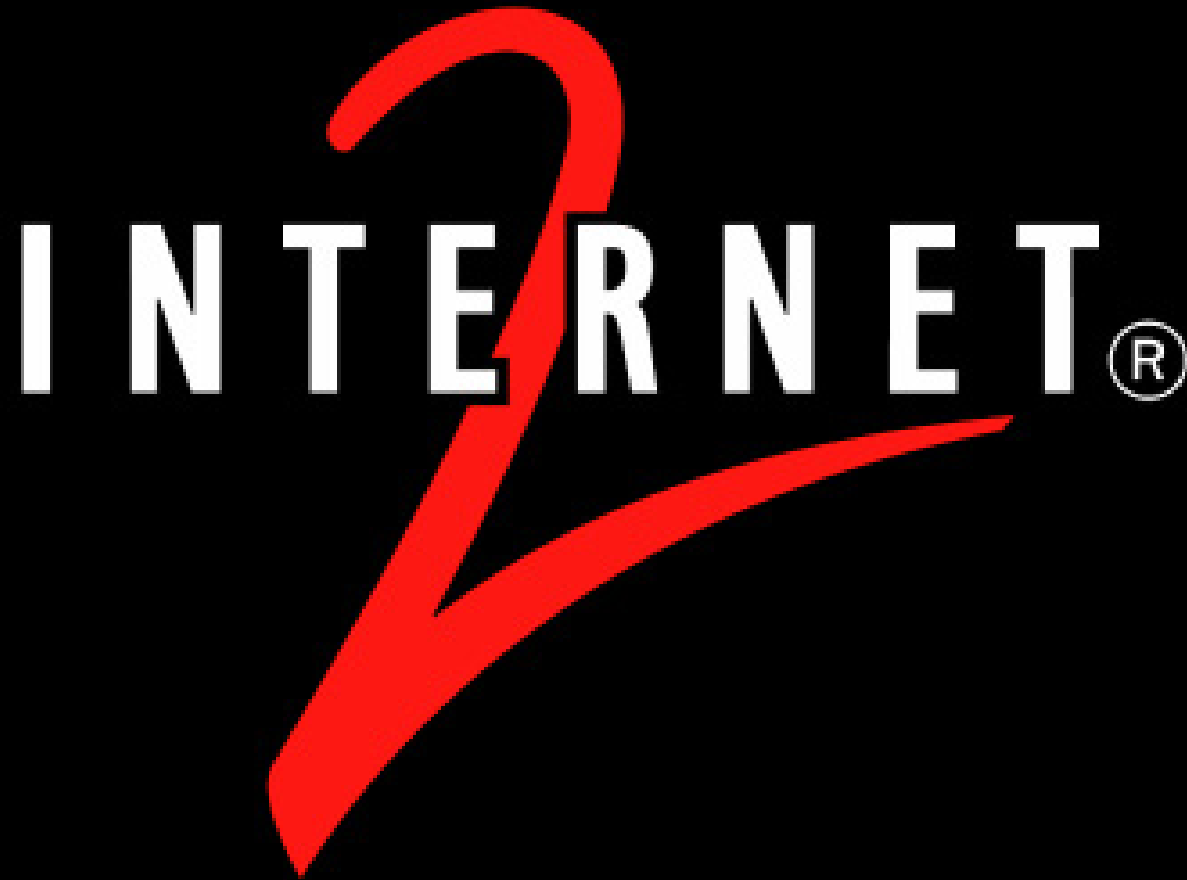
3025 Boardwalk #100

Ann Arbor, Michigan 48108

734.352.4960

tcyun @ internet2.edu

<http://www.internet2.edu/>



www.internet2.edu

Security defined...



- Information leakage:
 - Access to data by unauthorized parties
- Integrity violation:
 - Destruction, modification, or falsification of data
- Illegitimate use:
 - Access to resources (processing cycles, storage or network) by unauthorized users
- Denial of Service:
 - Preventing legitimate users from accessing resources

NSF Cyber Trust



- Cyber Trust promotes a vision of a society in which systems are:
 - more predictable, more accountable, and less vulnerable to attack and abuse;
 - developed, configured, operated and evaluated by a well-trained and diverse workforce; and
 - used by a public educated in their secure and ethical operation.
- http://www.nsf.gov/pubsys/ods/getpub.cfm?ods_key=nsf04524

Environmental Scans

- Cyberdiversity of machines and instruments on net
- Mobility requirements of machines
- Mobility requirements of users
- Highly distributed network management
- Distinctive privacy and security needs as public and academic institutions
- Inter-institutional collaborations predominate and create exceptional wide-area needs
- Widespread needs and limited resources preclude expensive point solutions

