Security at Line Speed: Workshop and Next Steps

Agenda

- Quick Contexts
  - The Educause/Internet2 Security Task Force
  - REN-ISAC
  - Relationship to private/public sectors
- The NSF-funded Security at Line Speed Workshop
  - Background
  - Findings
- Next steps
  - SALSA
    - S@LS follow-ups
    - Network authentication and authorization
    - Diagnostics
  - Effective practices and vendor interactions

Internet2/EDUCAUSE Security Task Force

- Partnership of EDUCAUSE and Internet2
- Primary focus to date has been on user education, management awareness building, policy development
- New foci of
  - Effective practices
    - Policy
    - Technical
  - Advanced technical issues

REN-ISAC

- DHS-designated Cybersecurity ISAC (information security and analysis center) for research and higher ed sector
- Located at Indiana University in close proximity to Abilene NOC and CS Security Research Institutes
- Provides information to DHS and to ISAC's in other sectors
- Helps protect Abilene and other research backbones
- May facilitate operational security interactions among higher ed and research enterprises
- Project needing stable funding and business plan

Higher Ed/Government/Corporate Security Relationships

- R&E relationships with the corporate sector
  - R&E members consume security products
  - R&E community produces 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

Project 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

- Contexts
  - the intersection of security and performance
  - environmental scan
  - tradeoffs
  - trends
- Findings
  - General
  - Technical tools, architectures and local factoring
  - Case studies
  - Policy requirements
  - Research agenda

By “Line Speed”, we really mean…

- High bandwidth
- Exceptional low latency, e.g. remote instrument control
- End-to-end clarity, e.g. Grids
- Exceptional low jitter, e.g. real time interactive HDTV
- Advanced features, e.g. multicast

Security topics

- 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

Security X High Performance

- Difficulty in realizing performance in end-end high bandwidth connections
- Difficulty in deploying and using videoconferencing
- Difficulty in deploying grids
- Limited remote instrument control use
- Lack of scalable approaches
- Inability to identify what's broken
- Things not broken but just incompatible

Environmental Scan: Requirements of R&E

- 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

Tradeoffs

- Host versus border security
- Deny/Allow versus Allow/deny approaches
- Unauthenticated versus authenticated network access
- Central versus end-user management
- Server-centric versus client-centric
- False positives versus zero-day attacks
- Organizational priorities between security and performance

Trends

- More aggressive and frequent attacks, resulting in
  - Desktop lockdowns and scanning
  - New limits at the perimeter
  - Increased tunneling and VPN's
  - More isolation approaches
- Changes in technology
  - Rise of encyption
  - 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

General Findings

- 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
- We are entering diagnostic hell

The Tool Matrix

- For a variety of network and host based security tools,
  - Role in prevention/detection/reaction/analysis
  - Description
  - General issues
  - Performance implications
  - Operational Impacts
- Network Tools include host scanning, link registration, VLAN, Encrypted VPN's, Layer 3 VPN's, Stateless Firewalls, Source Address Verification, Port Mirroring, etc…
- Host Tools include host-based encryption, host-based intrusion detection/prevention, secure OS, automated patching systems, etc.

The Architectural Frameworks

- The virtual perimeter: a mix of perimeter defenses, careful subnetting, and desktop firewalls
- Open and closed networks
- Separation of internal and external servers (e.g. SMTP servers, routers, etc…)
- Managed and unmanaged desktops
- Client versus client/server desktop orientation
- Types of authenticated network access control

Local Factors

- Size of class B address space
- Local fiber plant
- Medical school
- Geographic distribution of departments on campuses
- Distance to gigapops
- Policy Authority of Central IT
- Desktop diversity
- …

Case Studies/Examples

- Generic Academic Case
- Novel Academic Alternative
- LBL and Bro
- Lightly Authenticated Wireless Network
- Denial of Service Protection
- Network Auditing at CMU

Case Study Structure

- Background and Intro
- Alternative Approaches and Selected Implementation
- Pros and Cons
  - Specifics on attack vectors
  - Ramifications on advanced computing
  - etc

Applied Research and Research Computing

- Policy-based firewalls
- Easier connections of IDS with other enterprise services and systems
- Unlisted IP addresses – asymmetric connectivity
- Framework for the integration of tools
- Tools to automatically chart baselines and compare current behavior to
- Testbed, mirroring real networks, to permit security research

---

- Inform research computing environment developers (e.g. Grids) about the real world security issues and approaches being deployed.

Non-technical issues

- Proposals may be funded that haven't gotten agreements from campus IT on architecture
- Policies on encryption
- Policies on viewing packet contents
- Policies on permitting new applications (e.g video)
- Inconsistencies on what campuses will permit will affect inter-institutional collaborations
- Trust fabrics need to underpin security
- Pulling policies from several disparate but applicable sources is getting harder, especially for the labs
- Who pays: guilty or innocent? Masses or elite?

SALSA

- 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.

Salsa 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 testbed and pilot opportunities
- Involvement with diagnostic developments

Integration with middleware

- Network authentication and authorization
  - Of users
  - Of devices
- What is done after authentication?
  - Access
  - Scanning
  - Patching
  - Configuration of local firewalls
  - Subnetting
  - Configuration of performance parameters
- Accommodating distinctive needs of higher education
  - Network mobility
  - Role-based access

Diagnostics

- Initiated by Middleware Diagnostics initiative and e2e performance initiative
- Network security compounds the diagnostic process greatly
- Middleware security makes diagnostics harder (preserving privacy while doing diagnosis)
- December NSF workshop at SDSC on performance and diagnostics at network/middleware layers

Vendor interactions and effective practices

- Educause white paper on standards
- Nascent STF Corporate forum
  - –What to turn on, what to turn off
  - –Better input into the functional requirements processes
  - –Heterogenity
- Working with router vendors on
  - –Federated network management
  - –Security at Line Speed issues
    - Performance
    - Port management