Research and Educational Networking Information Analysis and Sharing Center (REN-ISAC)

Doug Pearson
Director, REN-ISAC
ren-isac@iu.edu

Copyright Trustees of Indiana University 2003. Permission is granted for this material to be shared for non-commercial educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of Indiana University. To disseminate otherwise or to republish requires written permission from Indiana University (via email to ren-isac@iu.edu)
REN-ISAC
Background

Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC:

• is an integral part of higher education’s strategy to improve network security by providing timely warning and response to cyber threat and vulnerabilities, improving awareness, and improving communications,

• supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure, and

• receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education.
REN-ISAC
Background

- REN-ISAC membership, or rather, constituency, includes all of US higher education.
- Initial core membership is focused on Internet2 members. Outreach to all of US higher education will be pursued.
REN-ISAC
Background

Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC:

- is an integral part of higher education’s strategy to improve network security by providing timely warning and response to cyber threat and vulnerabilities, improving awareness, and improving communications.

- supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC infrastructure.

- receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education.
an integral part of higher education’s strategy…

Relationships and Outreach

• REN-ISAC has core complimentary relationships with:
  – EDUCAUSE
  – Internet2
  – EDUCAUSE and Internet2 Security Task Force
  – Indiana University (IU) Global NOC
  – IU Internet2 Abilene network engineering
  – IU Advanced Network Management Lab
  – IU Information Technology Security Office
  – US Department of Homeland Security
  – ISAC Council
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary organizations and efforts
  – IT-ISAC
  – US-CERT
  – CIFAC
  – SALSA
  – Internet2 / CANARIE / GEANT2

• Future
  – Regional ISACs (?)
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – EDUCAUSE
    • Nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. EDUCAUSE membership includes over 1,600 educational institutions and is international.
    • REN-ISAC participates in the EDUCAUSE / Internet2 Security Task Force.
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – Internet2
    • A consortium of US universities working to develop and deploy advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet. Membership includes over 200 U.S. universities working with industry and government.
    • Internet2 Abilene R&E backbone network.
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – EDUCAUSE / Internet2 Security Task Force
    • Granted by the US National Science Foundation (NSF) to identify and implement a coordinated strategy for computer and network security for higher education.
  • Strategic goals:
    – Education and Awareness
    – Standards, Policies, and Procedures
    – Security Architecture and Tools
    – Organization, Information Sharing, and Incident Response
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – Indiana University Global Network Operations Center
    • Provides network help desk and engineering support for US national and international networks, including:
      – Internet2 Abilene
      – National LambdaRail
      – TransPAC
      – STAR TAP
      – AMPATH
      – MANLAN
    • IU Global NOC engineers and REN-ISAC possess a unique operations and engineering perspective of these networks.
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – SALSA
    • S@LS Workshop (Security at Line Speed), NSF-sponsored, invitational; 30 participants US higher ed; 12-13 Aug 2003.
      – “Line Speed” focus on requirements for support of applications that require high bandwidth, low latency and jitter, end-to-end clarity, and advanced features, e.g. real-time multimedia, Grids, multicast-based applications.
      – Deliverables included: Effective practices whitepaper, research agenda suggestions, recommendations for mechanisms for maintenance of the above, SALSA
an integral part of higher education’s strategy…

**Relationships and Outreach**

- Complimentary relationships
  - SALSA, ongoing activities
    - Extend the S@LS deliverables: Case studies, cookbooks, architectural frameworks
    - Increase data collection, analysis, and sharing: Assemble knowledge, experience tools. Work with REN-ISAC to establish information sharing framework
    - Increase linkage of security researchers and Internet2 Abilene backbone activities, e.g. Abilene Observatory
    - Net AuthN/Z: Identify areas where middleware can support inter-realm security
    - Inter-realm security: Federated context for diagnosis, early warning, and response
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – Internet2 / CANARIE / GEANT2
    • Ann Arbor, Michigan; 18-19 December 2003
    • Identified areas of potential collaboration; wrt security:
      – trusted circles; registries
      – international ties, e.g. REN-ISAC to GN2
      – share information regarding tools, techniques, and approaches
      – services to enable community teams
      – sharing of threat information, i.e. early warning, and notification
      – more…
an integral part of higher education’s strategy…

Relationships and Outreach

• Complimentary relationships
  – Internet2 / CANARIE / GEANT2
    • Areas of potential collaboration continued…
      – develop an organizational structure for information sharing
      – common monitoring of international connections
      – common incident classification schemes
      – development of tools and monitoring: weather services, anomaly detection, netflow analysis
      – coordinated response and incident handling
      – understanding of respective policy and privacy considerations and requirements
REN-ISAC
Background

Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC:

• is an integral part of higher education’s strategy to improve network security by providing timely warning and response to cyber threat and vulnerabilities, improving awareness, and improving communications.

• supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC infrastructure.

• receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education.
supports efforts to protect national cyber infrastructure…

Relationships and Outreach

• Complimentary relationships
  – US Department of Homeland Security
    • Information Analysis / Infrastructure Protection Directorate
      – Among the Directorate objectives:
        » Implement the national strategy as guided by the National Strategy to Secure Cyberspace
        » Promote and support public/private partnership for information sharing and analysis – ISACs.
      – REN-ISAC is among the many ISACs encouraged through the DHS IA/IP.
supports efforts to protect national cyber infrastructure…

Relationships and Outreach

• Complimentary relationships
  – ISACs
    • Encouraged in each critical sector of national security and the economy, e.g. IT, water, agriculture, energy, transportation, finance, etc.
  – ISAC Council
    • Body of the private sector ISACs, promotes cooperation, sharing, and coordinated relation to DHS.
supports efforts to protect national cyber infrastructure…

Relationships and Outreach

• Complimentary relationships
  – US National Cyber Security Summit (NCSS)
    • First in a series of invitational meetings was held 3 December 2003. 350 people from government, industry and academia attended. The public-private collaboration is focused on developing perspectives on how the DHS National Cyber Security Division can continue to implement the President’s National Strategy to Secure Cyberspace and convert strategies into action. Task forces were established.
supports efforts to protect national cyber infrastructure…

Relationships and Outreach

• Complimentary relationships
  – US NCSS Task Forces
    • Awareness – promote a comprehensive national awareness program for business, workforce, and the general population
    • Early Warning – develop and promote effective information collection, analysis and dissemination
    • Governance – develop and promote a framework to drive implementation of effective information security programs
    • Technical Standards and Common Criteria
    • Security Across the Software Development Life Cycle – increase security by embedding it within software development, installation and patch management
supports efforts to protect national cyber infrastructure…

Relationships and Outreach

• Complimentary relationships
  – US National Cyber Security Summit
    • REN-ISAC is a member of the Early Warning Task Force
    • Task Force objectives:
      – National Early Warning Contact List; methodology and process; the top layer of a hierarchy of trusted circle contact mechanisms
      – Survey of existing automated data collection methods
      – Crisis Coordination Center
    • Deliverables due ~March 2004
REN-ISAC
Background

Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC:

• is an integral part of higher education’s strategy to improve network security by providing timely warning and response to cyber threat and vulnerabilities, improving awareness, and improving communications.

• supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC infrastructure.

• receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education.
receives, analyzes, and disseminates network security…

Information is derived from:

- Network instrumentation
  - Abilene NetFlow data
  - Abilene router ACL counters
  - Arbor PeakFlow analysis of NetFlow data
  - Abilene NOC operational monitoring systems
- Constituents – related to incidents on local networks
- Network engineers – national & int’l R&E backbones
- Daily Status calls with other ISACs, US-CERT & DHS
- Network security collaborations, e.g. closed NSP lists
- IA/IP Daily Open Source Report
- Vendors
receives, analyzes, and disseminates network security…

Abilene NetFlow Analysis

- Through partnership with Internet2 and the Indiana University (IU) Abilene NOC, the REN-ISAC has access to Abilene NetFlow data.
- In conjunction with the IU Advanced Network Management Lab the NetFlow data is analyzed to characterize general network security threat activity, and to identify specific threats.
- Custom analysis tools, and
- Arbor Networks Peakflow
receives, analyzes, and disseminates network security…

Abilene NetFlow Analysis

• Custom analysis
  – Aggregate reports
  – Detailed reports
    • Data anonymized to /21
Abilene NetFlow Analysis

• REN-ISAC & Internet2 NetFlow data policy agreement, highlights:
  – Publicly reported information is restricted to aggregate views of the network. Information that identifies specific institutions or individuals cannot be reported publicly.
  – Detailed and sensitive information must be communicated with designated representatives of the affected institutions and refer only to local activity, unless otherwise authorized.
receives, analyzes, and disseminates network security…

Abilene NetFlow Analysis

• Development in process:
  – Enhanced reporting methods to reduce processing time. Single pass run on data currently takes ~3 hrs.
  – Ad hoc queries.
  – /32 (per host) reporting on approval of an institution for “owned” data; backed by the REN-ISAC Cybersecurity Registry of authorized contacts.
receives, analyzes, and disseminates network security…

Abilene Router ACL Statistics

- Access Control List (ACL) counters on Abilene router interfaces.
- Current data views are by router and backbone aggregates.
- Soon to be deployed: per-interface views.
  – Privacy considerations?
Abilene Stats: Port 135, Current Day by Router
Arbor PeakFlow Analysis on Abilene

- Processes Abilene NetFlow data
- Intelligent identification of anomalies
- Abilene is by nature an anomalous network, e.g. bursts of high bandwidth flows.
- Need to:
  - Tune the PeakFlow system to reduce bogies.
  - Incorporate into standard watch desk procedure.
Anomaly Snapshot

<table>
<thead>
<tr>
<th>Current Totals</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ongoing</td>
<td>14</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Recent</td>
<td>2569</td>
<td>309</td>
<td>2216</td>
</tr>
<tr>
<td>Last 24 Hours</td>
<td>3346</td>
<td>171</td>
<td>2157</td>
</tr>
</tbody>
</table>

Anomaly Activity over Last 24 Hours

Top 5 Ongoing Anomalies

<table>
<thead>
<tr>
<th>ID</th>
<th>Traffic</th>
<th>Importance</th>
<th>Duration</th>
<th>Start Time</th>
<th>Direction</th>
<th>Type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>161364</td>
<td><img src="image1" alt="Traffic" /></td>
<td>High</td>
<td>28 hrs 59 mins</td>
<td>11:47, Nov 4</td>
<td>Incoming</td>
<td>Syn (Misuse)</td>
<td>6&lt;hidden&gt; world6</td>
</tr>
<tr>
<td>164263</td>
<td><img src="image2" alt="Traffic" /></td>
<td>Medium</td>
<td>3 mins</td>
<td>11:37, Nov 5</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>1&lt;hidden&gt; world4</td>
</tr>
<tr>
<td>164260</td>
<td><img src="image3" alt="Traffic" /></td>
<td>Low</td>
<td>5 mins</td>
<td>11:35, Nov 5</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>1&lt;hidden&gt; world4</td>
</tr>
<tr>
<td>164255</td>
<td><img src="image4" alt="Traffic" /></td>
<td>Low</td>
<td>2 mins</td>
<td>11:38, Nov 5</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>1&lt;hidden&gt; world4</td>
</tr>
<tr>
<td>164264</td>
<td><img src="image5" alt="Traffic" /></td>
<td>Low</td>
<td>2 mins</td>
<td>11:36, Nov 5</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>1&lt;hidden&gt; world2</td>
</tr>
</tbody>
</table>
REN-ISAC
Background

Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC:

• is an integral part of higher education’s strategy to improve network security by providing timely warning and response to cyber threat and vulnerabilities, improving awareness, and improving communications.

• supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC infrastructure.

• receives, analyzes, and disseminates network security operational, threat, warning, and attack information within higher education.
provide timely warning and response to cyber threat…

Warning and Response

• REN-ISAC Watch Desk
  – 24 x 7
  – Co-located and staffed with the Abilene NOC
  – +1 (317) 278-6630
  – ren-isac@iu.edu

• Public reports to US higher education community regarding analysis of aggregate views.

• Private reports to specific institutions regarding active threat. Reports contain only “owned” information.
provide timely warning and response to cyber threat…

Example: Response to Blaster/Nachi

• Disseminated reports\(^1\) regarding the nature of the worm threats along with successful defense measures.

• Disseminated reports\(^1\) regarding ongoing aggregate infection rates.

• Sent reports directly to many institutions regarding their specific infection rates, and counts per subnet (/21).

• Reports resulted in measurable reductions in infection rates.

\(^1\) Reports were sent to EDUCAUSE Security, Internet2 Security Working Group, and Abilene Operators listservs
Response to Blaster

initial warning to community

… a worm exploit of the Microsoft DCOM RPC vulnerability, W32/Blaster, was unleashed …

Worm traffic on Abilene is high, peaking at 7% of all packets on the network.

Recommendations for network border filtering … Filters should be defined as input and output …

References …
Response to Blaster notifications to Top 20

Your network AS has been identified among the top twenty sources of port 135 scans on the Abilene network.

Worm propagation can be mitigated by the installation of filters at network borders. Recommendations …
Response to Blaster notifications to Top 20

... your network AS was among the top twenty sources of port 135 scans ...

Worm propagation can be mitigated by ...

A breakdown of port 135 scans sourced from your AS, to Abilene, is provided ...

<SAMPLE FOR ILLUSTRATION>

Format: AS, total count from AS /21, and count from /21

<table>
<thead>
<tr>
<th>AS</th>
<th>211449</th>
<th>192.168.0.0</th>
<th>25317</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.16.0</td>
<td>23456</td>
</tr>
</tbody>
</table>

A breakdown of port 135 scans sourced from your AS, to Abilene, is provided ...

<table>
<thead>
<tr>
<th>AS</th>
<th>211449</th>
<th>192.168.112.0</th>
<th>13093</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.128.0</td>
<td>12943</td>
</tr>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.144.0</td>
<td>10987</td>
</tr>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.160.0</td>
<td>9840</td>
</tr>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.176.0</td>
<td>5432</td>
</tr>
<tr>
<td>AS</td>
<td>211449</td>
<td>192.168.192.0</td>
<td>4076</td>
</tr>
</tbody>
</table>
Response to Blaster
status regarding windowsupdate.com

... conferred with lead technical representatives of Microsoft regarding the anticipated, Saturday August 16, DDoS attack against windowsupdate.com, coming from W32/Blaster.

Based on current understanding of the worm, Microsoft has a sound and effective approach to mitigate the attack.
Response to Blaster

status reports to community

… continuing to perform analysis…
Identify top network AS sources of port 135 scans on Abilene… E-mail notifications…

… infection attempts on Abilene, while still high, are down by at least half. A graph, produced …

Worm propagation can be mitigated by …
provide timely warning and response to cyber threat...

Response to Blaster and Nachi

http://www.ren-isac.net/library.html
REN-ISAC Cybersecurity Registry

- Early warning and response to threat requires the communication of timely and sensitive information. The proper contact is one who can act immediately, with knowledge and authority upon conveyed information, and who is cleared to handle potentially sensitive information.

- Publicly published contact points rarely serve those requirements. Privacy considerations prevent deep and rich contact information from being publicly published.
REN-ISAC Cybersecurity Registry

• To provide contact information for cyber security matters in US higher education, the REN-ISAC is developing a cyber security registry. The goal is to have deep and rich contact information for all US colleges and universities.

• The primary registrant is the CIO, IT Security Officer, organizational equivalent, or superior.

• All registrations will be vetted for authenticity.

• Primary registrant assigns delegates. Delegates can be functional accounts.
provide timely warning and response to cyber threat…

REN-ISAC Cybersecurity Registry

• Aiming for 24 x 7 contact, with deep reach – a decision maker, primary actor, with clearance for sensitive information.

• Optional permissions for REN-ISAC to send reports regarding threat activity seen sourced from or directed at the institution – reports may identify specific machines.

• Related Registry information to serve network security management and response:
  – address blocks
  – routing registry
  – network connections (e.g. Abilene, NLR)
Summary of Activities

• Within US higher education, provide warning and response to cyber threat and vulnerabilities; improve awareness, information sharing, and communications.

• Support efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure.

• Receive, analyze, and disseminate network security operational, threat, warning, and attack information.

• REN-ISAC Cybersecurity Registry

• Operational 24 x 7 watch desk

• Daily information sharing with ISACs, US-CERT, DHS and others

• Cultivate relationships and outreach to complimentary organizations and efforts
Links

- REN-ISAC
  - [http://www.ren-isac.net](http://www.ren-isac.net)
- Internet2
  - [http://www.internet2.edu](http://www.internet2.edu)
- EDUCAUSE
  - [http://www.educause.edu](http://www.educause.edu)
- EDUCAUSE and Internet2 Security Task Force
  - [http://www.educause.edu/security/](http://www.educause.edu/security/)
- Indiana University Global NOC
  - [http://globalnoc.iu.edu](http://globalnoc.iu.edu)
- IU Internet2 Abilene network engineering
  - [http://globalnoc.iu.edu](http://globalnoc.iu.edu)
Links

• SALSA:
  – http://www.internet2.edu/security
• IAIP Daily Open Source Report
  • http://www.nipc.gov/dailyreports/dailyindex.htm
• IU Advanced Network Management Lab
• IU Information Technology Security Office
• IT-ISAC
• US-CERT