Internet2 Security Initiatives

DICE Meeting

Joe St Sauver, Ph.D.
(joe@internet2.edu or joe@uoregon.edu)
Manager, Internet2 Security Programs
Internet2 and the University of Oregon
http://www.uoregon.edu/~joe/dice/

Disclaimer: The opinions expressed in this document are strictly those of the author, and should not necessarily be taken as expressing the opinion of any organization. These slides are provided in detailed format for those who may not be present at this meeting, for ease of indexing, and to insure accessibility for the hearing impaired.

My Regrets...

- I'm very sorry that that I couldn't be with you all at this DICE Meeting in person, but at the time I learned of this meeting I'd already agreed to participate as an invited panelist at the Federal Trade Commission Spam Summit, a meeting which is being held on the 11th and 12th in Washington DC.
- Hopefully these detailed slides may nonetheless be of some interest or help to you when it comes to learning about the security-related initiatives Internet2 is currently pursuing.
- If you have any questions about any of the areas covered in these slides, or any other security-related area, please feel free to contact me by email or by phone

Security and Internet2

- Internet2 is both a physical network, and a community comprised of many participants, including
  -- leading American research and education institutions,
  -- federal and international partners,
  -- gigapops and regional optical networks,
  -- statewide K20 networks connecting as sponsored educational group participants,
  -- commercial partners,
  -- health care providers,
  -- sponsored participants, etc., etc., etc.
- Many, heck, ***ALL*** of those entities are very security conscious, and Internet2 itself most definitely recognizes and embraces the importance of computer and network security as well. A tangible expression of that is I2's Middleware and Security-related efforts.

Ugly Reality of Security's Importance

- Sometimes folks wonder, "Why DO all those entities care about security? Isn't security just one obscure area out of hundreds that each organization needs to consider, prioritize and manage?" Yes, yes it is.
- However, perhaps more than any other area, security is what I call a "third rail" issue. I call security a third rail issue because if it is neglected or improperly handled, security-related issues can reach out and "kill you" -- or your school.
- IT is so mission critical, and trusted with such a wide range of personal and important data, and given so many resources (comparatively!), and yet is so often incompletely understood. Take that service, and paint a bulls eye on it, because it is the target for a huge number of attacks...
- Wise IT leaders do **everything** they can to insure that IT security issues are being handled with the utmost priority.

A Collaborative Framework

- Our framework for security-related work is a collaborative one. A prime example of this is the Joint Educause/Internet2 Computer and Network Security Task Force (see http://www.educause.edu/security), with many participants from Internet2-affiliated sites.
- The Joint Security Task Executive Committee includes Internet2 staff participation and representation via:
  -- Gary Bachula, VP for External Relations, I2
  -- Ken Klingenstein, Director, I2 Middleware and Security
  -- Mike Roberts, Consultant, I2
- The Joint Security Task Force Leadership Team also has Internet2 participation, including:
  -- Chris Misra, I2 Salsa-NetAuth WG Co-Chair
  -- Mark Poepping, I2 Salsa Chair, and
  -- myself, as I2 Security Programs staff liason and former co-chair, Educause Security Effective Practices WG.

Another Security Collaboration Success Story: REN-ISAC

- Another security collaboration success story can be seen in the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) at Indiana University, see: http://www.ren-isac.net/
- Many of you have met and know Mark Bruhn, Doug Pearson and Dave Monnier, and they've been doing a great job when it comes to:
  -- creating a trusted community where information about security-related incidents can be shared with confidence,
  -- working security-related incidents, particularly those which originate in or directly affect Internet2-connected sites, and
  -- collecting and sharing in a timely manner information about emerging threats and trends.
- Thank you for all your hard work on behalf of the community!

Some Security-Related Activities Are Directly Homed At Internet2 Itself...

- **Internet2 SALSA:** The Internet2 SALSA effort was originally created as a community advisory group to insure that while striving to create a secure system and network environment, sites didn't deploy architectures which might interfere with network experimentation and the deployment of advanced applications, nor with the desire and need of network users to move bulk data at high bandwidth – we needed Security At Line Speed.
- I'm happy to say that SALSA has been uniquely successful to-date in encouraging sites to deploy their networks in way which promote security, yet which do not break Internet transparency or the end-to-end principle (for example, rather than deploying a stateful border firewall, a site might deploy a passive intrusion detection system, instead).

Additional I2-Homed Security Efforts

- There are also some groups which dig down and focus on particular subareas of interest to the community. Three examples of these include:

  -- **Salsa-DR:** This project focuses on the challenges and opportunities associated with insuring sites are prepared to handle disaster recovery and business continuity challenges

  -- **Salsa-Netauth/Salsa-FWNA:** This effort focuses on federated network authentication, including federated wireless network authentication, and

  -- **Computer Security Incidents-Internet2 (CSI2):** The CSI2 Working Group has been hard at work developing a secure structured framework for sharing computer and network security incident data, as well as a variety of other projects.

Some Security Areas Which I've Emphasized at Internet2 Meetings

- I'd like to also take a minute or two to highlight a few security-related areas which I've attempted to emphasize via my own presentations at I2 Member Meetings or I2/ ESNet Joint Techs, including why these areas are important
- Hearing that, I'm sure you're thinking "Oh, great! A chance for Joe to tout a bunch of his talks!" Actually, that's **not** my goal. The reason I'm going to mention some of my talks is so you can get some sense of what ***I*** believe important emerging priority security areas may be, **and** so you can see if any of these areas are worth discussion and attention in **YOUR** user communities.
- We'll cover these topics in alphabetical order, and with only one slide per topic, you WILL need to dig into the supplied URLs if you want any substantive level of detail.

My General Selection Criteria for Areas Meriting Priority Security Attention

- **Areas affecting or particularly relevant to backbone network operations, or campus systems and networks.**
- **Mass scale phenomena** involving millions of users (or more): spam, worms, bots/zombies, malware, etc.
- **High impact phenomena** which can really hurt: distributed denial of service attacks; attacks which employ cyber events to affect tangible facilities, such as SCADA systems which control pipelines, factories and other facilities; etc.
- **Highly publicized phenomena** – if the media broadly covers an area (such as system breaches involving personally identifiable information), it is hard for that area **not** to become a priority area.
- **Emerging threats** which **aren't** being adequately covered

The Tricky Bits

- Everyone's already really, really, really busy, and there are a tremendous number of potentially relevant security issues
- Attacking some issues is distinctly non-trivial and may involve significant pain (paid in cash or karma)
- I've got no direct authority to compel sites to do (or not do) things: I need to persuade or advise, not direct or command
- Meetings may (or may not) have the appropriate folks – security issues of concern may be **policy** level issues which need to be addressed by CIOs, **technical network** issues appropriate to network architects or senior network engineers, **technical system/server issues**, **end user issues**, you need to assume that the meeting attendees may only be conduits to the right people "back at the ranch."
- Many security issues go FAR beyond just higher ed
- You also have to avoid accidentally educating the bad guys.

A Sample Security Area: CALEA

- CALEA, the Communications Assistance for Law Enforcement Act, is designed to insure that law enforcement will be able to get the access they need to lawfully intercept communications, when circumstances require this to occur and a court order authorizes it. Originally a phone thing, because of the emergence of VoIP and increasing criminal use of the Internet, CALEA was extended to cover facilities based broadband networks. Similar lawful intercept legislation exists in many other countries, too.
- CALEA has been an interesting area for higher education networks – what's covered, and what's not? Who's responsible for complying? What about advanced services unique to higher ed? If you'd like to read more about this: **Upcoming Requirements from the US Law Enforcement Community to Technically Facilitate Network Wiretaps,** www.uoregon.edu/~joe/calea-requirements/terena.ppt

Capacity Planning and System and Network Security

- We're all moving from the old Abilene network to a new, faster, network, and at the same time, we continue to see volume-related security phenomena, including surging levels of spam, huge bot networks, unprecedented denial of service attacks, etc. It is common to hear people mention that "We're in an arms race with the miscreants."
- I think that's true, and the **real** cyber arms race is one of sheer capacity, where the ultimate outcome of that “war” will be determined by the capacity of the bad guys to source brute force attack traffic via bots, versus the capacity of the good guys, e.g. **you**, to soak up that traffic via high capacity connections and systems while continuing to do business. For more on this topic, see http://www.uoregon.edu/~joe/i2-cap-plan/internet2-capacity-planning.ppt

Disaster Recovery

- The traditional paradigm for disaster recovery, involving identification of off site space, backups to tape, shipment of replacement systems from vendors, etc., simply isn't sufficient for today's complex and critical systems and networks. Recovery time objectives measured in hours (if not minutes) and ever increasing system complexity effectively requires sites to deploy continually-synchronized redundant **hot sites** – nothing else we've yet been able to identify will keep facilities (and your organization!) functioning in the event a natural disaster (similar to Katrina) or accident (such as a facilities fire). Lambdas may help facilitate the secure interconnection of those hot sites
- For a discussion of some considerations relating to DR, see: **Disaster Recovery and Business Continuity Planning BOF: Some Introductory Comments**, www.uoregon.edu/~joe/dr-bcp-bof/disaster-recovery-bof.ppt

DNSSEC and the Security of DNS

- Although the domain name system (DNS) underlies virtually everything we do online (can you imagine having to remember and enter 72.14.253.147 instead of www.google.com?), DNS is, in fact, woefully insecure. Miscreants have a number of strategies they can use which may undermine the trustworthiness of that critical service.
- While DNSSEC doesn't fix all of the vulnerabilities associated with the domain name system, it is an important first step, cryptographically ensuring that DNSSEC-signed DNS records are authentic and "untampered-with." Unfortunately, DNSSEC roll out has been slow. If you'd like to understand more about DNSSEC, and its struggles, see: **Port 53 Wars: Security of the Domain Name System and Thinking About DNSSEC,** www.uoregon.edu/~joe/port53wars/port53wars.ppt

Distributed Denial of Service (DDoS) Attacks

- Another important security-related area is the problem of distributed denial of service (DDoS) attacks. During the Spring of 2005, I realized that at many sites, senior administrators might not be familiar with traffic flooding, or "DDoS" attacks, or their potential implications for campus operations. Because of that gap, I put together a talk entitled, Explaining Distributed Denial of Service Attacks to Campus Leaders, focusing not so much on the mechanics or the technology involved in DDoS attacks, but rather on what DDoS attacks can do and what mitigation strategies work and won't work. That talk, reportedly the highest- attended Internet2 Member Meeting netcast as of that date, is available online at http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.ppt

Mass Real Time Notification

- I've already mentioned disaster recovery, but it might be helpful to mention a specific example of how disaster recovery goes beyond just creation and connection of hot sites: mass real time notification.
- The recent tragic shooting at Virginia Tech underscored the potential importance of mass real time notification capabilities for campus communities, and generated a lot of interest among senior university administrators across the country in this area.
- We responded to that interest by providing a briefing on real time notification system options and considerations, see **Real Time Notification During a Disaster or Other Emergency**, http://www.uoregon.edu/~joe/notification/emergency-notification.ppt

Route Injection

- Just as DNS is a critical piece of our network infrastructure, we all also rely on BGP4 to handle routing of traffic on our wide area networks. Unfortunately BGP is not a very secure protocol, and it is possible for bad guys and gals to hijack network address ranges via a variety of mechanisms, including just announcing more specific advertisements, or announcing large covering routes and just using the miscellaneous crumbs of address space which aren't otherwise being normally announced.
- Because this is an area that has not received much attention, many people believe that the party responsible for traffic from a given IP address is the person listed in whois, failing to recognize that someone else very well may be using all or part of a netblock they don't own: See **Route Injection and the Backtrackability of Cyber Misbehavior,** http://www.uoregon.edu/~joe/fall2006mm/fall2006mm.ppt

SCADA

- Finally, I'd also like to mention security issues relating to SCADA ("Supervisory Control and Data Acquisition" systems). As important as it may be to keep our enterprise systems and networks secure, there's an entire additional world of industrial control system networks, responsible for making sure that energy flows to our campuses and homes, that machines and processes in factories continue to work as intended, etc. Those systems and networks are at least five to ten years behind where enterprise systems are when it comes to security, and terrorists know it. Thus, both at an Internet2/ESNet Joint Tech meeting, and in broader fora such as the FBI's Infragard program, I considered SCADA security to be an area worthy of attention. For more, see **SCADA Security and Critical Infrastructure,** http://www.uoregon.edu/~joe/scadaig/infraguard-scada.ppt

Other Outreach Activities

- Some examples of additional recent security-related talks:
  -- **The 2nd Joint London Action Plan-CNSA Workshop** ("Infected PCs Acting as Spam Zombies: We Need to Cure the Disease, Not Just Suppress the Symptoms")
  -- **The Anti-Phishing Working Group** ("We Need a Cyber CDC or Cyber World Health Organization")
  -- **The Pacific Institute for Ethics and Social Policy Conference on Technology, Intelligence, and the Preservation of Civil Liberties** ('We Regret to Inform You That "Due to Insecurities Beyond Our Control, Your Privacy Has Been Cancelled for Your Convenience"')
  -- **IT Security: A Call To Action for the Education Community, Fargo** (Security "Monsters:" Current Security Threats & What You Should Be Doing to Address Them)
  -- I also routinely present at the **Messaging Anti-Abuse Working Group**, the carrier/large ISP anti-spam forum.

Conclusion

- I'm hoping that the preceding slides have given you a little better understanding of security-related activity at Internet2, and some of the areas which I personally believe are a high priority for the days ahead.
- Because I'm unable to be here with you today, it won't be possible for me to immediately answer any questions you may have, but I'd be happy to tackle those questions by email, or feel free to contact me at (541) 346-1720 if you'd prefer to chat.
- Thank you for your time today!