Security Activities Update

Internet2/ESnet Joint Techs
College Station TX, February 4th, 2009

Joe St Sauver, Ph.D.
Manager, Internet2 Security Programs
(joe@uoregon.edu or joe@internet2.edu)

http://www.uoregon.edu/~joe/sec-update-2009/

Disclaimer: The opinions expressed in this talk do not necessarily reflect the opinion of any other party.

Goal Of This Session

- This session is meant to bring you up to speed on some of the things that have been going on in the higher ed security community, including:

  -- some Internet2-community security activities, and
  -- emerging security issues you should be tracking.

- Since this is only a twenty minute slot, you're only going to get a "20,000 foot" view, but feel free to drop me a note if you have any questions following today's talk

(1) Security and Internet2

- The Internet2 Security Program is part of the **Internet2 Middleware and Security Area**, led by Ken Klingenstein.
- Security activities within Internet2 have traditionally been guided by **SALSA**, a technically focused group currently led by Chris Misra of the University of Massachusetts.
- Over the last year or so, Internet2 has established also established senior advisory councils to help advise and shape the work of Internet2. Within Internet2, the Security Area is advised and guided by the **Applications, Middleware and Services Advisory Council (AMSAC)**, chaired by Ray Ford of the University of Montana.
- During the Fall Internet2 Member Meeting AMSAC met in public session and had a chance to consider a two page table listing twenty or so security areas which the Internet2 community could potentially work on.
- Topics on that list included (in no particular order)…

Twenty Potential Security Topics

Spam	FWNA/Netauth (Federated Wireless Net Access)
Malware	REN-ISAC Incident Handling and Trust Community
Phishing	Development and Distribution of Security Tools
DDoS	Mobile Devices
Encryption, Sniffing and Privacy	Disaster Planning and Recovery
Replacing Traditional Passwords	Convening Senior Campus Leadership & the Campus Expectations Task Force
Firewalls, Middleboxes and End-to-End Transparency	Security Technology Evangelism and Leadership
IPv6 and Security	Security Policies
Domain Names, IP Addresses, DNS and DNSSEC	Engaging Standards Bodies (IETF, etc.) Regarding Security Issues
Switching and Routing Security (including Securing BGP)	Management/Security Support for Distributed Servers

Some Notes About That "Security Areas" Document

- For each security area mentioned, we provided AMSAC with:
  -- a nutshell description of the topic
  -- an explanation of why it was a potentially worthy area
  -- a sense of "just how bad is this problem?"
  -- some key potentially relevant technologies, and
  -- some potential commercial/technical partners

  If you'd like to see the actual table, it is available on the web at http://www.uoregon.edu/~joe/security-tasks.pdf
- Please note three things about that table:

  -- That chart only included the most urgent of issues; additional important security issues also exist which probably exceed our available capacity
  -- Topics in the table are NOT listed in priority order
  -- For some security topics, Internet2 might be a supporting partner rather than the lead for that area

What Security Topics Would <u>You</u> Like to See Us Work On?

- While that table lists some potential security areas we could work on, Internet2 is and should be a **member-driven organization**, so we'd love to hear from you about the security topics you'd like to see us focus on. If you have comments or suggestions please feel free to contact me: joe@oregon.uoregon.edu or joe@internet2.edu

- Just to help get that conversation started:

  -- **Is** security an issue or concern for you and your site?
  -- Are you primarily concerned about **short term operational security threats**, or would you rather see Internet2 focused more on **intermediate (or longer term) security issues**?
  -- Internet2's portfolio obviously embraces the national **backbone**, but should it also have an **end-to-end security focus**, including regional networks, campus networks, and host and app security?

We're Also Explicitly Asking For Your Help

- Internet2 does not have a huge staff of employees working on security issues, so if we're going to make progress on some of these issues, **we need your help and involvement**
- Many times, you can help the community tremendously just by employing security best common practices on your own network (e.g., deploy BCP38 anti-spoofing filters, harden your DNS servers, monitor your own routes, etc), and by responding to any security incidents which may come to your attention.
- Ideally, however, **we'd love to see you and/or your security people go beyond that and actively help work on Internet2 security projects and areas**, perhaps volunteering to work on (or even lead!) a working group tackling one security area or another.
- Also, should we be increasing student involvement in security, perhaps offering **distributed security internships** to help get more students involved in the community's security work?

(2) DOJ Grant and Security Workshop

- You may recall that a year or two ago the community received a grant from the Department of Justice Office of Justice Programs supporting a workshop and a number of other activities (e.g., see mail.internet2.edu/wws/arc/i2-news/2007-03/msg00001.html)
- I'm pleased to be able to report that another year of funding has been received from DOJ.
- That funding will underwrite a **two day invitational security workshop** which will be held in spring or early summer, most likely in the Baltimore, Maryland area. The workshop will focus on **data driven approaches to collaborative system and network security in high performance networks**, and will bring together members of the academic security community, private sector security researchers, and government/law enforcement participants.
- If you're interested in potentially attending or presenting at this workshop, please send me email.

(3) One Example of Work Funded by the DOJ Grant: SES (Security Event Standardization)

- Work underway: REN-ISAC, Internet2 CSI2, DOJ grant
- Coordinated with similar work at Argonne National Lab for the Department of Energy.
- If you:
  - operate an IDS or firewall
  - have ACLs, or iptables
  - collect netflow or similar data
  - operate a DNS server and log requests
  - run an sshd, or
  - etcetera
- Then you have the potential to collect valuable security intelligence

SES (Security Event Standardization)

- Security event information is being shared, but most current methods are cumbersome, are not easily automated, aren't based on a standardized data representation, and are not structured for correlation and analysis.

- SES: In real-time, and in a standardized (IDMEF*) representation, **share** security event information within a trusted federation, and among federations

---

* IDMEF == Intrusion Detection Message Exchange Format, see RFC4765

SES (Security Event Standardization)

- Phase I Solution
  - Local log (IDS, firewall, sshd, DNS, darknet sensor, etc.) parsing to yield “mid-level events”.
  - Normalized data description in IDMEF
  - Transport, storage, and retrieval
  - In the context of a trusted federation
  - Pilot and production deployments (spring/summer) in REN-ISAC
  - Framework:
    - incorporation of additional correlation and analysis tools
    - Interface with systems that notify abuse contacts regarding infected systems, e.g. the REN-ISAC notification system
    - Interface with systems that treat higher-level incident information in a federated context

SES (Security Event Standardization)

- Extending the framework
  - Long term intelligence storage
  - Feed of security intelligence to other federations and mitigation communities
  - Threat analysis platform
  - The Future
    - Rapid application development
    - “Super Crunching” of data

SES (Security Event Standardization)

- If you're interested, please contact:
  - Doug Pearson
    - dodpears@ren-isac.net
  - Wes Young
    - wes@barely3am.com

- Now let's look at some changes that are coming to the REN-ISAC.

(4) REN-ISAC

- Most of you already are familiar with the REN-ISAC, higher ed's security incident handling trust community. However, if you're not familiar with the REN-ISAC, there are some great introductory overview documents you can check out:

  REN-ISAC flier (8.5 x 11 color glossy):

  http://www.ren-isac.net/docs/ren-isac_brief.pdf

  Executive Overview:

  http://www.ren-isac.net/docs/ren-isac_executive_overview.pdf

- Membership is open to:
  - institutions of higher education,
  - teaching hospitals,
  - research and education network providers, and
  - government-funded research organizations;
  - international, although focused on U.S.
- Current membership: 261 institutions, 563 individuals

14

Please Note That The REN-ISAC Membership Model Is Changing

- Objectives of the new model are to:
  - Extend the reach of REN-ISAC more broadly in the R&E community (make it easier for entry-level participation), while retaining, a strongly trusted information sharing core
  - Establish a long-term sustainable business model
- Feb 2009 – a new, tiered membership model.
  - Institutions (not individuals) join, represented by a “management representative” and one or more “member representatives”.
  - General and XSec (eXtraSecure) member representatives. The tiers differ in the criteria for membership, the degree vetting that member representatives undergo, and the classification of sensitive information shared in the tier.
- July 2009 – a modest membership fee
- Changes described in: "Membership Model Changes - 2009" http://www.ren-isac.net/docs/ren-isac_membership_20090127.pdf

15

REN-ISAC Contacts

Executive Advisory Group, see https://secure.ren-isac.net/eag/

Jack Suess, Chair EAG, jack@umbc.edu

Mark Bruhn, Executive Director, mbruhn@iu.edu

Doug Pearson, Technical Director, dodpears@ren-isac.net

Gabriel Iovino, Principal Security Engineer,
giovino@ren-isac.net

http://www.ren-isac.net

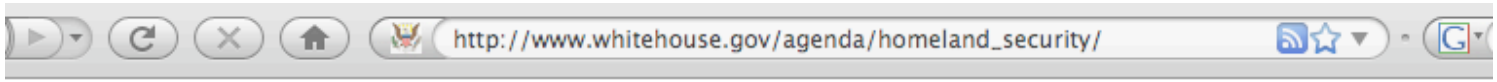
24x7 Watch Desk:

soc@ren-isac.net

+1 (317) 278-6630

(5) Federal Cyber Security Initiatives

- Over the last year or so a number of federal agencies have been working on their **medium to long term roadmaps for their network security research initiatives** (including potentially future community security research funding opportunities).
- We've participated in a number of those roadmap workshops, along with other members of the higher ed security community, government agency staff members, and researchers from private sector security firms. Attendees would commonly hear a number of invited presentations, and then break out into groups to consider issues the community faces.
- The synthesis of those various agency roadmaps, along with input from independent groups (such as the Commission on Cyber Security for the 44th Presidency, http://www.csis.org/tech/cyber/), will likely profoundly influence the new administration's cyber security programs and research initiatives. We're already seeing signs that the White House takes cyber security very seriously….



Protect Our Information Networks

Barack Obama and Joe Biden -- working with private industry, the research community and our citizens -- will lead an effort to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security. They will:

- **Strengthen Federal Leadership on Cyber Security:** Declare the cyber infrastructure a strategic asset and establish the position of national cyber advisor who will report directly to the president and will be responsible for coordinating federal agency efforts and development of national cyber policy.
- **Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure:** Support an initiative to develop next-generation secure computers and networking for national security applications. Work with industry and academia to develop and deploy a new generation of secure hardware and software for our critical cyber infrastructure.
- **Protect the IT Infrastructure That Keeps America's Economy Safe:** Work with the private sector to establish tough new standards for cyber security and physical resilience.
- **Prevent Corporate Cyber-Espionage:** Work with industry to develop the systems necessary to protect our nation's trade secrets and our research and development. Innovations in software, engineering, pharmaceuticals and other fields are being stolen online from U.S. businesses at an alarming rate.
- **Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit:** Shut down the mechanisms used to transmit criminal profits by shutting down untraceable Internet payment schemes. Initiate a grant and training program to provide federal, state, and local law enforcement agencies the tools they need to detect and prosecute cyber crime.
- **Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches:** Partner with industry and our citizens to secure personal data stored on government and private systems. Institute a common standard for securing such data across industries and protect the rights of individuals in the information age.

(6) ICANN GNSO Fast Flux Working Group

- We've also been busy with key non-governmental community networking organizations.
- Some of you may be familiar with the notion of "fast flux hosting." Fast flux hosting is a technique in which a miscreant rotates a domain name across a pool of **botted PCs** (via automatically-updated DNS entries with short TTLs), using those hosts to provide highly survivable web hosting or for other purposes.
- Sites hosted on fast flux web sites often include malware, phishing sites, pirated software sites, child porn sites, sites selling narcotics and other illegal prescription drugs, etc. -- illegal content that legitimate hosting companies obviously will not tolerate.
- We were invited to participate in the ICANN GNSO Fast Flux working group, and that group recently released a 121 page initial report for public review and comment (through 15 February 2009). If you'd like to **read that report and offer comments**, please see www.icann.org/en/announcements/announcement-26jan09-en.htm

This GNSO Report Has Gotten Press Worldwide

ICANN не знает, как бороться с Fast Flux

Игорь Крейн

Безопасность | Новости | 28.01.2009 09:49

комментарии (4)
версия для печати

Рабочая группа
связанные с тех
киберпреступни
результатов сво

Fast Flux позволяет постоянно, раз в не

ars technica

All Apple Business Gadgets Gaming Hardware Microsoft Open Source Science Tech Po

News Guides Reviews

Law & Disorder : Ars covers the world of tech policy

ICANN tries to tackle botnet-friendly fast flux hosting

origins and stay active for longer. ICANN is
g back and arguing that ICANN has no right to
egal purposes.

PC World » Business Center » Security » News

ICANN Ponders Ways to Stop Scammy Web Sites

Jeremy Kirk, IDG News S

Tuesday, January 27, 200

The overseer of the Inte
fix a problem that is ena

The Internet Corporatio
issued an initial report
name to resolve to mul

A Noteworthy Report on Fast Flux Hosting

Jan 26, 2009 8:45 PM PST | Comments: 1 | Views: 520

By Suresh Ramasubramanian

Comment | Print

This very interesting document was released by ICANN's Generic Names Supporting Organization (GNSO) for public comment yesterday. And it asks some fundamental questions while at the same time pointing to sources such as the Honeynet Alliance's reports on fast flux.

It also points out the benefits of "legitimate" fast flux—such as its use by content distribution networks, or by DDoS protection systems. An additional use is of course a simple attempt at using multiple A records with short (< 1 minute) TTL in a basic attempt to load balance.

This Is Your Chance to Weigh In On What You'd Like to See ICANN Do (or Not Do)

- This is a somewhat pivotal moment for ICANN. During the last ICANN Meeting (held in Egypt), I'm told that there was an unprecedented level of attendee interest in cyber security issues.
- Many attendees in Egypt were urging ICANN to take a more active role in addressing cyber abuse issues; at the same time, there are others who would strongly prefer that ICANN minimize or avoid taking on any new activities in the security area.
- What would YOU like to see? Is Fast Flux (and other security issues) a problem that ICANN should tackle? Should ICANN ignore these issues?
- If you have an opinion about this issue, be sure to send your comments about the Fast Flux report to ICANN no later than 15 February 2009.

(7) Cyber Infrastructure Architectures, Security and Advanced Applications

- At the Spring 2008 Member Meeting, we talked about how cyber security often comes up -- but not for the right reasons. **More often than not, security practices and security-oriented network architectures hinder, rather than help, user to do their work.**
- **Firewalls are a special area of concern.** In that paper we talked about why people turned to them, their strengths and weaknesses, and some alternatives to a classic perimeter firewall architecture. The risk we face is that if we aren't careful, eventually only the web (and things which tunnel traffic in web-like ways) will remain.
- We also talked about a new potential role, the "network usability officer," a person who is really is the third leg of an institutional network policy triad (the other two legs would be the institutional chief information security officer and the site's privacy officer).
- See www.uoregon.edu/~joe/architectures/architecture.pdf

(8) Security and DNS

- The Domain Name System (DNS) is fundamental to everything we do on the Internet, but it remains woefully insecure. Because of that insecurity, DNS is becoming an increasingly popular target for abuse. Common DNS attacks now include DNS poisoning, DNS amplification attacks, and "DNS changer" attacks.
- *DNS poisoning:* EVERYONE must now run a DNS server product that is resistant to the DNS poisoning vulnerabilities Dan Kaminsky identified; check yours using https://www.dns-oarc.net/oarc/services/dnsentropy (see next slide)
- *DNS amplification via spoofed traffic:* The DNS attack *de jour* uses spoofed DNS queries asking for root NS info; again, a web based tester is available, see: http://isc1.sans.org/dnstest.html
- *DNS changer:* Malware substitutes the IPs of the bad guy's name servers for yours; once they control your DNS servers, game's over! Watch for customer DNS going directly to odd IP addresses!

http://4cdca17ca38518694591afc3.et.dns-oarc.net/result/

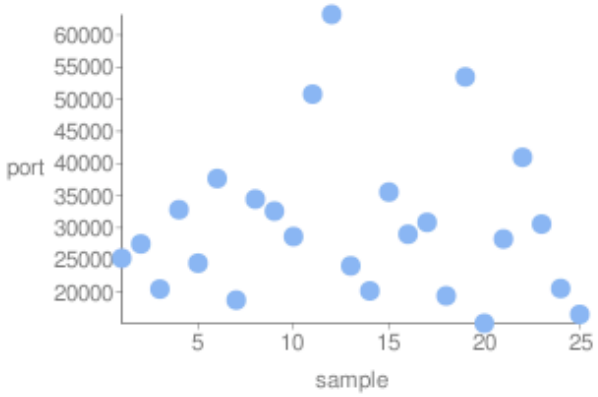
DNS Resolver(s) Tested:

1. 128.194.254.1 (dns-cache-1.net.tamu.edu) appears to have GREAT source port randomness and GREAT transaction ID randomness.

Test time: 2009-02-03 16:55:22 UTC

Note that standard deviation is usually, but not always, a good indicator of randomness. Your brain is a better detector of randomness, so be sure to take a look at the scatter plots below. If you see patterns (such as straight lines), the values are probably less random than reported.

128.194.254.1 Source Port Randomness: GREAT <== Good work, Texas A&M!



Number of samples: 25
Unique ports: 25
Range: 15110 - 63203
Modified Standard Deviation: 11810
Bits of Randomness: 15
Values Seen: 25242 27473 20443 32803 24470 37653 18731 34448 32577 28621 50788 63203 24058 20161 35542 28983 30827 19387 53475 15110 28243 40951 30562 20529 16497

Fixing DNS (If It Does Need Some Attention)

- As a basic matter, you need to get your DNS servers correctly architected (e.g., splitting your authoritative servers and your recursive resolvers), and you must also appropriately control non-customer access to your recursive resolvers.
- Beyond basic things like that, however, you should be planning for deployment of DNSSEC. DNSSEC uses cryptographic signatures so that IF a DNS entry has a valid signature, THEN we can trust the DNS responses we receive. While there are still many issues which the community needs to work through, DNSSEC is incredibly important, and something whose deployment your campus or site should be working on now.
- Interested in learning more about DNSSEC? Internet2 has a DNSSEC effort that holds periodic conference calls and which has a mailing list; to subscribe send email <sympa@internet2.edu> with the SUBJECT LINE: subscribe dnssec FirstName LastName
- We're also beginning to plan for an Internet2 DNSSEC workshop.

(9) Securing the Routing Infrastructure

- While DNSSEC has a lot of momentum right now, there are some other network security areas that have had a much slower start.

- For example, consider S*BGP. Cryptographic approaches to routing security just really haven't caught on despite demonstrated examples of stunning insecurities related to BGP.

- The good news is that DHS has announced a new emphasis on improving router security; you may have seen Douglas Maughans's comments in **"U.S. plots major upgrade to Internet router security: Millions to be spent adding cryptography to BGP,"** 1/15/2009, www.networkworld.com/news/2009/011509-bgp.html

- I'm happy to report that Douglas has agreed to come and provide a briefing on this new initiative for the Spring Member Meeting.

(10) Salsa-DR

- Our colleagues at Educause annually ask higher ed CIO's to rank their top ten IT issues. In 2008, the most recent year for which data is available, the number one issue was "Security" (a good and bad place to be!) but their number six issue was "Disaster Recovery & Business Continuity." (see http://tinyurl.com/EducauseTopTen)
- Internet2's primary effort to address the CIO disaster recovery concern is SALSA-DR.
- In addition to work on recommendations for IT disaster recovery best practices, Salsa-DR also pioneered work on campus real time emergency communication efforts (as mandated by the Clery Act), and now many of our campuses have reverse-911 service, reader boards, and other real time emergency communication capabilities.
- Opportunity: Salsa-DR's former head recently stepped down due to new state wide travel restrictions; if you're from an Internet2 site and would be interested in leading this work, please send me email.

(11) A "Mundane" Risk: The Insider Threat

- During the Fall Internet2 Member Meeting, we talked about “Loss of Network Control Incidents,” specifically the issues the city of San Francisco ran into whereby they were locked out of their network, allegedly the result of actions by a city employee. If you didn’t have the opportunity to attend that session, detailed slides are available at www.uoregon.edu/~joe/loss-of-network-control/
- **The insider threat continue to be a serious risk during this period of economic uncertainty.** A recently revealed example was the alleged Fannie Mae “logic bomb” incident (targeting data on 4,000 Fannie Mae systems for potential deletion). An FBI press release dated January 27th, 2009 describing the alleged incident is at http://baltimore.fbi.gov/dojpressrel/pressrel09/ba012709a.htm
- We urge you to review your policies and controls intended to limit potential misbehavior by insiders, including things such as policies enforcing separation of duties, code change reviews & testing, etc.

(12) Something A Little More Exotic: Cyber War

- Politically-oriented cyber attacks are a rare exception to the rule that most cyber attacks today are economically motivated. The latest nation state to come under cyber attack was Kyrgyzstan. See, for example "The Kyrgyzstan Cyber Attack That No One Is Talking About," http://intelfusion.net/wordpress/?p=509
- Multiple cyber attacks over the last year have even been called "cyber war" by the media, although those incidents often fail to justify that moniker when subjected to closer review.
- Nonetheless, given the frequency with which "cyberwar" was allegedly happening, I did a talk attempting to clarify what is and isn't real "cyber war." See http://www.uoregon.edu/~joe/cyberwar/
- If you are interested in the issue of cyber war, the NATO Center for Cooperative Cyber Defense in Estonia has issued a call for research papers for a conference on cyber warfare to be held June 17th-19th, 2009, see http://www.ccdcoe.org/20.html

Summary

- An awful lot is going on in the cyber security community right now, and we need your help, input and involvement, whether that's just keeping your own network secure, or helping with an existing effort, or leading a new security effort.
- The United States higher education community can't handle all these system and network security issues on our own; we need to work with other agencies and organizations for maximum effect.
- There are many exciting security-related areas that are still virtually "green field" and where will be substantial funding opportunities chasing a relatively limited number of security researchers. We encourage you and your staff and faculty to get involved!
- Are there any questions?