Internet2, Security, and DICE

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

Dante, Internet2, Canarie and ESNet (DICE) Meeting
Feb 12-13th, Athens, Greece

http://www.uoregon.edu/~joe/dice-2/

Disclaimer: The opinions expressed in this document are strictly those of the author, and should not necessarily be taken as expressing the opinion of Internet2, the University of Oregon, or any other 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.

I. Introduction

- It's a real pleasure to be with you today via H.323 video from the University of Oregon in Eugene (UO's shown below).
- For those who may not be familiar with Oregon, Eugene's in the middle of the Willamette Valley, about an hour north of San Francisco by air, and about a ninety minute drive from either the Pacific Ocean or the Cascade Mountains.
- We'd love to have you think about visiting Eugene sometime!

Backstory: DICE, July 2007

- During the July 2007 DICE meeting I was an invited panelist at the Federal Trade Commission's second Spam Summit in Washington DC, so Rick Summerhill was good enough to go over some security slides I'd prepared. Those slides are still available online, see: "Internet2 Security Initiatives" at http://www.uoregon.edu/~joe/dice/dice-meeting.pdf (or .ppt)

- My July slides provided context for some of Internet2's security work, and highlighted a number of security areas which I believed might have particular relevance to the advanced networking community, including collaboration with the REN-ISAC, CALEA (lawful network intercept), disaster recovery, DNSSEC, DDoS mitigation, real time notification systems, route injection risks, SCADA (control system security), and our security outreach efforts.

What We'll Talk A Little About Today

- Today we've got 20 minutes or so to talk. We'll give you an update on some of the topics I'd previously raised, and also introduce a few new topics. Since we only have 20 minutes and questions via remote video can sometimes be tricky, if possible, let's hold any questions until the end of my talk
- Because my colleague Doug Pearson from the REN-ISAC will also be speaking with DICE via H.323 today, I'm going to leave the critical topics of incident handling, information sharing within the REN-ISAC trust community, and related things to his very capable hands.
- Likewise, I believe Ken Klingenstein and others may be talking about the topics of middleware and identity management, so I'll also do my best to avoid stepping on those important security-related areas.
- Let's start by reviewing higher education's IT priorities.

Top 10 Issues for IT in Higher Education, 2007

- You may know that Educause annually surveys higher ed technology leaders to identify the top ten issues they face. As was described in http://connect.educause.edu/Library/EDUCAUSE+Review/TopTenITIssues2007/40702 , the **number two issue for 2007 was "Security"** (second only to "Funding IT"), the **number four issue was "Identity and Access Management,"** and **the number five issue was "Disaster Recovery/Business Continuity."**
- Clearly a variety of security-related issues remain very salient and a top priority for higher education IT leadership.
- But what are the top security issues that CIOs and other campus leaders have in mind? Surely there must be just a couple of security issues which we really need to be paying attention to, allowing us to set the rest aside for later?

Security Topics and Spinning Plates

- Unfortunately, no. Discussing IT security is always something of a challenge because there are so many diverse security issues in play at any given time. It would be great to be able to say, "We're just going to work on distributed denial of service attacks today" or "Let's just think about malware for a while," but you simply can't get away with doing that.
- Security work requires that we all **"spin plates,"** multitasking across multiple security issues more or less in real time, while continually adding new "plates" to our ongoing "routine"
- If you're not accustomed to juggling a bunch of issues that way, it can sometimes feel a little **overwhelming** as you hear about issue after issue after issue. How can we possibly keep them **all** spinning? The answer, I think, is lots of coffee. :-)
- Seriously, though, even though there's a lot going on, stay calm. The Internet (and Internet2!) are doing okay (although we'll hear about some possible future exceptions a little later)

"Hey! That's a Perfect Example of How Security People Are Always Focused On How Things Might Go Wrong!"

- That's sort of inherent in this line of work. Remember that IT security is an adversarial occupation, like being a policeman, lawyer, soldier, chess player or hockey goalie. There really **are** people out there trying to "get you" or "get your team."
- If existing security measures work properly in the face of those ongoing attacks, nothing happens – we have *status quo ante bellum* (things as they were before the conflict).
- On the other hand, if we fail to correctly think about how things may go wrong and our defenses are flawed, we may face an unpleasant surprise (such as a hacked system).
- So please bear with us as we worry about things that might go wrong – we do that in an effort to collectively avoid unpleasant surprises, not because we're pessimistic (most IT security folks are actually relentlessly optimistic and upbeat).

II. Some Substantive Security Issues

Top IT Issue #5: Disaster Recovery

- Last time, we mentioned:

  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.
- The importance of disaster recovery and business continuity planning continues to be brought home since that time.

"Users at Storage Decisions Hone Disaster Recovery Plans"

- (Dec 6, 2007) http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1285009,00.html
- "Many users at Storage Decisions this week said that disaster recovery has become their top priority for next year."
- 'Fleeing tape: A constant theme among users was the need to move away from tape to get data offsite. As the amount of data increases, recovery from tape becomes less practical. With the 30,000 tapes it takes to hold the 400 TB of data making up his environment, Dan Stillmaker, director of storage systems for Stanford University, said his shop "would be hard-pressed to meet our two week recovery window -- very hard-pressed." Stanford is currently testing virtual tape libraries (VTLs) [...] as well as data replication products.'

Some Headlines We Forget At Our Peril

- *"7 Dead as Mississippi River Bridge Falls Amid Rush Hour in Minneapolis,"* www.cnn.com/2007/US/08/01/bridge.collapse/ [that Interstate highway bridge was adjacent to the University of Minnesota campus, and while it didn't happen to be carrying fiber across the river, it easily could have been...]
- *"265,000 flee as massive wildfires char Southern California,"* edition.cnn.com/2007/US/10/22/wildfire.ca/
  [that event stands out because of how close it was in time to the Oct 2007 Internet2 Member Meeting held in San Diego]
- *"How one clumsy ship cut off the web for 75 million people,"* http://www.guardian.co.uk/business/2008/feb/01/internationalpersonalfinancebusiness.internet (Feb. 1, 2008)
- And there have been many other disasters, including ones as recent as the February 5th EF4-class (170+MPH) tornado which hit Union University in Tennessee.

Beyond Local/Regional Natural Disasters

- While Hurricane Katrina of August 2005 illustrated our vulnerability to certain **local or regional scale disasters**, the 2006 Spring Research Symposium, Homeland Security: Engaging the Frontlines (Institute for Infrastructure and Information Assurance at James Madison University), noted

  *"We need to plan for a class of **national scale disasters** that pose a significantly greater challenge than local or even regional disasters such as Hurricane Katrina. **Examples include nuclear EMP and national scale epidemics.** Such national scale disasters deserve particular attention to preparedness and recovery since assistance from non-affected regions of the nation could be scarce or non-existent. **A major problem with such disasters is maintaining communication and transportation line connectivity.** Communities and regions become isolated making it difficult to maintain their survival." [emphasis added]*

Hardening Advanced Networks Against Electromagnetic Pulse

- Responding to that finding, during the Fall Internet2 Member Meeting in San Diego, I talked about both electromagnetic pulse and pandemic flu-related scenarios in "Planning for Certain High Risk Security Incidents," see http://www.uoregon.edu/~joe/highrisk/high-risk.pdf (or .ppt).
- Among other recommendations made during that talk, I urged national and regional high performance networks to consider hardening their facilities against electromagnetic pulse-related damage, and just as I urged attendees at that session to do this, I'd urge **you** to begin gradually doing the same. A modest EMP shielding program can be gradually implemented on a rack by rack basis, and need not be prohibitively expensive. But let's not get stuck on the EMP issue. What about pandemic flu?

Why Would Pandemic Flu Impact IT System and Network Operations?

- Information technology impacts associated with pandemic flu may involve either personnel or infrastructure, or both:
  -- Unlike some business continuity scenarios, a pandemic is a failure of the human elements of the computer/network system. Key IT personnel (just like anyone else) may contract the flu and cease to be available for mission critical IT-related work; others may simply hunker down to avoid becoming infected. Absenteeism may be widespread.
  -- IT-critical infrastructural services (such as electrical power) may become unavailable during the outbreak, potentially causing cascading failures to occur. **Your** facilities may be fine--but you may still be impacted by failures **elsewhere**.
- In fact, IT systems and networks may play a crucial role in helping institutions to cope with pandemic influenza, as I discussed in my talk.

Others Have Also Begun to Talk About National Scale Disaster Risks

- For example, Doug Gale did a two part series for **Campus Technologies** entitled "Things That Go Bump in the Night" (see http://campustechnology.com/articles/56697_2/) and "Planning for the Next Disaster," (see http://campustechnology.com/articles/57154/), discussing precisely the two topics we raised in San Diego.
- The timeliness of the EMP topic may also be underscored by the USAF December 11th, 2007 announcement of a $75 million five year program to develop high power microwave weapons (www.fbo.gov/spg/USAF/AFMC/AFRLPLDED/ Reference%2DNumber%2DBAA%2D08%2DRD%2D01/ SynopsisP.html).
- Truly, it is really worth your time to begin thinking about these emerging threats.

Real Time Emergency Communications

- I've also been very pleased by the attention the community has paid to the issue of real time emergency communication systems. We introduced that topic at the Spring 2007 Internet2 Member Meeting in Crystal City, Virginia (see "Real Time Notification During a Disaster or Other Emergency," http://www.uoregon.edu/~joe/notification/) and since then many schools have done a great job of evaluating and deploying a variety of different systems.
- One indication of this was the front page of the *National Survey of Information Technology in U.S. Higher Education*, Oct. 2007, (see http://www.campuscomputing.net/sites/www.campuscomputing.net/files/2007-CCP_0.pdf) which reported that "IT Security and Crisis Management Pose Continuing Challenges," with some interesting statistics.

Additional Security "Plates" You May Want to Begin "Spinning"

1) IPv4 Address Exhaustion and IPv6 Security Appliance Readiness

2) Growth in the Internet Routing Table, Route Churn and Routing Fragility

3) Domain Name System Related Topics

4) The Missing Half of Netflow (Random Port Usage, the Everything-Over-Port 80 Internet, and Traffic Analysis)

5) The Emergence of Counterintelligence as an IT Security Concern

1) IPv4 Address Exhaustion and IPv6 Security Appliance Readiness

- You are likely aware that the Internet community is getting rather close to running out of IPv4 address space. For example, see Richard Jimmerson's "IPv4 and IPv6 Status" report from the December 2007 Joint Techs Meeting, see http://www.internet2.edu/presentations/jt2008jan/20080121-jimmerson.ppt , which mentioned:
  -- "RIRs are consistently allocating over 10 /8s per year"
  -- "The RIRs collectively allocated over 12 /8s for the first time in 2007"
  -- "Number of /8s remaining in IANA's unallocated pool: 42"
- **Let me do the math for you: 42/12=3.5 YEARS til we're <u>COMPLETELY OUT</u> of additional IPv4 address space, assuming our IP burn rate doesn't accelerate (or slow).**
- It might thus be "good" if we began migrating to IPv6, eh?

Not Surprisingly, There Was a Lot of Discussion of IPv6 During Joint Techs

- Ron Broersma, Chief Engineer for DREN, the Defense Research and Engineering Network, shared an excellent talk: "IPv6 Deployment Experiences," www.internet2.edu/presentations/jt2008jan/20080121-broersma.ppt
- A few quick quotes from Ron's slides:
  slide 3: "Reported to you previously:
  -- Most serious problem is lack of IPv6 support in many security products (firewall, IDS, IPS, VPNs, web proxy, etc)."
  slide 22: "Summary: Situation Today [...]
  -- Need to make security stacks fully IPv6 capable
  - Firewalls, IDS, proxies, IDP/IPS, ACLs
- My take: we **REALLY** need to start making some progress in the area of IPv6 and security or we **will** be wedged...

Some Additional Excellent IPv6 Talks Also From The Jan 2008 Joint Techs

- Bill Cerveny (Arbor Networks)'s "Enabling IPv6 in Products and Services," (see http://www.internet2.edu/presentations/jt2008jan/20080121-cerveny.pdf)
- Dave Farmer (Minnesota)'s "IPv6 Autoconfiguration: Plug & Play Dream or Security Nightmare?" (see www.internet2.edu/presentations/jt2008jan/20080122-farmer.ppt)
- Michael Sinatra (Berkeley)'s "Forcing the Issue: A Campus's (Ongoing) Experience in IPv6 Deployment," (see http://www.internet2.edu/presentations/jt2008jan/20080121-sinatra.pdf)
- Susan Estrada (Internet Society)'s Lightning Talk, http://www.internet2.edu/presentations/jt2008jan/20080123-estrada.ppt

One Story That Rather Concerns Me, Seen in Network World, Feb 6, 2008

- **"Who's afraid of IPv4 address depletion? Apparently no one. Network managers aren't worried enough to migrate to IPv6, survey finds"** http://www.networkworld.com/news/2008/020608-ipv4-address-depletion.html

  Only 16% of IT professionals consider IPv4 address depletion "a huge concern that has or will soon force us to migrate to IPv6," according to a BT INS survey of 310 IT professionals that was conducted in December 2007.

  A whopping 26% of IT professionals felt IPv4 address depletion was "no concern." These survey respondents said they can use network address translation combined with VPNs to alleviate the problem. [story continues]

2) Growth In the Internet Routing Table

- Yet another talk which could easily have been added to the "excellent IPv6 talk list" on slide 16 (but for the fact that it provides such an excellent bridge to the routing table growth issue), was Kevin Oberman (ESNet)'s presentation, "The Gathering Storm: The Coming Crisis in the Internet," http://www.internet2.edu/presentations/jt2008jan/20080121-oberman.ppt
- In a nutshell, among other issues, the IPv4 routing table has been continually growing in size, and is at or near a critical hardware threshold (244K routes) for some popular routers; "route churn is approaching the point where routes will never completely converge" (oops, a little problem there maybe!)
- And yes, fragile routing **can** be a security issue (without getting too explicit, consider intentional deaggregation of large prefixes if we're already teetering close to the edge)

A Meaty Topic For Those Interested in Network Security-Related Research

- Given the importance of reducing the size of the global IPv4 routing table, you may want to check out Dave Meyer's "LISP: A Level of Indirection for Routing," http://www.internet2.edu/presentations/jt2008jan/20080121-meyer-lisp.pdf

- This is tremendously interesting and important work, with potentially profound implications for network stability and security, and I know that Dave and colleagues would love your participation and input if you're interested and have time

- Let's now continue our whirlwind tour with a little about the domain name system (no, sorry there's no DNSSEC news)

3) DNS and Fast Flux

- Novel ways to use the domain system continues to be a major focus for the miscreants.
- It was thus particularly heartening in January to see the ICANN Security and Stability Advisory Committee release the "SSAC Advisory on Fast Flux Hosting and DNS" (see http://www.icann.org/committees/security/sac025.pdf). For those who may not be familiar with "fast flux," FF involves a spammer hosting his web site on a set of compromised consumer PCs, accessing that set of PCs via a domain name. As any individual compromised PC gets identified and taken offline for remediation, the old host simply gets replaced with a new one, and the DNS entry gets updated to reflect the changes in the list "participating" hosts.
- Efficiently dealing with fast flux hosts generally requires the cooperation of domain name registrars, because if you try disabling individual 0wn3d hosts, others just replace it.

The Availability of $0.14 Domain Names

- Thinking about fast flux hosts, clearly domain names are a key ingredient of miscreant operations, and prompt action from cooperating registrars is key to combating them.
- But what if domain names were so cheap that there was literally no margin available for processing abuse complaints?
- *"Experience .CN Domain Name for One Yuan Campaign" will extend till 31st December, 2008* http://www.cnnic.cn/html/Dir/2007/12/27/4953.htm
- 1 Yuan = USD 0.139 (or EUR 0.096 if you prefer) as of 2/10
- I bet you didn't know that YOUR institution's name is probably registered by someone in .cn! For example, internet2.cn is at 82.98.86.172 and if you check that page full of sponsored listings, you'll see that "This domain may be for sale by its owner!" At just $0.14/domain, domain name speculation and squatting is now rampant in the dot cn TLD.

Domain Tasting; DNS Redirection Issues

- An awful lot more is going on in the DNS area right now. Just to flag two of many topics for those who might be interested:

  -- We're on the cusp of seeing substantial improvement in the area of domain name tasting and domain name kiting, largely as a result of proposed changes to the five day "free" Add Grace Period which is currently being exploited.
  See for example http://gnso.icann.org/mailing-lists/archives/council/pdfKOCqNDwBV6.pdf (5 Feb 2008)

  -- DNS redirection: this is when a provider's name server, rather than returning NXDOMAIN when a domain isn't found, instead sends a user's web browser to an advertising page, thereby monetizing the user's "typo." No big deal you say? Well, consider the potential impact on DNSBLs where you really want to see an NXDOMAIN if an IP address isn't listed! See the discussion at http://www.surbl.org/faq.html#opendns

4) The Missing Half of Netflow (Random Port Usage, the Everything-Over-Port 80 Internet, and Traffic Analysis)

- Local area network administrators are routinely urged to "know their traffic" since that's a prerequisite to being able to identify traffic anomalies, configure perimeter firewalls, do capacity planning, etc. Well, it's equally important for national backbones to understand the traffic which they see.
- Internet2 routinely collects netflow data for the Internet2 Network, publishing weekly summaries of that data at http://netflow.internet2.edu/ -- including a port-based application-by-application breakdown.
- Unfortunately, 50% of that traffic (measured by octets) consistently ends up in an "unidentified" category. What is it? An important bread-and-butter application with non-standard port usage habits? A stealthy P2P (or other bandwidth intensive) app trying to hide? Attack traffic? (You can always spot the security types, can't you?) Something else?

Anonymized Internet2 Flow Data

- Fortunately, Internet2 makes anonymized flow data available for researchers, so you can request access to it and look for yourself. We did so, and reported on what we saw (and didn't see!) during the winter Joint Techs meeting in Hawaii (see "The Missing Half of Netflow (With an Additional Tutorial On How to Use The Internet2 Netflow Data Archives)," http://www.uoregon.edu/~joe/missing-half/)
- In a nutshell, while ports below 49152 are registered ports assigned by IANA, some measurement and bread-and-butter high performance applications (including LHC traffic) may be informally using ports from that registered range without having them formally assigned to them by IANA.
- Additional applications may be intentionally randomizing their port usage, or tunneling all traffic over port 80, making traditional traffic analysis difficult or virtually impossible.

Some Miscellaneous Flow Related Notes

- Because Internet2 is only collecting version 5 format Netflow (rather than version 9 Netflow), we can only see IPv4 traffic, so we do not have visibility into native IPv6 flows (it would probably be good to eliminate that "blind spot" if we're all going to need to be embracing IPv6 within just a few years!)
- A relatively small number of anonymized sources and destinations account for a surprisingly large % of all traffic:

  Total Anonymized Sources: 71,716
  Top 50 Anonymized Sources: **47% of all octets**
  Total Anonymized Destinations: 104,297
  Top 50 Anonymized Destinations: **29% of all octets**

  This degree of concentration has potentially favorable implications for dynamic circuit-based architectures.

5) Emergence of Counterintelligence As an Area of IT Security Concern

- It has long been known that the FBI's top three priorities are (in priority order) counterterrorism, counterintelligence and cybercrime. For the first time, counterintelligence is beginning to emerge as a major IT security concern for everyone, not just the FBI. Consider, SANS' "Top 10 Security Menaces for 2008," which now lists "Cyber Espionage Efforts By Well Resourced Organizations Looking To Extract Large Amounts Of Data - Particularly Using Targeted Phishing" as its #3 threat (see http://www.sans.org/2008menaces/)
- Also check out the Dec 4, 2007 speech by Joel F. Brenner, National Counterintelligence Executive, "Counterintelligence in the 21st Century: Not Just a Government Problem," www.ncix.gov/publications/speeches/AFCEASpeech.pdf

III. And A Security "Discussion" Topic: Are We Making This All Too Difficult?

Are We Worrying About The Right Sort of Security Issues?

- As you know, Internet2 is currently engaging in strategic planning, a very important activity for our organization.
- Looking at the Internet2 Strategic Planning Wiki (see https://wiki.internet2.edu/confluence/display/I2SP) I was interested to note the comment that had been posted there by David Lassner on behalf of "an Internet2 corporate member from a networking gear company." The corporate member's comments were particularly striking to me because they largely focused on security issues, but not on particularly cutting edge security issues.
- Specifically, the member's security-related topics of concern were spam e-mail, wireless security, one non-security-related topic (power and cooling efficiency), making people less gullible to things like phishing, and Internet privacy.

Those Are All Really Good Topics

- Those topics all really resonate with me – remember, for example, that I played "hooky" from the last DICE meeting so I could talk about spam with the FTC. :-)
- Similarly, if you're on Bill St Arnaud's list, on February 6th you may have seen Bill mention Olivier Martin's paper on the evolution of the Internet and academic R&E networks (www.ictconsulting.ch/reports/NEC2007-OHMartin.doc) Martin's paper includes a discussion of security issues, and the topics which he mentioned were spamming, phishing, identity theft and DDoS – again, very much meat-and-potato topics as far as security topics go.
- Or, if I were to talk to campus IT leaders, I suspect that many of them might tell me that *their* biggest concern is unauthorized access to personally identifiable information (PII), a mandatory notification item now in many areas.

Parameterizing the Security Space

- Seeing things like that, I want to make sure the Internet2 community in general (and me in particular!) focus on the right security topics to meet the community's needs.
  For example:

  -- Should we worry about near term operational security threats, or take a longer term perspective, perhaps looking five years out? (a 5 year horizon was stipulated for DOE's "Cybersecurity Research Needs for Open Science," see http://cybersecurity.colostate.edu/ and the letter and final reports at www.sc.doe.gov/ascr/WorkshopsConferences/WorkshopsConferencesArchive.html See also https://wiki.anl.gov/cybercommunity/ for another DOE Cybersecurity R&D workshop happening right now)

Other Security Parameters

- As a networking organization, should Internet2 focus largely on security as it relates to the **network?** Or should Internet2's security portfolio remain end-to-end, recognizing that our members operate workstations and servers; write and download and install and use software; and have user- and campus-level security issues?
- As Internet2 adds new participants, such as FCC Rural Health Care awardees, should we be giving a particularly close look at security issues which are uniquely germane to those new constituents, such as HIPAA requirements?
- Is security **research** important, or do we only care about **operational** issues? How about security policy issues?
- Or are we making this too hard? Should we simply focus on things like spam, phishing, wireless security, PII, DDoS, and similar issues that touch us all everyday?

Spam Really Can Be A Very Important Driver For IT In Higher Education

- Now that spam exceeds 90% of all email traffic (see http://www.senderbase.org/home/detail_spam_volume), a growing number of universities are finding it increasingly hard to run email locally. Running mail in an environment where spam, malware and phishing are rampant, while ultimately still doable, may require substantial investments in hardware, software, services and experienced staff effort.
- It's not surprising, then, that at least some major universities are outsourcing campus email (for "free!") to third party providers, at least for their students if not for their faculty.
- Outsourcing email (a very basic institutional service) this way can have potentially profound implications, and may be yet another example of an increasingly commoditized approach to IT (c.f., http://www.nicholasgcarr.com/bigswitch/)

Let's Think A Little About Outsourcing Email In the Face of Overwhelming Spam

- Just as you struggle with spam, so do the large providers of outsourced email services (in fact, everyone does!)
- Do you know how those outsourced email service providers filter spam on their sites? What if, for example, you outsource email to a site which follows AOL's lead and rejects mail from any site that doesn't meet specific technical standards, such as rDNS? (postmaster.aol.com/guidelines/standards.html) Will universities be able to "live with that?" If they find they can't, will their outsourced email provider be willing to change their filtering methodology for them? Assuming outsourced email providers are in a take-it-or-leave-it mood, will universities have options, or the in-house expertise they'd need down the line needed to bring mail back "in-house?" Or is email outsourcing effectively a one-way trap door function, leaving you stuck with whatever service you select?

Another Spam-Related Consideration

- Something which may be particularly relevant to those of you in Europe: since we've chased many spammers out of the United States through aggressive enforcement activity, spammers may now be settling (like an unwanted plague) in Europe. (I first noted this in June, 2006 – even at that time nearly 50% all email traffic was from European sources, see www.uoregon.edu/~joe/maawg7/maawg7.pdf at slides 2-3, but now this is becoming mainstream news, e.g., CNET is reporting, "Europe still top source of spam," see http://www.news.com/2100-7349_3-6229352.html)
- I'm sure many Europeans easily remember when a major American ISP dropped all email from Europe for a period of time, and I'm sure you're all also familiar with country coded DNS services such as http://countries.nerd.dk/
- Working to preserve email as a worldwide communication channel might be a rather worthwhile community goal....

Should We Be Collaborating With Industry Or Law Enforcement To Attack Basic Security Issues?

- For example, should the academic community be working more closely with industry's Messaging Anti-Abuse Working Group (MAAWG), or the Anti-Phishing Working Group (APWG)? I'd note that they even periodically meet in Europe!
- Or should we heed the comments of some in the anti-cybercrime community who assert that if we continue to just engage in "technical contests" and only "play defense" against the miscreants, we're only educating them and making them stronger? (The most commonly heard analogy is that this is sort of like taking an incomplete course of an antibiotic, thereby inadvertently creating particularly nasty antibiotic resistant bugs or security-measure-resistant miscreants). Has the time come for us to more aggressively share information about the threats we're seeing every day, working to get cyber attackers fined or arrested?

If We Do Want To Go On The Offense...

- If the time has come to go from just taking a defensive approach to dealing with cyber threats to one that's more active, perhaps working with law enforcement (LE) to get miscreants arrested, we need to understand the sort of cases which law enforcement agencies can work.
- By this I mean that while it would be great if LE could go after any and all cybercriminals, the reality is that they simply can't – they don't have the resources, and some cases are either too complicated or have sentences which are too minor to bother with. LE has to pick and choose, generally working only particularly egregious cyber cases.
- If you'd like to get an idea of what sorts of cybercrimes have actually proven to be workable by law enforcement, you can see some examples by checking the "Tour of Cybercrimes" that's at http://www.uoregon.edu/~joe/tour/cybercrime.pdf

Thanks for the Chance to Talk Today

- Thanks for the chance to talk today, and I appreciate your patience with this remote presentation.

- Are there any questions, or do you have any feedback on any of these issues? I'd be happy to talk about them now if we have time, or if not, my email is joe@internet2.edu or joe@oregon.uoregon.edu, or you can give me a call at 541-346-1720

- These slides are available in PDF and PowerPoint format at http://www.uoregon.edu/~joe/dice-2/

- Many of my other public talks are available as links from http://www.uoregon.edu/~joe/