Some Frontiers of IT Security Work

Joe St Sauver, Ph.D.

joe@uoregon.edu or joe@internet2.edu
Manager, Internet2 Security Programs
Internet2 and the University of Oregon

Educause, Seattle Washington
4:55-6:10 PM Wednesday, October 24th, 2007
Ballroom 6E, Table 41

http://www.uoregon.edu/~joe/frontiers/

Disclaimer: All opinions expressed are solely those of the author.

Introduction

- Security of systems and networks in higher education is a universally important topic which resonates with us all.
- Many universities engage in what I'd call "mainstream information technology security" work – they deploy firewalls and antivirus software, patch systems (and watch for systems that still end up compromised), develop and enforce security policies, etc. Those are all important areas, and all parts of the "civilized world" of IT security.
- But there are also IT security areas which remain "wild and untamed" -- frontiers, if you will -- where effective solutions are still being worked out, and other IT security areas which, while once well under control, are now seeing an erosion of control and a possible return to chaos...
- Those areas -- the point of the IT security spear moving forward -- those are the areas we'll explore a little today.

IT Security Frontier #1: Disaster Recovery

- Many universities don't have a usable disaster recovery plan
- When a plan does exist, it may never have been tested
- Would your plan allow you to meet your site's recovery time objectives? (being offline for multiple days is no longer OK!)
- For most schools, meeting recovery time objectives will likely require creation of a mirrored "hot site" data center
- Disaster preparedness also involves things like being ready to deliver real time emergency communications, both to meet pragmatic needs and for compliance with the Clery Act
- We also need to begin planning for national scale disasters (disasters worse even than regional catastrophes such as Hurricane Katrina) – prime examples are planning for EMP (electromagnetic pulse) and planning for pandemic flu.

Frontier 2: Bots and Botnet Remediation

- A bot, sometimes also called a "zombie," is a Windows PC which has been hijacked by a miscreants without the knowledge or permission of the PC's intended user.
- Bots are commonly used to send spam; to flood other sites with traffic they didn't request; to scan other hosts for vulnerabilities; to sniff unencrypted traffic as it is sent over the network; to host child pornography, pirated intellectual property, or malware; to perpetrate click fraud; and for other purposes. There are millions of botted hosts, and malware makes new ones every day.
- The biggest botnet-related problem is that no one has accepted responsibility for securing bot'd hosts. End users don't not have the expertise, tools or inclination to do so; ISPs can't afford to do so; software vendors haven't done so, and the government doesn't view it as their job, either.

Frontier 3: Malware (Viruses, Trojan Horses, Rootkits, Spyware, etc.)

- Signature-based antivirus software is ubiquitous in higher education but unfortunately it is increasingly ineffective against today's enhanced malware threat.
- To understand why, note that antivirus companies release updated signatures for their software once/day (or perhaps several times/day) while some miscreants now repack and reseed their malware dozens of times/day, insuring that at least some systems will always be able to be infected, even if they're running the latest antivirus software and signatures
- Detection of specific malware can vary widely from product to product as shown by http://www.virustotal.com/
- Some things which help: use alternate operating systems and browsers, disable scripting, avoid html & binary content in email, and try http://www.mynetwatchman.com/tools/sc

Frontier 4: Distributed Denial of Service Attacks (DDoS)

- Distributed denial of service ("DDoS") attacks attempt to overwhelm sites by flooding them with automated connection requests or sheer network traffic volume.
- Attacks in the 10's of Gbps range have been seen, and one recent attack took the government of Estonia offline
- Large DDoS attacks can take down any site on the Internet today, or at least make that site work very hard to stay up
- Why do some sites get DDoS'd? Typically a site gets DDoS'd because a miscreant is unhappy with someone. E.G., spammers have repeatedly DDoS'd Spamhaus.
- You can make it harder for someone to successfully DDoS your university by increasing the capacity of your systems and connections, and by having staff ready to divert attack traffic upstream via blackhole communities.

Frontier 5: DNS Security and DNSSEC

- The domain name system ("DNS") is the service that converts domain names (such as www.educause.edu) into numeric IP addresses (such as 207.145.239.180)
- DNS servers used to do DNS resolution often are misconfigured and vulnerable to attack or abuse; abuse often consists of misdirecting users to alternative hostile IPs. Be sure to do a free evaluation of your school's DNS servers by visiting http://www.dnsreport.com/
- Once you've taken care of any vulnerabilities that tool finds, you may also want to look into DNSSEC. DNSSEC, while not fixing all of DNS's woes, is at least able to protect the domain system from some nasty attacks. Unfortunately very, very few sites currently use DNSSEC – this is a great opportunity for your site to show IT security leadership in an emerging and important area.

Frontier 6: Routing

- Routing is the process by which Internet packets get from their source to their destination. Wide area routing is controlled by a protocol called BGP. Sites using BGP are identified by autonomous system numbers, or "ASNs."
- Rogue ASNs may use (or "announce") network addresses which don't belong to them, potentially including your school's address space. Depending how that's address hijacking is done, it may massively disrupt your network or you may never even know it's happening if you aren't monitoring routing of your address space. (You should be!)
- You should also know that growth of the global routing table continues, and aging routing gear from at least one major vendor may no longer be large enough to hold a full table. If you reach that point, routing may become slow or erratic until your hardware gets upgraded or filters are applied.

Frontier 7: IPv6

- Another sign that the Internet has been wildly popular can be seen in the fact that we're literally only a couple of years away from running out of regular (IPv4) IP addresses.
- Many colleges have relatively large historical allocations of IP addresses, and thus may not worry much about this issue, but the rest of the world has begun to scramble to get ready to do IPv4 and IPv6.
- Why does the introduction of IPv6 amount to a security "frontier?" There are actually a variety of reasons, including:
  -- IPv6 traffic is often simply overlooked by IT security folks
  -- many IT security appliances such as firewalls have limited IPv6 support/functionality
  -- IPv4-only users end up relying on a variety of IPv4 to IPv6 transition technologies such as tunnels and gateways; those technologies can compromise security architectures

Frontier 8: Personally Identifiable Information (PII) Breaches

- Of all IT security threats, it is the unauthorized disclosure of personally identifiable information (such as social security numbers, drivers license numbers, credit card numbers, etc.), which seems to cause the greatest popular dismay (and substantial journalistic coverage). People really hate it.
- Legislatures are taking action to address PII breaches, including here in the Pacific Northwest. For example, in Oregon, SB583 went into effect October 1st, 2007, mandating notification in the event a PII breach occurs.
- Individual universities can take a variety of steps to reduce their risk of a PII spill, including adopting a data stewardship policy, minimizing the collection of PII, mandating encryption of PII on portable devices and backup tapes, purchasing cyber insurance, etc. What's your school doing in this area?

Frontier 9: Security of Web Applications

- For many people, the World Wide Web is synonymous with the Internet, and increasingly everything ends up accessed over the web, even complex and mission critical applications. The miscreants have noticed, and they've also noticed that at least some web-based applications have been deployed complete with material vulnerabilities which can easily be exploited. Begin by seeing item C1 in the recommendations of the SANS Top 20 experts at http://www.sans.org/top20/ then visit the OWASP Project.
- Beware of obscure (but potentially huge holes!) such as web proxy autodiscovery; is wpad.yourschool.edu defined?
- On desktops and laptops, check for old versions of Java.
- Less urgently, you may also want to see if your wikis/blogs have been discovered by spammers and are now hosting web spam (e.g., try googling for cialias site:yourschool.edu)

Frontier 10: Assessment and Prioritization of Vulnerabilities

- If you're a security officer and you're facing dozens (or hundreds!) of new vulnerabilities each day, how do you decide which vulnerabilities are important and must be dealt with immediately, and which ones are issues which you can deal with as you have time?
- There have been many informal ranking or prioritization schemes used over the years, but now there's the Common Vulnerability Scoring System (see http://www.first.org/cvss/) and at least one hugely influential security standards body, the Payment Card Industry, has mandated use of the CVSS system "wherever possible" for PCI approved scanning vendors effective June 30th, 2007. That factor alone means that CVSS is here to stay, and thus CVSS is something which you should become familiar with.

Frontier 11: Balancing Perimeter Firewalls and Internet Transparency

- One reason Internet2 initially got involved in the IT security space was concern that the community might build fantastic high speed networks, only to see them "protected" in ways which rendered them useless for their intended purposes.
- For example, many conventional firewalls have had a hard time keeping up with scientific data transfers at gig or 10gig rates, and firewalls have also interfered with H.323 video, IP multicast video, and peer-to-peer application architectures.
- One example of an approach that some people are considering to address those issues is the use of dynamic circuit-based architectures. Those tightly constrained point-to-point connections have very limited accessibility, and thus there's little need for hardware firewall deployment there.
- Use of interior (subnet-based) firewalls is now also popular.

Frontier 12: The Diminishing Value of Passive Monitoring and Active Scanning

- For a long time, passive monitoring of network traffic using an intrusion detection system such as Snort or Bro, and active scanning with tools such as Nessus, were traditional cornerstones of IT security work. Unfortunately, a side effect of changes which have hardened our networks and network architectures is diminishing returns from those approaches.
- For example, as more and more traffic is encrypted, passive monitoring devolves from content analysis to pure traffic analysis (you may be able to tell where traffic's coming from and going to, but the contents of that channel are opaque to analysis). Similarly, as more and more people deploy interior firewalls, or IPv6 gets more widely deployed, scanning entire networks can become a frustrating and not particularly productive exercise

Frontier 13: Incident Handling and Sensitive Information Sharing

- From time to time even the best run site may have a system get compromised. When incidents of that sort occur, or new vulnerabilities get discovered, it is critical that information about that incident or vulnerability gets shared with trusted parties who need to know about it ASAP. For that to happen, we need a community of trustworthy individuals who have the ability to take appropriate action while not compromising sources/methods, or tipping off the bad guys
- In the higher education security community, that incident handling and sensitive info sharing process often takes place via the REN-ISAC (the Research and Educational Network Information Sharing and Analysis Center).
- If your IT security officer isn't part of the REN-ISAC, he/she may want to review membership requirements and apply!

For More Information

- It's been a real pleasure to share some thoughts on the frontiers of IT security with you today.
- For more information on the topics mentioned, and opportunities to get involved in these areas, please see the one page handout available on the table or online at http://www.uoregon.edu/~joe/frontier/
- I'd also be pleased to address any questions you might have, either face-to-face today or by email once Educause is over.
- Thanks for checking out this poster session!