IT Security: What's Our Status Within Higher Education?
Current Issues Roundtable
Wednesday, November 05, 2003
Moderators: Cedric Bennett, Stanford University
Mark Bruhn, Indiana University
Note taker: Valerie Vogel

The 34 attendees discussed three very relevant issues:
1. What are our policies and practices with regard to proactive scanning
2. What are our policies and practices with regard to patch management?
3. What practices are we following to respond to worm attacks?

Proactive Scanning
- Virus scanner that executed automatically at noon (Norton), could last 1 hour or more and individuals couldn’t reconfigure the set time that was pushed out – quit using that scanner.
- Another school had a patch management set for midnight (ZenWorks).
- Mark clarified the difference between Virus and Vulnerability Scanners.
- One school uses Retina and Nessus (uses this more now) – scan campus in 3-4 hours. Looking at question of distributive scanning capability (Lightning by Nessus).
  o Someone recommended the web interface for Nessus.
    ▪ Doesn’t necessarily allow for authenticated distributed scanning.
- Anyone dealt with privacy issues?
  o Difference between privacy and anonymity.
  o If it’s a school computer, their answer is “you’re being scanned.” If they’re going against acceptable use policy, justified in scanning a student’s private machine.
  o SNORT product used (because of price) – a lot of flexibility. Indiana gets 3 reports every morning for various viruses. Setting up automated scans/reports as long as problems remain. Can then attempt to locate machines and isolate from network.
- Home-grown tools being used
  o Univ. of Colorado, Boulder collaborated with Microsoft (machine scanned before connecting to the Internet and sent to subnet to be patched and then checked again before finally set up).
- Automated pre-scan
  o Newly connected connections in residence halls, new MAC addresses, etc. – can redirect to web page.
  o Indiana used UConn Scanner – false positive rate was practically nonexistent. NetReg scanner: plug in machine, goes to scanner before going to registration page, if ok, directed to registration page. If not ok, send them to page with proper patches.
  o ISS and MS scanners had high false positive rates.
  o Used 4 Sun servers – scanned through portal. Tactical way of dealing (address ‘problem of the day’). Used UConn code. Web based authentication.
    ▪ UMBC does something similar. Can scale it if you do it in the background. (As soon s they power up, computers are scanned; network authentication to ResNet).
- Sometimes there isn’t a chance to scan.
- What do you do for faculty machines connecting in classrooms, etc.?
  - MAC address registrations.
  - Re-register wireless?
  - One school cancels them every semester for all students in dorm connected and wireless. (Uses Cisco wireless on campus.)
    - Assuming that once they’re registered, tomorrow they’re ok.
  - UMBC says if you’re faculty and staff, mandating that they’re on the update service to get an Ethernet address.
- Switch from McAfee to Symantec. Desktop firewall rollout – can’t scan a lot of machines. (UT-Austin)

[Most schools here are MS networks. 4-5 are Novell.]
- Some scans time out because firewalls are up, but hard to detect if updates are current.
- Scanning is only a snapshot for that particular moment.
- Hard to hand out ‘run me first’ CDs to thousands of students during first week of school.
- Notre Dame – machines with firewalls were becoming infected. They set up a lab with unpatched machines – when rebooting, there’s downtime where the computers can get infected.
- Indiana has a scanner based on ISS. Web interface to ISS scan engines (4-5 behind this). Admin can go in and select machine they manage scanned one time or scanned automatically, periodically. Person associated with machine gets email every 28 days (e.g.) that says machine has been scanned. Usually says there are no substantial risks. With medium level risks, URLs are provided. Any admin on campus can go to this web space. Can provide IP block and give selected # of days to have it scanned and have report sent to themselves and the person who owns the machine. One step closer to mandating these scans.

Patch Management
- How many require windows updates? UNE images and puts them out. Using Novell, people don’t know how to change it.
- One school can (i.e., has the right to) re-image a PC at any time.
- One person asked if other schools have a problem with security patches or service packs sent out and people’s machines crashing.
  - Policies for security patches can differ from those for service packs.
- ZenWorks used to push out patches to faculty. Effective and successful. Try to spread out over 3 days. Done silently with no notice to user that it’s been patched. Typically suppress reboot.
- ZenWorks, with Norton on the desktop – some people would turn automatic update off. Made it policy to auto and push DAT file.
- Mark mentioned HF NetCheck Pro – Shavlik.
  - Someone attending CSI heard that Symantec trying to purchase Shavlik.
- SUS – anyone using it with great deal of success?
  - Yale uses great deal of SUS servers. Some servers serve 1000s, some serve 20-100. Most students don’t use SUS server.
  - Can have early adopters group on separate server. Then put on main server once tested.
- What about older legacy systems like NT, W9x?
Those weren’t always susceptible, but trying to get rid of those. Bit of
dichotomy right now.
Indiana won’t support anything prior to W2K at the end of 2003.
- Anyone using SMS?
  o One school got hammered using SMS because of Port 135.
- Cross platform patch management?
  o BigFix (Stanford is evaluating it as a technology to support patch
    management. Anyone can download a free client from the vendor site
to look at it.
- Set Windows Update to run as a service? Vulnerabilities will come up at some
  point.

Worm Response
- Everyone did block ports. (Blocked all NetBios ports at UT Austin; Stanford
  and Indiana already had theirs blocked). Got hit badly anyway because of
  high number of vulnerable machines and the worm just “walked in” (carried
  on laptops that initially get hacked while they are outside the perimeter).
- 1433/1444 still blocked on some campuses and people have to request access
to those ports.
- How many have authority to pull the plug, unilaterally decide to block FTP
  traffic. Almost everyone can or someone on campus has that authority.
  o Harvard pulled the plug on email and the press reported it.
- One school put up web site with vulnerable machines every day, with IP
  addresses (no authentication). Someone commented that this provides
  anyone with a list of vulnerable machines – may not be a good idea.
  o Indiana uses authentication, then people can see IP addresses.
- NetReg might provide a little more control – look at more automated answers
  (UT-Austin).
- Did anyone start with everything blocked and opened only when needed?
  o UMBC has people on secure VLAN – then request open VLAN (then
    have to authenticate through VPN for service).
  o Indiana has 25-30k workstations. Don’t need to be visible to the
    outside world – bought firewalls and will build private vs. public
    network. (Will decide later what qualifies as a workstation and what
    doesn’t.)
- Anyone using intrusion prevention products?
  o Too new – need to give them time to mature.
- Running IDS?
  o Some are, in various forms.
- How to monitor students who work for universities or students attacking from
  inside the university? Sometimes system administrators don’t even follow
  their own admin rules (they’ll set the password as “password”, etc.).
- Someone mentioned that IT/security folks should meet monthly with auditors
to review. If they see problems within a department, call the audit team. Can
  be very helpful.