Dealing with Public Ethernet Jacks: Switches, Gateways, and Authentication

Bob Beck
beck@bofh.ucs.ualberta.ca
University of Alberta

The Problem: Public Ethernet Jacks.

- **Public access points to our campus network, Insecure PC (Windows and Macintosh) labs as well as public Ethernet jacks for laptops**
  - **People off the street walk in, then use/abuse.**
  - **Students may use the labs to cause mischief on or off campus.**

- **In the past, to prevent abuse labs weren't routed off our campus. (Internet use by proxy only). Still a source of attacks on campus.**

- **More and more demand for mobile plug-in type access, and other protocols we didn't want to proxy. We needed a better solution.**

What Did We Want?

The same level of control we have with our student access UNIX systems.

- **We already make use of Kerberos (we have about 50,000 User IDs).**
- **Needed a solution to work both with public plug-in access and labs of insecure PC's (win95, win98, Mac).**
- **Wanted something to integrate with the Kerberos IDs we already give out to all students and staff.**
- **Must prevent unauthorized net usage**
- **Must ensure authorized usage can be easily tracked.**
- **Must be relatively secure and attack resistant.**

What We Looked At.

- Windows NT
- Nontransparent Proxies (FWTK etc.)
- Commercial firewall products
- DHCP registration systems

We found nothing that did what we wanted at a price we could afford.

What We Did.

- An authenticating gateway, which when placed in front of a lab forces the user to authenticate before allowing access from their IP address.
- Once authenticated, everything is allowed, (although much is logged). To do this we wrote some custom software for our gateways.
- We ensure our gateways are configured to avoid problems with IP spoofing.
- We use only switched networks with the switches configured appropriately to prevent sniffing and hijacking.

The Switches.

- Our system authenticates a used based on their source IP address.
- To do this in a reasonable manner, we needed a network which was not vulnerable to spoofing or hijacking attempts.
  - MAC-lock switches where possible.
  - Where not possible, ensure they do not broadcast unknown traffic
- Ensure nothing in the lab can talk to the switch.
- Goal: ensure nobody can see anyone else's session

The Gateways

- **Our gateways are built using OpenBSD (version 2.5).**
- **The gateways by default blocks all outgoing traffic from the labs using packet filters (ipf).**
- **Our gateways allow a user to connect and authenticate using their Kerberos ID and password.**
- **On successful authentication the gateway adds rules to allow out all traffic (and log some of it).**
- **As soon as the authenticating session disconnects, the filter rules added above are removed.**

authipf - Our Program For Filter Rules

- **Users connect to gateway with telnet (Why telnet? because they all have it and can use it!)**
- **User authenticates with login, login runs authipf, a program which adds filter rules when started, removes when done.**
- **TCP KEEPALIVE values tuned to ensure that unresponsive sessions go away in under a minute.**
- **authipf logs to syslog when users authenticate, and when they disconnect. It also puts in rules to log tcp sessions.**

Security and Configuration Issues

- To reiterate, switches must be configured properly to avoid traffic snooping and hijacking
  - MAC lock each port or..
  - Turn off unknown unicast flooding.
- We periodically review switch configs to ensure we haven't made mistakes
- Our switches deal with traffic at the MAC level, yet we authenticate based on IP address - this means that there is a potential problem..

IP spoofing

- An attacker can fake a ARP reply, or just try to use an IP address from the lab to get an IP address that is in use in the lab and already authenticated.
- We react to this possibility by having the gateway watch for the occurence of such events. ARP changes are logged by OpenBSD.
- When we see an ARP table change, we use swatch to ensure that if there is a running authipf process for that address, it gets killed.
- This ensures that if an IP address is taken over, it is no longer authenticated, and must reauthenticate
- We also get notified when this happens.

Other Issues

- Students can walk away.
  - We deal with this in our traditional way of dealing with the "Oh gee, you left yourself logged on" cases.
- Users must know how to telnet to the gateway and authenticate. We put big posters everywhere, and icons on the desktops in the labs of machines.
- This does not address the (in)security of the client machines due to what is running on them.
  - The laptop is the users problem.
  - Labs of machines reload an image regularly on boot to minimize trojan/virus exposure (and warn users in big letters)

Other Nice Stuff

- **Gateway intercepts IDENT (rfc 1413) requests aimed at inside hosts. answers them with the authenticated user.**
- **We intercept and proxy IMAP and SMTP outbound to our main central servers which use the same id and passwords. These proxies then substitute in the username/password for those connections with the one used to authenticate.**
- **We don't regularly proxy http on the gateways, but have the capability to do it when tracking problems (at our site we watch http requests elsewhere)**

Well, Does it work?

- Deployed in front of student residences and over 30 labs and laptop areas at University of Alberta. More all the time.
- Students rapidly became used to how it works. very little user training necessary.
- Other on campus departments now less fearful of connections from public labs (some used to block them entirely!)
- No more off-street people showing up to abuse labs (It's not interesting if they have no Internet connection). Places without this installed are now requesting it.
- Time to identify the user responsible for harrasing e-mail from these locations via hotmail is down to about 60 seconds. (other stuff quick to find too) This saves *lots* of work.

Possible Future Enhancements

- ssh
- netbios
- More proxies
- Support for more/different authentication mechanisms (YP, LDAP, etc.)

Dealing with Public Ethernet Jacks: Switches, Gateways, and Authentication

- ftp://sunsite.ualberta.ca/pub/Local/People/beck/authipf
- http://www.ualberta.ca/~beck/lisa99.ps

Bob Beck
beck@bofh.ucs.ualberta.ca
University of Alberta