IAB - Bad Traffic Workshop
Session 7

Gregory M. Lebovitz

2006.03.09

gregory.ietf@gmail.com

What Problems are Most Important?

Stateful Inspection Firewalling (SIF) becoming irrelevant

- L 3 / 4 inspection not enough for access control anymore
  - Everything-over-HTTP
  - Lots of apps preferring TLS, SSH tunnels
  - Apps that hop ports until find an opening (e.g. Skype, Kazaa, etc.)
  - GRE / IP-in-IP
  - v6-in-v4, v4-in-v6, ESP-null encryption (MSFT NAP method)

… SIF irrelevance (cont.)

- IPv6
  - Does away with NAT, Link local and global only
  - People do not want their network mapped; accustomed to topology hiding
- Rise of TLS/SSH tunneling / encpasulation
  - Admin's can't discern what is transitting the perimeter
  - Encrypted VoIP signaling leaves SIF blind to negotiated Media ports

Responses to SIF irrelevance

- Deepened Parsing for “true” flow classification
- Increased use of application proxies
  - HTTP, TLS, SSH
  - VoIP Session Border Controllers
  - IPv6 “Proxies” for all externally destined traffic, and any inbound traffic

Mobility

- Users come from everywhere
  - Office location
  - Wireless in someone else's office
  - Conference room network
  - Hand held
  - Home
  - Kiosk at airport or hotel business center
- Access Control Policies based on IP address decrease in pertinence
- User-to-Locality binding issue
  - Need better, standard, ubiquitous infrastructure for this
- Network Authentication not seamless enough
  - Too much user interaction needed
  - Hard for Apps to succeed during L2 transitions
  - How will we do WiMAX hand-offs from LAN to wireless carrier efficiently if we need two-factor authentication and 6 configuration steps to gain access to the wireless network

Pipeline Stuff

Layer 5-7 Awareness

- Not enough to detect SOAP, need to figure out what application is calling / receiving data, what structures they are allowed, etc. OASIS
- Multi-layer, hierarchical classification engines
  - What is the app in the HTTP on port 3465?
  - It's GRE, but what is IN the GRE?
- MS-RPC – UIDs (a DLL or other Function), each UID has multiple functions, exploits w/in the function's data structure
- VoIP, IP-TV, etc: Watch every control channel message for changes.

Increase the Speed: behavioral analysis

- [Bryan] Detect by behavioral analysis of headers
  - Pretty reliable detection methods
  - Feasible @ in 100s Gbps
  - w/in 5 years will be able to do near Tbps speed
- Lock down worms pretty quickly
- Over time, can develop a library to “spot” very specific actions by their statistical pattern, not actual observation of the payload data
  - FTP login in an encrypted channel
  - Key strokes
  - Email programs in TLS
  - Etc.

Move Security into the (Enterprise) Core

- Traditionally hard, crunchy outside security principle. But strategies focusing on hardening up the hosts, and their access to LAN
- NAC / NAP / UAC / TCG
- Moving security more into the core of the LAN. Focuses:
  - Host integrity – clean up the attaching host, automate
  - Network access rights – control who can get on, and once on, where they can reach, at L2 and L3
- Ability to capture ID for a User-to-Locality binding that can then be used by other policy-enforcing elements in the network

Move to the core

- Machines/users need to auth to get frames/packets to move
  - Works for user desktops
  - Test machines? Printers? Services/servers?

Access Control based on User instead of IP

- People write policies around Users, not IP addresses
- Things that help us create user/current-locality bindings are good
- Find way to quickly access and leverage the binding for multiple arenas of policy enforcement

Fragments?

- One method for buffer overflow attacks
- Is there a useful reason for them anymore?
- Becoming standard practice to drop them if originating from the LAN
- Still valid and in use on WANs? Is bandwidth high enough that no longer needed?
- Should we move to deprecate?

BCP type tools

- Not IETF “BCP” necessarily, but tips, tricks, sample deployments
- For point products
- For “areas” of network. Examples:
  - Secure “Guest” network provisioning wless/wlan
  - Secure Internet Perimeter for Enterprise
  - Secure NOC perimeter

“Secure” Coding

- Boundary & parameter checking
- Force user constraints to inputs
- Automation of tools for checking this stuff
  - Bunch of tools maturing; need developers to use them
  - Lic? Certification of secure coding processes?
- QA for Abnormal use, instead of functional QA
- Etc…

Conclusion

- New era of flow/app classification
- Trend toward proxies
- Identity / Locality distinguishers & binding
- Usability & How To’s

Appendix

Prepared, but not presented

Problems

Speed is an Issue

- Network price performance increasing faster than deeper-parsing technology
- No quantum leaps needed in detection methods, at present.
- Problem is speed. Getting that deep into the payload costs.
- Disintegration of the “fast path”
- Branch sites – not an issue
- HQ, DataCenter, ISP networks - issue

Human Vulnerability

- Server attacks are lowering
- Host attacks rising; Trick users into loading bad software
- Human vulnerability threat
  - Phishing
  - Email worms
  - No underlying vulnerability; people just too trusting
  - Trust agencies getting lax

Authentication

- Needs to be bi-directional
  - User auth'ing to company
  - Company auth'ing to user
  - TLS not cutting it
    - eBay.com , where "Y" is a valid IDN int'l character that is rendered same as an ASCII character
    - Creditunion.net (instead of .com) with fully registered SSL license, and site not discernable from the real credit union.
      - http://isc.sans.org/diary.php?storyid=1118

Pipeline

DoS Protection: Fighting Spoofed packets

- BCPs on Spoof-prevention - BCP38
  - No reason a spoof packet should ever make it past the first PE router upstream of the sending host, even if multi-homed BGP used by the site
  - Hand-slapping consequences if caught?
- The “trusted” IP address range of the provider’s infrastructure should not be very hard for an attacker to obtain
- Filtering on all edge, customer-facing interfaces would solve a TON; right thing to do. Yet providers resist!
  - Filter source addresses at ingress
    - Only properly situated sources allowed
    - Deny internal loopback address sources on all externally-facing interfaces
  - Filter destination addresses at ingress points
  - Issues:
    - Many edge routers cannot perform while routing
    - Intensive to implement and keep updated

DoS Protection

- Distributed Network Response to DoS
  - Coordinated detection
  - Back-tracing
  - Rapid policy installation to blackhole and/or honey-pot attacking traffic
  - Find and terminate access for CNC
- Makes DDoS harder
  - Bad guys'll focus on other methods, but at least we win one battle
  - Looks like this is already done.