What is Actively Being Researched?

Vern Paxson, Stefan Savage, Helen J. Wang

IAB Workshop on Unwanted Traffic

Two orthogonal dimensions

- What is addressed?
  - Hosts being exploited
    (scans, worms, viruses, etc)
  - Individual applications
    (DDoS, SPAM, phishing, spyware, etc)
- Where is being addressed?
  - Hosts
  - Networks

Exploit Traffic I

- **Prevention**
  - Testing/Model checking automation
  - StackGuard, ASLR, ISR, program shepherding (Usenix Security 02), control flow integrity
  - Off by default! (HotNets 05), separate client/server address space (Handley, et al FDNA 04)
- **Detection**
  - Scan detection (TRW)
  - Network telescopes/blackhole monitors (random traffic)
  - Honeypots/Honeyfams (GQ/Roleplayer, Potemkin, Collapsar, vGround)
  - HoneyMonkey

Exploit Traffic II

- **Defense**
  - Automated attack signatures (Earlybird, Autograph, Honeycomb)
  - Known vulnerability filters (Shield, Browsershield, Symantec GEB)
  - Automated vulnerability signatures (Vigilante, Sting, DACODA)
  - Connection rate limiting

IDS/IPS improvements

- Whole conference on this: RAID
- Performance
  - High-speed normalization
  - High-speed exact and approx match
- Ongoing anomaly/ detection improvements
  - Behavior context
  - On-line code analysis in network
- Exfiltration

Application DDoS

- Challenge: DDoS and flash crowd hard to distinguish
- Detect and filter zombie requests
  - CAPTCHA
    - Botz-4-sale (NSDI 2005)
  - BINDER (Usenix 2005)
- Alternatively: more capacity via caching
  - Akamai, Coral

Network DDoS

- Infer application-unwanted traffic
  - Packet Symmetry (IMC04, HotNets 05)
  - Dynamic source address validation
- TTL-based filtering
- Community tagging (nets using src valid)
- Traceback
- Pushback
- Traceback with filtering (Pi)
- Capability-based transmission (SIFF)

Overlay-based evasion/filtering

- Hide true endpoints
- Traffic enters overlay via ingress
  - Can have lightweight authentication
  - Overlay nodes tag pkts
- Makes it easy to filter non-legit traffic
- SOS, Mayday

Network: Bandwidth Attacks

- First goal: defeat low cost DDoS attacks where a single compromised machine sends many DoS messages
- Deadlock (Greenhalgh, et al SRUTI 05)
  - No source address spoofing because of no filtering mechanism
  - Little deployment of ingress filtering because of no source address spoofing
  - No automated filtering because attacks could source-address spoof to bypass it
- Greenhalgh et al SRUTI 05
  - Server-net filtering mechanism using routing/tunneling assuming no source spoofing
- Internet Accountability (Simon et al 06 under submission)
  - Ingress filtering among “good” ISPs, others’ traffic marked with “evil” bit with worse treatment during peak traffic
  - Filtering infrastructure

Spyware

- Crawler-based & passive measurement
- Taint analysis to automatically determine what info is leaked
  - How does input related to output?

Forensic Aids

- What caused this and what else did it do?
  - Backtracker
- Origin tracking via side-effects
  - Witty
- Backtracking over stepping stones
  - Time, dynamics, content correlation

- Blue sky: Packet attribution
  - Physical origin tagged on each pkt, normal observer can't interpret but **can** tell if its valid

Measurement/Analysis

- Measurements
  - Telescope/blackhole: backscatter (DoS), worms
  - Passive monitors: bots, spyware
  - Honeypots: worms, scans, bots
  - Crawlers: spyware, malware (honeymonkey)
  - SPAM sinkholes
- Netflow improvements
  - Scale, performance, specificity
- Automated Protocol Classification
  - Network analysis without port numbers
  - Trained vs untrained, content vs behavioral

Infrastructure

- Securing BGP
  - We understand there is work being done here
- Secure forwarding
  - Secure TR, Listen/Whisper, Fatih

Aside: What we do for the bad guy?

- Anonymity
  - Onion routing & Mix networks (Tor, etc)
- Distributed C&C
  - DHTs, gossip protocols
- Faster worm design
- Mimicry/obfuscation
- Automated exploit discovery

Where do we or could we help?

- The research community is ignorant and fickle, and tremendously insecure
  - However, **huge** amounts of creative horsepower
  - Largely being wasted (e.g., 100s of traceback papers)
- Tremendously easy to direct
  - Two knobs: money & “fame”
- Key issue is communication
  - A little data goes a long way (BGP example)
  - Problem definition: broad enough to be exciting, but narrow enough to not go off the deep end
  - Communicate reason for constraints
- Only need to convince a handful
  - Herd mentality; public blessing is key

Issues for IAB/IETF/IESG/IRTF

- Protocol design issues
  - Design Guidelines for Robust Internet Protocols
  - Be conservative in what you believe
  - Problems with “loose” specifications/implementaions
- Protocol analysis languages
  - E.g. vulnerability filter specification
- If you want to influence researchers
  - Problems & whisper in NSF’s ear