Cyber crime

PC World: Web of Crime
August 22, 2005

“We were getting a lot of panic attacks from our customers saying they were under attack and they were being held for ransom and could we help them,” Quintana says. Proxix, a company founded in 2003 that protects businesses against DDoS attacks, repels at least one major version every week, according to chief technical officer Barrett Lyon. Of those, slightly less than half involve one business attacking a competitor, as happened to Expert Satellite, he says. Most of the rest are extortion attempts, where a criminal may threaten a DDoS attack unless a company pays protection money (as much as $250,000). Very few attacks occur without financial motivation, Lyon says.
Cyber crime

- Botnets

Internet attacks

- Mapping
  - Analysis of target domain
    - Network topology
    - Contact information
  - Tools
    - Ping, traceroute
    - Port scanners

- Packet sniffing
  - Ethernet interface in promiscuous mode

- Spoofing
  - Forging of IP source address
  - Actual sender hard to identify

- End-system intrusion
  - Exploit software vulnerabilities to gain access
  - Steal data or control system to launch attacks
Internet attacks

- Denial of service (DoS) attack
  - SYN flooding
    » TCP state exhaustion
  - Smurf attack
    » ICMP echo request converge on single host
  - Distributed DoS (DDoS) attacks
    » Large number of hosts attack single node
    » Much better scalability of attack

- Hijacking of connections
  - Eavesdrop on connection state
  - DoS attack on one side
  - Spoof towards other side

Firewalls

- Forwarding if connection established from inside
  - Firewall keeps connection state
  - Binary decision
Intrusion Detection Systems

- IDS checks packet content

Diagrams:
- Internal network architecture
- Application gateway
- Internet

- De-facto standard: snort
  - Tool for scanning
  - Set of rules

- Snort rule example
  ```plaintext
  alert tcp any any -> any 80 (content: "cgi-bin/php"; offset:4; depth:20;)
  ```
  - IP addresses and port numbers from packet header
  - Content rules require payload scanning

- Payload scanning
  - Translation of rules (regular expressions) into automata
  - Automata can become large depending on type of rule

- Example
  - Automaton to detect "ECE" or "IEEE" or "ICE"
    - Alphabet \{C,E,I\}
Payload scanning

- Complex state machine even for simple expressions

- Implementation
  - Ideal for specialized hardware
    - Custom ASIC
    - FPGA
  - Many extensions for special cases

- Probabilistic methods
  - Possible false positives in initial scan
  - Careful scan of packets with potential detections

- Firewalls and IDS are provide first level of defenses
  - How can protocols provide security (in the broadest sense)?
Secure communication

- What are the properties of secure communication?
  - Confidentiality
    - Content is hidden
  - Authentication
    - Source is verified
  - Message integrity and non-repudiation
    - Message is unchanged and undeniable
  - Availability and access control
    - Legitimate users should have access
  - Examples in the Internet?

Assignments

- Read
  - Kurose & Ross: Chapter 8
- SPARK
  - Assessment quiz