Networking Review

CS461 / ECE422 – UIUC Spring 2016

Simon Kim

Topics

- Networking Basics (Lecture 15)
- Attacks (Lecture 16, 17, 20)
  - Sniffing
  - IP Spoofing
  - DDoS
  - Worms (Lecture 20)
  - Botnets (Lecture 20)
- Defense (Lecture 18)
  - Firewall
  - IDS
  - SSL, IPsec
  - VPN
  - 802.11 Security
- Anonymity (Lecture 19)
- MP4
  - Traffic analysis
  - Capturing in monitor mode

Networking Basics

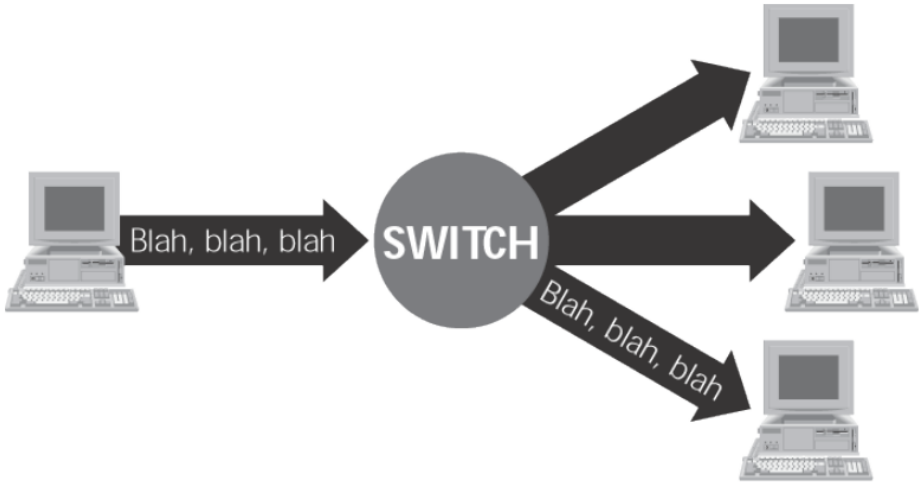
- OSI Layer
- TCP/UDP
- Packet Encapsulation
- Network interface – promiscuous vs monitor
- MAC and IP addresses
- CIDR (Classless Inter-Domain Routing) – subnets
  - E.g. 192.168.100.1/24
- NAT (Network Address Translation) – between internal (private) address and external (public) address

Attacks

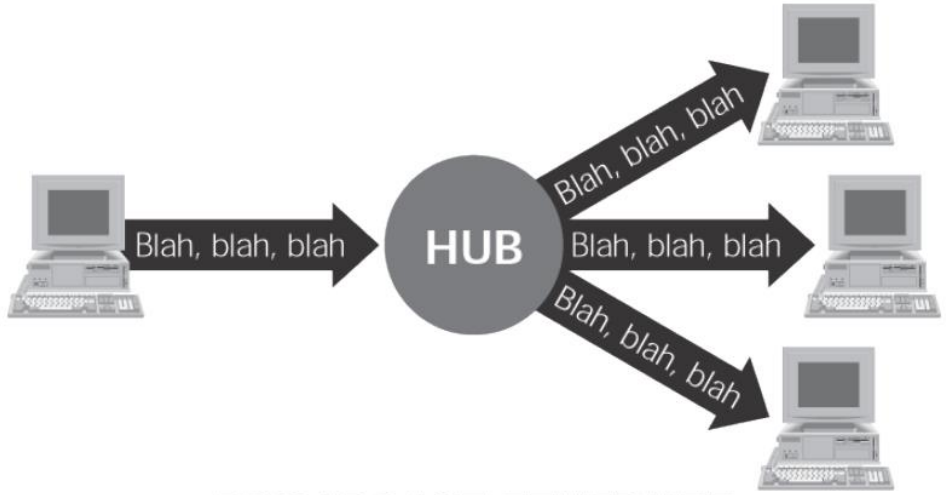
- Possible at all layers of the network
  - Data-link
  - Network
  - Transport
  - Application
- Compromises all 3 security properties
  - Confidentiality (e.g. sniffing, eavesdropping)
  - Integrity (e.g. spoofing, content forgeries, MITM)
  - Availability (e.g. denial-of-service)

Attacks – Sniffing

- Active – packets from a local network built with a switch
- Passive – packets from a local network built with a hub or a wireless network



Active



Passive

Attacks – Sniffing (cont.)

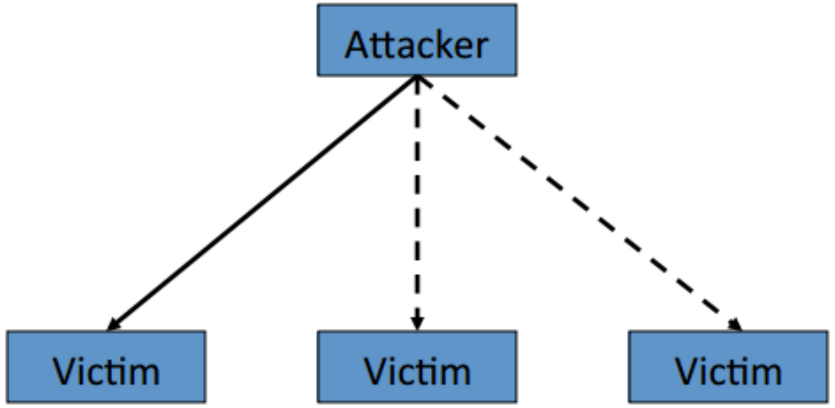
- Active Sniffing
  - Need to fool the switch in order to intercept the packets
  - MAC flooding – fill up switch's memory with random MAC addresses
  - ARP spoofing – change victim's ARP table
    - ARP – no authentication

Attacks – IP Spoofing

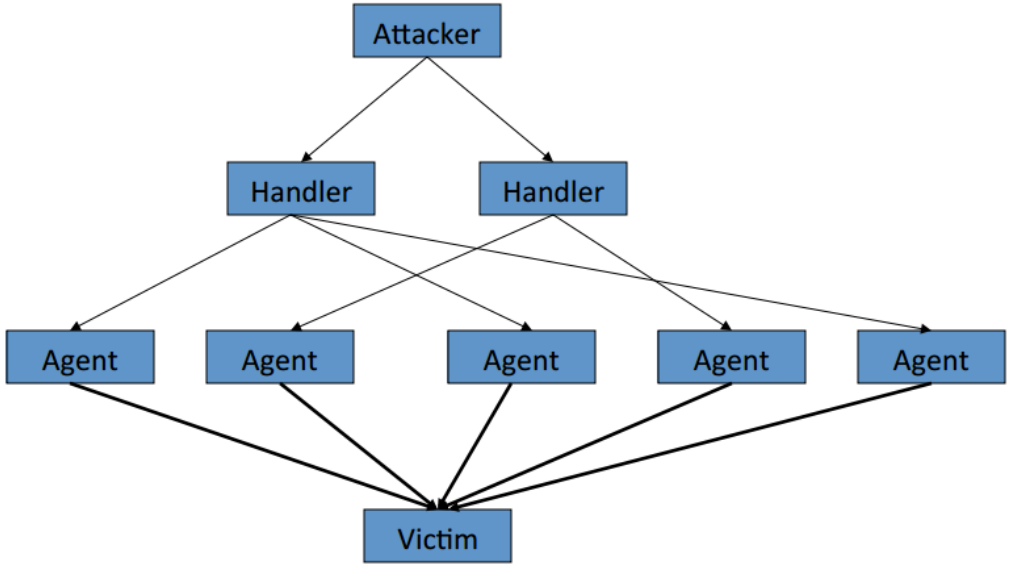
- IP spoofing – faking the source IP address to the target's
- Blind spoofing – attack from any source
- Non-blind spoofing – attack from the same subnet
- Common usage
  - Denial-of-Service
  - TCP Session hijacking – Lecture 16 slide 22-26
  - Man in the Middle

Attacks – DDoS

- Distributed Denial of Service – attack against availability
  - Consume target's computing and network resources (e.g. fork bomb, fill disk, flooding)
  - Make service unavailable (e.g. crash or exploit system/service)



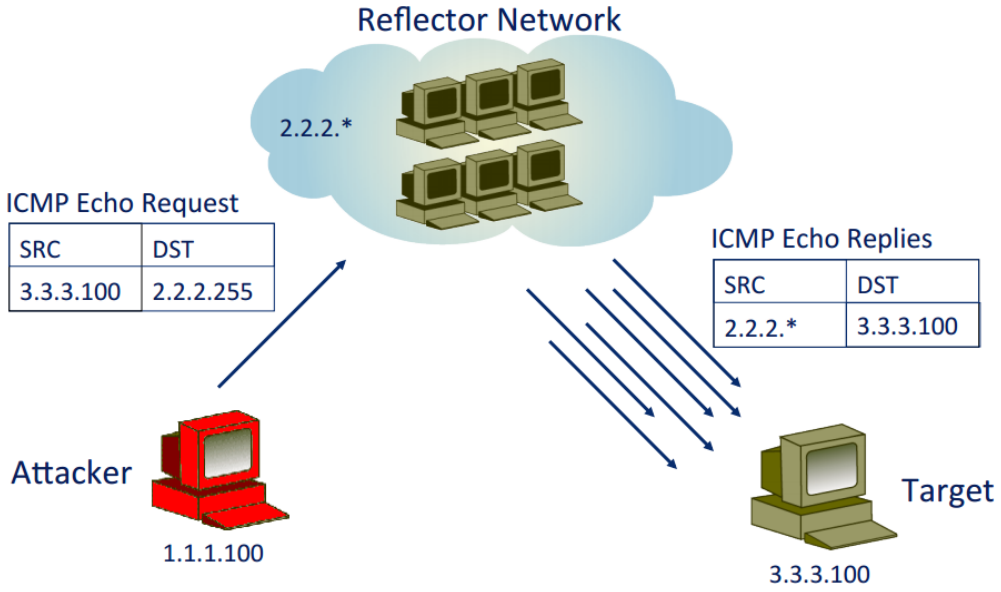
Simple DoS



Distributed DoS

Attacks – DDoS (cont.)

- Amplified DDoS attack – small request, large response
  - Often relies on properties of several UDP-based protocols
    - Spoofability
    - Broad deployment
    - Large response to small request
  - NTP DDoS – using NTP protocol special diagnostic modes (6 or 7)
- Blind spoofing – e.g. TCP SYN flood



Blind spoofing

Attacks – DNS

- DNS hijacking – change the IP associated with a server
- DNS spoofing – DNS response is easily spoofed
- DNS Cache poisoning – give DNS servers false records

Attacks – Worms (Lecture 20)

- *Self-replicates, spreads* through the network
- vs Virus, Trojan horse
  - Virus and Trojan horse rely on human intervention
- Can be used to:
  - Launch DDoS attacks (install bot networks) - availability
  - Access sensitive information – confidentiality
  - Corrupt the sensitive information - integrity

Attacks – Worms (cont.)

- Propagation
  - Scanning – chooses random address
  - Coordinated scanning – different instances scan different addresses
  - Flash – propagate along pre-assembled tree of targets
  - Meta-server – ask server for vulnerable target
  - Topological – use information from infected
  - Contagion – propagate along with normal communication

Attacks – Botnet (Lecture 20)

- Bot – a servant process on a compromised system
  - Installed by Trojans or worms
- Botnet – a network of compromised hosts (i.e. bots, controllers)
- Provides
  - Anonymity
  - Powerful delivery platform
- Lifecycle
  - Propagation – infection
  - Communication – command and control
  - Attack – i.e. DDoS

Attacks – Botnet (cont.)

- Application level
  - Emails
  - Webpage contents
  - SNS (social engineering)

Defense – Firewall

- Controls incoming and outgoing network traffic
- Incoming
  - DDoS attack – e.g. SYN flooding
  - Unauthorized access
- Outgoing
  - Bandwidth control
  - Internet usage – e.g. games, pornography, SNS
  - Privacy
- Types
  - Application level
  - Packet-filtering

Defense – Firewall (cont.)

Simple firewall policy configuration

Source	Dest	App	Action
any-inside	dmz-mail	SMTP	allow
any-inside	any-outside	SMTP	drop
any-inside	any-outside	HTTP	allow
any-inside	any-outside	FTP	allow
any-inside	any-outside	any	drop
any-outside	any-inside	any	drop

Defense - IDS

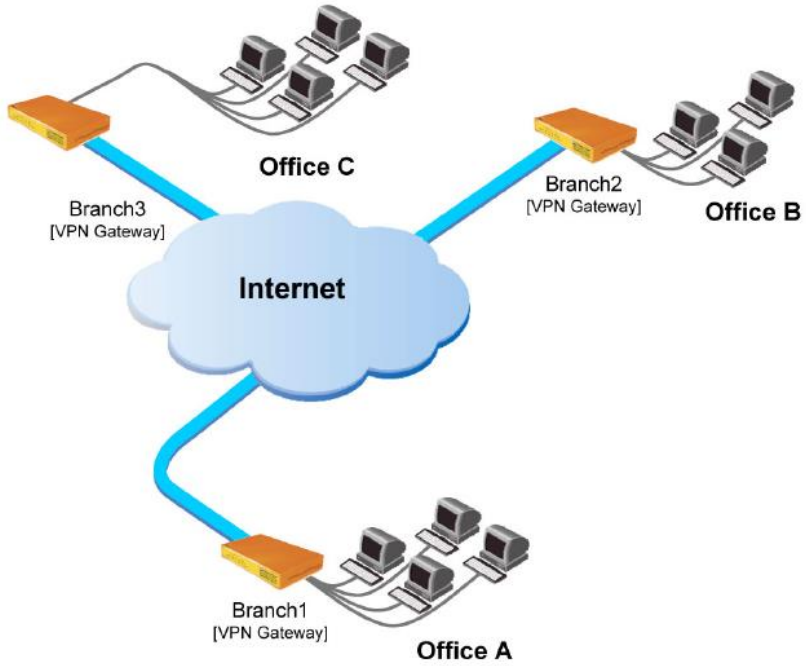
- IDS – intrusion detection system
  - Alerts when anomalies detected
  - Post-hoc
- Misuse Detection – defines what is abnormal using attack signatures
  - Rule-based – requires prior knowledge on attacks
  - Less false-positives
- Anomaly Detection – defines what is normal using profiles
  - Statistical analysis on typical traffic flow

Defense – SSL, IPsec

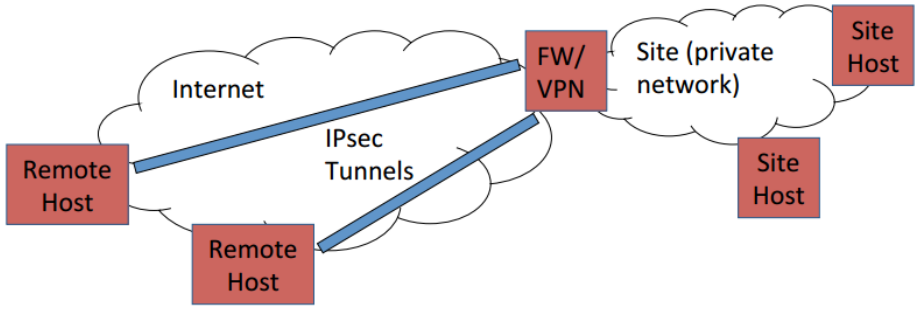
- SSL – Lecture 18 slide 21-22
  - Transport layer security to TCP-based applications
- IPsec – Lecture 18 slide 23-25
  - Network layer security
  - More complex
  - Difficult to define and maintain
  - More suitable for site-to-site VPN

Defense – VPN

- VPN – Virtual Private Network
- IP (site-to-site) VPN
- End-to-end VPN
  - Connect remote hosts to a firewalled network (e.g. vpn.cites.illinois.edu)
  - https://answers.uillinois.edu/illinois/47667



Site-to-site VPN



End-to-end VPN

Source: http://sysnetnotes.blogspot.in/2015/06/vpn-basics-site-to-site-vpn-and-remote.html

Defense – 802.11 Security

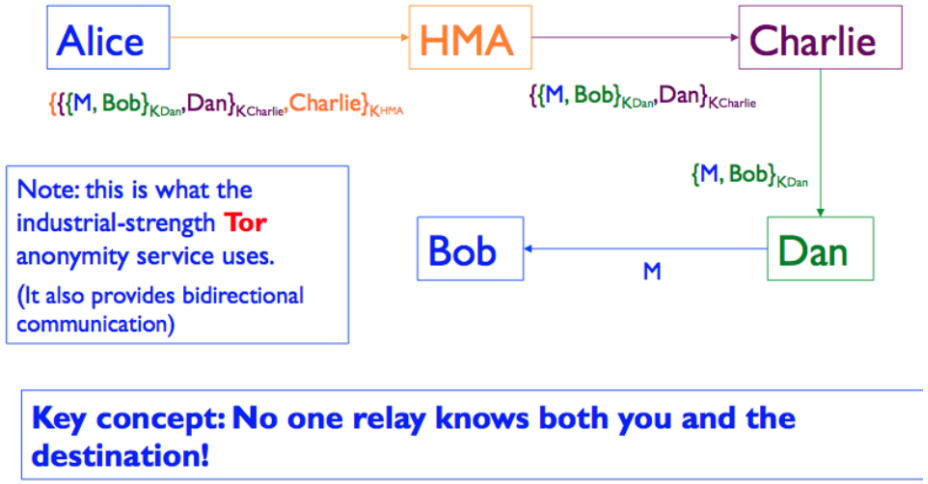
- WEP (Wired Equivalent Privacy)
  - insecure, broken
  - (Lecture 18 slide 27-29)
- 802.11i
  - WPA (WiFi-Protected Access) – draft 802.11i standard (2003)
  - WPA2 – full 802.11i standard (2004)

Anonymity

- Anonymity – concealing your *identity* (not contents)
  - In communications, concealing the identity of source and/or destination
- Nymity Spectrum
  - Verinymity – credit card #s, driver's license, address
  - Pseudonymity – pen names, many blogs
  - Linkable anonymity – loyalty cards, prepaid mobile phone
  - Unlinkable anonymity – paying in cash, Tor

Anonymity (cont.)

- How?
  - Proxy – intermediary that relays traffic
  - VPN
    - https://www.bestvpn.com/blog/4085/proxies-vs-vpn-whats-the-difference/
  - Tor
    - Onion routing
    - Does not provide end-to-end encryption (use HTTPS!)
    - https://www.torproject.org/docs/faq.html.en
    - Attacks/defense – slide 50-52



Lecture 19 slide 43

Other relevant topics

- Desirable communication properties
  - Forward secrecy
  - Deniability
- Off-the-record
  - Message confidentiality
  - Authentication
  - Perfect forward secrecy
  - Deniability

MP4

- Traffic analysis
  - Active vs. Passive FTP
  - Other common network activities
    - e.g. gateway (router), DNS, DHCP, HTTP/HTTPS
  - Port scanning
    - e.g. TCP SYN scanning
- Capturing in monitor mode
  - Wireless network terms
  - Purpose of each Aircrack-ng Suite tool used for the MP