University of Calgary – CPSC 329
Guest Lecture: Carey Williamson

Network Security

Agenda

- What is “network security”?
- Types of attacks
- Real-world examples
- Wrapup and questions

What is "network security"?

- The field of network security is about:
  - how the "bad guys" attack computer networks (or users)
  - how the "good guys" defend networks against attacks
  - how to design architectures that are immune to attacks

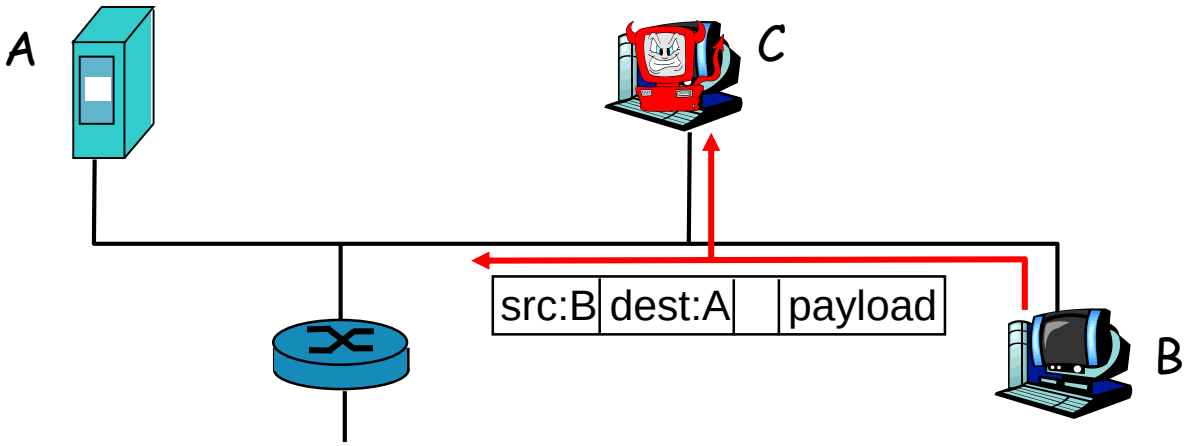
- Note that the Internet was not originally designed with (much) security in mind…
  - *original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers have been playing "catch-up" by trying to add security features to existing protocols
  - Security considerations are needed in all protocol layers!

Common Types of Attacks

- Packet sniffing (to steal confidential personal information)
- Spoofing (to forge identity, location, or other credentials)
- Playback (to record and replay valid credentials later)
- Scanning (to actively probe for vulnerable hosts or ports)
- Malware (malicious software, to exploit vulnerabilities)
- DoS: Denial of Service (to make a service inaccessibly slow)
- DDoS: Distributed DoS (like DoS on steroids, using botnets)
- Inference attacks (to learn implicit structural information)

Packet Sniffing

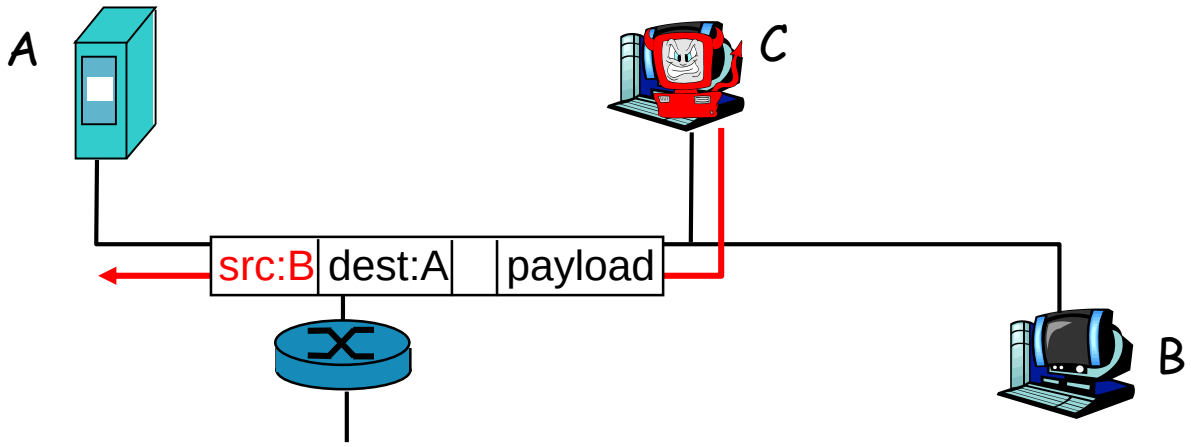
- The bad guys can observe packets on a LAN
  - shared broadcast media (classic Ethernet, WiFi hotspots)
  - promiscuous network interface can read and record the contents (including passwords!) of all transmitted packets



Wireshark software is an example of a "packet sniffer"

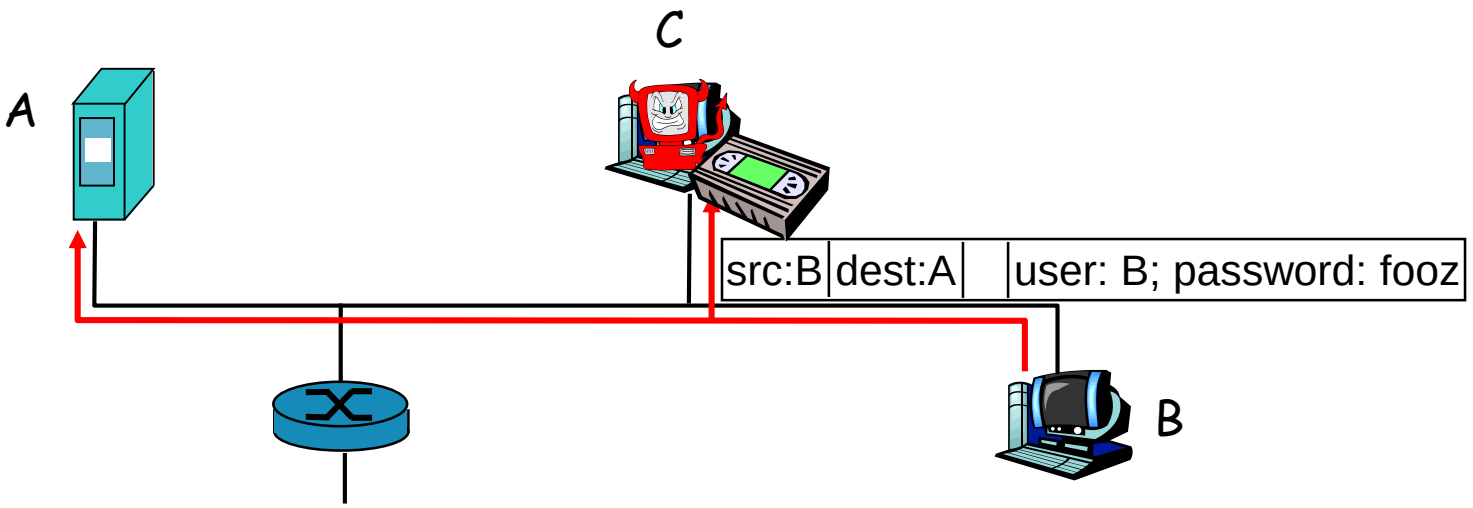
IP Spoofing

- The bad guys can use false source addresses
  - *IP spoofing:* send packet with false source address



Playback

- The bad guys can record/playback packets
  - sniff sensitive info (e.g., password), and use later
    - password holder *is* the legit user from system point of view



Malware

- Malware can get in host from a virus, worm, or trojan horse.
- Spyware malware can record keystrokes, web sites visited, upload info to collection site.
- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.
- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Types of Malware

- Trojan horse
  - Hidden part of some otherwise useful software
  - Today often on a Web page (Active-X, plugin)
- Virus
  - infection by receiving object (e.g., e-mail attachment), actively executing
  - self-replicating: propagate itself to other hosts, users
- Worm:
  - infection by passively receiving object that gets itself executed
  - self- replicating: propagates to other hosts, users

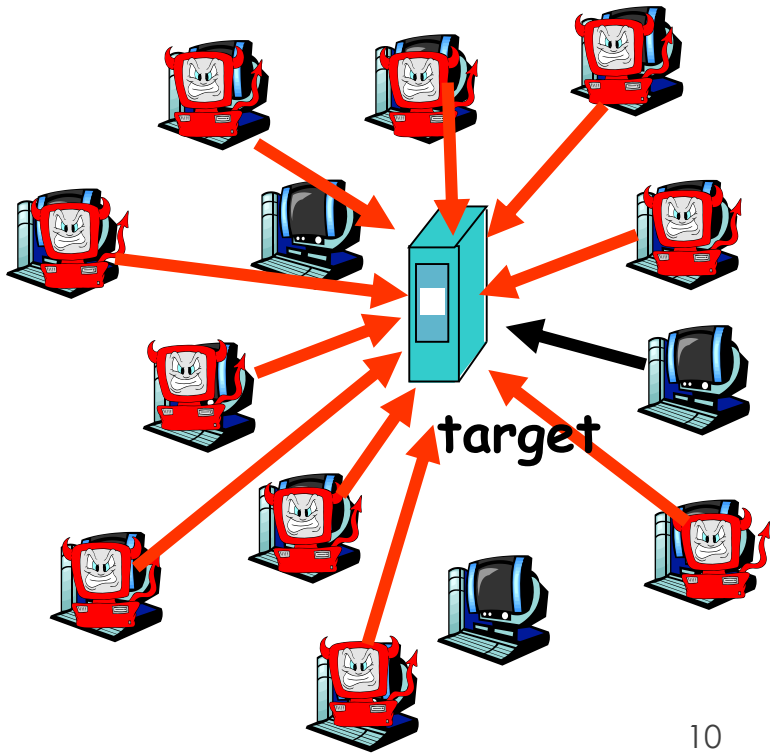
Denial of Service (DoS)

- Bad guys can attack servers and network infrastructure
  - Denial of service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target

2. break into hosts around the network to create a "botnet"

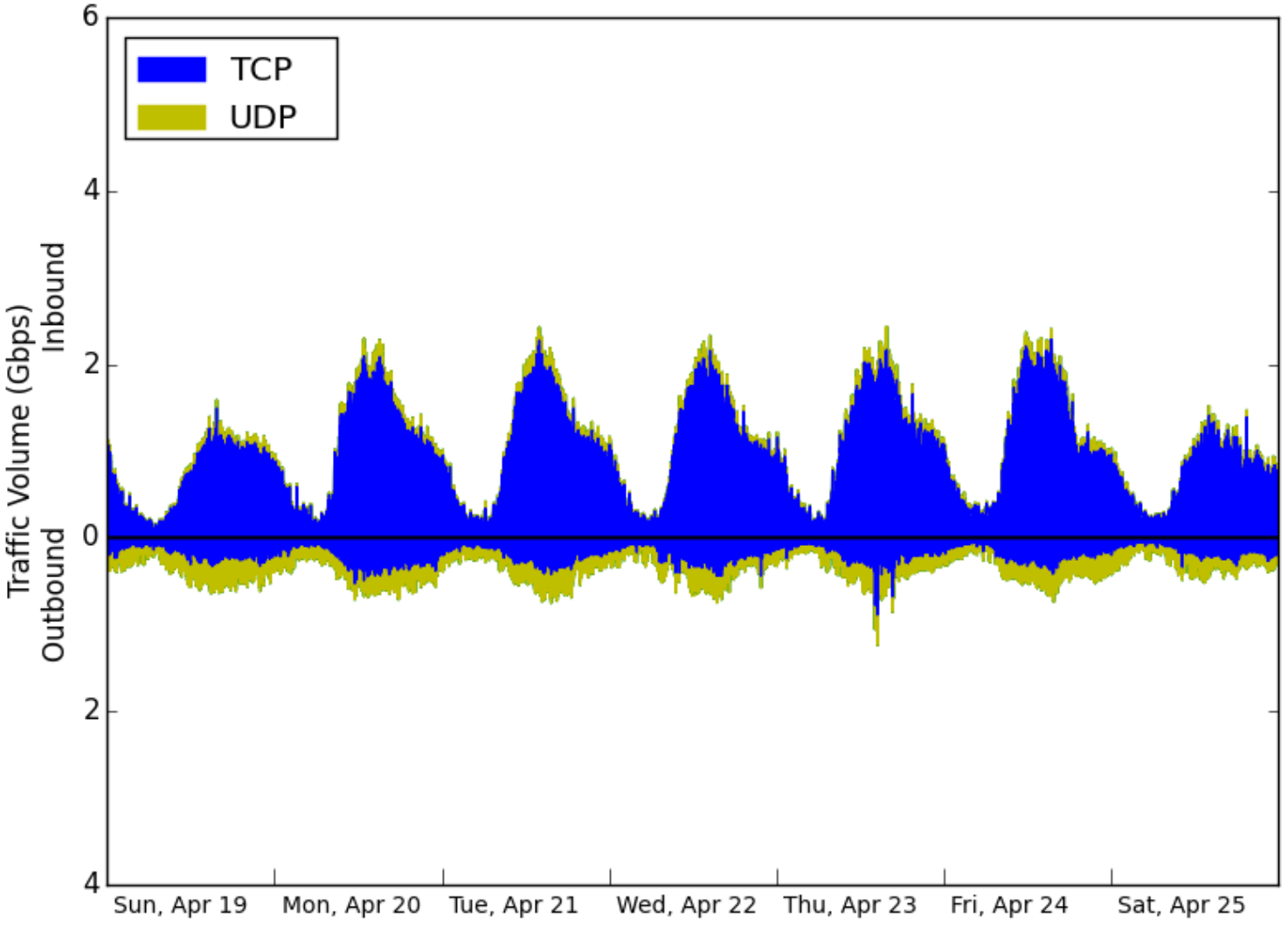
3. send packets toward target from compromised hosts



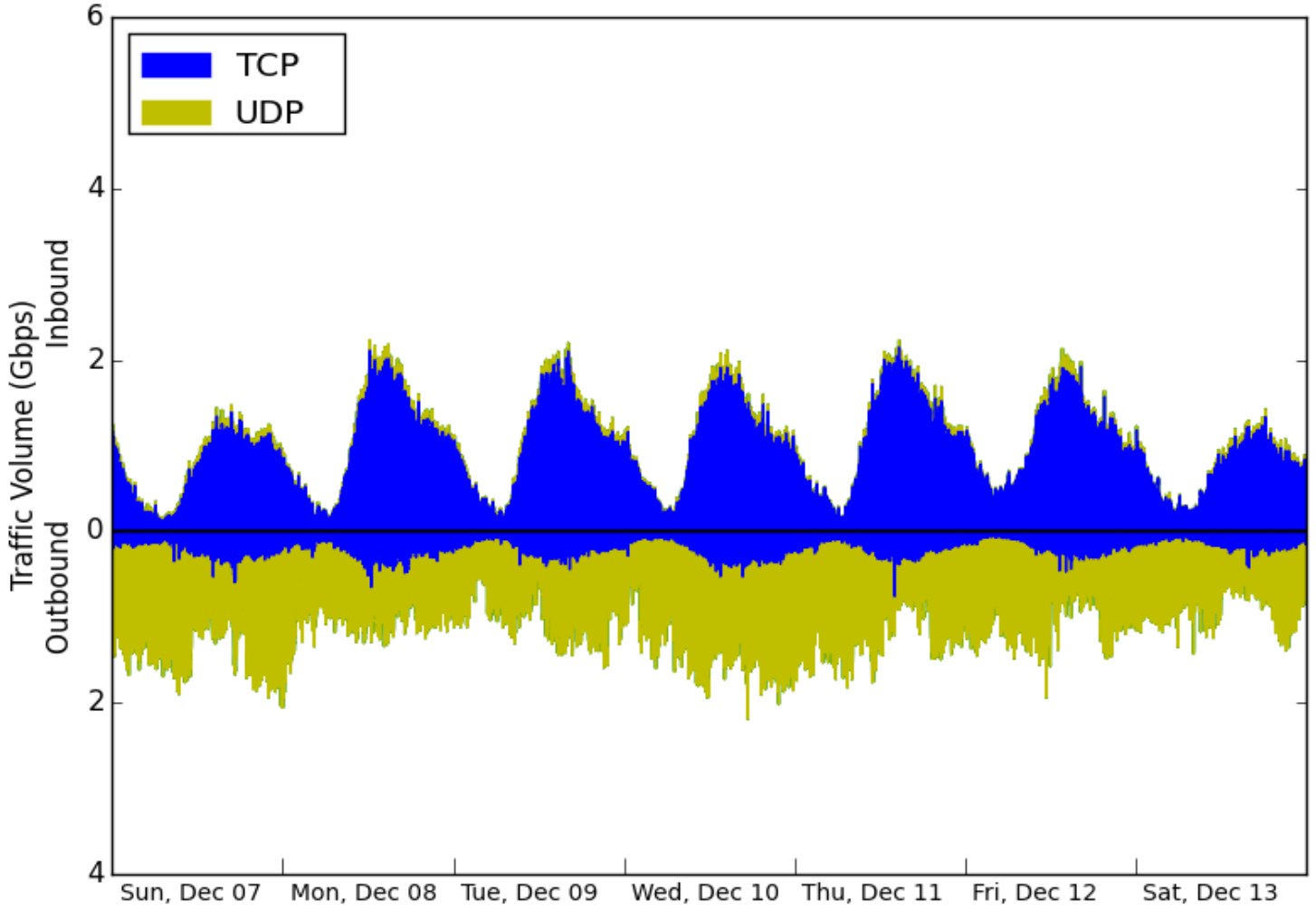
U of C Traffic Examples

- As a networking researcher, I have seen many strange and mysterious things on the U of C network, including these:
- Port scanning
- NTP amplification attacks 
- RIP attacks
- Viruses/malware 
- SSH attacks
- DoS attacks
- Spam bots 

Normal U of C Traffic (Apr 2015)



NTP Amplification Attack (Dec 2014)



Heavy Hitters

Outbound Traffic Totals for February 2016

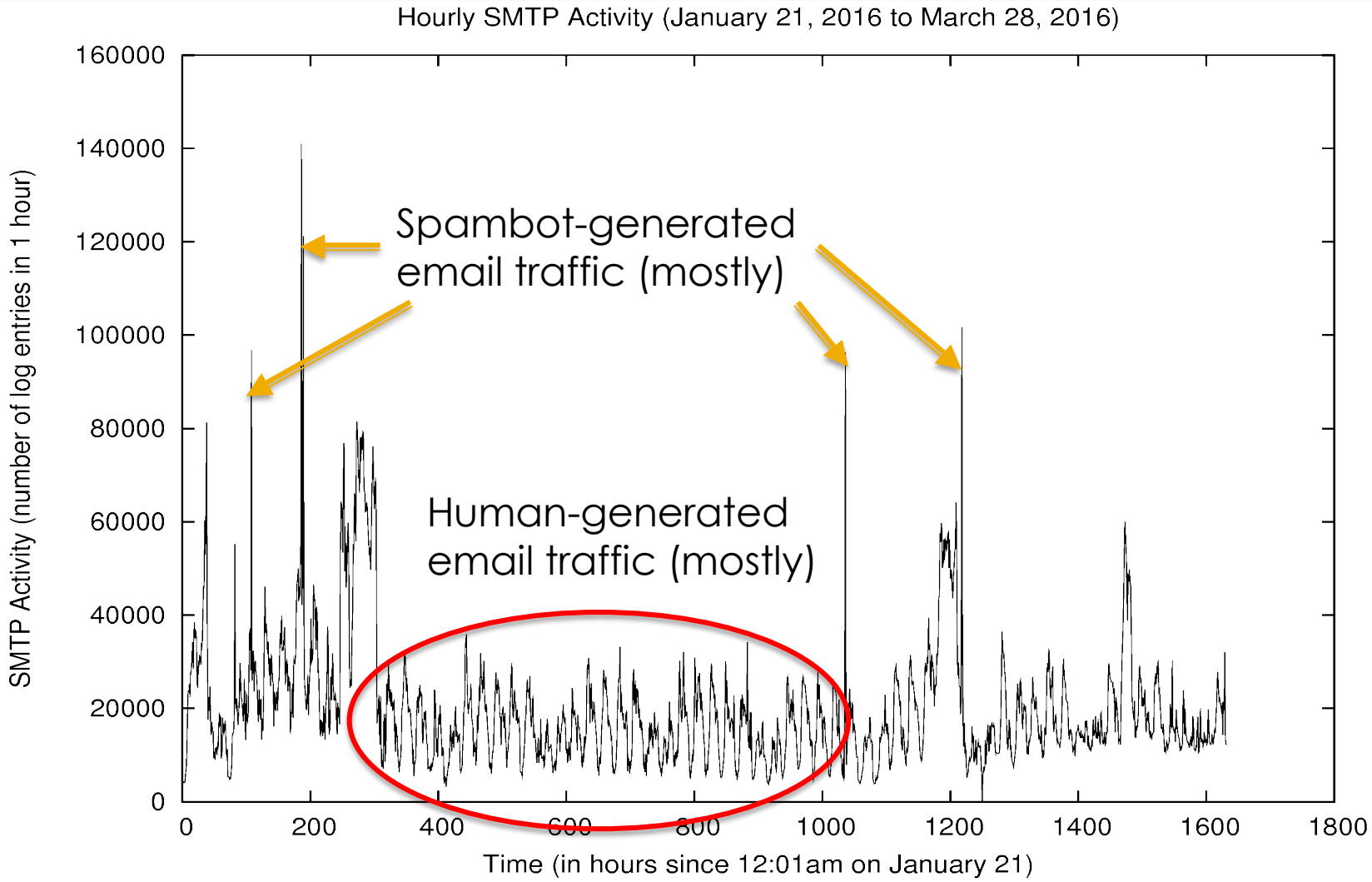
#	IP	Name	Protocol	Port	Service	Volume	Issue?
1	518.90		UDP	123	NTP	9.8 TB	Yes
2	334.148	rb1-s	UDP	53	DNS	6.5 TB	
3	334.130	rb1	UDP	53	DNS	2.9 TB	
4	649.196	gvpn	TCP	10433	VPN	2.9 TB	
5	951.98	aurora	TCP	80	HTTP	2.8 TB	
6	742.7	ns4-a	UDP	53	DNS	2.3 TB	
7	742.5	ns2-a	UDP	53	DNS	2.1 TB	
8	906.25	www	TCP	80	HTTP	1.7 TB	
9	819.141		TCP	443	HTTPS	1.5 TB	Maybe
10	742.6	ns3-a	UDP	53	DNS	1.5 TB	

Possible Malware Activity

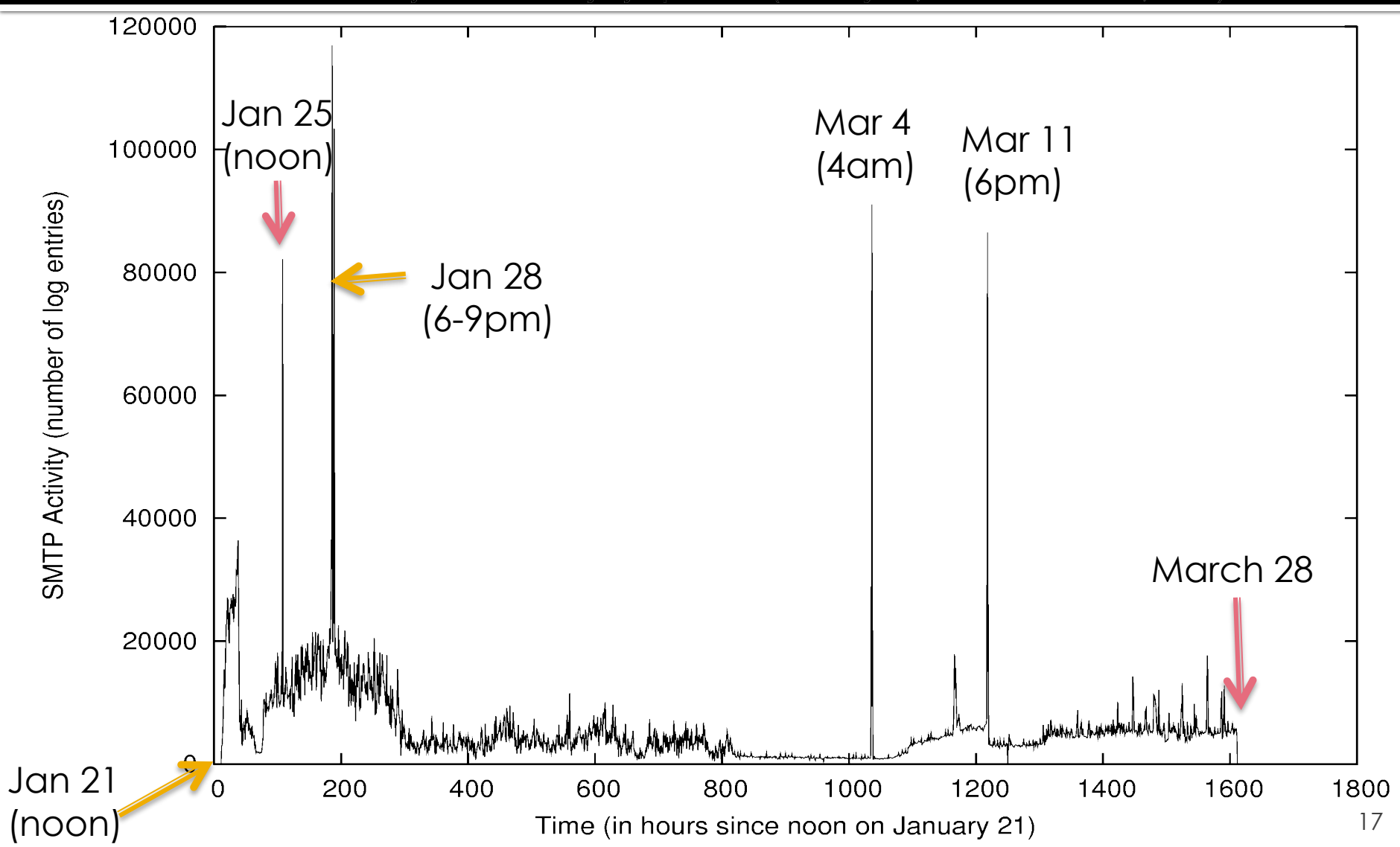
Connection Counts for January 2016

#	IP	Name	Protocol	Port	Service	Conns	Issue?
1	293.8	pc8	UDP	665		908 M	Yes
2	293.9	pc9	UDP	665		778 M	Yes
3	293.7	pc7	UDP	665		702 M	Yes
4	293.8	pc8	UDP	655		538 M	Yes
5	293.9	pc9	UDP	655		502 M	Yes
6	529.230	pc230	UDP	137	NetBios	476 M	Yes
7	293.7	pc7	UDP	655		469 M	Yes
8	518.90		UDP	123	NTP	324 M	Yes
9	334.148	rb1-s	UDP	53	DNS	261 M	Maybe
10	334.51	nassrv3	UDP	520	RIP	240 M	Maybe

SMTP (email) Traffic Activity



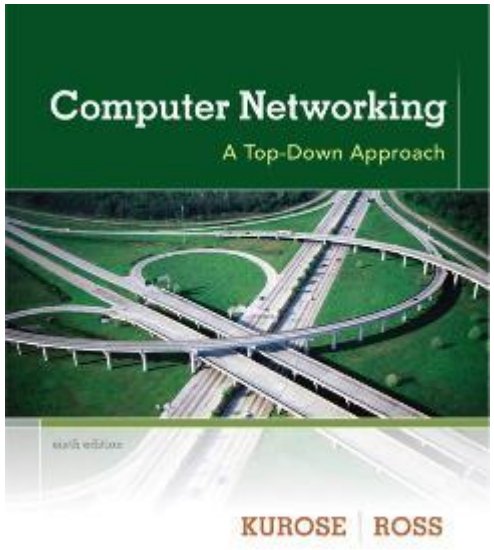
Spam Bot Activity



Curious for more?

- Take CPSC 441: **Computer Networks**
  - Learn about the Internet and its protocol stack
- Take CPSC 526: **Network Systems Security**
  - Course Description: "Attacks on networked systems, tools and techniques for detection and protection against attacks including firewalls and intrusion detection and protection systems, authentication and identification in distributed systems, cryptographic protocols for IP networks, security protocols for emerging networks and technologies, privacy enhancing communication. Legal and ethical issues will be introduced."

Some of these slides are courtesy of:



Computer Networking:
A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012