Assymetric Cyber Warfare

Prof. Paul A. Strassmann
George Mason University
October 13, 2009

Outline

Part I: Internet Basics

Part II: User Attacks

Part III: Attacks on Switches

Part IV: Attacks on Routers

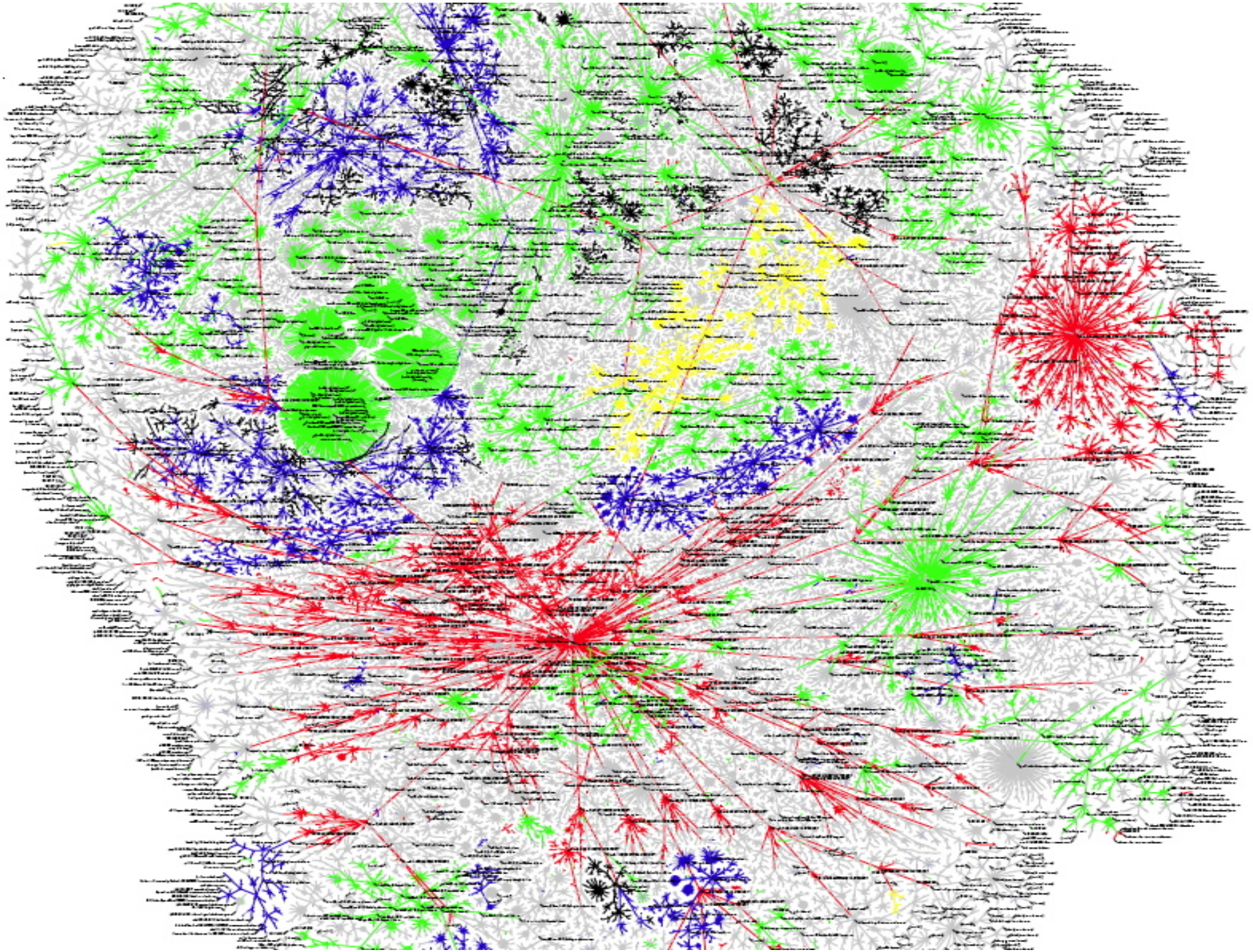
Part V: Attacks on Domain Names

Summary

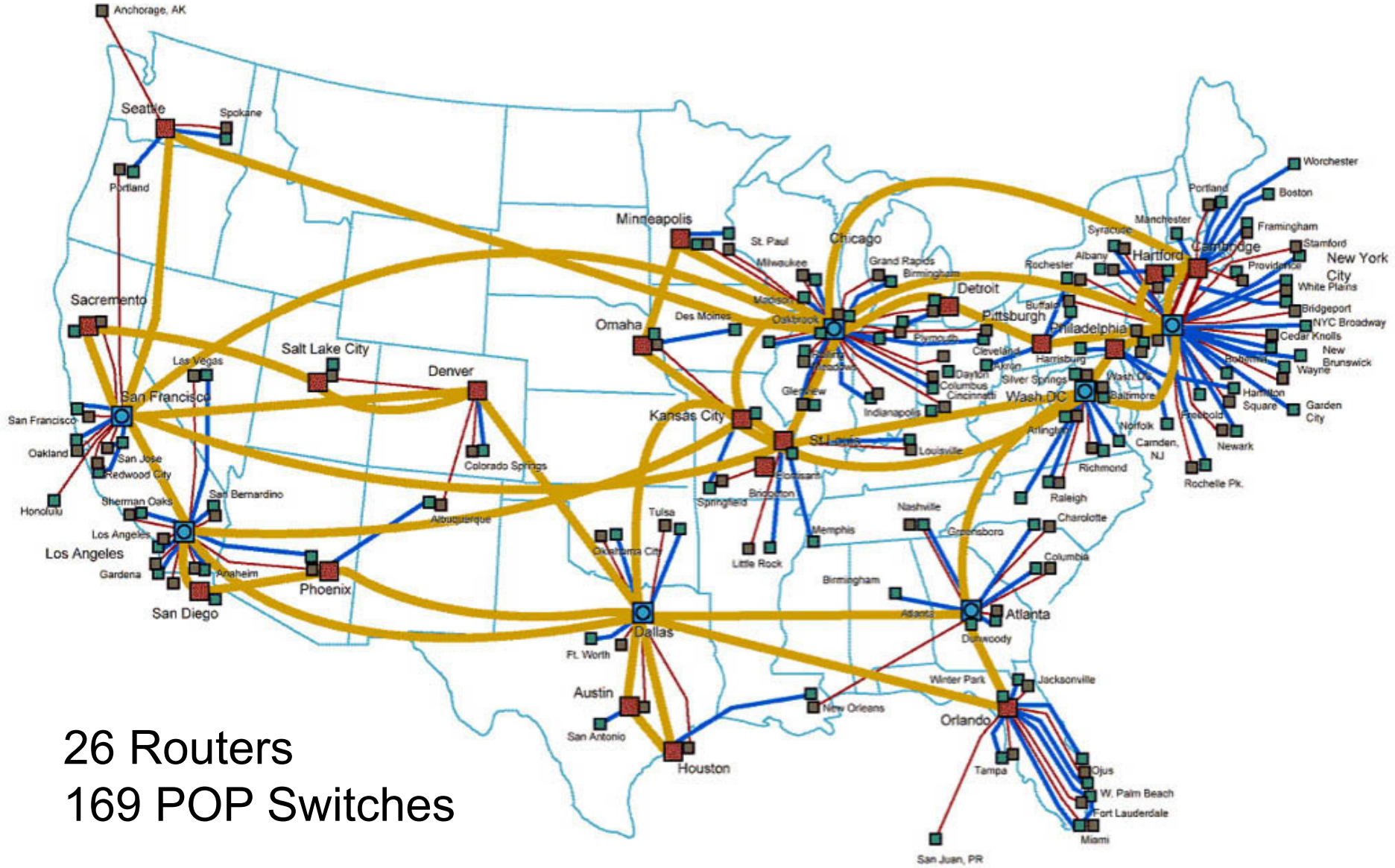
Internet Statistics (June 2009)

- 1.6 billion global Internet users
- 252 million Internet users in North America.
- 74% of North American population are Internet users.
- 200,000+ links between ISP's and the Internet

- Two billion Google web searcher/day
- Internet attacks from China are 28% of all attacks.



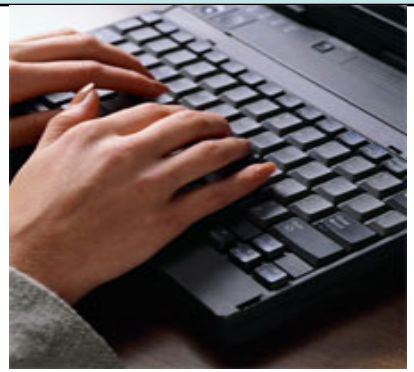
Example: AT&T Internet Service Provider's Network (USA)_



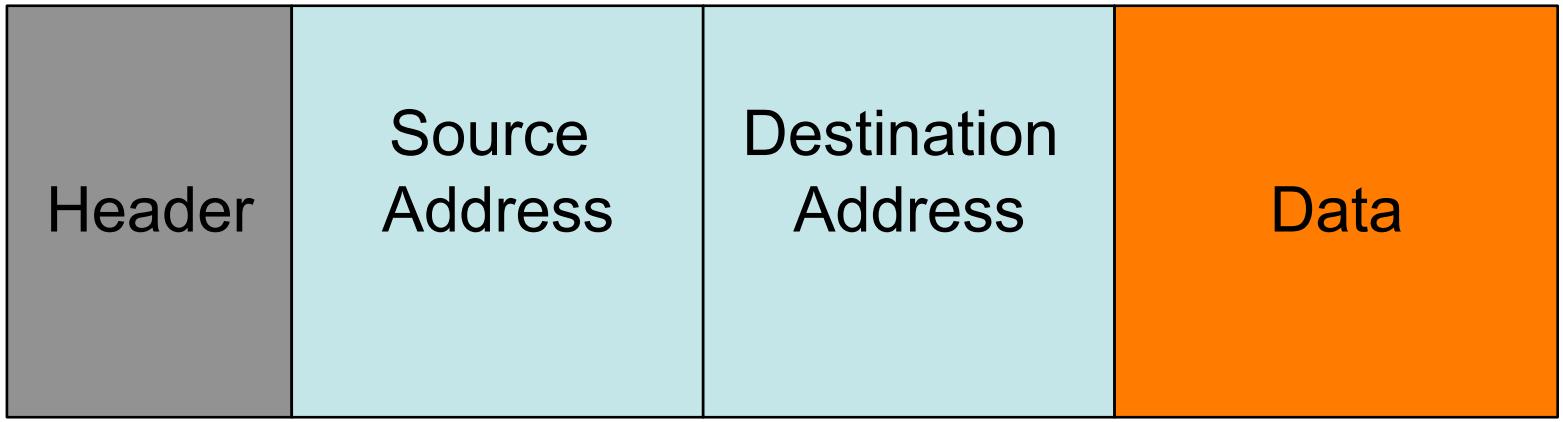
26 Routers
169 POP Switches

How Internet is Organized

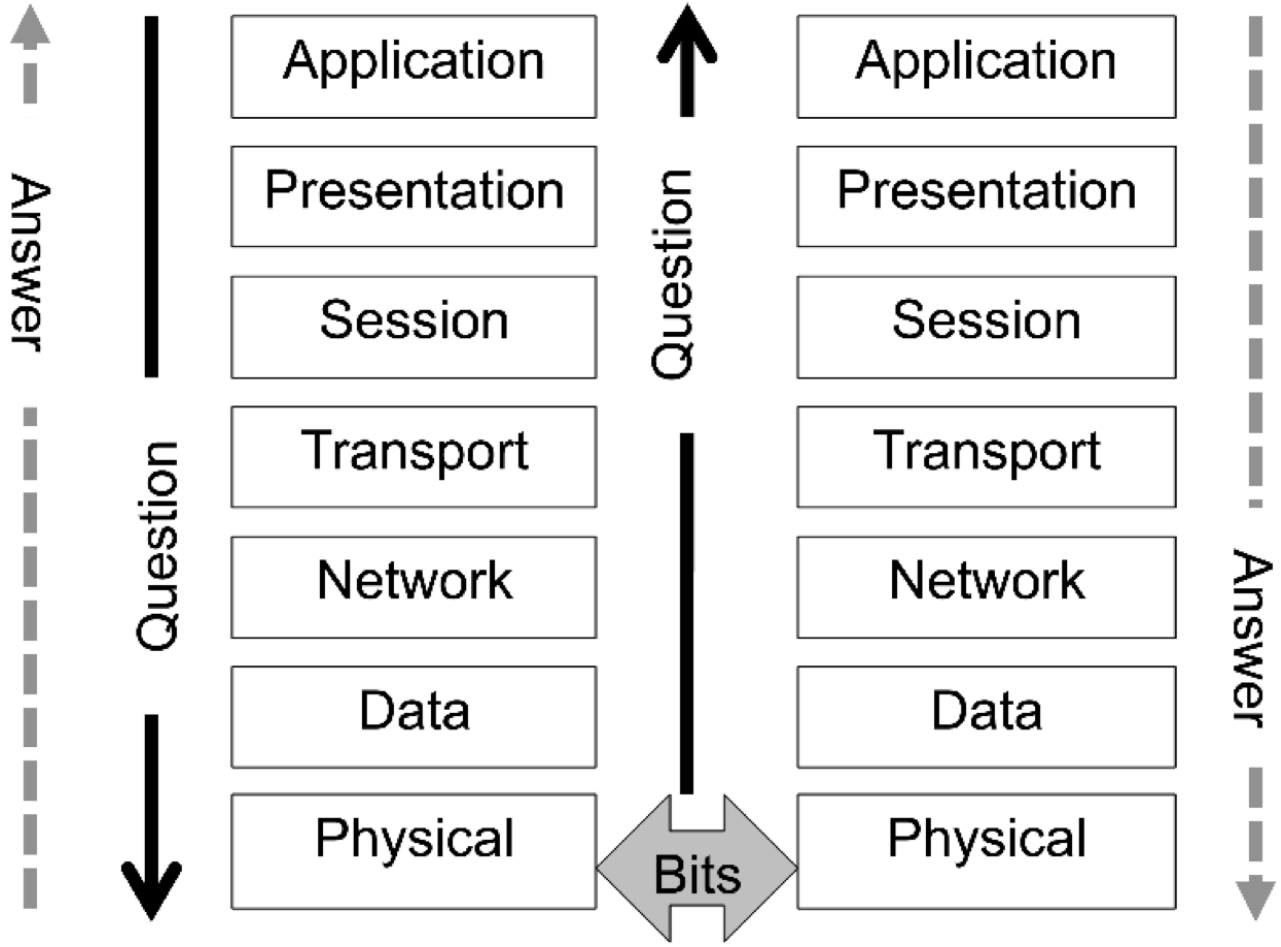
Backbone Connections	9.6 Gb/sec
Internet Service Providers	622 Mb/sec
Points of Service	52 Mb/sec
Wide Area Networks	20 Mb/sec
Local Area Networks	5 Mb/sec



All Internet Transmissions via "Packets"



All Packets Traverse Open System Interconnection Layers



All Internet Transmissions are in "Hops" (Elapsed time 6 seconds)

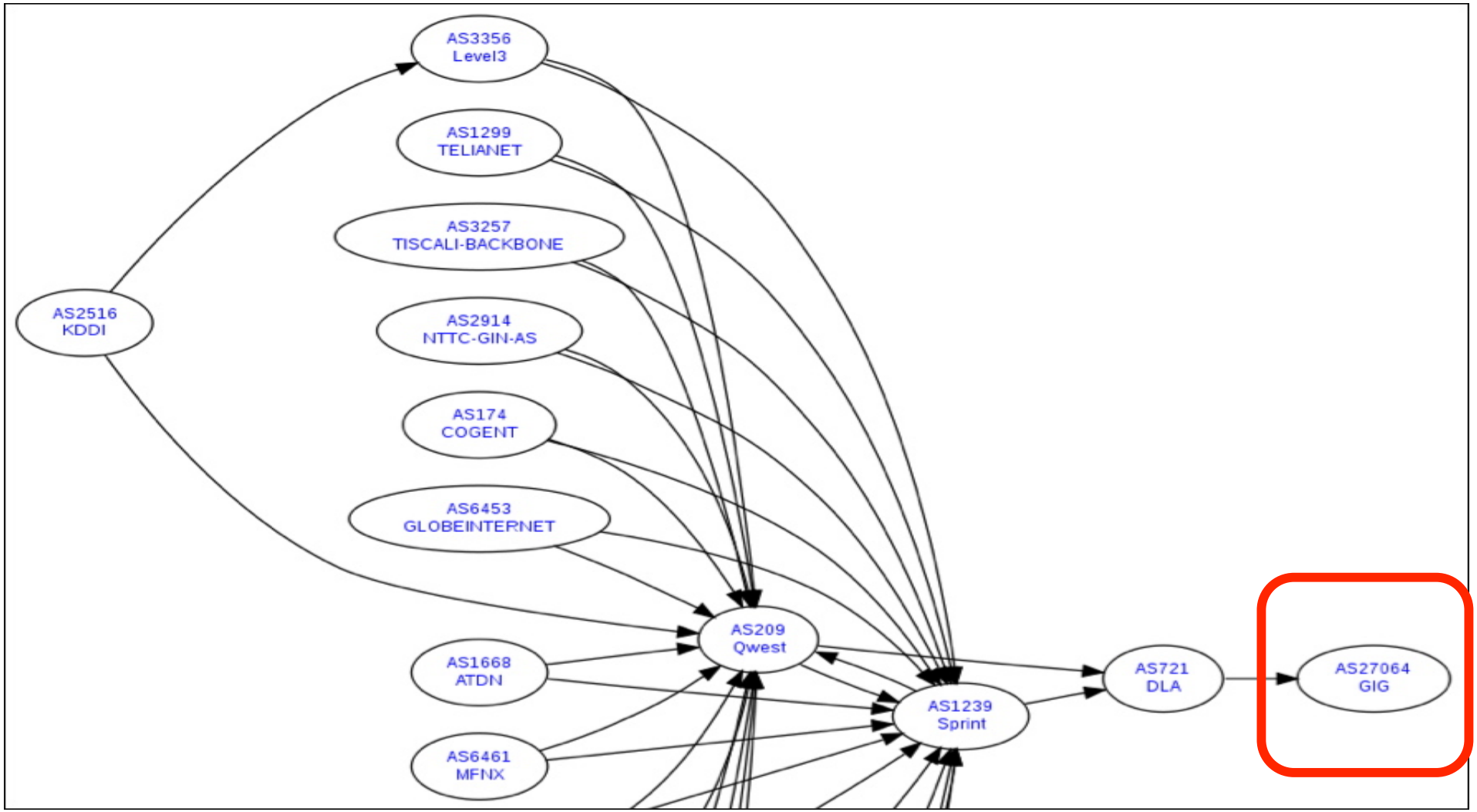
From: jtmessert@optonline.net 7 Dec 2008 15:05:39

1. Received: from 48151 invoked from network
2. Received: from localhost (localhost [127.0.0.1])
3. Received: from rn-out-0910.google.com
4. Received: by rn-out-0910.google.com
5. Received: by 10.100.255.10
6. Received: by 10.100.124.12
7. Received: by 10.65.53.19
8. Received: from qs1473.pair.com
9. Received: from localhost [127.0.0.1]
10. Received: from mta3.srv.hcvlny.cv.net
11. Received: from [10.240.3.210]

Forwarded-To: paul@strassmann.com 7 Dec 2008 15:05:45

Above message = 29 "packets"

Connections to and from the Global Information Grid (GIG)



Part II

Part I: Internet Basics

Part II: User Attacks

Part III: Attacks on Switches

Part IV: Attacks on Routers

Part V: Attacks on Domain Names

Summary

New Trojan Viruses

- Generic Packed.c!29595758b285 07/24/2009
- Backdoor-DZP!b13e8317ce76 07/24/2009
- Downloader-BPJ!8d0c2b001a6d 07/24/2009
- Backdoor-DZP!3e294099cc63 07/24/2009
- PWCrack-Winspy!d0623f353f1f 07/24/2009
- Generic.dx!92676e1876bf 07/24/2009
- Generic FakeAlert!htm 07/24/2009
- Generic PWS.y!ea5cb29986ea 07/24/2009
- FakeAlert-DI!7eb610c60513 07/24/2009
- Downloader-BRW!9953f6b81173 07/24/2009

List of Botnets

Top Botnets on 07/22/2009	Millions of Compromised US Computes	Function
Zeus	3.6	Steals user names, passwords, account numbers and credit card numbers.
Koobface	2.9	Take control over the entire computer
TidServe	1.5	Techniques to run inside the root of Windows
Trojan.Fakeavalert	1.4	Downloads other malware
TR/Dldr.Agent.JKH	1.2	Posts encrypted data to its command-and-control domains and receives instruction.
Monkif	0.52	Downloads adware
Hamweq	0.48	Worm makes copies of itself to distribute information from the compromised system

New Microsoft Security Vulnerabilities

- Office Web Components ActiveX Code Execution Vulnerability 07/13/2009
- Cumulative Security Update of ActiveX Kill Bits 07/14/2009
- DirectShow Video ActiveX Control Vulnerability 07/04/2009
- DirectShow DirectX Size Validation Vulnerability 07/14/2009
- DirectShow DirectX Pointer Validation Vulnerability 07/14/2009
- Virtual PC and Virtual Server Privileged Instruction Decoding Vulnerability 07/14/2009

About Attacks on Desktops, Laptops and Smart Phones

- Inadequate protection from anti-virus software;
- Inadequate protection provided by firewalls.

- Damage is local (LAN's, WAN's).
- Damage is limited and temporary.

- Cyber warfare attacks the Internet infrastructure.

Part III

Part I: Internet Basics

Part II: User Attacks

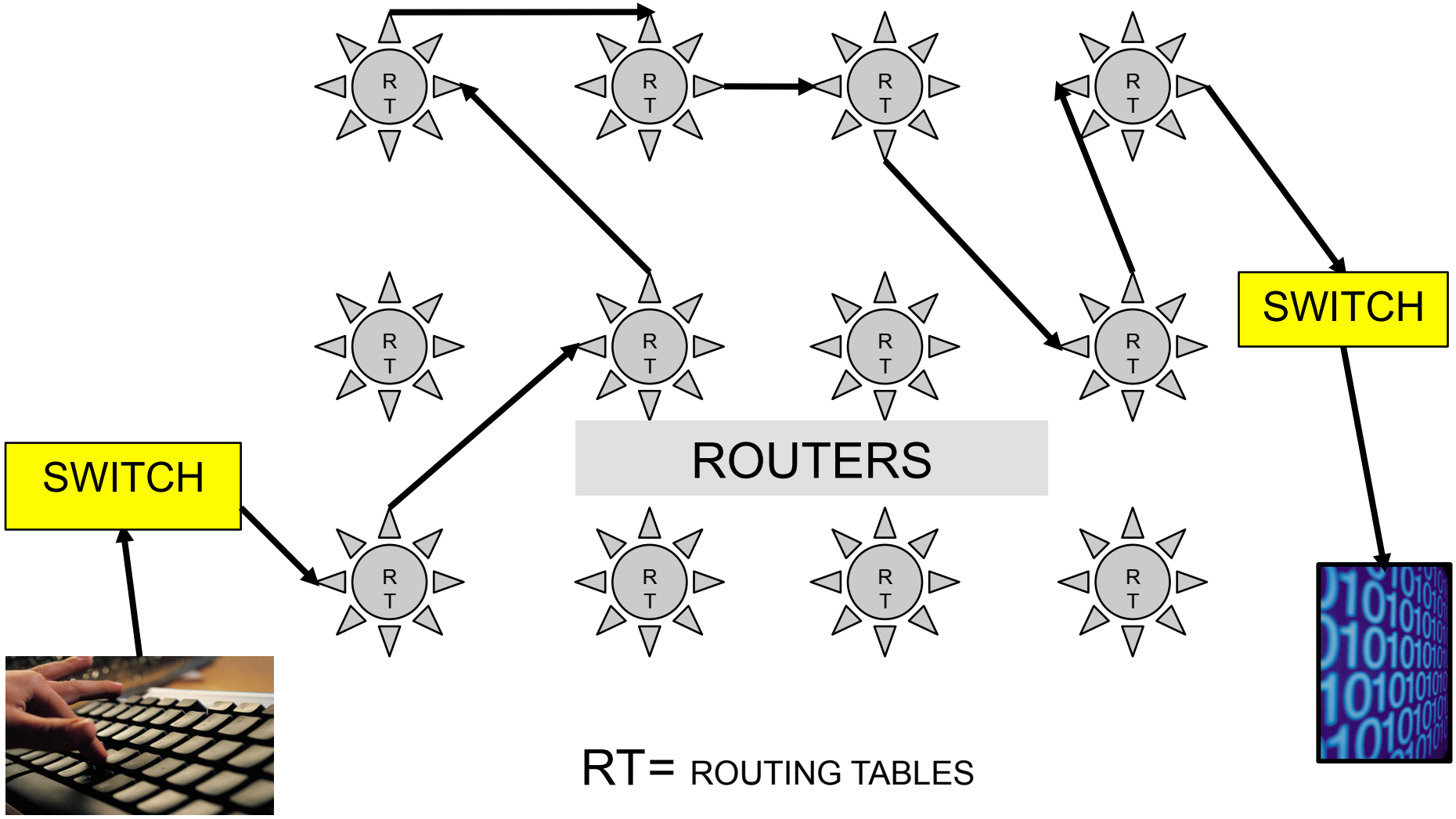
Part III: Attacks on Switches

Part IV: Attacks on Routers

Part V: Attacks on Domain Names

Summary

Routing INTERNET Messages through Routers & Switches



Internet Switch that Connects POPs to ISPs

Principal Attack Scenarios on Internet Switches

- Flooding Attacks on a Switch
- Address Resolution Spoofing
- “Man-in-the-Middle” Attack
- Denial of Service Attack
- Switch Hijacking Attack
- Spanning Tree Attack
- The Root Claim Attack
- Forcing Eternal Root Election Attack
- VLAN Hopping Attack

Flooding Attacks on a Switch:

- There are attack tools that can auto generate over 100,000 bogus entries per minute, which then overloads the switch so that it malfunctions.

Address Resolution Spoofing

- Allows an attacker to sniff the data flowing to a local area network. The traffic is either modified, or a denial of service condition is created.

"Man-in-the-middle" Attack

- Adds a third party destination without the legitimate recipients being aware. The third party can extract passwords and confidential data.

Denial of Service Attack:

- The switch will be jammed and therefore will not deliver packets. The switch will then time out, stopping all traffic.

Switch Hijacking Attack

- The switch will inject illegitimate connections that will pretend to be authentic. The added connections will take over control without the recipients being aware.

Spanning Tree Attack

- Allows the inclusion of spare links as backup paths. Communications are then routed also to illegitimate links.

The Root Claim Attack

- Bogus bridge protocols are used to designate the attacker's station as the new root bridge. Once in control a variety of malicious attacks can be then launched from the attacker.

Forcing Eternal Root Election Attack

- Makes the network unstable by tampering with the routing algorithm to keep searching for the root switch, without ever finding it. Transactions time out.

VLAN Hopping Attack

- Subdivision into different local area networks will be compromised if an attacker manages to send messages to the wrong links.
- When LANs support separately the NIPRNET and the SIPRNET one of them can be used to initiate a denial of service attack on the other.

Part III

Part I: Internet Basics

Part II: User Attacks

Part III: Attacks on Switches

Part IV: Attacks on Routers

Part V: Attacks on Domain Names

Summary

Internet Routers That Connect ISPs to Backbone Nets

Principal Attack Scenarios on Internet Routers

- Promiscuous Mode Corruption
- Router Table Attacks
- Router Information Attacks
- Shortest Path Attacks
- Border Gateway Attacks
- Border Gateway Poisoning

Promiscuous Mode Corruption

- The router masquerade as a “super-user” with software control privileges. Many router operating systems make “super-user” privileges available for maintenance or for software updating reasons.
- The attacker uses the vendor instructions to acquire “super user” status.

Router Table Attacks

- An attacker creates messages that look legitimate and can be then inserted into the routing table so that transactions can be redirected.

Router Poisoning Attacks

- Router poisoning is a method used to prevent formation of routing loops within networks.
- A “hop” count will then indicate to other routers that a route is no longer reachable and should be removed from their respective routing tables. The desired destination for the packets will cease to function.

Shortest Path Attacks

- Each router passes the status of its links to its neighbors who in turn forward this information to other routers in the network.
- As result of such passing each router has the link information for all other routers and eventually has the picture of the entire network topology.
- In a compromised table the calculated shortest paths will be incorrect and the shortest paths will be purged.

Border Gateway Attacks

- The Border Gateway protocol does not assure data integrity and does not provide source authentication. This protocol is the core routing protocol of the Internet, but can be tampered with by making changes to the router software.

Black Hole Attack

- By making use of router vulnerabilities, various kinds of attacks can be launched to compromise the routing through software changes.
- A special case is the “Black Hole” attack where the router directs a packet to a network where packets enter but do not come out.

Part V

Part I: Internet Basics

Part II: User Attacks

Part III: Attacks on Switches

Part IV: Attacks on Routers

Part V: Attacks on Domain Names

Summary

Principal Attack Scenarios on Domain Name System (DNS)

- Address Starvation Attack
- Attacks Using Rogue Servers
- Attacks Using Bogus Default Gateway
- DNS Database with Malicious Records
- DNS Spoofing With a Sniffer
- DNS Flooding Attack
- Spoofed Responses to a DNS Server
- Buffer Overflow Attack
- Denial of Service Attack

Summary

About Attacks on Internet

- It is Asymmetric Warfare.
- Principal technique is masquerading.
- Public Key Infrastructure Authentication mandatory.
- Every transaction must be monitored.
- Use intelligence methods to investigate cases.

Immediate Priority: Control Routers and Switches

- Separate GIG routers and switches from public Internet.
- Centrally manage dedicated routers and switches on the GIG.
- Intercept “malware” in the GIG, not at user end.

Implement Cloud Computing and Protect Databases

- Consolidate all servers through virtualization.
- Architect “cloud” connectivity.
- Eliminate “fat clients”.
- Encrypt databases.

Take Away

For follow up questions:

- pstrassm@gmu.edu