Fundamental Internet Security Flaws

Prof. Paul A. Strassmann
George Mason University
Center for Information Systems Security
November 5, 2009

Outline

Part I: Concepts

Part II: Attacks on Switches

Part III: Attacks on Routers

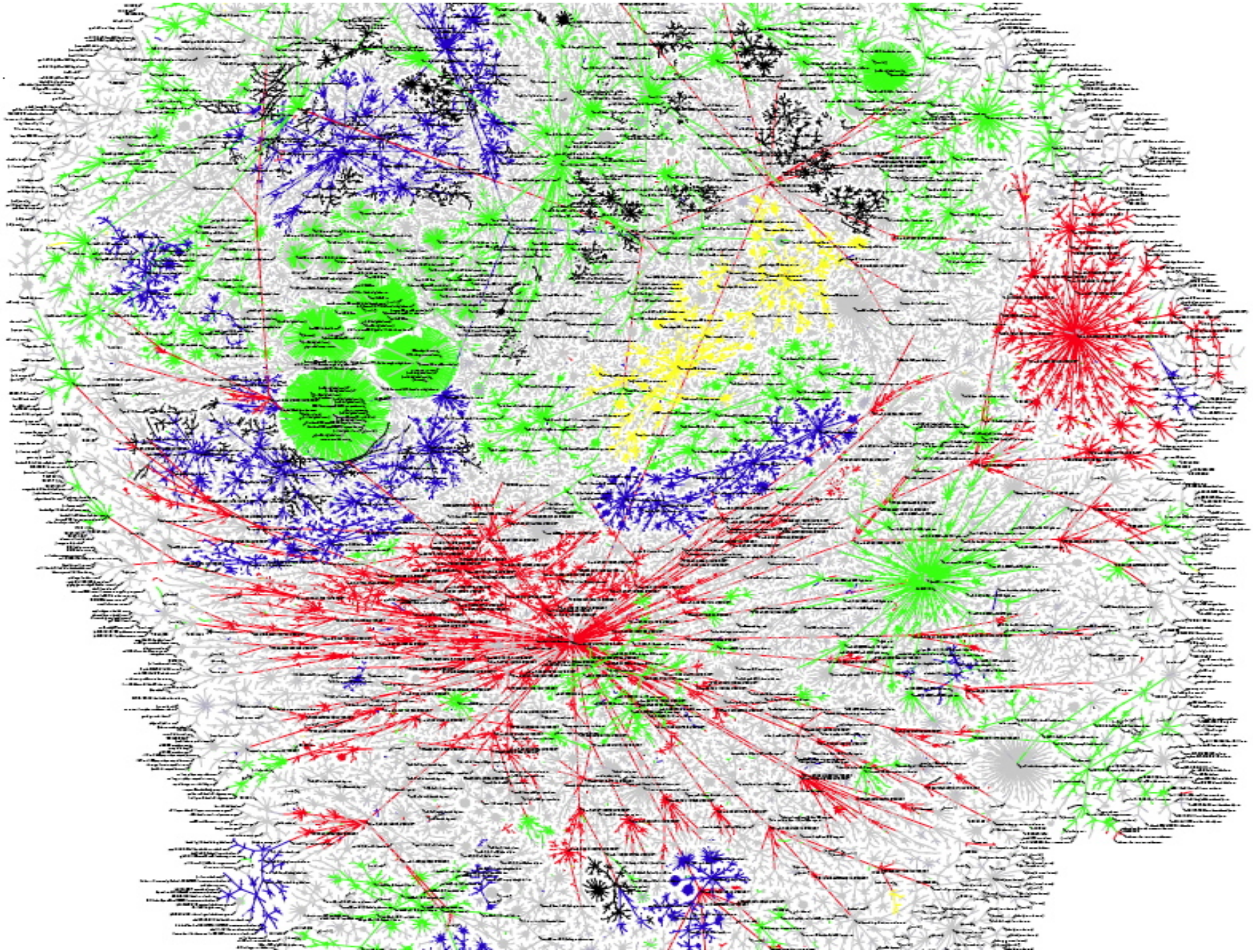
Part IV: Attacks on Domain Names

Summary

Internet Statistics (June 2009)

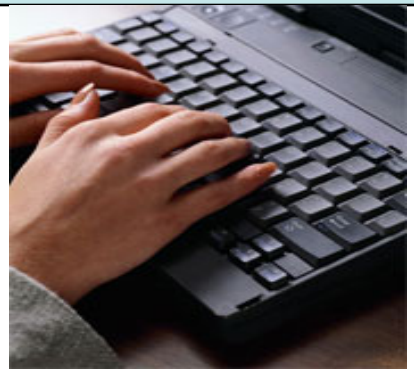
- 1.6 billion global Internet users
- 252 million Internet users in North America.
- 74% of North American population are Internet users.
- 200,000+ links between ISP's and the Internet

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

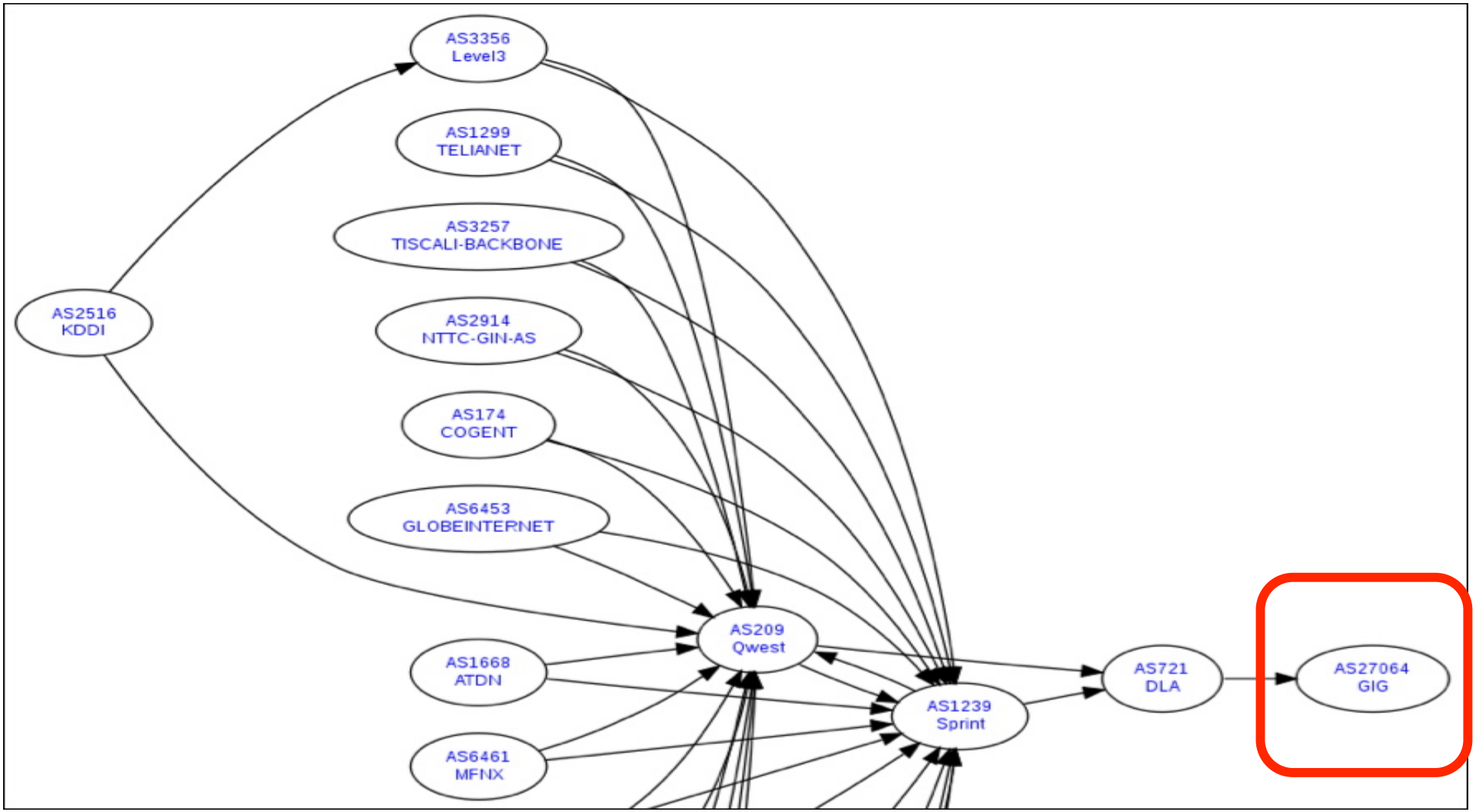


How Internet is Organized

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



Connections to and from the Global Information Grid (GIG)



Part II

Part I: Concepts

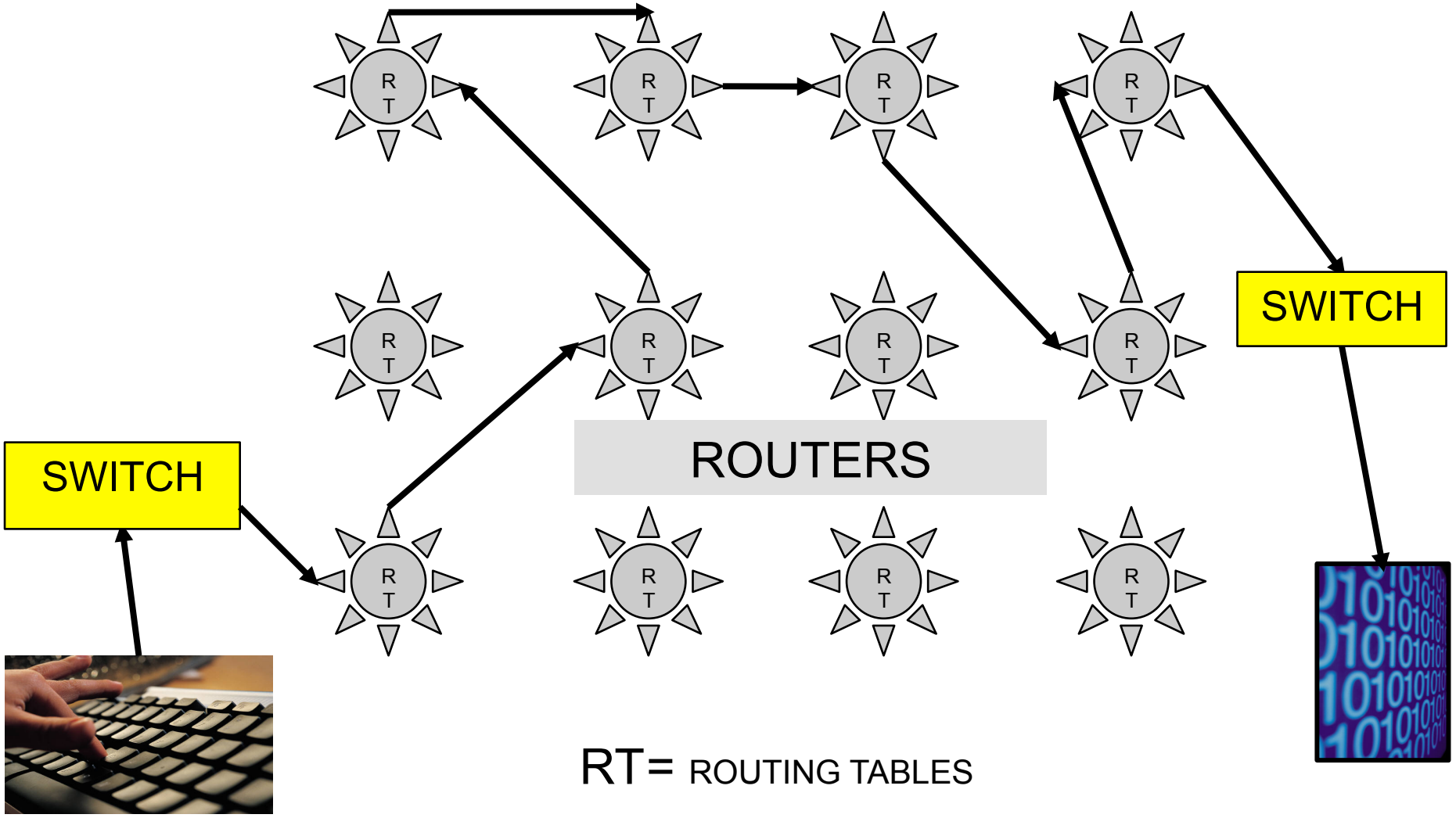
Part II: Attacks on Switches

Part III: Attacks on Routers

Part IV: 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

- The Media Access Control (MAC) protocol defines for a switch what transmissions are allowed to access which connection.
- A switch will keep a Content Addressable Memory (CAM) table for identification of MAC destinations. CAM tables have a limited memory and will overflow.
- Attack tools that can auto generate +100,000 bogus entries per minute, which then overloads the switch so that it malfunctions.

Address Resolution Spoofing

- Attacker replaces the ARP cache on a switch with a forged mapping and causes traffic to be redirected from the correct target to a target of the attacker's choice.
- Allows an attacker to sniff the data flowing to a local area network. The traffic is then modified.

"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 connection of multiple switches for LAN redundancy or as of spare links to form automatic backup paths.
- If the Spanning Tree Protocol (STP) is corrupted, communications will be re-routed 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 launched by the attacker, including the sniffing of all messages for sensitive information and for passwords.

Forcing Eternal Root Election Attack

- Makes the network unstable by tampering with the STP routing algorithm to keep searching for the root switch, without ever finding it.
- The network will be always in the root selection process, which will make the network unstable and potentially disabled.

VLAN Hopping Attack

- Virtual LANs (VLAN) make it possible to group users into logically separate networks.
- A switch partitions local area networks into isolated VLANs. The computers and peripherals are then restricted from communicating with each other.
- Separate subnets are compromised if an attacker manages to send across different zones (hopping). That will make VLAN subdivisions useless.
- For instance, a NIPRNET LAN could be used to initiate a denial of service against computers on SIPRNET.

Part III

Part I: Concepts

Part II: Attacks on Switches

Part III: Attacks on Routers

Part IV: 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.
- A promiscuous computer can monitor traffic to and from other computers on the Internet.

Router Table Attacks

- The content of a routing table update is continually modified to reflect changes in the configuration of the surrounding networks. An attacker will create messages that look legitimate and can be then inserted into the routing table.
- An attacker creates messages that look legitimate and can be then inserted into the routing table so that transactions can be redirected.
- Attacks on the routing table updates represent a high risk in the absence of a strong authentication mechanism. Password are insufficient for protecting military grade routers.

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 (BGP) is the core routing protocol of the Internet. It maintains tables of networks that can be reached from routers. BGP makes routing decisions based on path availability, network policies and operating rules.
- 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 IV

Part I: Concepts

Part II: Attacks on Switches

Part III: Attacks on Routers

Part IV: 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

Priority: Control Routers and Switches for the GIG

- 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.

Edge Computing Remedy

- Reduce the number of “hops” through placement of distributed servers for close access.
- 40,000+ local servers placed globally by Akamai reduce Internet “hops” to < 2 hops in most cases.
- Akamai revenue are <$1 billion

- The potential cost of DoD Global Information Grid (GIG) is <$5 - 8 billion.
- The GIG manages its Routers and Switches.

Take Away

For follow up questions:

- pstrassm@gmu.edu