Segurança sob a perspectiva dos Service Providers

Carlos Pereira – carlos.pereira@cisco.com

 # 8567

Same facts …

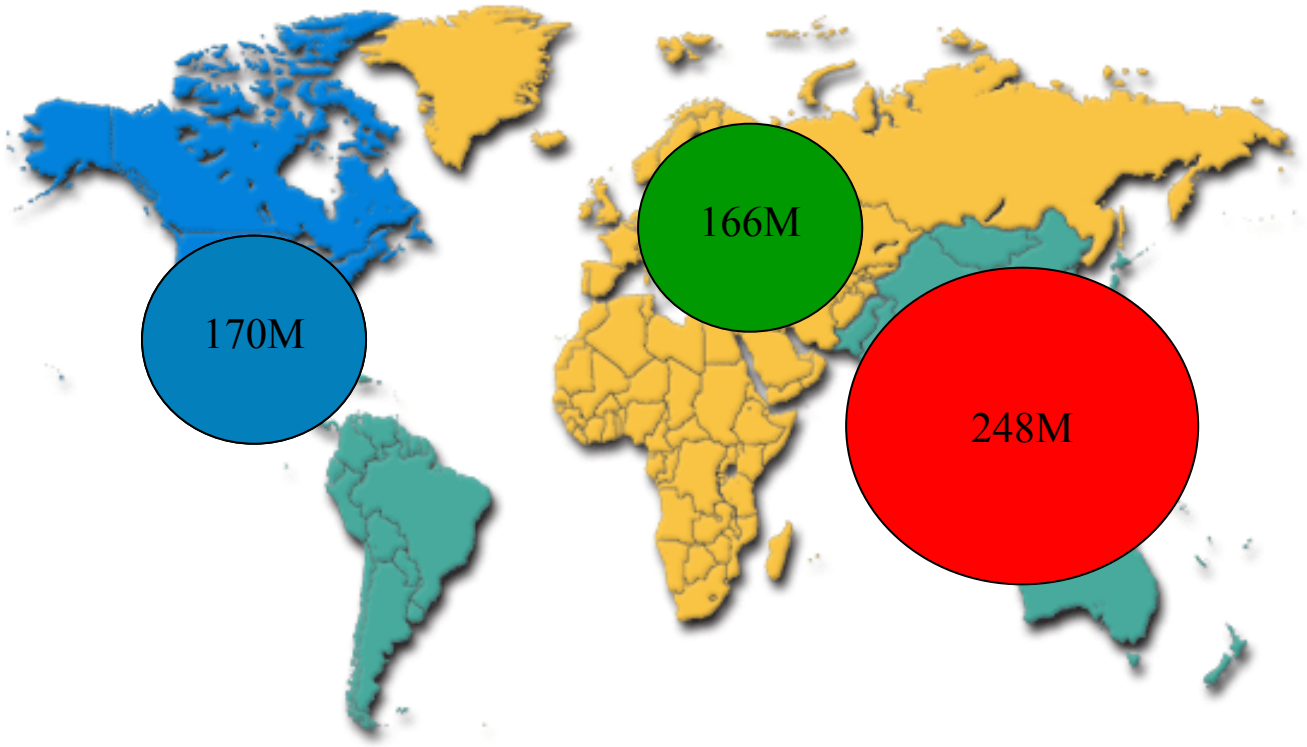
- **Exploits are forever**
  - ✓Once discovered, attack techniques persist and become increasingly automated and easy to implement
- **Internet is a non-American Internet – the world has just not woke up to that fact. Largest growth in Asia-Pacific**
  - ✓China second in number of home users with only 5% of its population online, Japan third, and South Korea sixth.
  - ✓Nearly 50% of all broadband deployments are in Asia-Pacific
- **Attacks result in collateral damage and exposure**
- **Emerging business model: Networked Virtual Organization (NVO)**
- **Emerging high-growth markets**
  - ✓ IP telephony, Storage, WLAN, Security
  - ✓ Metro, MPLS core and edge, IP VPNs, Cable convergence

… to take note

- There are no magic knobs, grand security solutions, or super vendor features that will solve all ISP Security problems.
- Likewise, there is no rocket science involved. Just hard work that is within all ISP's grasp.
- What follows are tools and techniques that might or might not work for you.

The Changing Face of the Internet

2004



The ISP's World Today

- **Changing threat**
  - ✓ **User friendly tools make it easier for the amateur cyberpunks to do more damage**
  - ✓ **eCommerce provides a monetary motivation**
  - ✓ **Geopolitical and religious issues provide lots of motivation.**
  - ✓ **Direct attacks on the Internet's core infrastructure means that the NET is not sacred anymore**
  - ✓ **Common for ISPs to have several calls per day from their customers to help defend against attacks**

More attacked sites “yesterday”

TER - 2003

Cisco.com

CNN.com

MAIN PAGE
WORLD
U.S.
LOCAL
POLITICS
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technolo
SPACE
HEALTH
ENTERTAINMENT
BOOKS
TRAVEL
FOOD
ARTS & STYLE
NATURE
IN-DEPTH
ANALYSIS
myCNN
Headline News brief

sci-tech > computing > story page

From...
COMPUTERWORLD
AN IDG.net SITE

'Immense' network assault takes down Yahoo

CNN.com technology > computing

CNN Sites

myCNN | Video | Audio | Headline News Brief | Free E-mail | Feedback

MAINPAGE
WORLD
U.S.
LOCAL
POLITICS
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
BOOKS
TRAVEL
FOOD
ARTS & STYLE
NATURE

INSURGENCY on the internet
in-depthreports

Main Page | Bracing for Cyberwar | Hacking Primer | Scenes from the 'Hacker Underground' | Hacking: Two Viewpoints | Timeline | Gallery | News Archive | Discussion | Related Sites

Cyber-attacks batter Web heavyweights

Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack

February 9, 2000
Web posted at: 9:56 a.m. EST (1456 GMT)

In this story:

YAHOO!

amazon.com

CNN.com

ebay™

E*TRADE℠

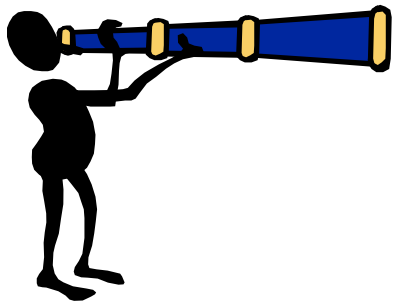
More attacked site “TODAY”

Networking Attacks Fundamentals:

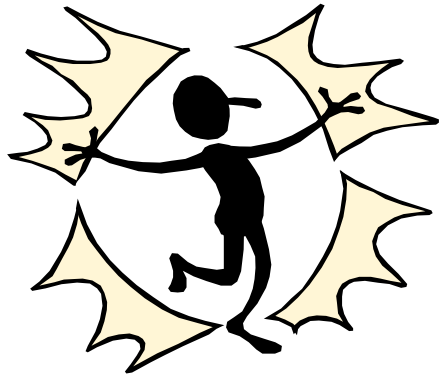
Three Key Threat Categories

Classes of Attacks

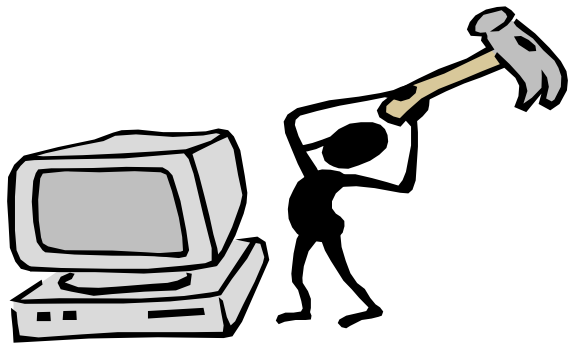
- **Reconnaissance**
  - ✓Unauthorized discovery and mapping of systems, services, or vulnerabilities



- **Access**
  - ✓Unauthorized data manipulation, system access, or privilege escalation



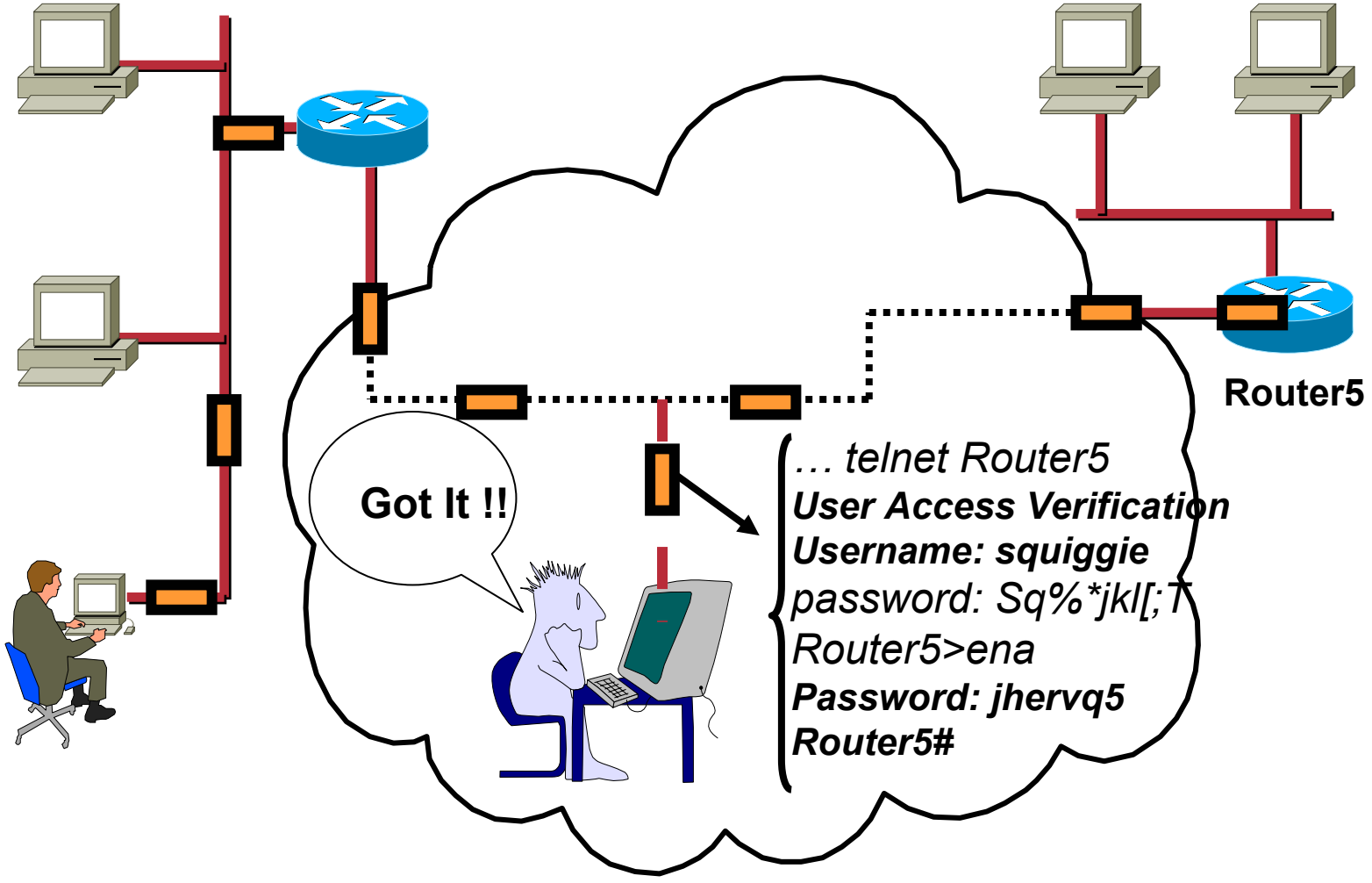
- **Denial of Service**
  - ✓Disable or corrupt networks, systems, or services



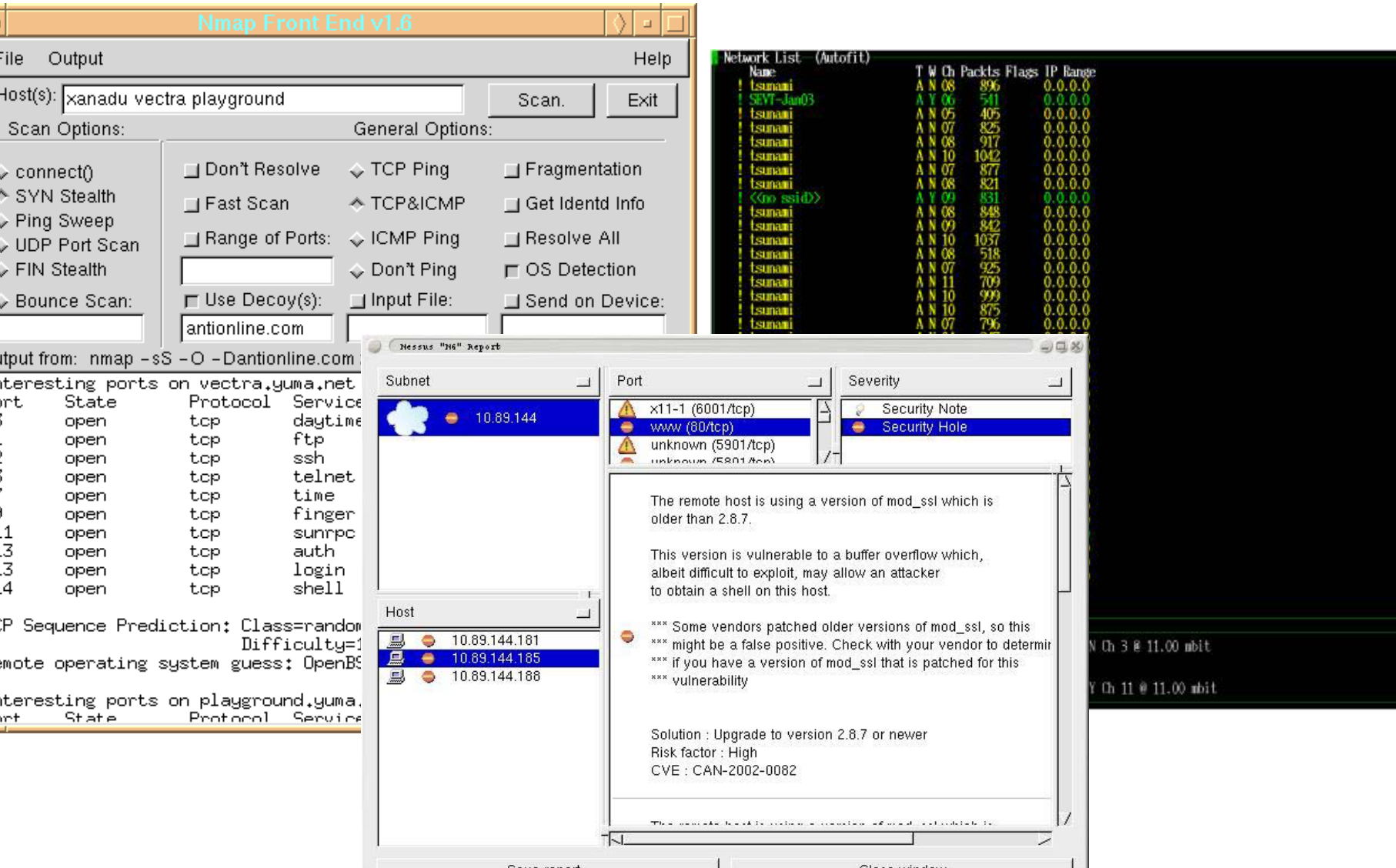
Three Key Threat Categories

Reconnaissance

Network Sniffers



Nmap, Nessus, Kismet



Why Do You Care?

- **Reconnaissance is part of the "security noise of the Internet." It doesn't bother me.**
  - ✓**Wrong!**
- **The more information you have, the easier it will be to launch a successful attack:**
  - ✓**Map the network**
  - ✓**Profile the devices on the network**
  - ✓**Exploit discovered vulnerabilities**
  - ✓**Achieve objective**

Three Key Threat Categories

Access

Access Methods

- **Exploit easily guessed passwords**
  - ✓ **Brute force**
  - ✓ **Cracking tools**
- **Exploit mis-administered services**
  - ✓ **IP services (anonymous ftp, tftp, remote registry access, nis, ...)**
  - ✓ **Trust relationships (spoofing, r-services, ...)**
  - ✓ **File sharing (NFS, Windows File Sharing)**

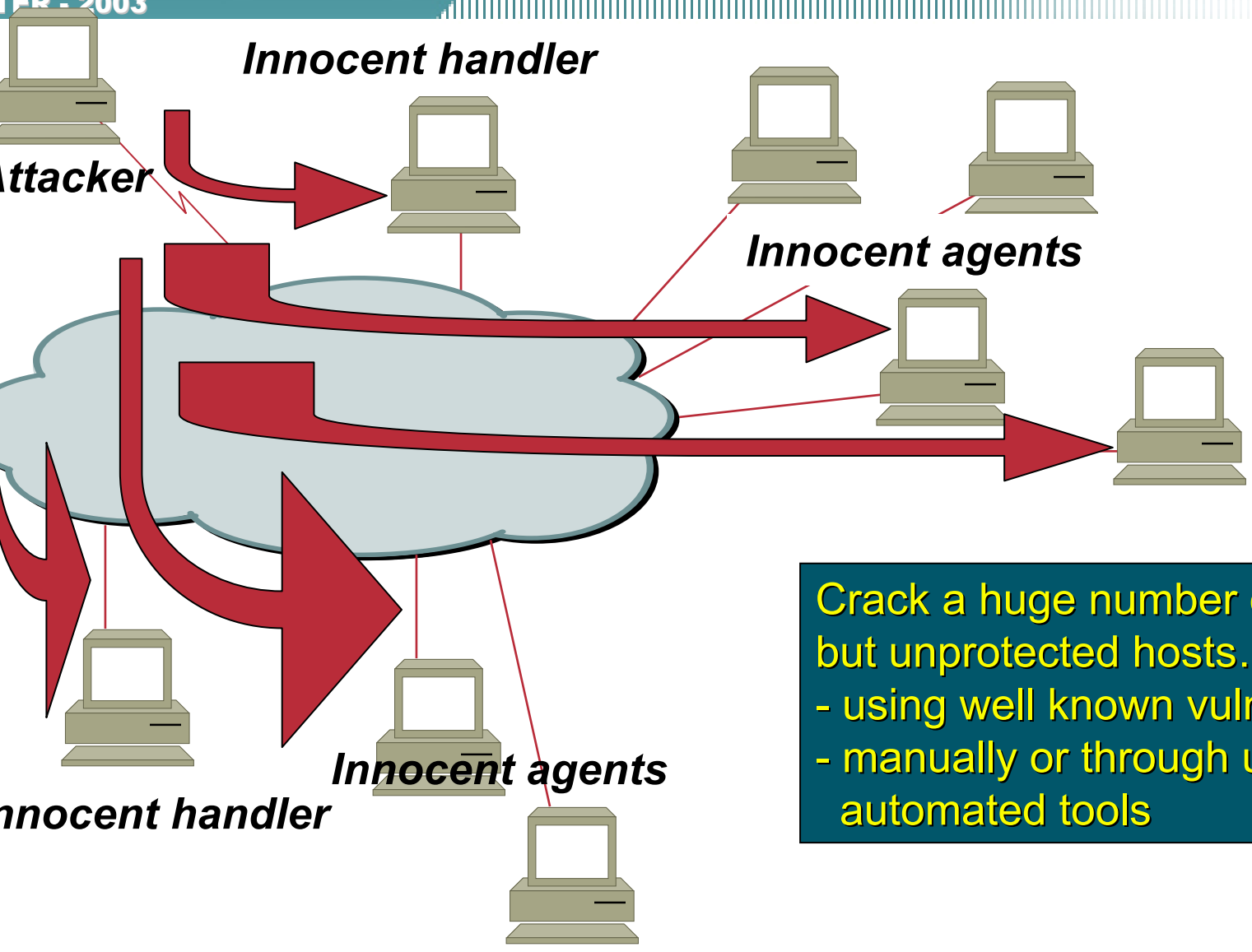
Three Key Threat Categories

Denial of Service

Denial of Service and ISPs

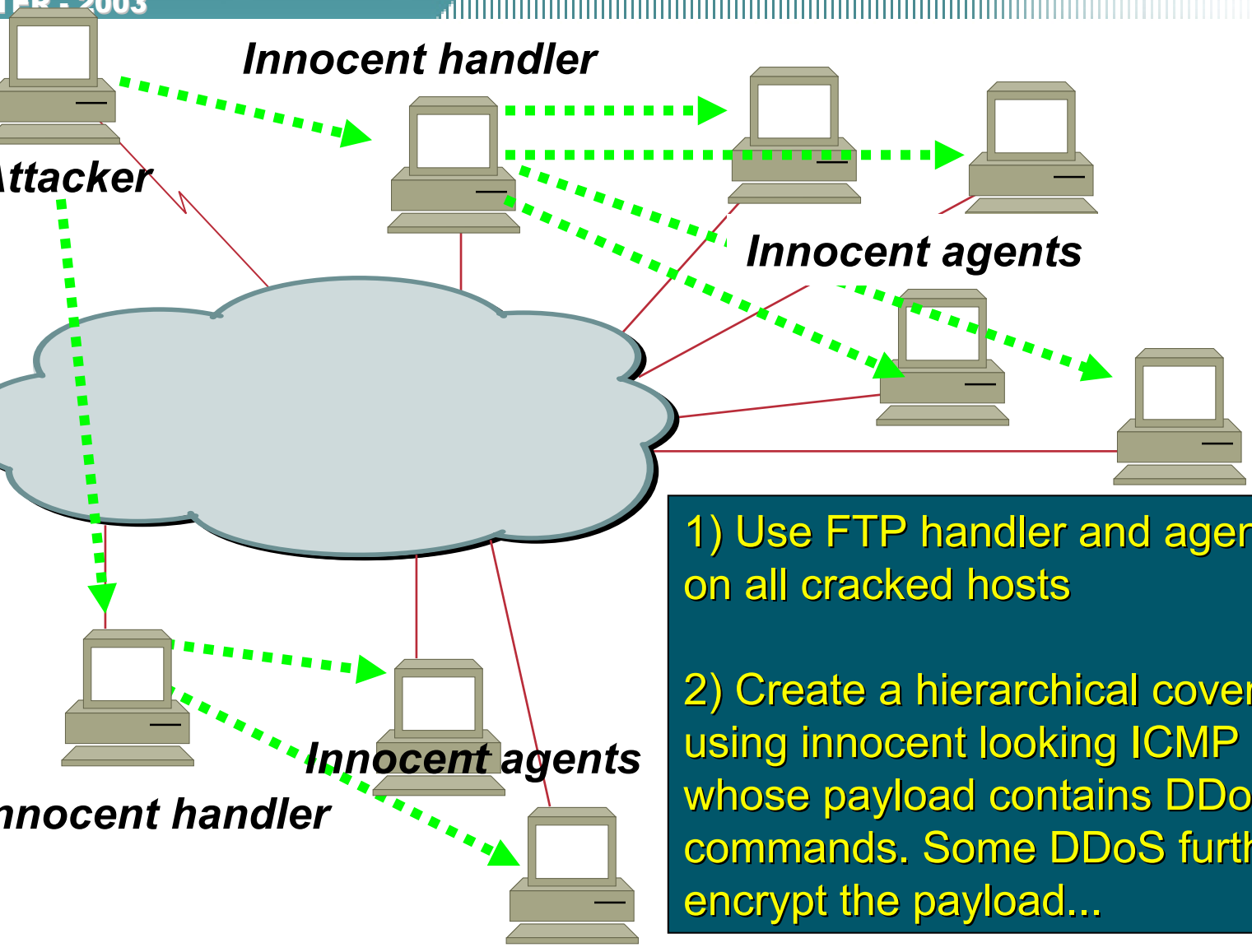
- DOS can ….
  - ✓ target an ISP.
  - ✓ target an ISP's customer.
  - ✓ target the core of the Internet.
- DOS cannot be ignored by an ISP. It always come back to bite you.

DDoS Step 1: Crack Handlers and Agents



Crack a huge number of innocent but unprotected hosts…
- using well known vulnerabilities
- manually or through use of automated tools

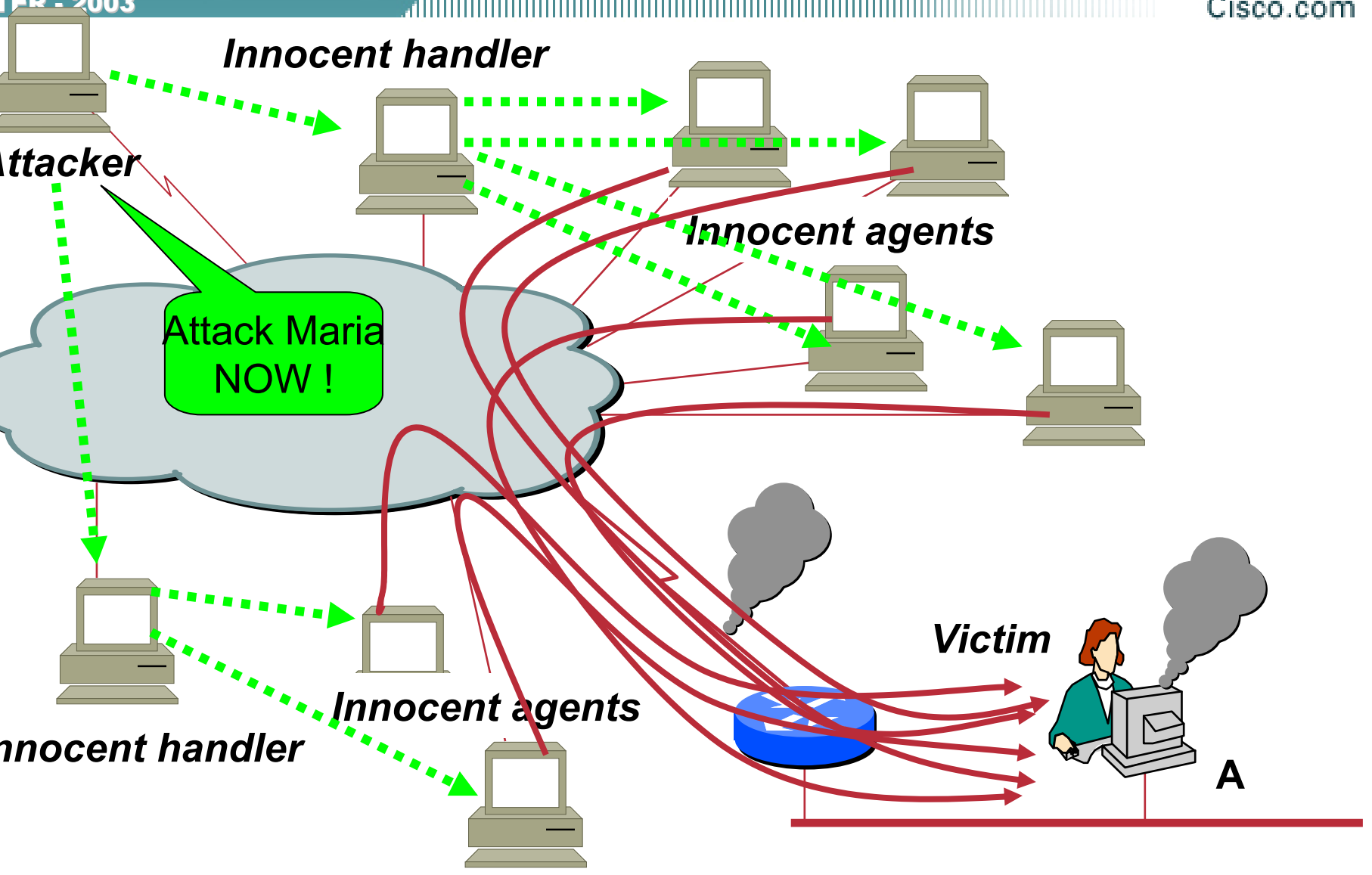
DDoS Step 2: Install Trojan & Covert Communication Channel



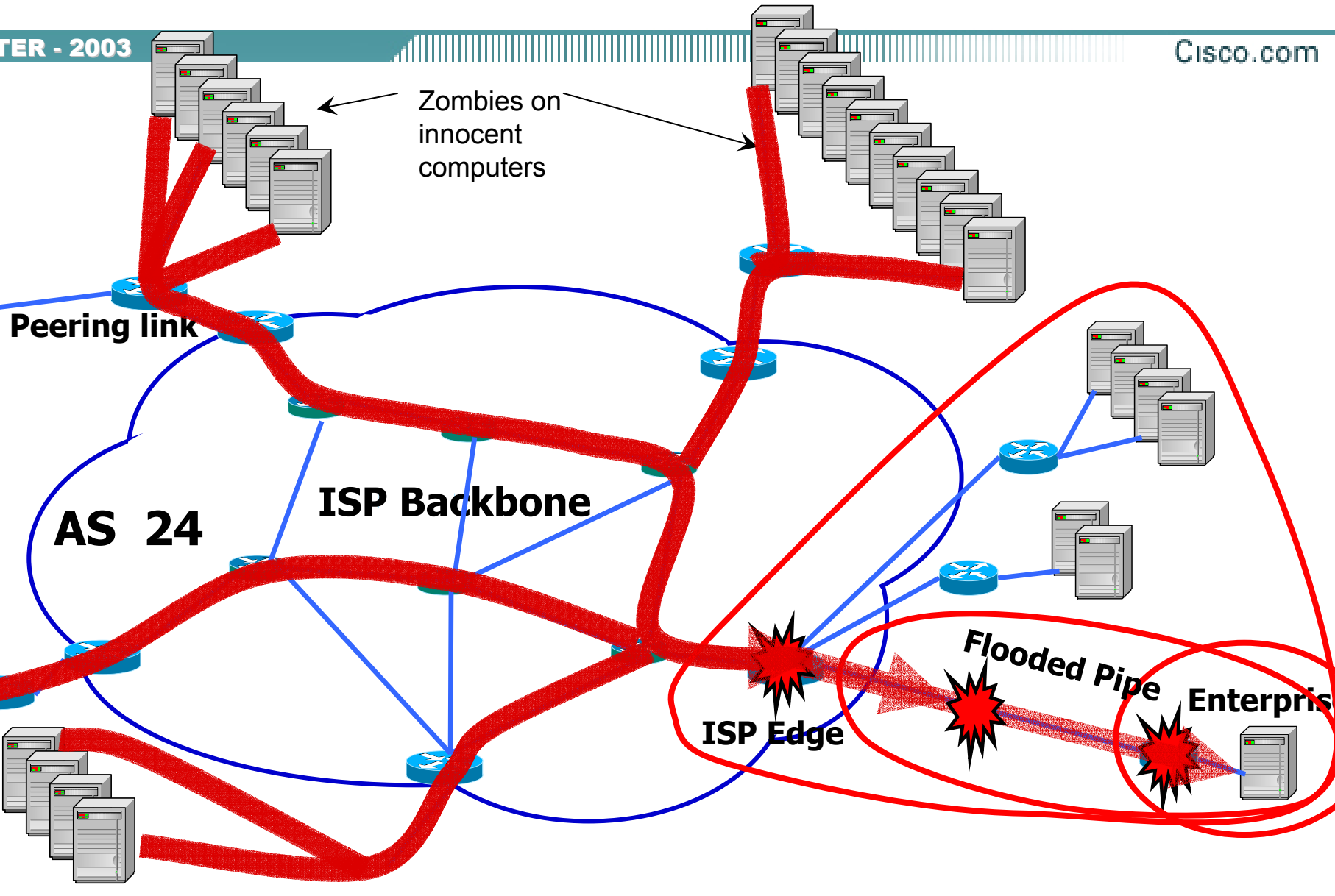
1) Use FTP handler and agent programs on all cracked hosts

2) Create a hierarchical covert channel using innocent looking ICMP packets whose payload contains DDoS commands. Some DDoS further encrypt the payload...

DDoS Step 3: Launch the Attack



Distributed Denial of Service

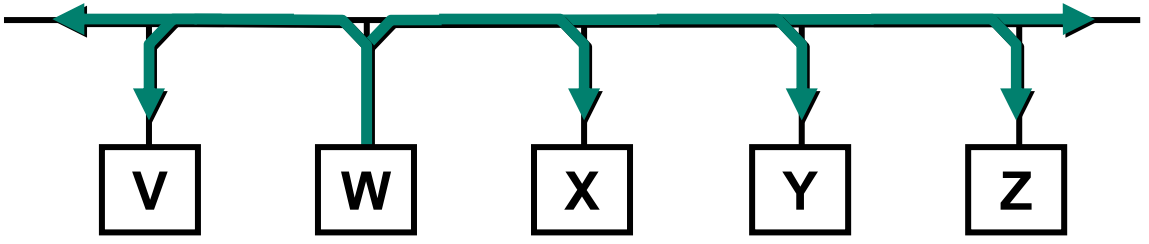


More “interesting” Attacks ☺

ARP, DDOS Reflection

Gratuitous ARP

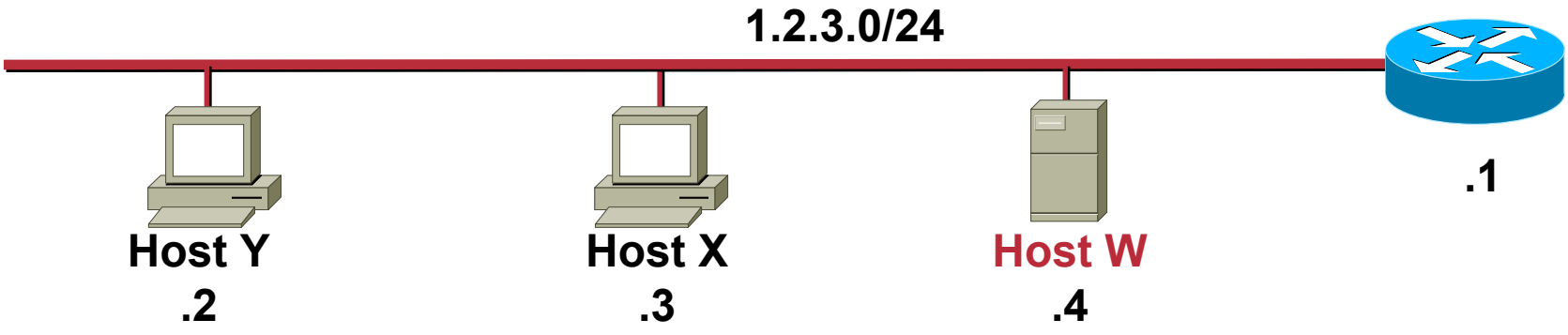
- Gratuitous ARP is used by hosts to “announce” their IP address to the local network and avoid duplicate IP addresses on the network; routers and other network hardware may use cache information gained from gratuitous ARPs
- Gratuitous ARP is a broadcast packet (like an ARP request)



- HOST W: Hey everyone I’m host W and my IP Address is 1.2.3.4 and my MAC address is 12:34:56:78:9A:BC

Misuse of Gratuitous ARP

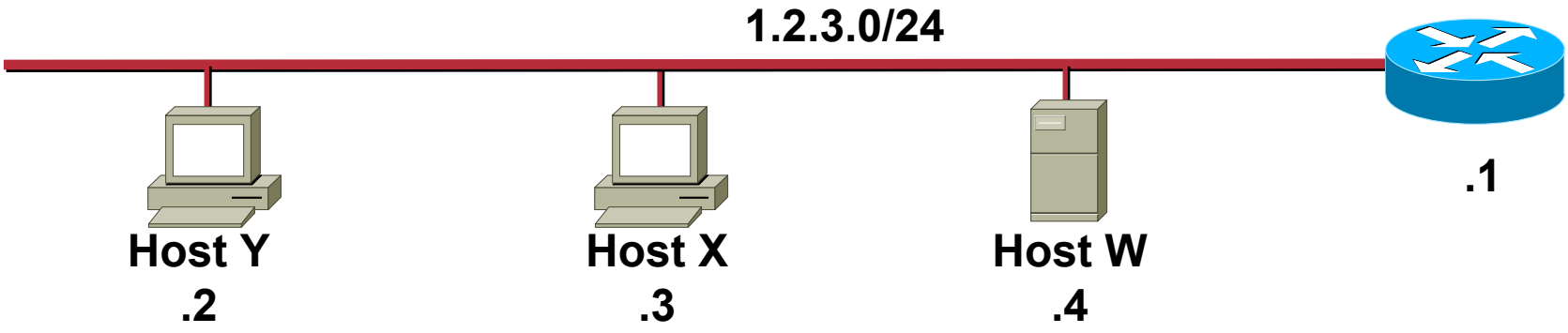
- ARP has no security or ownership of IP or MAC addresses
- What if we did the following?



- Host W broadcasts I'm 1.2.3.1 with MAC 12:34:56:78:9A:BC
- (Wait 5 seconds)
- Host W broadcasts I'm 1.2.3.1 with MAC 12:34:56:78:9A:BC

A Test in the Lab

- Host X and Y will likely ignore the message unless they currently have an ARP table entry for 1.2.3.1



- When host Y requests the MAC of 1.2.3.1 the real router will reply and communications will work until host W sends a gratuitous ARP again
- Even a static ARP entry for 1.2.3.1 on Y will get overwritten by the Gratuitous ARP on some OSs (NT4,WIN2K for sure)

Dsniff—A Collection of Tools to Do:

- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH/SSL interception

Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff

Arpspoof in Action


```
[root@attack-lnx dsniff-2.3]# ./arpspoof 10.1.1.1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp repl
10.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp repl
10.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp repl
10.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp repl
10.1.1.1 is-at 0:4:4e:f2:d8:1u
```

```
C:\>test

C:\>arp -d 10.1.1.1

C:\>ping -n 1 10.1.1.1

Pinging 10.1.1.1 with 32 bytes

Reply from 10.1.1.1: bytes=32 time<10ms TTL=255

C:\>arp -a

Interface: 10.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  10.1.1.1              00-04-4e-f2-d8-01     dynamic
  10.1.1.25             00-10-83-34-29-72     dynamic
C:\>arp -a

Interface: 10.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  10.1.1.1              00-10-83-34-29-72     dynamic
  10.1.1.25             00-10-83-34-29-72     dynamic
```

Selective Sniffing

- **Once the dsniff box has started the arpspoof process, the magic begins:**

```
[root@attack-lnx dsniff-2.3]# ./dsniff -c
dsniff: listening on eth0
-----------------
07/17/01 10:09:48 tcp 10.1.1.26.1126 -> wwwin-abc.cisco.com.80 (http)
GET /SERVICE/Paging/page/ HTTP/1.1
Host: wwwin-abc.cisco.com
Authorization: Basic c2NvdlghV9UNMRH4lejDmaA== [myuser:mypassword]
```

Supports More than 30 Standardized/Proprietary Protocols:

FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL

SSL/SSH Interception

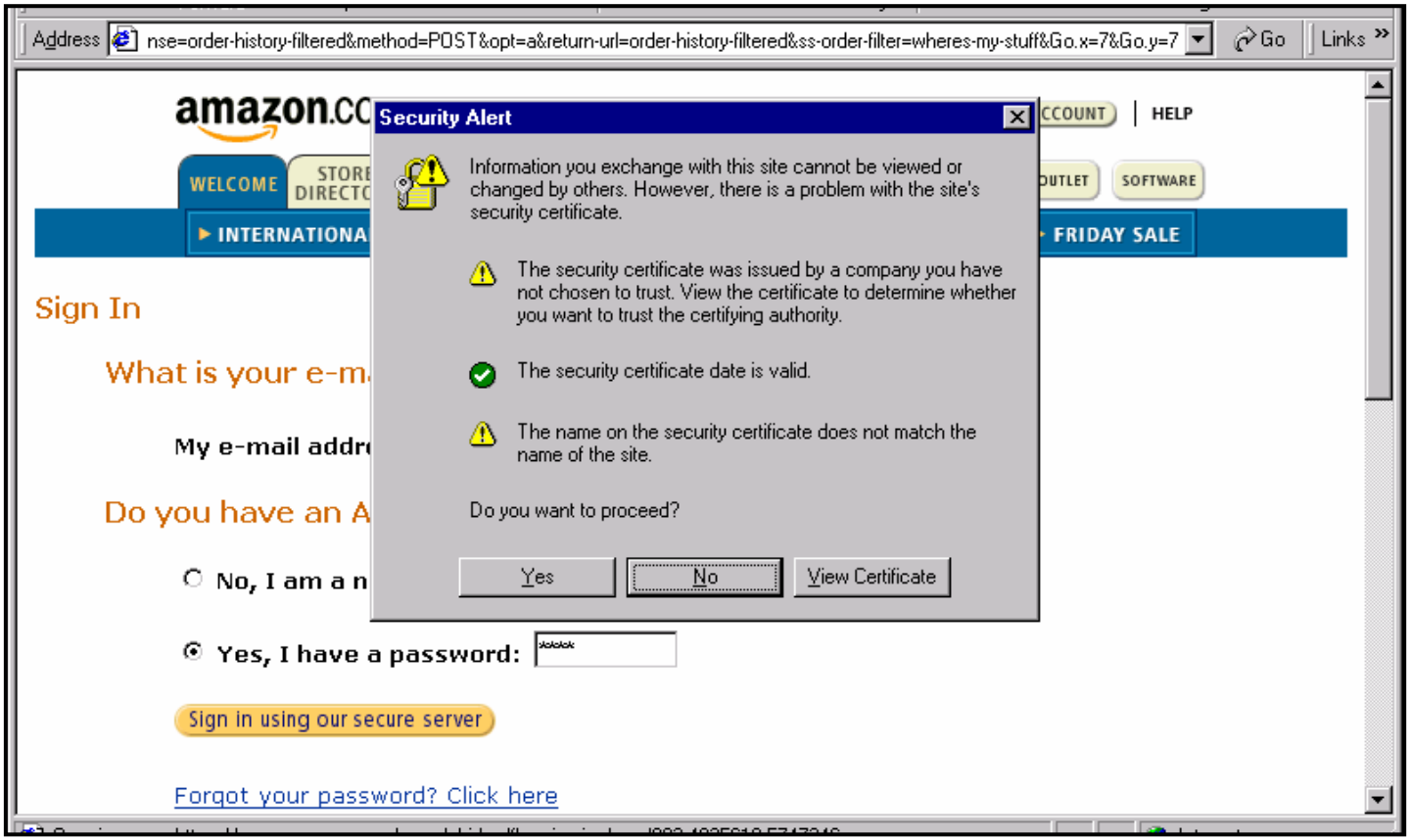
- Using dnsspoof all web sites can resolve to the dsniff host IP address:

```
C:\>ping www.amazon.com

Pinging www.amazon.com [10.1.1.25] with 32 bytes of data:

Reply from 10.1.1.25: bytes=32 time<10ms TTL=249
Reply from 10.1.1.25: bytes=32 time<10ms TTL=249
Reply from 10.1.1.25: bytes=32 time<10ms TTL=249
Reply from 10.1.1.25: bytes=32 time<10ms TTL=249
```

- Once that happens you can proxy all web connections through the dsniff host

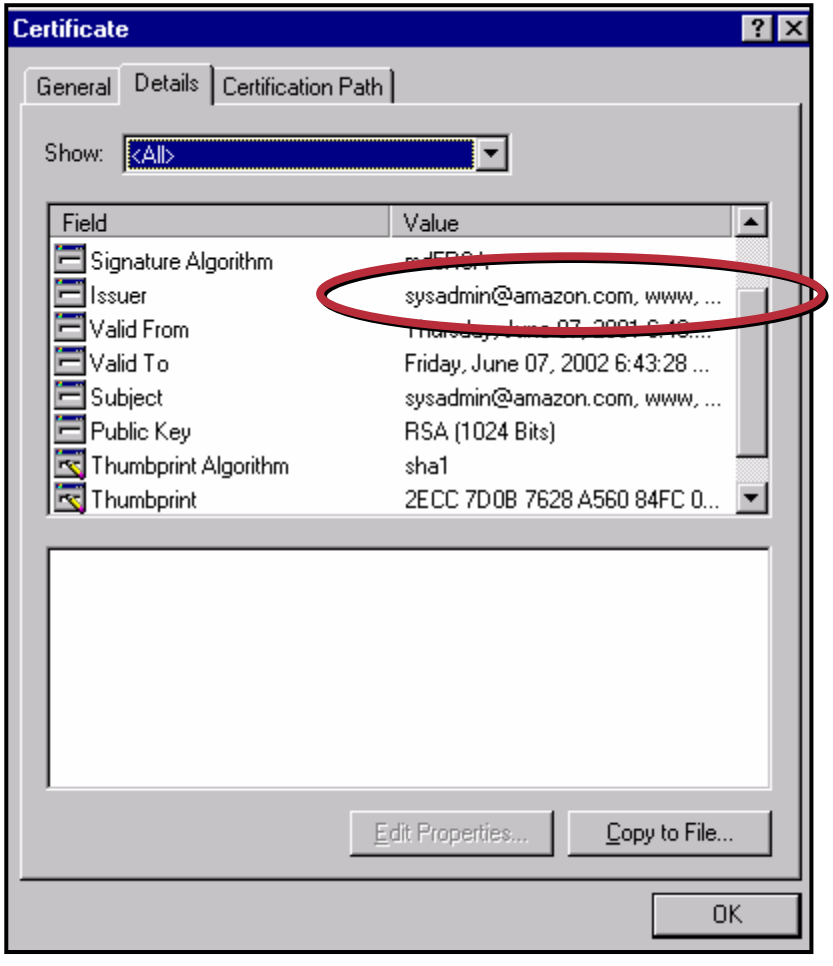
SSL/SSH Interception

- **Using dsniff (webmitm) most SSL sessions can be intercepted and bogus certificate credentials can be presented**



SSL/SSH Interception

- **Upon inspection they will look invalid but they would likely fool most users**



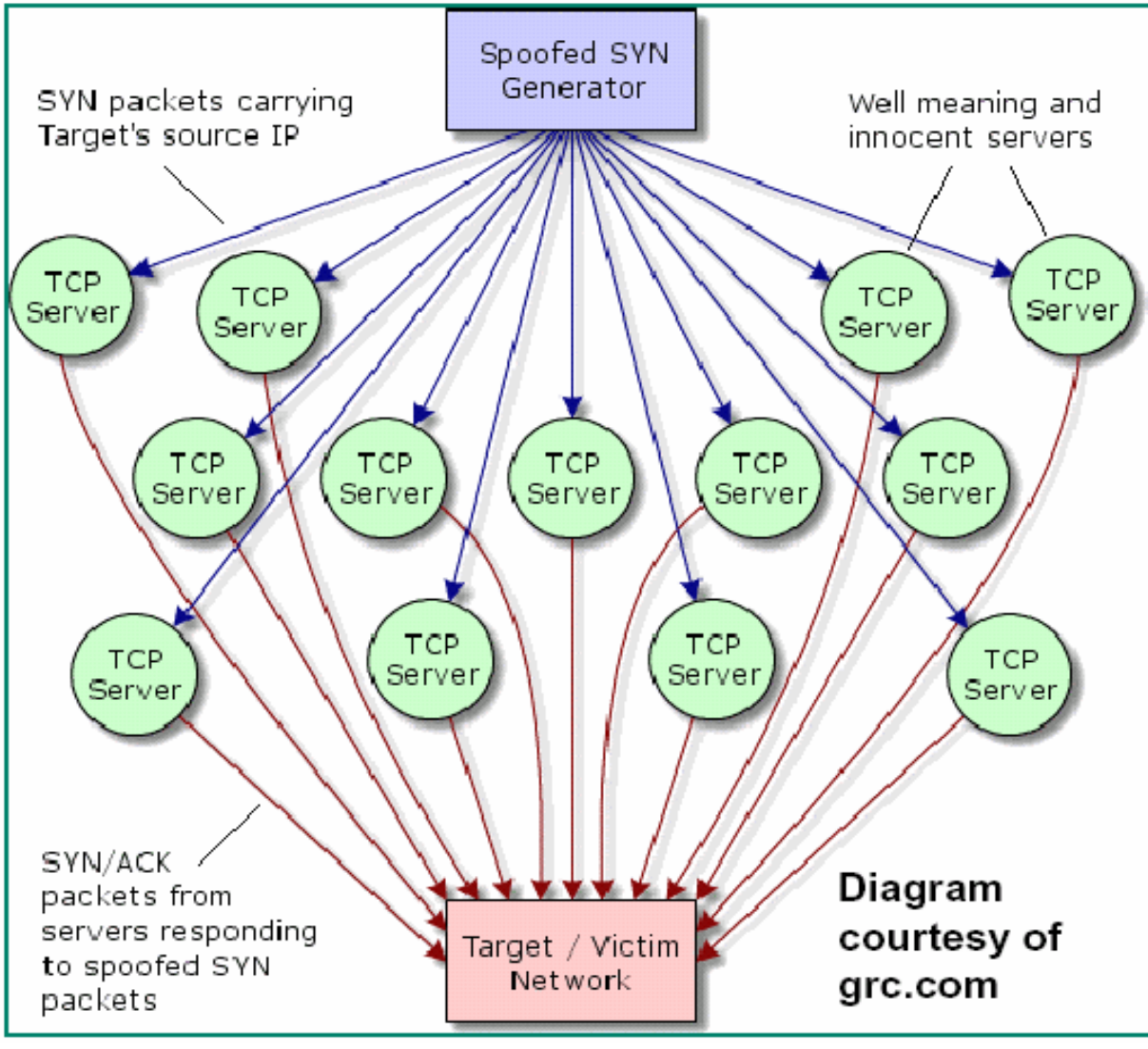
invalid

Dsniff evolves: Ettercap

- Similar to dsniff though not as many protocols supported for sniffing
- Can ARP spoof both sides of a session to achieve full-duplex sniffing
- Allows command insertion into persistent TCP sessions
- Menu driven interface
- http://ettercap.sourceforge.net/

TCP DDOS Reflection Attacks

- Newer DDoS technique using TCP basics
- Similar to DNS reflection attack on register.com
- No requirement to compromise hosts
- Traffic looks normal
- Attack sources are legitimate and spread over the entire Internet
- Sites acting as reflector will likely not notice performance degradation
- No easy attack mitigation options
- RFC2827 PLEASE!!!!!



TCP DDOS Reflection Attacks

- **Reflectors= returns a packet if one is sent**
  - ✓**Web servers, DNS servers and *routers***

    Returns SYNACK or RST in response to a SYN or other TCP packets with ACK

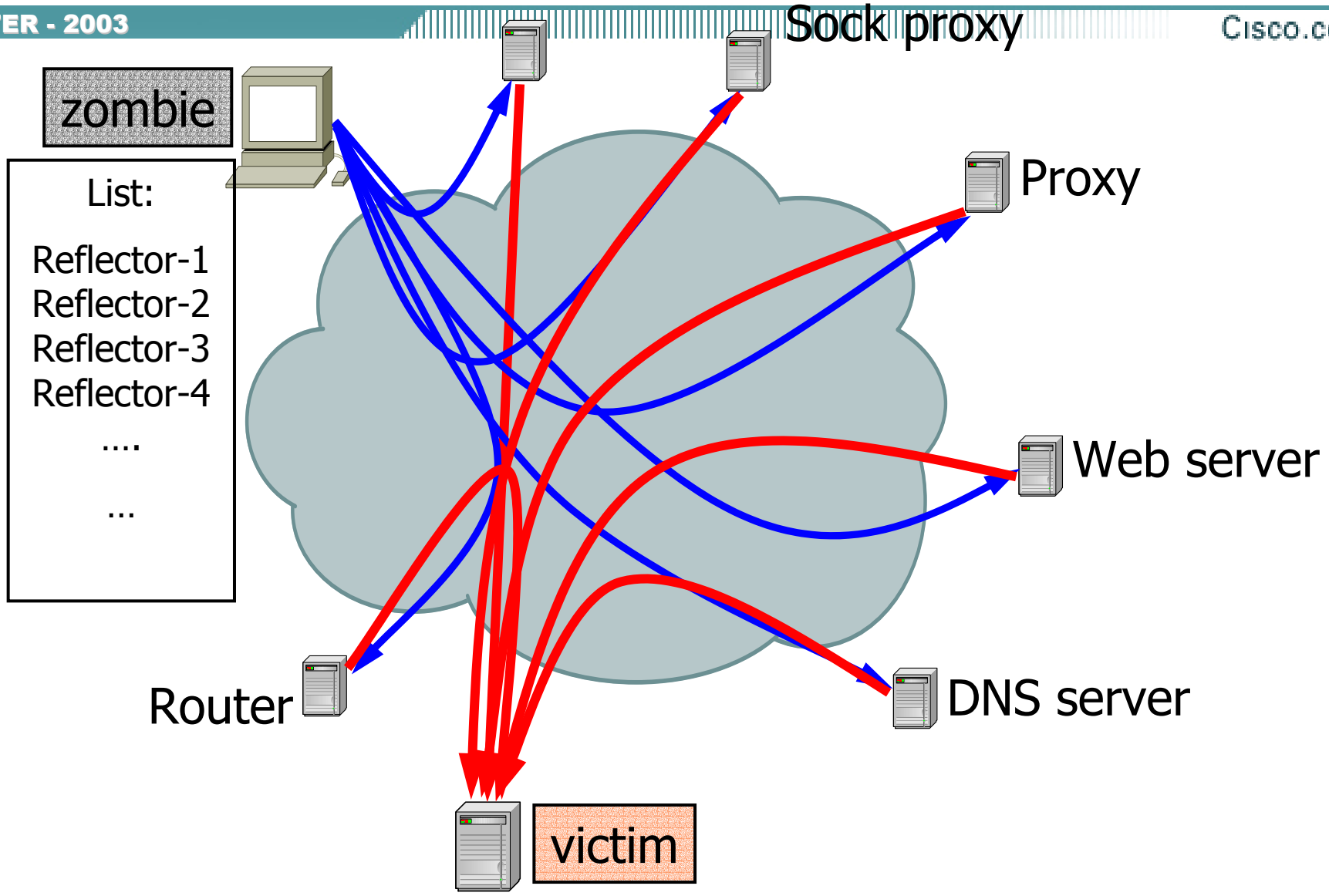
    or query reply in response to a query

    or ICMP Time Exceeded or Host Unreachable in response to particular IP packets
  - ✓**Attackers spoof IP addresses from a zombie**

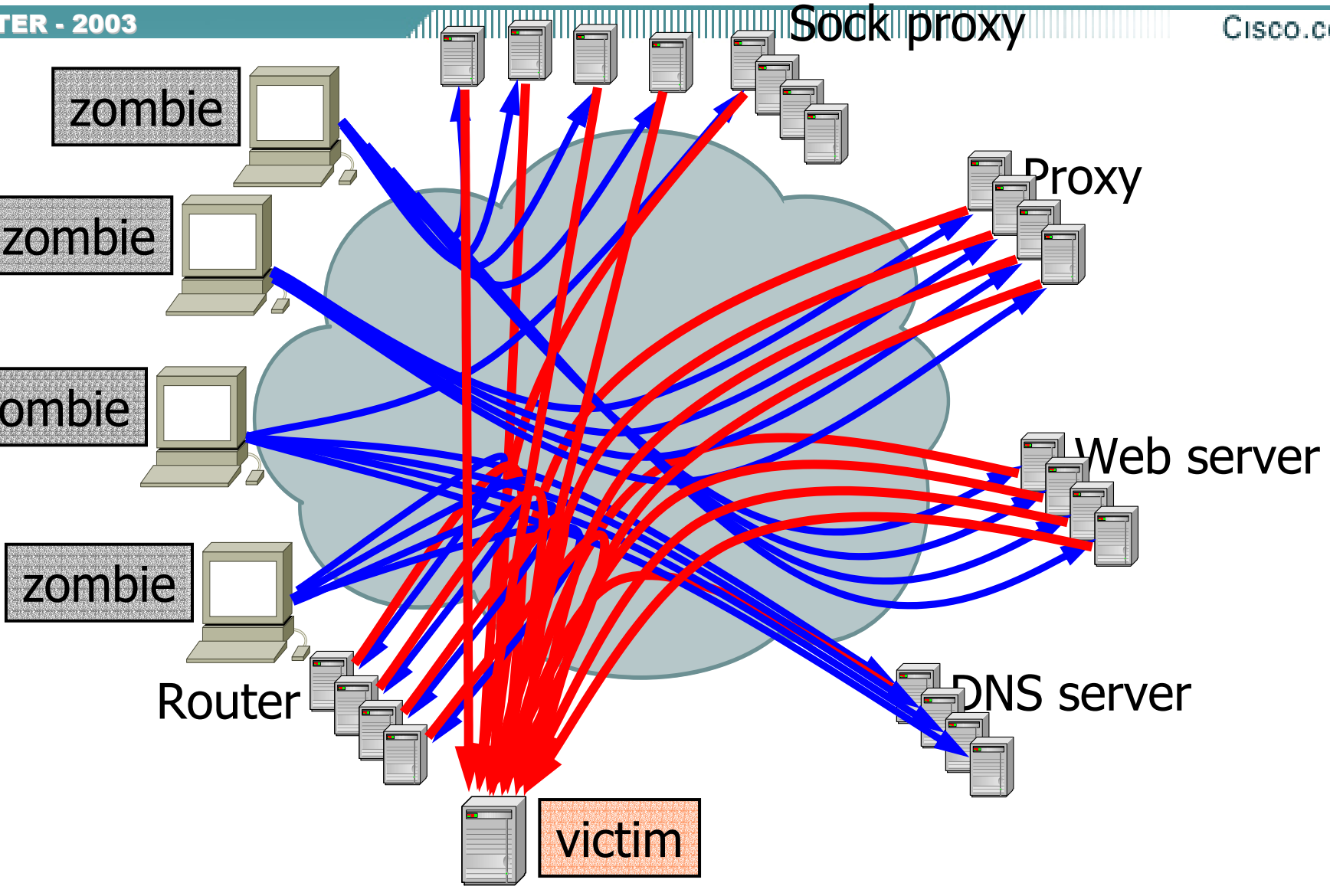
    http://www.aciri.org/vern/papers/reflectors.CCR.01.pdf

    http://staff.washington.edu/dittrich/misc/ddos/grc-syn.txt

TCP DDOS Reflection Attacks



TCP DDOS Reflection Attacks

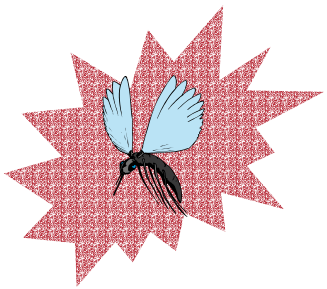


Co-Lateral Damage

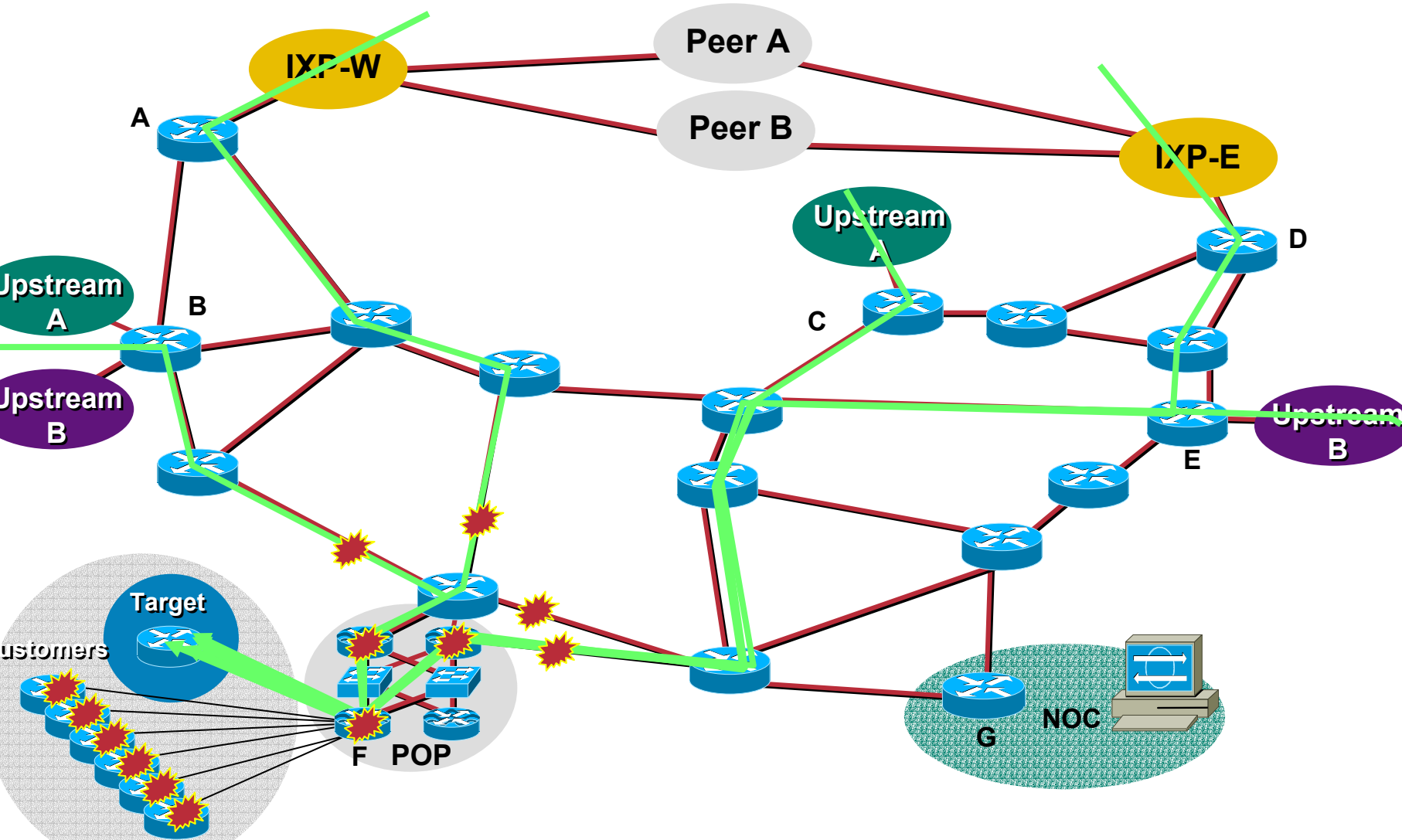
How DOS Attacks on One Customer can Effect the Entire Network

What is Co-Lateral Damage?

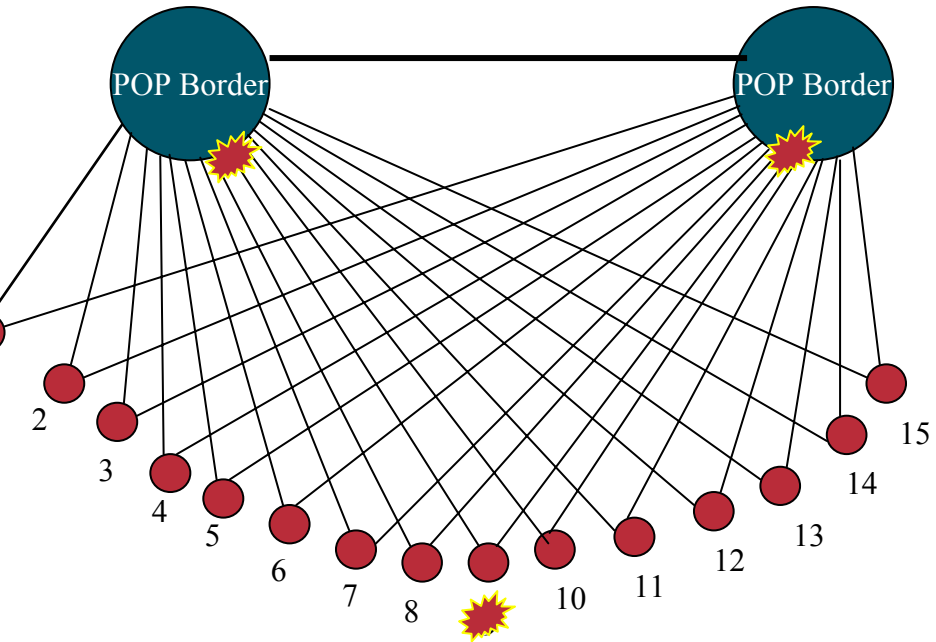
- Co-Lateral Damage hurts others around the target of attack.
- Some attackers work very hard to minimize co-lateral damage (cruse missile strike).
- Others do not care (use a tank to swat a mosquito).
- Co-Lateral Damage is core reason why ISPs must respond to their customer's DOS attacks.



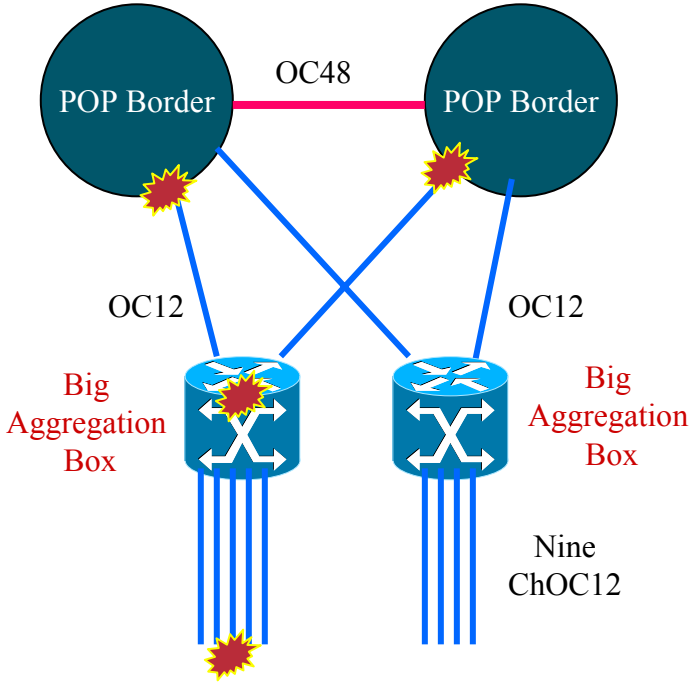
What is Co-Lateral Damage?



Increased Risk from Co-Lateral Damage

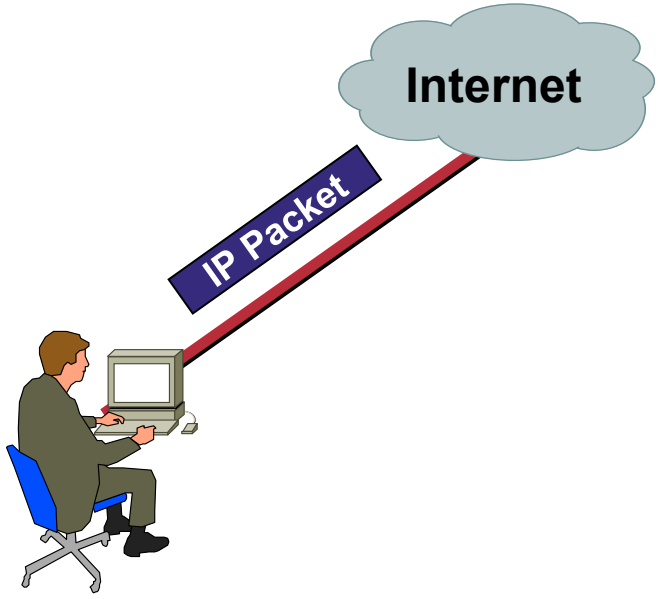


Lots of Aggregations Routers with 10s to 100s of customers per router.



Few Aggregations Routers with 100s to 1000s of customers per router.

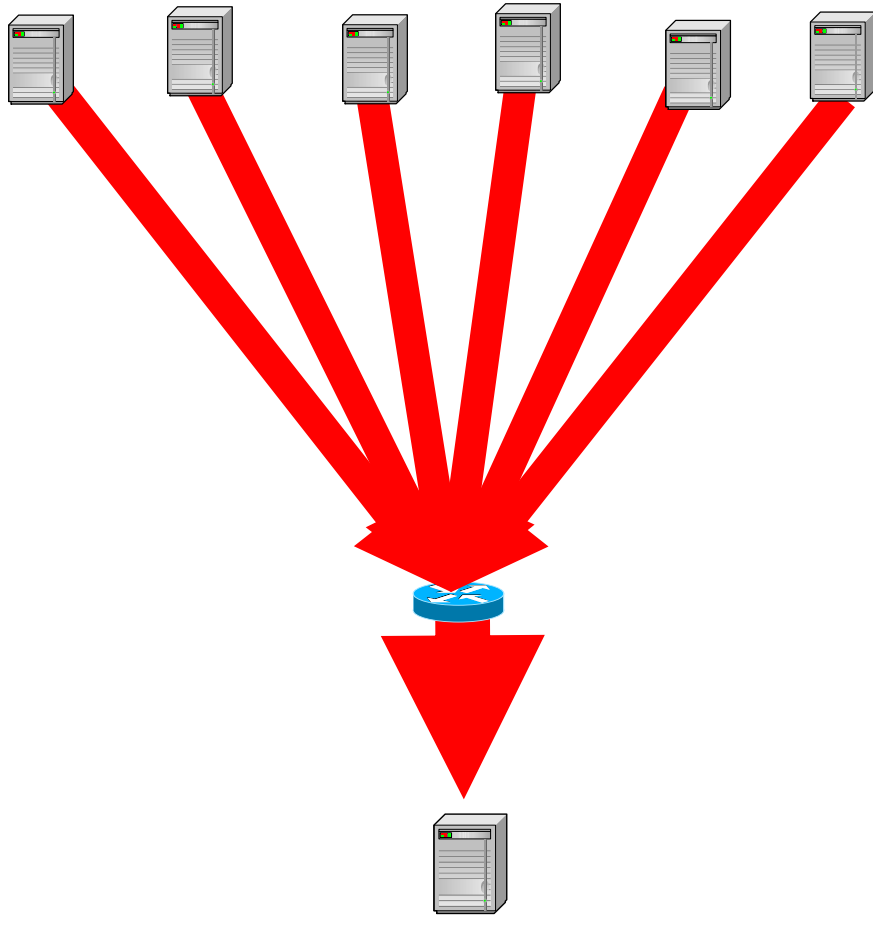
It is all about the packet ……



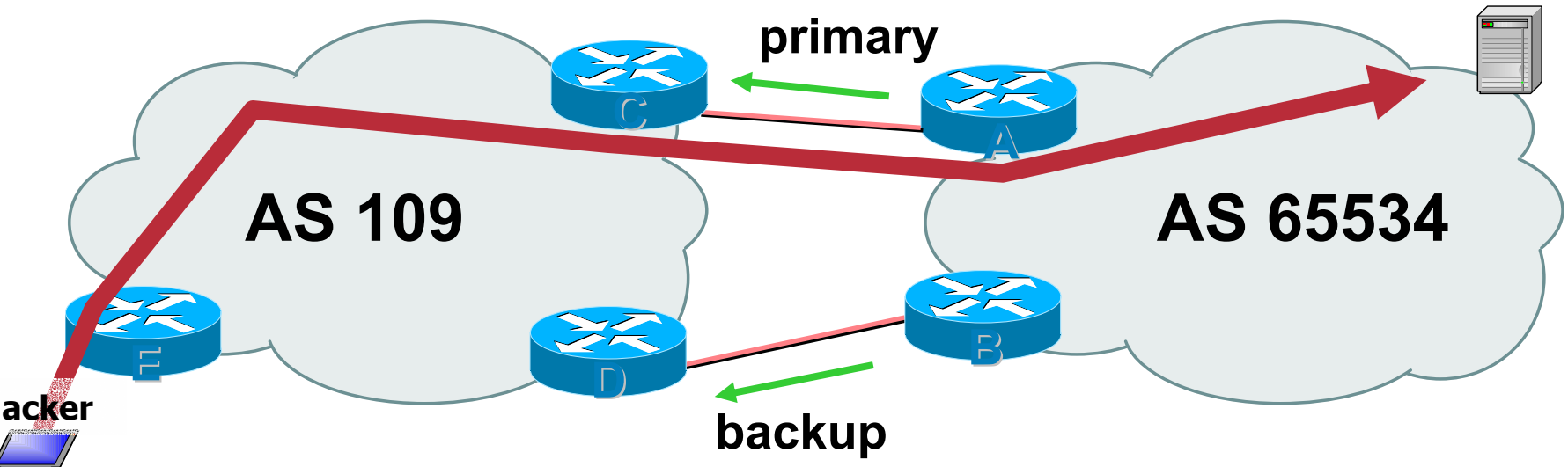
- It is all about the packet …..
- Once a packet gets into the Internet, someone, somewhere has to do one of two things:
  - ✓*Deliver the Packet*
  - ✓*Drop the Packet*
- In the context of a DOS attack, the question is *who* and *where* will that drop that packet.

Who drops the packet when ……..

- Single Homed Customer's Circuit Saturates from a DOS Attack.
- Which router has the static route?
- Which router has the aggregate route?

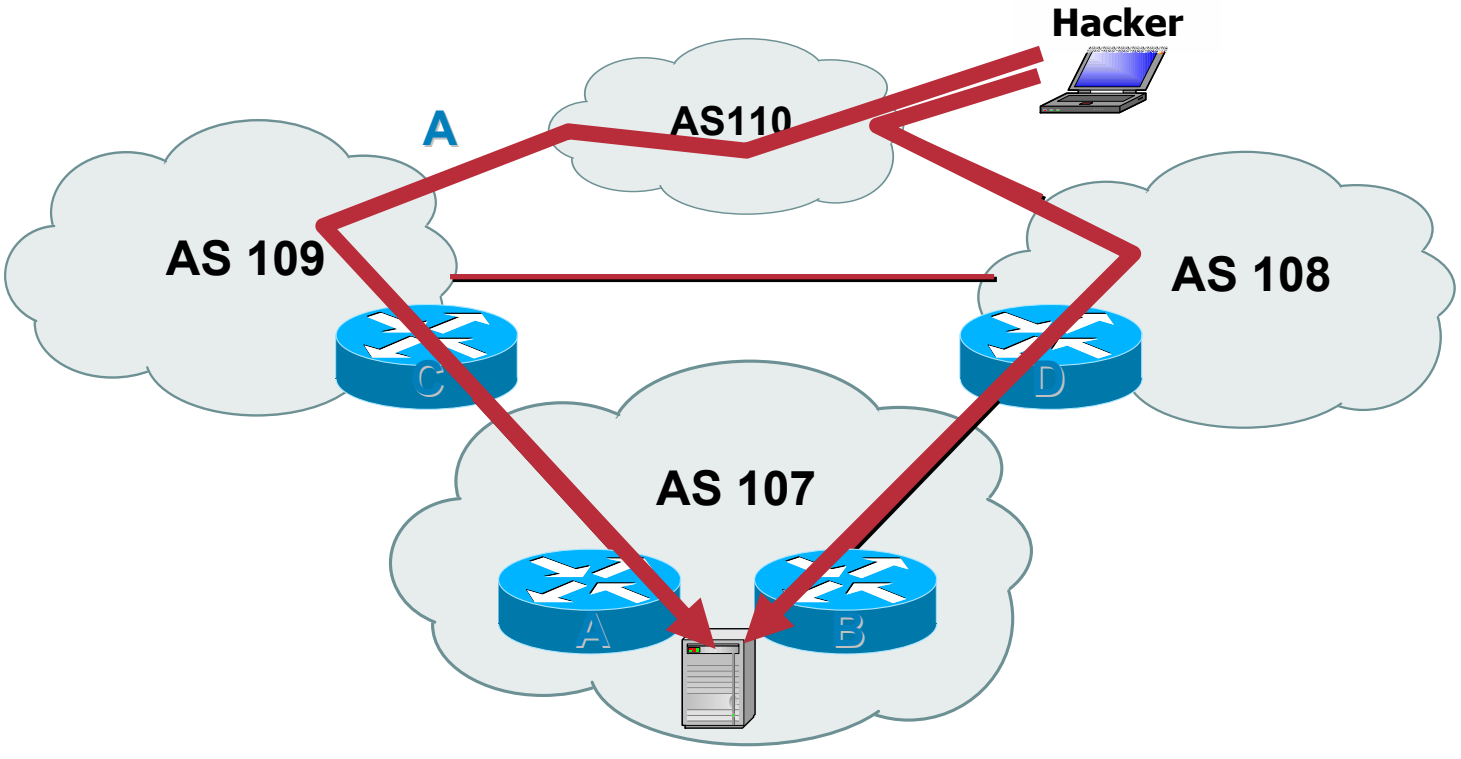


Who drops the packet when …….



- **Multihomed Customer's Primary Link get saturated?**
  - ✓Link saturation causes BGP to drop
  - ✓BGP drop on the primary means that the back-up is used
  - ✓Who drops the packets during convergence?
  - ✓Back-up path saturates, dropping BGP, then what? Back to primary?

Who drops the packet when …….



- **Multihomed Customer to two ISPs gets hit.**
  - ✓ **Line saturates, BGP drops, attack shifts OR attack aggregates!**

Co-Lateral Damage is Real

- Co-Lateral Damage is Real. If you have not yet experienced it, you will.
- How you architect your network, your routing, and your provisioning effects the extent of co-lateral damage.
- All those “VPN Tunneling Solutions” are just as vulnerable to co-lateral damage.
- What tools and techniques you prepare affects how you can mitigate the effects of co-lateral damage.
- Do nothing and you may find that a simple DOS attacks against one customer turns into a network nightmare.

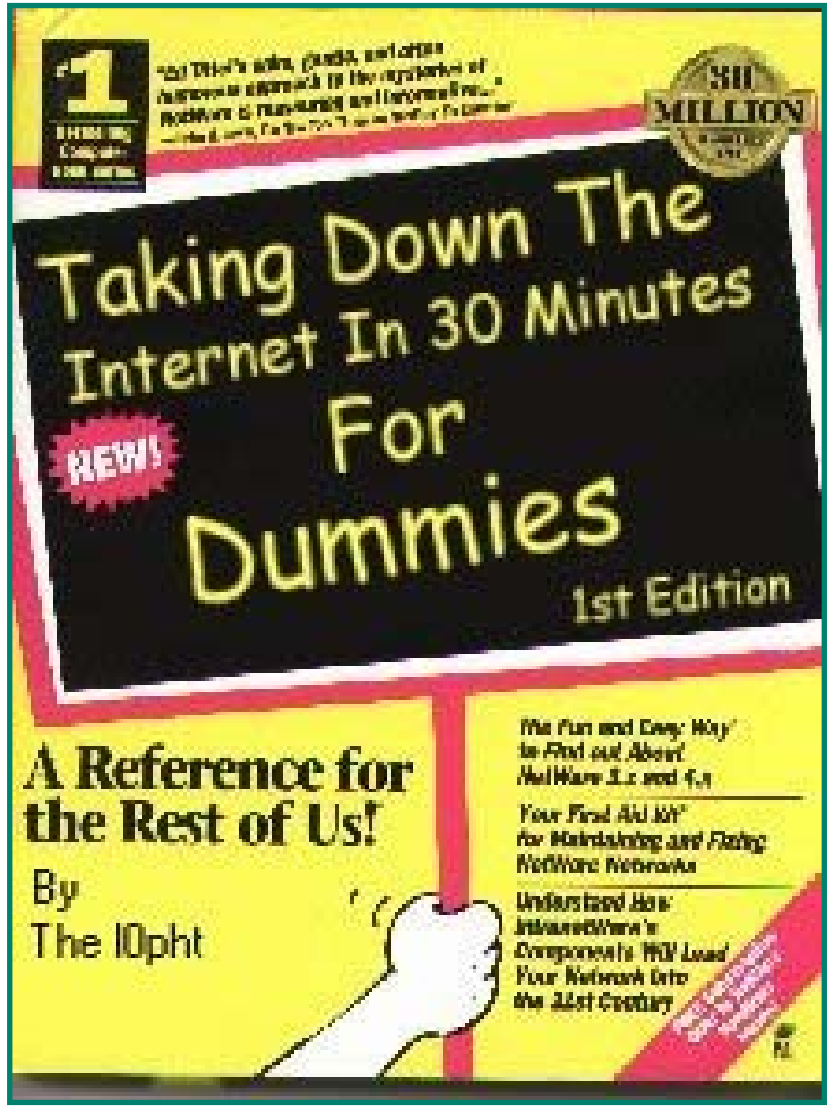
Six Phases of How a ISP Responds to a Security Incident

DOS/DDOS Attacks Today

- **The attackers have shifted the attack to their target's infrastructure.**
  - ✓ **ISPs and IXPs have and will be directly attacked to get at the target!**
  - ✓ **Co-Locations Companies are used as reflectors to hit other companies**
  - ✓ **DDOS agains OSPF and BGP ☹**

ISP Security

- ISPs need to:
  - ✓ Protect themselves
  - ✓ Help protect their customers from the Internet
  - ✓ Protect the Internet from their customers
  - ✓ At any given time there are between 20 to 40 DOS/DDOS attacks on the Net



Hardware Vendor's Responsibilities

- **Cisco System's example:**
  - ✓ **Operations people working directly with the ISPs**
  - ✓ **Emergency reaction teams (i.e. PSIRT)**
  - ✓ **Developers working with customers and IETF on new features**
  - ✓ **Security consultants working with customers on attacks, audits, and prosecution**
  - ✓ **Individuals tracking the hacker/phracker communities**
  - ✓ **Consultants working with governments/law enforcement officials**

ISP Networking Security Actions

- **ISP Security Actions are broken into the following task:**
  - **Protect the Router from Direct DOS Attack or Break-in**
  - **Protect the Routing Protocol from Direct Attack or Route insertion**
  - **Protect the Network from Direct Attack or Redirection**
  - **Trace Back Attacks and Stop/Rate-Limit them on the edge of the Network**
  - **Collect data on the attack for Law enforcement actions.**

- **First priority is item #1 – protecting the router from attack.**

What Do ISPs Need to Do?

- **Implement Best Common Practices**
  - ✓ **ISP infrastructure security (backbone)**
  - ✓ **ISP network security (internal LAN)**
  - ✓ **ISP services security (CPE)**
- **Work with operations groups, standards organizations, and vendors on new solutions**
- **But HOW ???**

ISP Security Incident Response

- ISPs are *transit networks*, so response happens is differently
- Mitigate the effects and trace it back *upstream* to its source.
- Working with ISP Security Teams have demonstrated six distinct phases in the way ISPs response to security incidents.

ISP Security Incident Response

- ✓Preparation
- ✓Identification
- ✓Classification
- ✓Traceback
- ✓Reaction
- ✓Post Mortem

Preparation

- **Preparation: All the work the ISP does to prepare he network, create the tools, test the tools, develop the procedures, train the team, and practice.**
  - ✓ **#1 Most critical phase of how a ISP responds to a security incident.**
  - ✓ **Big difference between ISPs who have prepared and those who have done nothing.**

Preparation

- Know the Enemy !!!
- Create the Security Reaction Team
- Prepare the Management Plane
- Prepare the Control Plane
- Prepare the Data Plane
- Prepare the Tools

Identification

- **Identification – How do you know you or your customer is under attack?**
  - ✓ **It is more than just waiting for your customers to scream or your network to crash.**
  - ✓ **What tools are available?**
  - ✓ **What companies are working on tools?**
  - ✓ **What can you do today on a tight budget?**

Classification

- **Classification – Understanding the type of attack and what damage is it causing.**
  - ✓ **You need to know what you (or your customer) are getting hit with.**
  - ✓ **Determines the rest of the incident response.**
  - ✓ **What tools are available?**
  - ✓ **How can you do this without crashing my router?**

Traceback

- **Traceback – From where is the attack originating?**
  - ✓ **Deterrence works. Traceback a few attacks to their source, capture the attacker, prosecute, and lock them up and you will have a credible deterrence.**
  - ✓ **Foundation Techniques**
  - ✓ **How to traceback to the edge of the Network?**
  - ✓ **How to continue traceback over the ISP – ISP boundary.**

Reaction

- **Reaction – Doing something to counter the attack – even if you choose to do nothing.**
  - ✓ **Should you mitigate the attack?**
  - ✓ **It is more then just throwing an ACL onto a router.**
  - ✓ **How to keep the attack from shifting from your customer to your network?**

Post Mortem

- **Post Mortem – Analyzing what just happened. What can be done to build resistance to the attack happening again.**
  - ✓ **The step everyone forgets!**
  - ✓ **Was the DOS attack you just handled, the real threat? Or was it a smoke screen for something else that just happened?**
  - ✓ **What can you do to make it faster, easier, less painful in the future?**

http://www.cisco.com/public/cons/isp/security/