DDoS: Protection Money or Mitigation

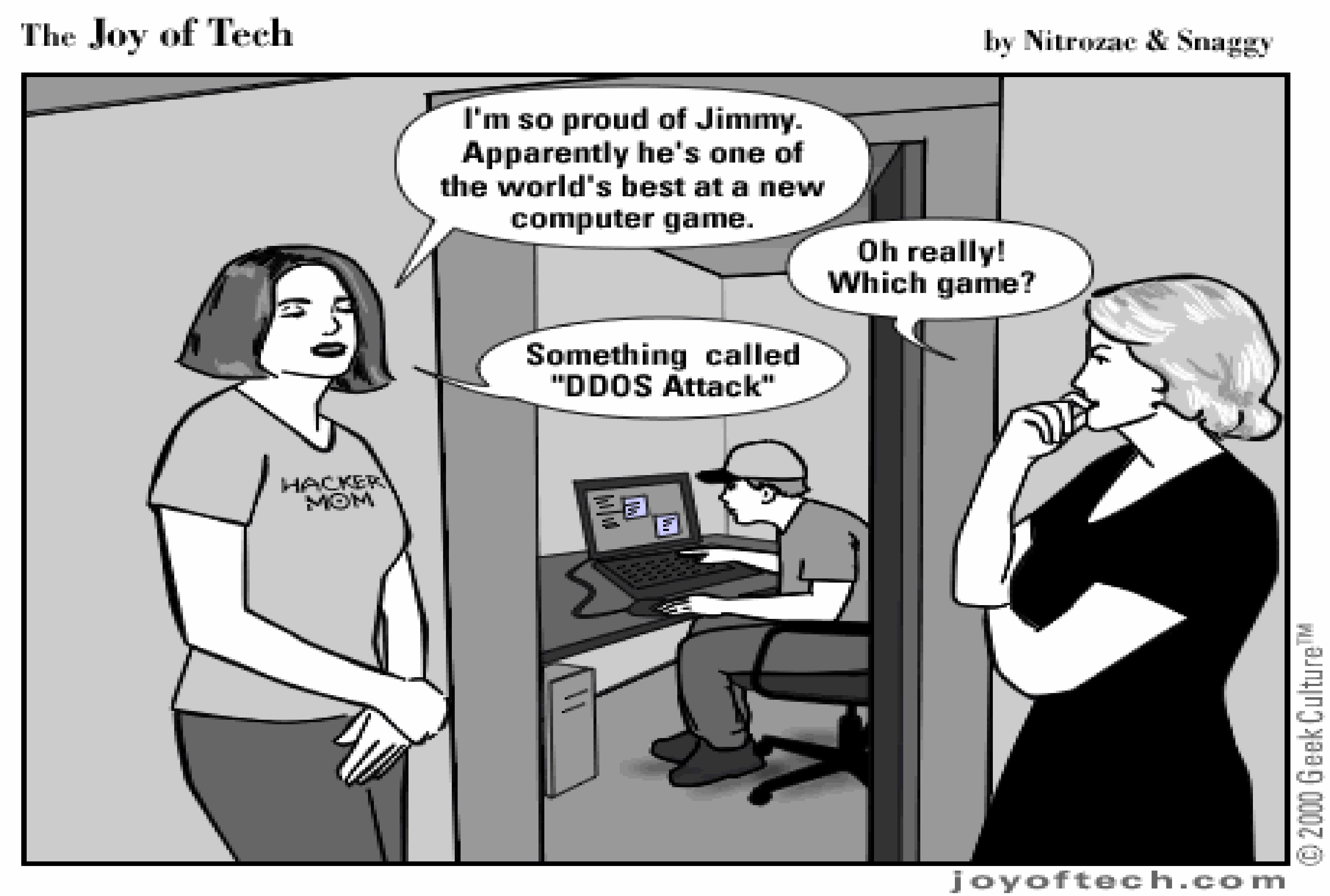
Bernie Trudel

Principal Consultant, Security

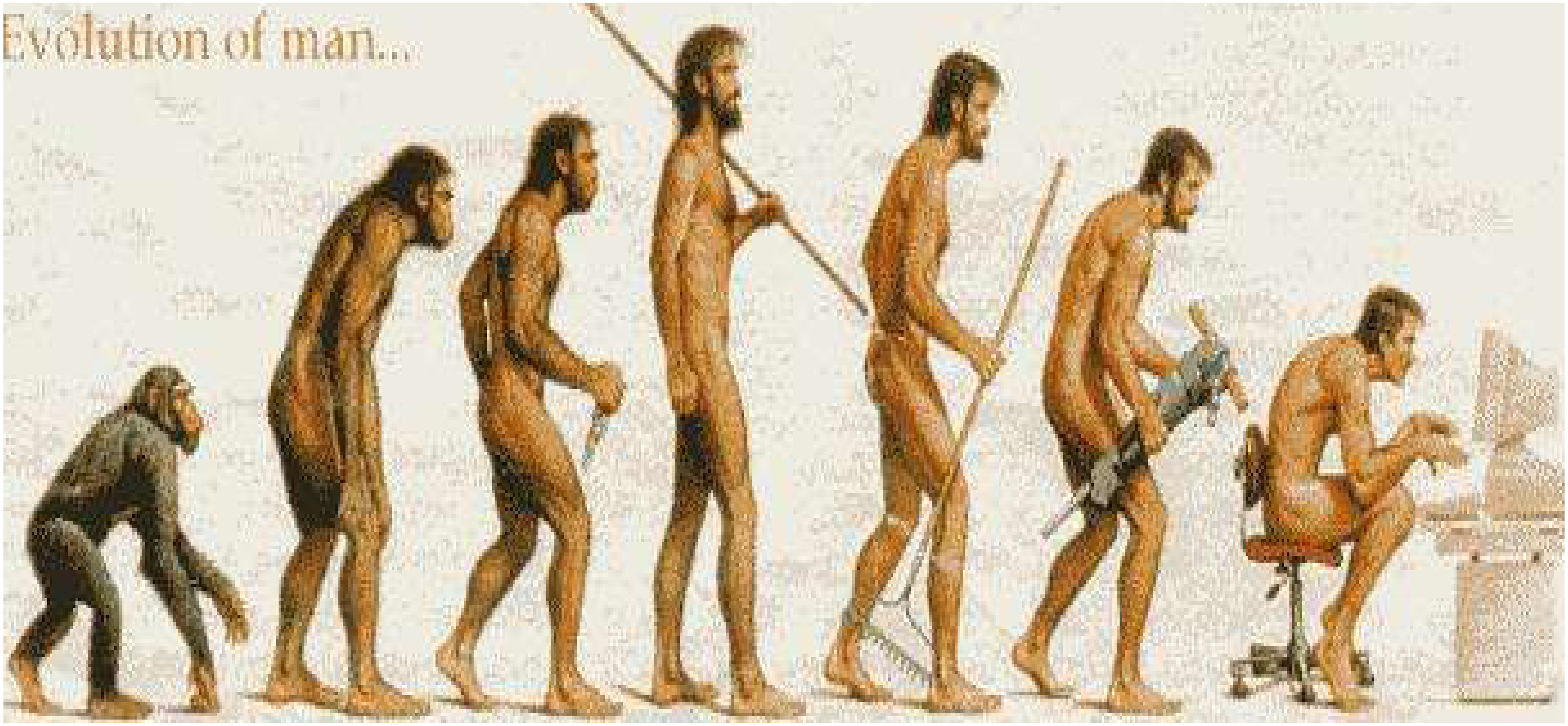
Cisco Systems APAC

btrudel@cisco.com

DDoS is a game


The Joy of Tech
by Nitrozac & Snaggy
I'm so proud of Jimmy. Apparently he's one of the world's best at a new computer game.
Oh really! Which game?
Something called "DDOS Attack"
HACKER MOM
© 2000 Geek Culture™
joyoftech.com

DDoS: the latest step in evolution of weapons?



Agenda

How serious are DDoS Attacks?

Detecting DDoS Attacks

Tracing DDoS Attacks

Mitigating DDoS Attacks

How serious are DDoS attacks?

News: January 22, 2002
Cloud-Nine Officially Closes ISP!

By: mark.j @ 10:44:AM—Comments (35)—SendNews [HERE]/PrintNews [HERE]

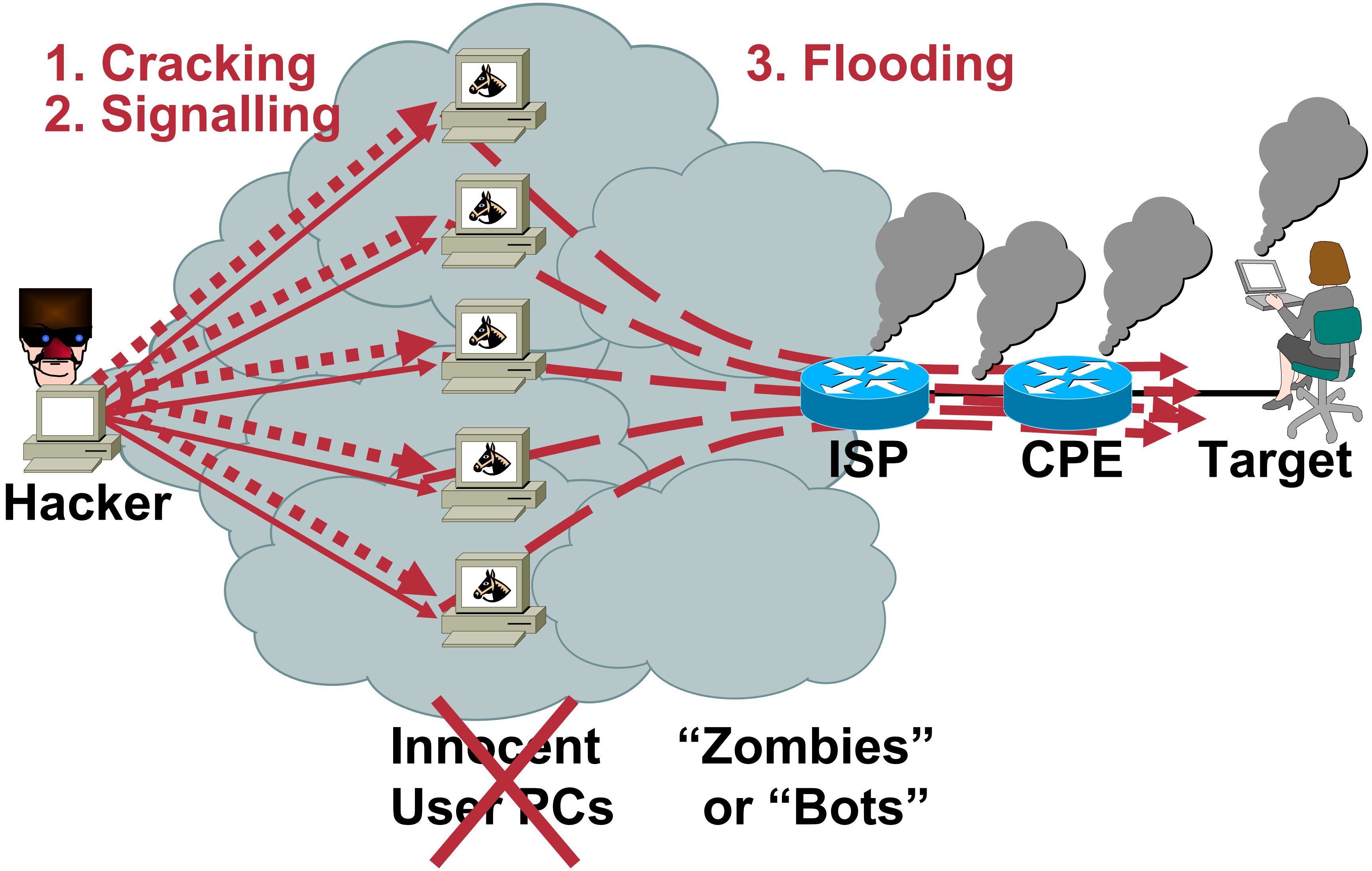
- Today looks set to be a sad and frustrating one for anybody who was ever a customer of the once popular unmetered dialup and broadband ISP Cloud-Nine
- At precisely 10:16 am a few minutes ago Emeric Miszti (CEO) and John Parr (Operations Director) of the C9 ISP posted what's likely to be their final announcement on our forums; C9 is now the latest ISP to close, although it's the first we've ever seen to go from a hack attack!:

> Cloud Nine regret to announce that at 7:45 this morning the decision was taken to shut down our Internet connections with immediate effect
>
> We tried overnight to bring our web servers back online but were seeing denial of service attacks against all our key servers, including email and DNS; these were of an extremely widespread nature
>
> http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619

Denial of Service Attacks

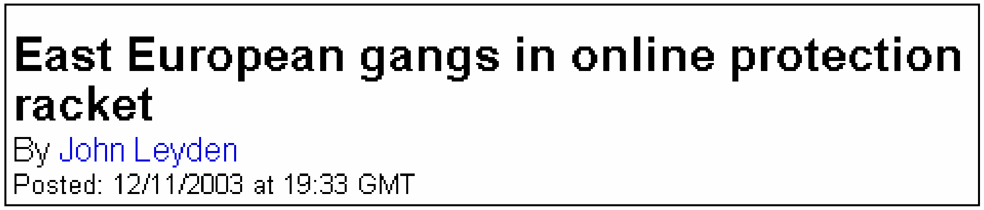
- We understand intrusions: Do things right, and you're okay
- What about DoS? Do things right, and still get drowned…
- DoS is often driven by financial motivation
    - DoS for hire :-(
- DoS cannot be ignored, your business depends on effective handling of attacks
- Worms and DoS are closely related
    - Secondary worm effects can lead to denial of service
    - Worms enable DoS

DDoS: The Procedure



DDoS Today: From Fun to Protection Money

The goal of an attacker is to cause the online company to be down without attracting too much public attention

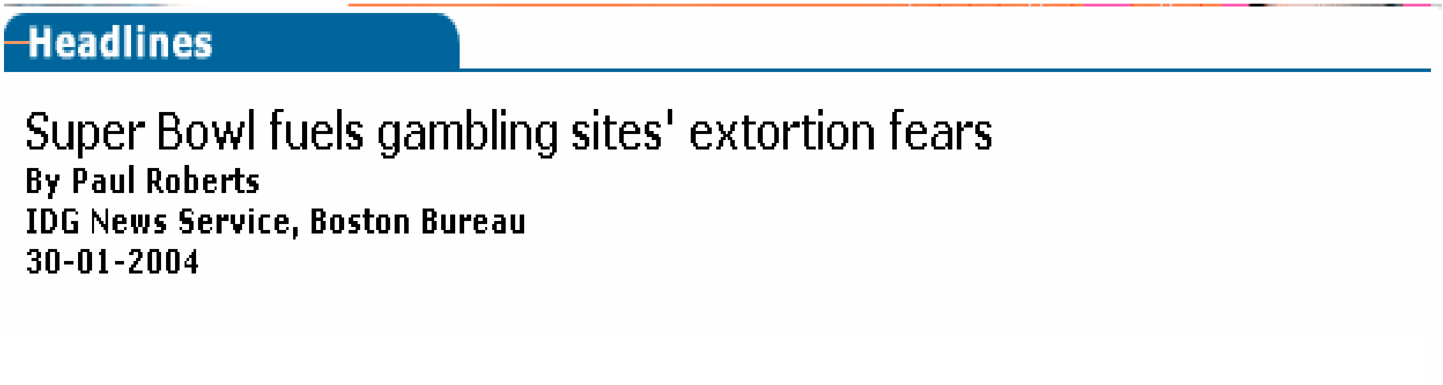


East European gangs in online protection racket

By John Leyden

Posted: 12/11/2003 at 19:33 GMT

- **Email: “Hello, allow me to introduce myself…, please provide us with $$$ or by next weekend your site is toast.”**
- **Next weekend, “hello its me again ☺”**
- **By the third weekend. “ our account number is ….”**



Super Bowl fuels gambling sites' extortion fears

By Paul Roberts

IDG News Service, Boston Bureau

30-01-2004

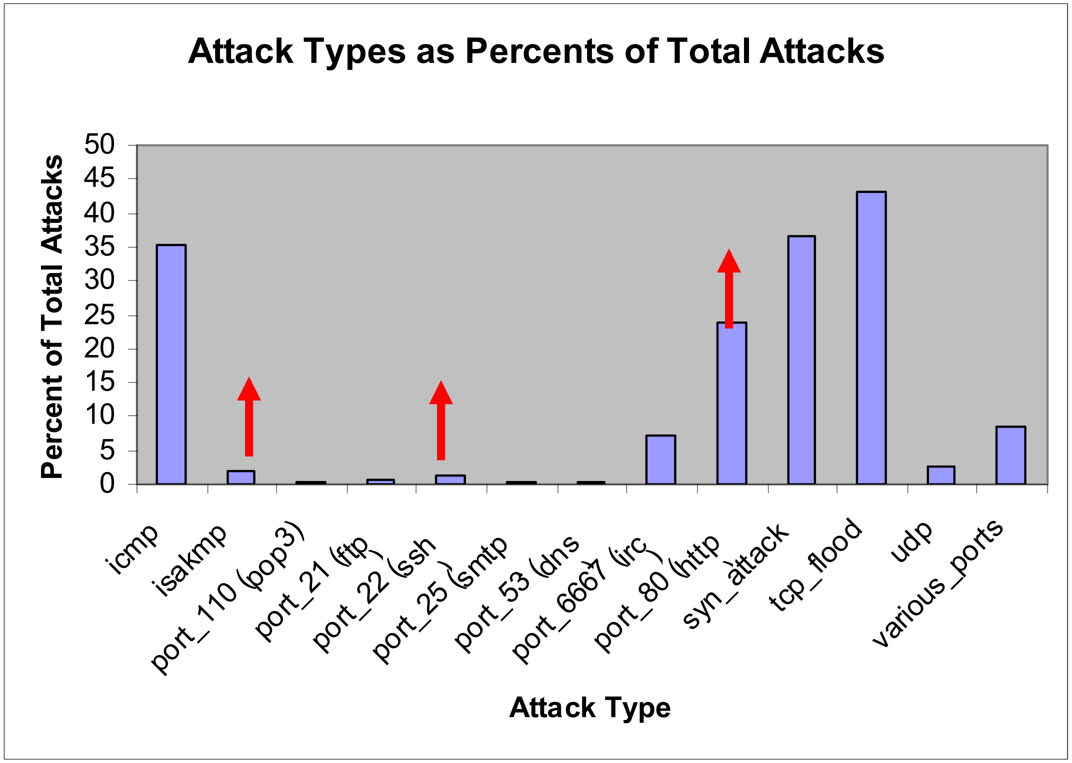
DETECTING DDOS ATTACK

Network Baselines

- Network baselines from a variety of sources
- Unexplained changes in link utilization
  - Worms can generate a lot of traffic, sudden changes in link utilization can indicate a worm
- Unexplained changes in CPU utilization
  - Worm scans can affect routers/switches resulting in increased CPU both process and interrupt switched
- Unexplained syslog entries
- These are examples
  - Changes don’t always indicate an attack or worm!
  - Need to know what’s normal to identify abnormal behavior

Trends in attack traffic

- Increase in port 80 non spoofed attacks
- Increase IPSec/SSH attacks
- Spoofed SYN attack still widely used
- ICMP still popular



*** Based on Cisco information**

Ways to Detect and Classify DoS Attacks

- Customer call
- SNMP: Line/CPU overload, drops
- NetFlow: Counting flows
- ACLs with logging
- Backscatter
- Sniffers
- Specialized Anomaly detectors

Abnormal CPU Load

A: CPU Total Utilization

B: CPU at Interrupt Level

```
router>sh proc cpu
CPU utilization for five seconds: 99%/97%; one minute: 78%; five minutes: 23%
```

- If A≈B: “Too much traffic to forward”

  Interrupts: Packet switching (fast switching)

- If A >> B: “Too much central processing”

  Packets to/from the router (e.g. SNMP, ICMPs, vty and console, IPsec (w/o h/w), routing…)

  Process switched packets or switching problem

  If attack, targeted at the router itself!

Netflow: Detection and Classification

- Netflow provides enough data to develop a baseline
    - What's normal --> what's abnormal
- Changes in Netflow indicative of changing traffic patterns
    - Might be DoS
    - SPAM and other mass mailers (e.g. a virus)
- Real-time Netflow display
    - Show ip cache flow; Use inc command as needed
- Data analysis
    - Export data for external analysis
    - Scripts, Netflow tools, Arbor Networks

Classifying DoS with ACLs

- **Requires ACLs to be in place (for detection)**

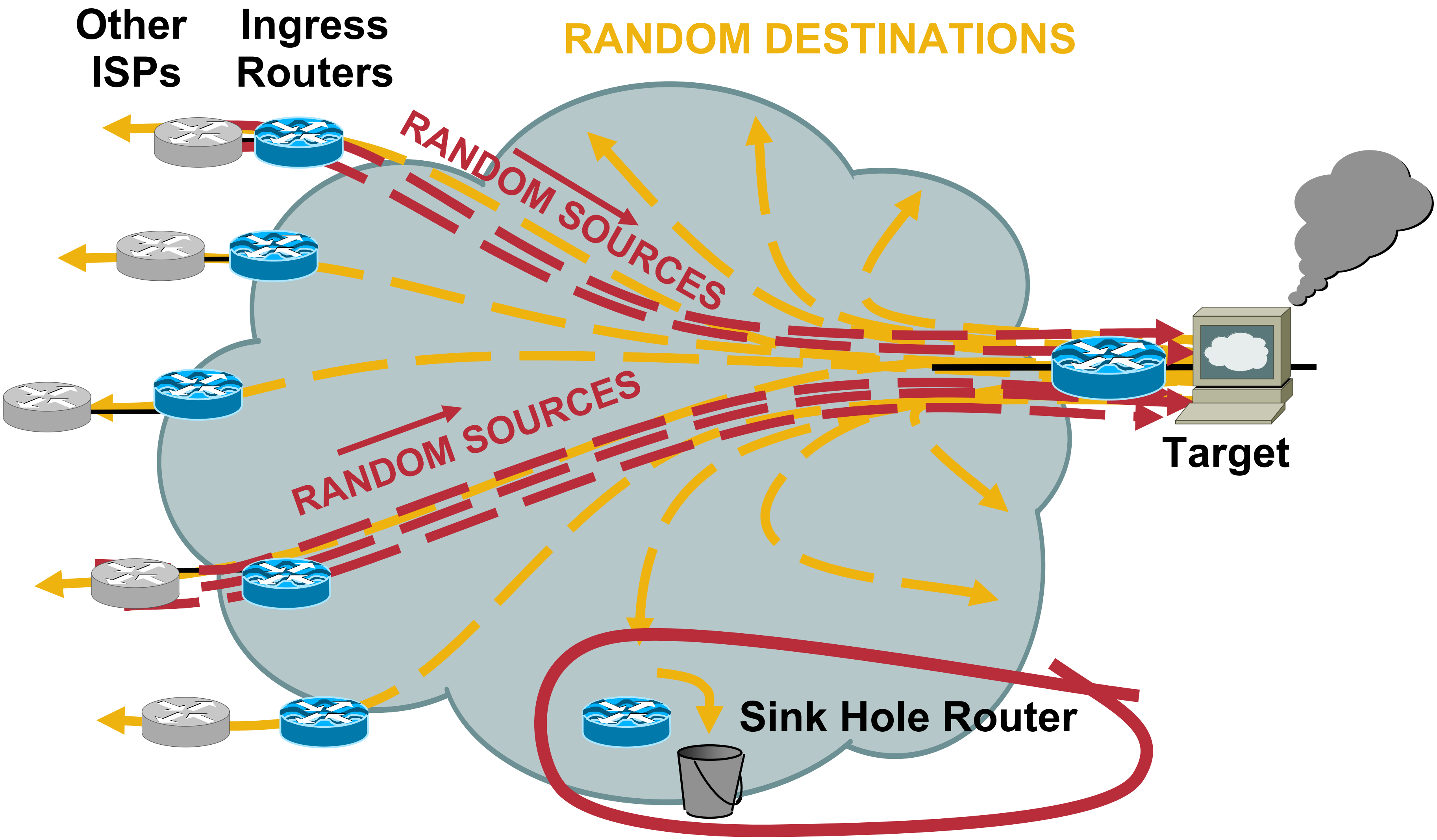
```
Extended IP access list 169
          permit icmp any any echo (2 matches)
          permit icmp any any echo-reply (21374 matches)
          permit udp any any eq echo
          permit udp any eq echo any
          permit tcp any any established (150 matches)
          permit tcp any any (15 matches)
          permit ip any any (45 matches)
```

Found:
- **Attack type**
- **Interface**

Looks Like Smurf Attack

- **Watch performance impact**
- **Used on demand, not pro-active**
- **More used for checking than for detection**
- **Some ASIC based LCs do not show counters**

Backscatter Analysis



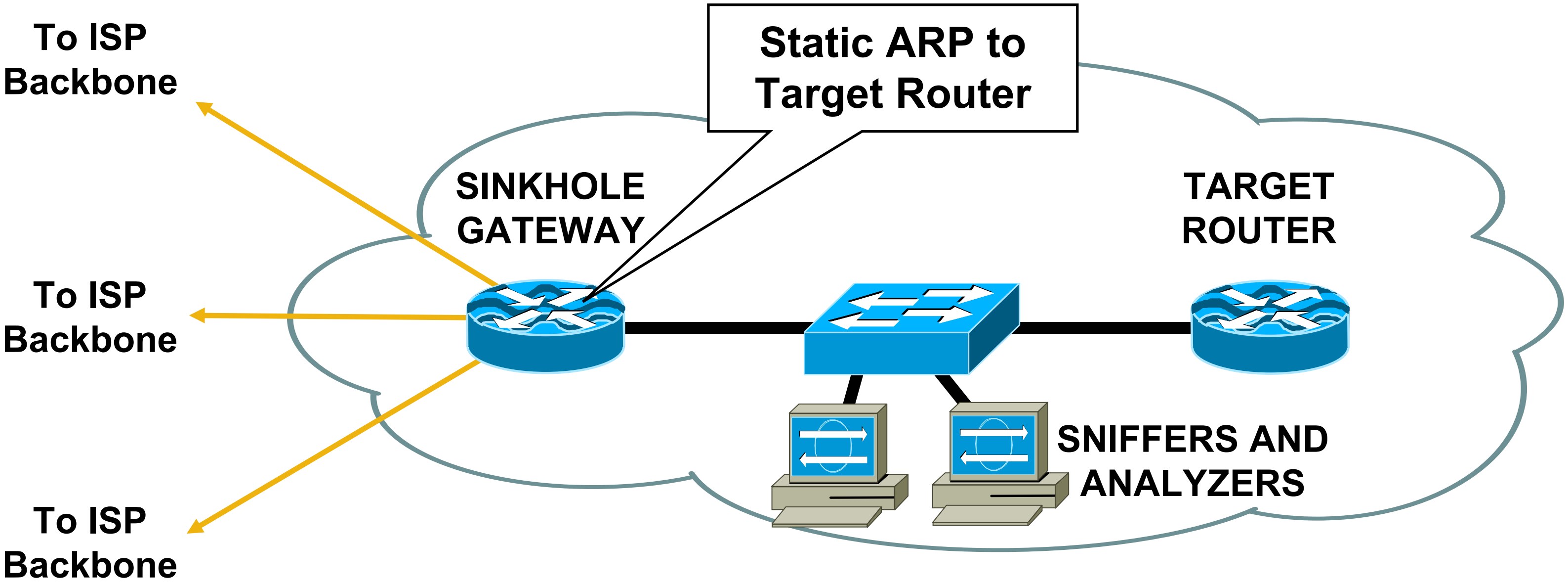
Backscatter Analysis

- Sink hole router: Statically announce unused address space (1/8, 2/8, 5/8, …)
  (see http://www.iana.org/assignments/ipv4-address-space)

  Note: Hackers know this trick: Use also unused space from your own ranges (aka DarkIP)

- Or, use default (if running full routing)
- Victim replies to random destinations
- → Some backscatter goes to sink hole router, where it can be analyzed

Sink Hole Architecture



- Dedicated network component to attract traffic
- Can also be used "on demand": pull the DoS/DDoS attack to the sinkhole
- Sink Hole design can also incorporate other elements

TRACING DDOS ATTACKS

Tracing DoS Attacks

- If source prefix is not spoofed:
  - → Routing table
  - → Internet Routing Registry (IRR)
  - → Direct site contact
- If source prefix is spoofed:
  - → Trace packet flow through the network
  - → Find upstream ISP
  - → Upstream needs to continue tracing

The Internet Routing Registry (IRR): AS Info

```
madrid% whois -h whois.arin.net  as109

OrgName:        Cisco Systems, Inc.
OrgID:          CISCOS-2
Address:        170 West Tasman Drive
City:           San Jose
StateProv:      CA
PostalCode:     95134
Country:        US

ASNumber:       109
ASName:         CISCOSYSTEMS
ASHandle:       AS109
 […]
TechHandle:     MRK4-ARIN
TechName:       Koblas, Michelle
TechPhone:      +1-408-526-5269
TechEmail:      mkoblas@cisco.com

OrgTechHandle:  DN5-ORG-ARIN
OrgTechName:    Cisco Systems, Inc.
OrgTechPhone:   +1-408-527-9223
OrgTechEmail:   dns-info@cisco.com
```

- **Europe: whois.ripe.net**
- **Asia-Pac: whois.apnic.net**
- **USA and rest: whois.arin.net**

Also, if domain known: abuse@domain

Tracing Back with Netflow

Routers Need Netflow Enabled

Victim

```
router1#sh ip cache flow | include <destination>
Se1      <source>    Et0       <destination>    11 0013 0007   159
…. (lots more flows to the same destination)
```

The flows come from serial 1

```
router1#sh ip cef se1
Prefix           Next Hop          Interface
0.0.0.0/0          10.10.10.2        Serial1
10.10.10.0/30       attached           Serial1
```

Find the upstream router on serial 1

Continue on this router

Tracing Back with ACLs

- **Create ACL:**

```
access-list 101 permit ip any <target> log-input
```

- **Apply to interface for a few seconds:**

```
interface xxx
ip access-group 101 in
   (wait a few seconds)
no ip access-group 101
```

- **Log shows interface the attack comes from**

```
14:17:21: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 105.12.73.84(0) (FastEthernet0/0
   0006.d780.2380) -> 192.168.1.1(0), 1 packet
14:17:22: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 166.159.237.65(0) (FastEthernet0/0
   0006.d780.2380) -> 192.168.1.1(0), 1 packet
```

mac Address

src Interface

IP Source Tracker

- Traditional way of tracking DoS: ACL or NetFlow
  - Limitation in performance and cross LC support

Line Card

- Source Tracker:
  - Across LCs, low performance impact
- Availability:
  - GSR E0,1,2,4: 12.0(21)S
  - GSR E3: 12.0(26)S
  - GSR E4+: 12.0(21)S (POS), (23)S (other)
  - 7500: From 12.0(22)S
  - Other: 12.3(7)T

Trace-Back in One Step: ICMP Backscatter

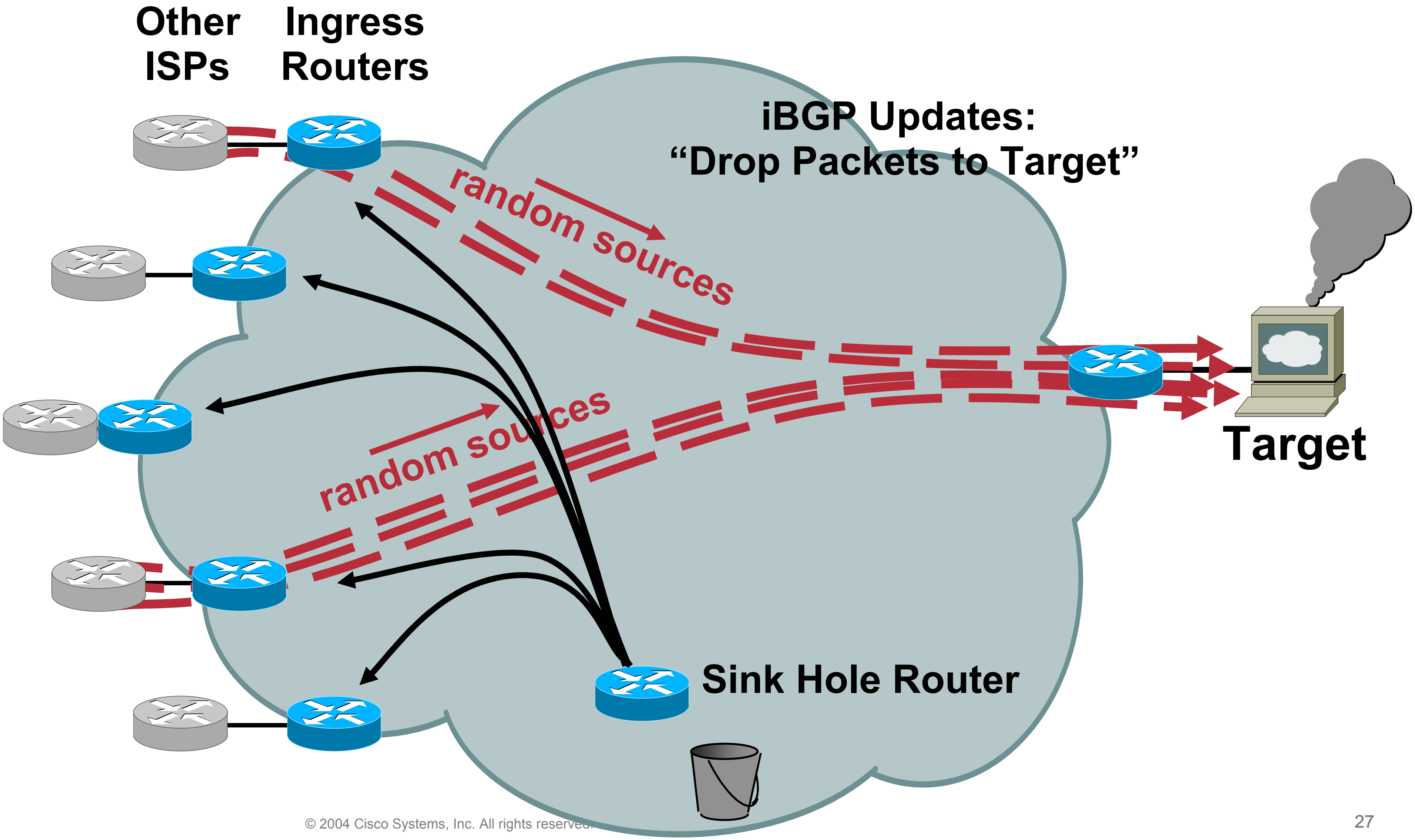
- **Border routers: Allow ICMP (rate limited)**
- **From sink hole router:**

  iBGP update to all ingress routers:
  “drop all traffic to <victim>” (details later)

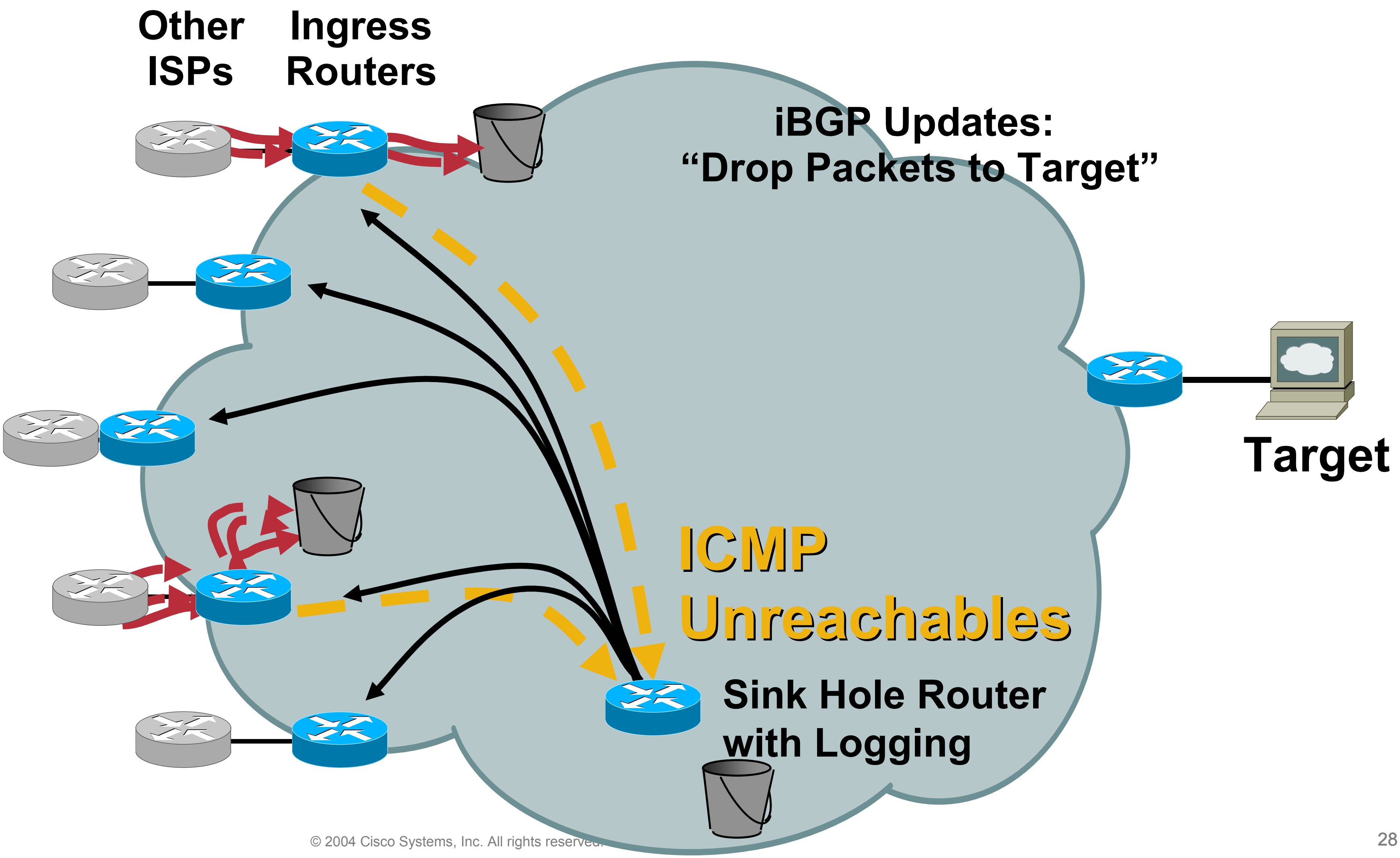
- **All ingress router drop traffic to <victim>**
- **And send ICMP unreachables to source!!**
- **For spoofed sources:**

  Sink hole router logs the ICMPs!

Trace-Back in One Step: ICMP Backscatter



Trace-Back in One Step: ICMP Backscatter



Summary Tracing DoS Attacks

- Non-spoofed: Technically trivial (IRR)

  But: Potentially tracing 100’s of sources…

- Spoofed:

  IP Source Tracker: router by router

  NetFlow:
  Automatic if analysis tools are installed
  Manually: Router by router

  ACLs:
  Has performance impact on some platforms
  Mostly manual: Router by router

  Backscatter technique:
  One step, fast, only for spoofed sources

MITIGATING DDOS ATTACKS

Response Options

- Wide range of response options exists
    - Access-control lists
    - QoS tools such as CAR
    - IDS, FWs, NBAR, etc.
- At an SP level we need to react with rapid, widespread solutions:
    - BGP Triggered Tools
    - Packet Scrubbing

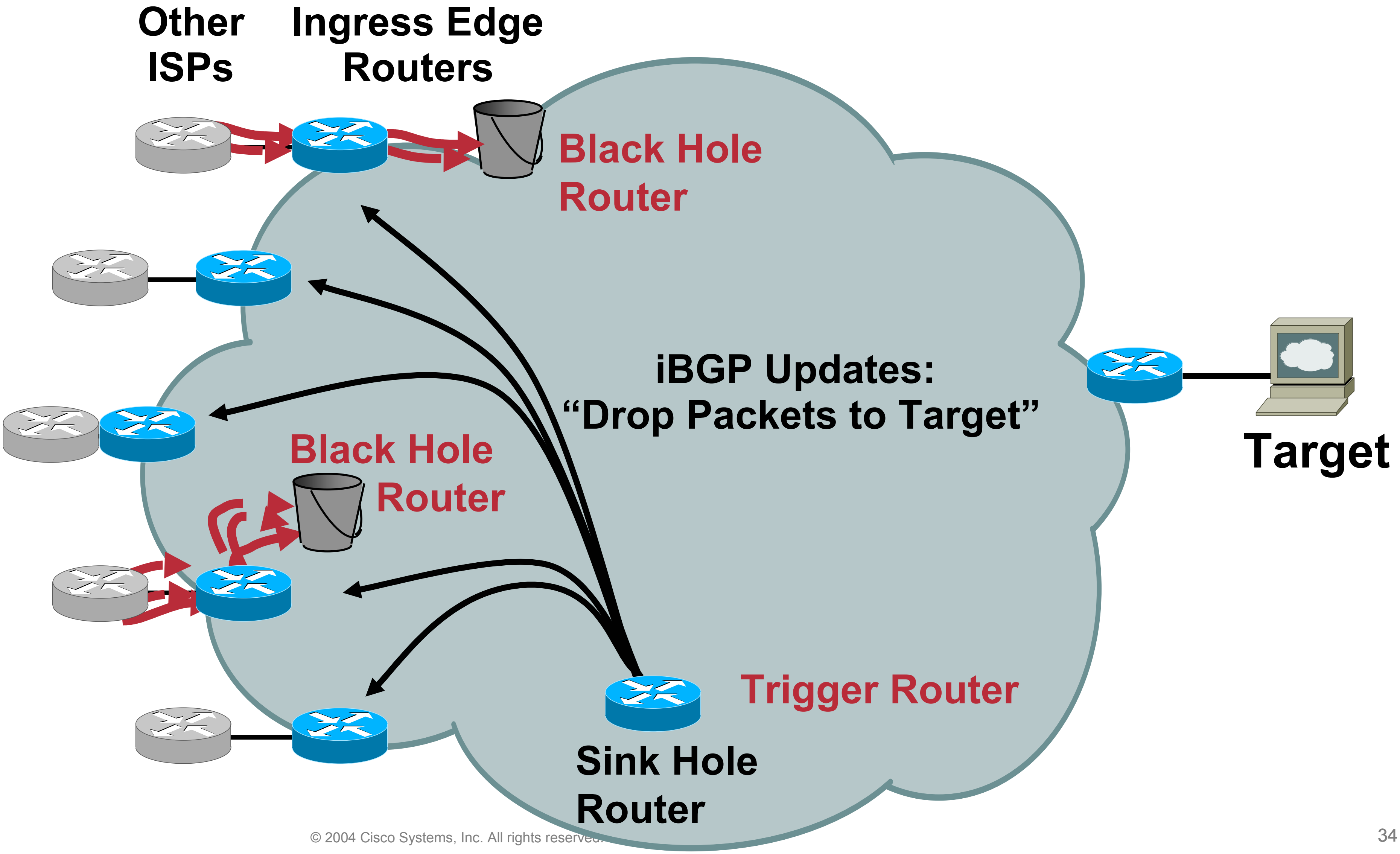
Remotely Triggered Black Hole Filtering

- We will use BGP to trigger a network wide response to an attack
- A simple static route and BGP will enable a network-wide destination address black hole as fast as iBGP can update the network
- This provides a tool that can be used to respond to security related events and forms a foundation for other remote triggered uses
- Service: Customer Triggered
  - Customer trigger the update yourself, SP doesn't get involved
  - Implication: customer detects and classifies, etc.

Remote Triggered Black Hole

- Configure all edge routers with static route to null0 (must use “reserved” network):
  - ip route 192.0.2.1 255.255.255.255 null0
- Configure trigger router
  - Part of iBGP mesh
  - Dedicated router recommended
- Activate black hole
  - Redistribute host route for victim into BGP with next-hop set to 192.0.2.1
    - Use route-map set next-hop 192.0.2.1
  - Route is propagated using BGP to all BGP speaker and installed on routers with 192.0.2.1 route
  - All traffic to victim now sent to null0

Remote Triggered Black Hole

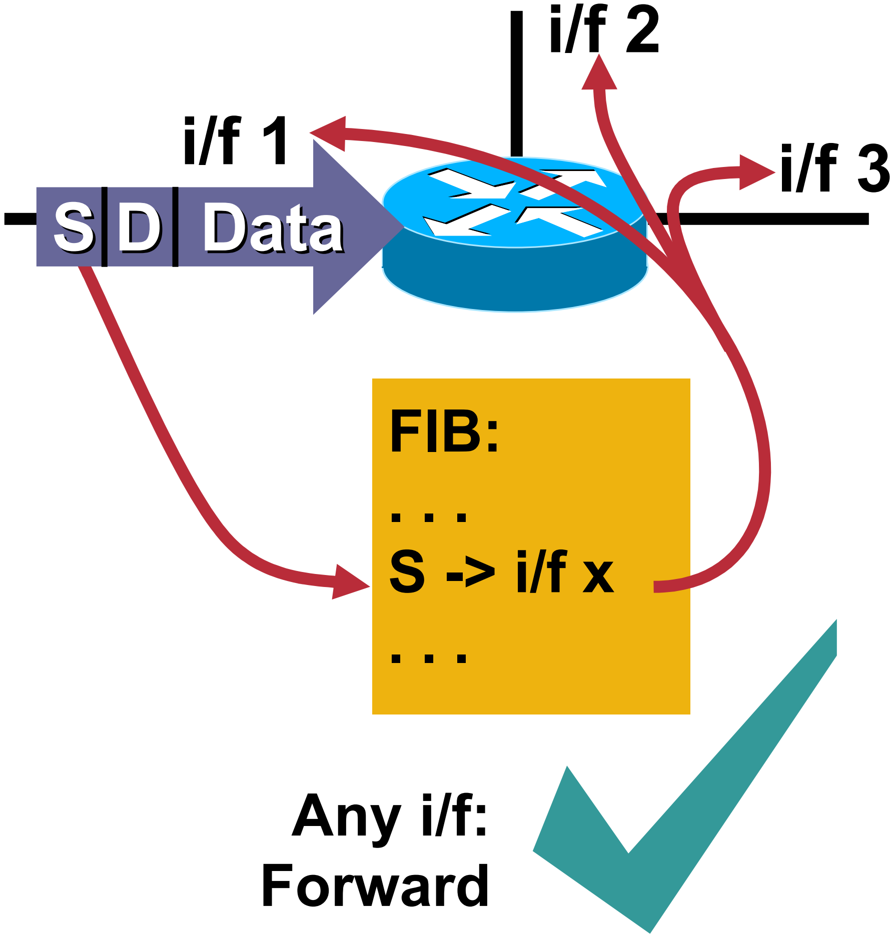


Flipping It Around: Triggered Source Drops

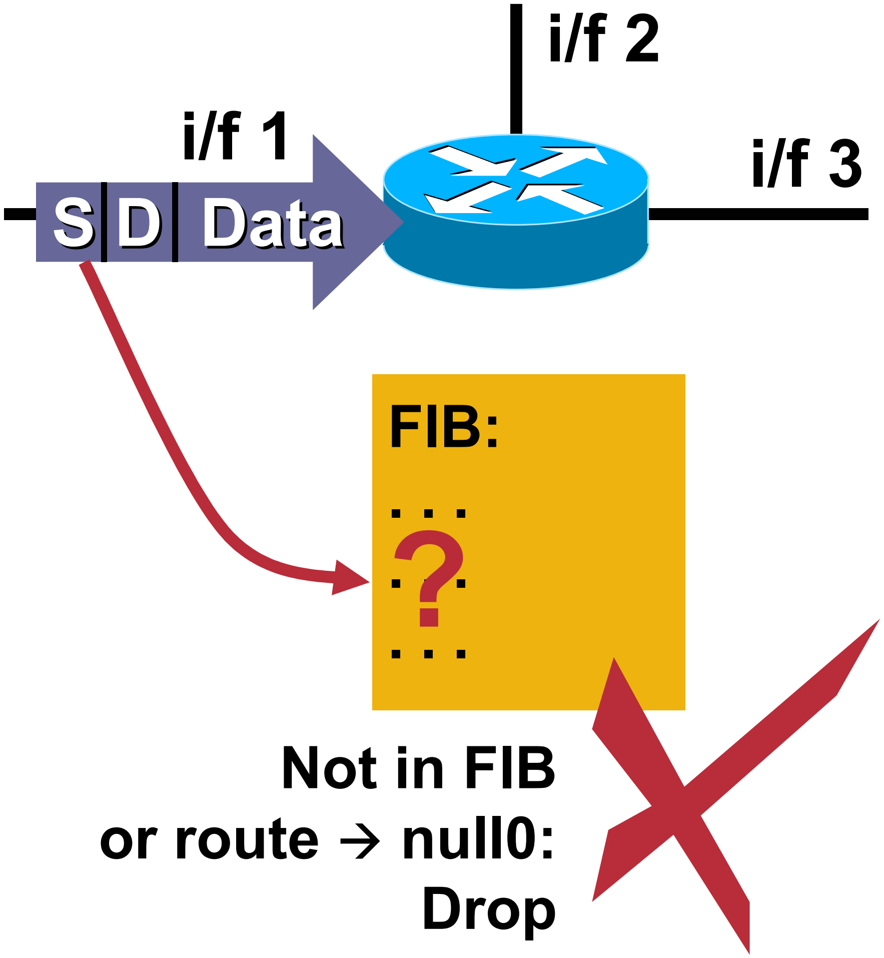
- Dropping on destination is very important
    - Dropping on source is often what we really need
- Reacting using source address provides some interesting options:
    - Stop the attack without blackholing real services
    - Filter command and control servers
    - Filter (contain) infected end stations
- Must be rapid and scaleable
    - Leverage pervasive BGP again

Loose uRPF Check (Unicast Reverse Path Forwarding)

router(config-if)# **ip verify unicast source reachable-via any**



Any i/f:
Forward



Not in FIB
or route → null0:
Drop

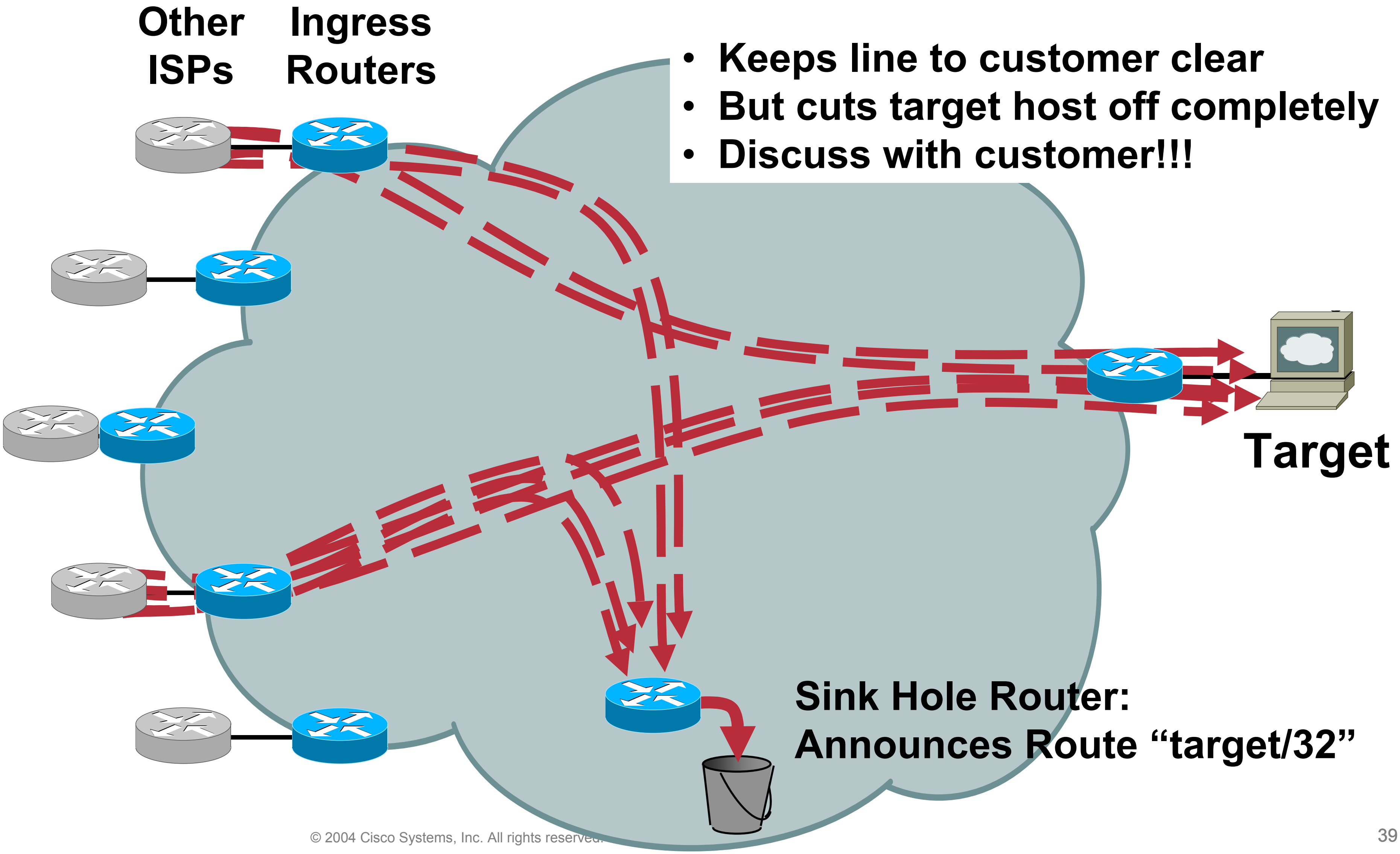
Source-Based Remote Triggered Black Hole Filtering

- **What do we have?**
  - **Black Hole Filtering—If the destination address equals Null 0 we drop the packet**
  - **Remote Triggered—Trigger a prefix to equal Null 0 on routers across the Network at iBGP speeds**
  - **uRPF Loose Check—If the source address equals Null 0, we drop the packet**
- **Put them together and we have a tool to trigger drop for any packet coming into the network whose source or destination equals Null 0!**

Evolution of DDoS impact

Distribution	**Management**	**# Attackers** (Bandwidth)	**Type of attack**	**Protection**
–Email attach –Download from questionable site –via "chat" –ICQ, AIM, IRC –Worms	Via botnets	**~X00,000 attackers** (X-X0 Gbps)	**•Legitimate requests** **•Infrastructure elements (DNS, SMTP, HTTP…)**	**•Blackhole (?)** **•ACL (?)** **•DDoS solutions** **•Anycast (?)**
–Email attach –via "chat" ICQ, AIM, IRC…	Manually	**~X00-X,000 Attackers** (X00 Mbps)	**•All type of applicatios (HTTP, DNS, SMTP)** **•Spoofed SYN**	**•ISP/IDC** **•Blackhole** **•ACL** **•DDoS solutions**
Manually (hack to servers)	Manually	**X0-X00 attackers** (X0 Mbps)	**Spoofed SYN** **Protocols (eg ICMP)**	**•Enterprise level** **•Firewall/** **•ACL access router**

Re-Directing Traffic from the Victim



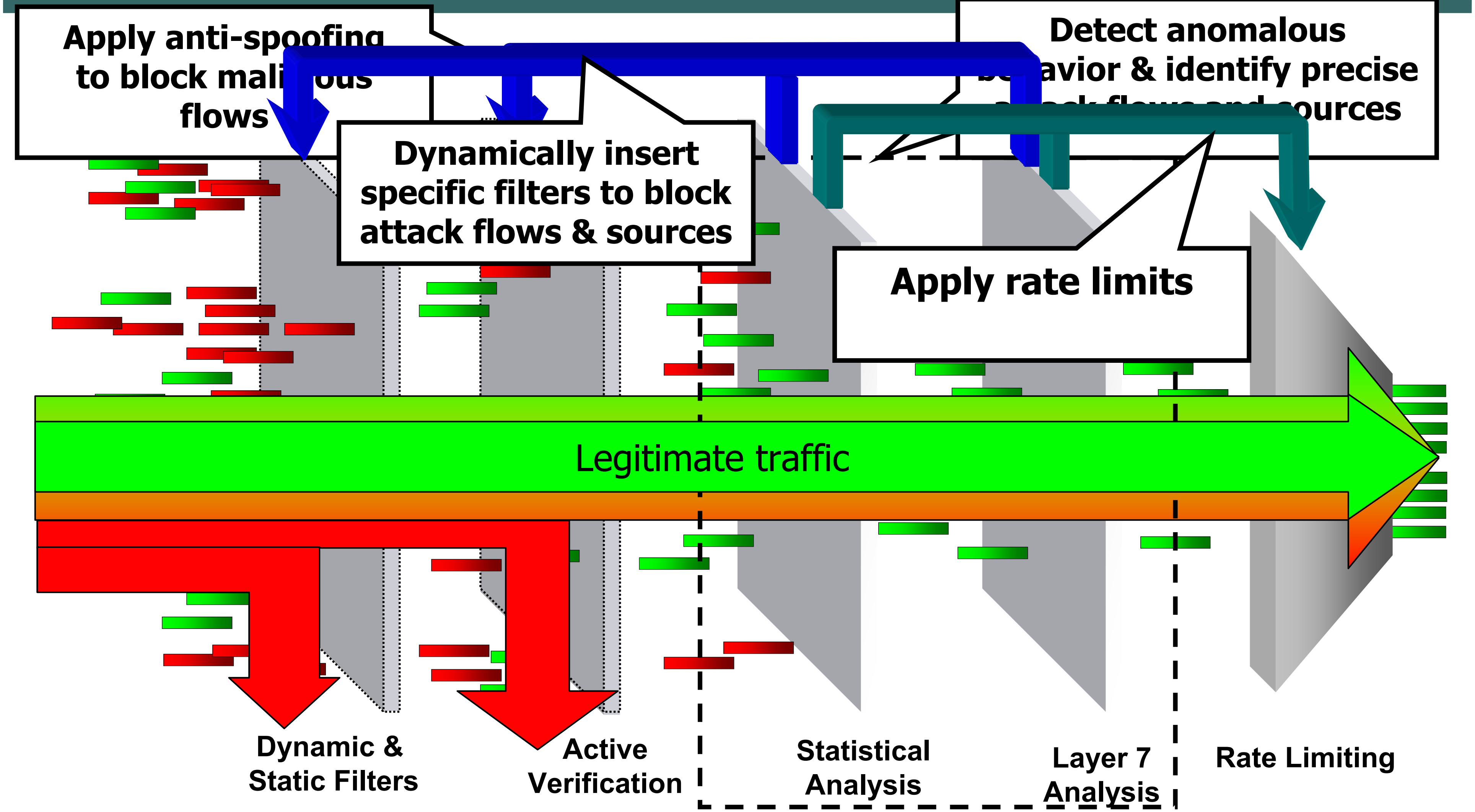
- Keeps line to customer clear
- But cuts target host off completely
- Discuss with customer!!!

Sink Hole Router:
Announces Route “target/32”

Mitigation: Packet “Scrubbing”

- Use the same BGP mechanism to redirect traffic to scrubbing devices
- Activate redirection:
  - Redistribute host route for victim into BGP with next-hop set to scrubbing devices
  - Route is propagated using BGP to all BGP speaker and traffic redirected
- When attack is over, BGP route can be removed to return to normal operation

Multi-Verification Process (MVP) – Packet Scrubbing



Apply anti-spoofing to block malicious flows
Dynamically insert specific filters to block attack flows & sources
Detect anomalous behavior & identify precise attack flows and sources
Apply rate limits
Legitimate traffic
Dynamic & Static Filters
Active Verification
Statistical Analysis
Layer 7 Analysis
Rate Limiting

Wrap-Up

What Can Be Done Now

- Detect DoS Attacks (SNMP, NetFlow, ACL)
- Trace back random packet floods (NetFlow, ACLs, IP source tracker)
- Shun a destination (routing, ACL)
- Shun a source (uRPF, ACL)
- Limit attacking traffic (CAR)
- Remote trigger via iBGP
- For sophisticated attacks; scrub the traffic

References

- **DoS Detection:**

  “Tackling Network DoS on Transit Networks”: David Harmelin, DANTE, March 2001 (describes a detection method based on NetFlow) [http://www.dante.net/pubs/dip/42/42.html]

  “Inferring Internet Denial-of-Service Activity”: David Moore et al, May 2001; (described a new method to detect DoS attacks, based on the return traffic from the victims, analysed on a /8 network; very interesting reading) [http://www.caida.org/outreach/papers/backscatter/index.xml]

  “The spread of the code red worm”: David Moore, CAIDA, July 2001 (using the above to detect how this worm spread across the Internet) [http://www.caida.org/analysis/security/code-red/]

- **DoS Tracing:**

  “Tracing Spoofed IP Addresses”: Rob Thomas, Feb 2001; (good technical description of using NetFlow to trace back a flow) [http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html]

- **Cisco:**

  NetFlow Performance White Paper

  [http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ntfo_wp.htm]

  DDoS Anomaly Detector (XT5600) and Guard (XT5650) Technology [http://www.cisco.com/go/security]

What Will the Future Bring?

- More PCs always online (DSL, Cable)
  - The vulnerabilities are here!
  - Need quarantine and containment solutions
- More vulnerabilities and zombies?
- Better integration of detection and reaction
- Improved distinction of “good” from “bad” packets
- Increased infrastructure attacks
- More and more DDoS: it pays well

Other Types of DoS :-)

THANK YOU! QUESTIONS?

CISCO SYSTEMS