IFIP Workshop: Infrastructure Security Overview and Operational Survey Results

Annapolis, MD
June 29, 2006

danny@arbor.net

USA
HOME OF ~~2006~~ 2010 World Cup Champions!

Agenda

- Network Architecture Evolution
- Security Survey Overview

Economics Dictation…

- Re**new**ed focus on profitability

--> Optimizing OPEX driving IP-based network services convergence

  - Vanilla Internet connectivity a commodity; industry consolidation
  - Ethernet/ATM/FR -> Layer 2 VPNS (PWE3, VPLS)
  - FR/ATM -> IP VPNs
  - PSTN -> VoIP
  - Cable/Voice/Video -> Triple Play (+Mobile == Quad)

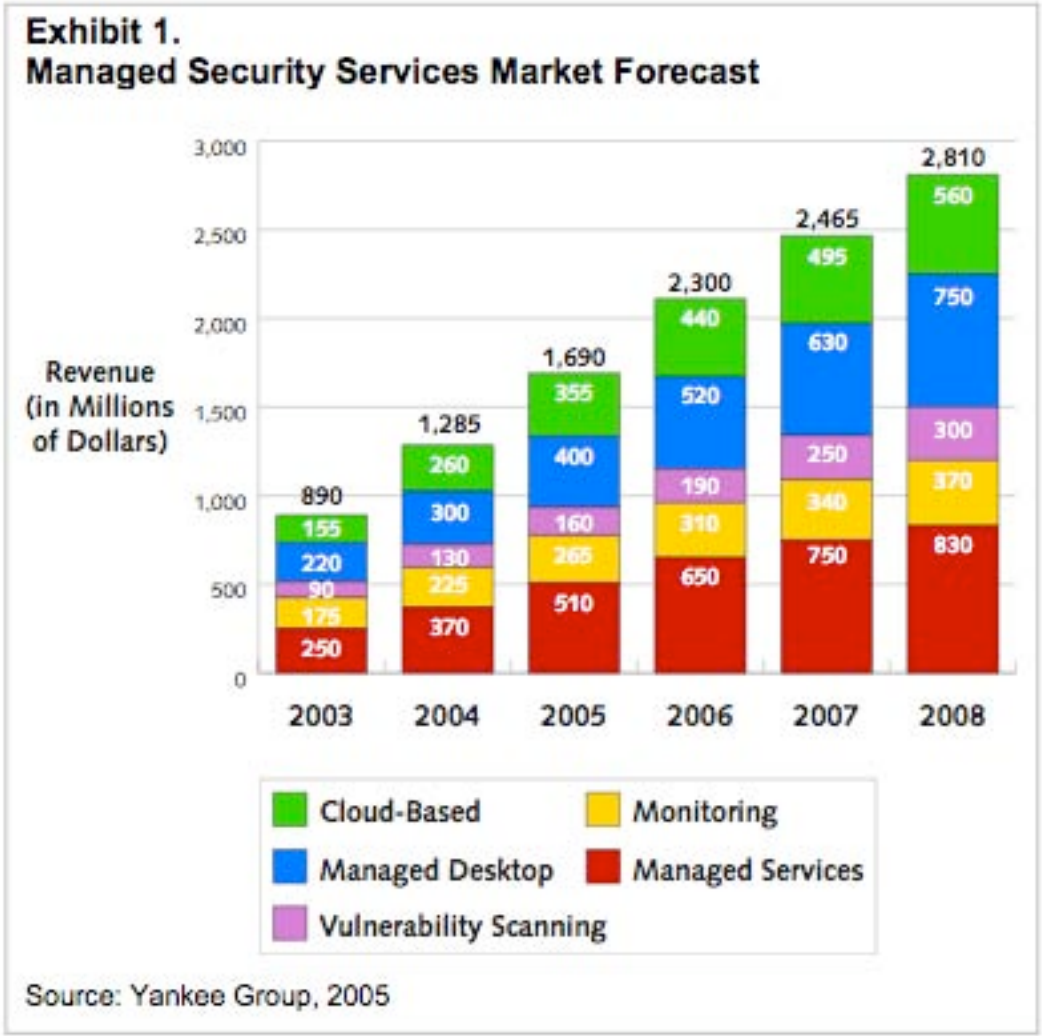
----> Network Convergence drives availability

------> Availability driven by traditional expectations:

  - Performance (latency, jitter, packet loss)
  - Redundancy/Resiliency
  - Security

Market Sizing Forecast

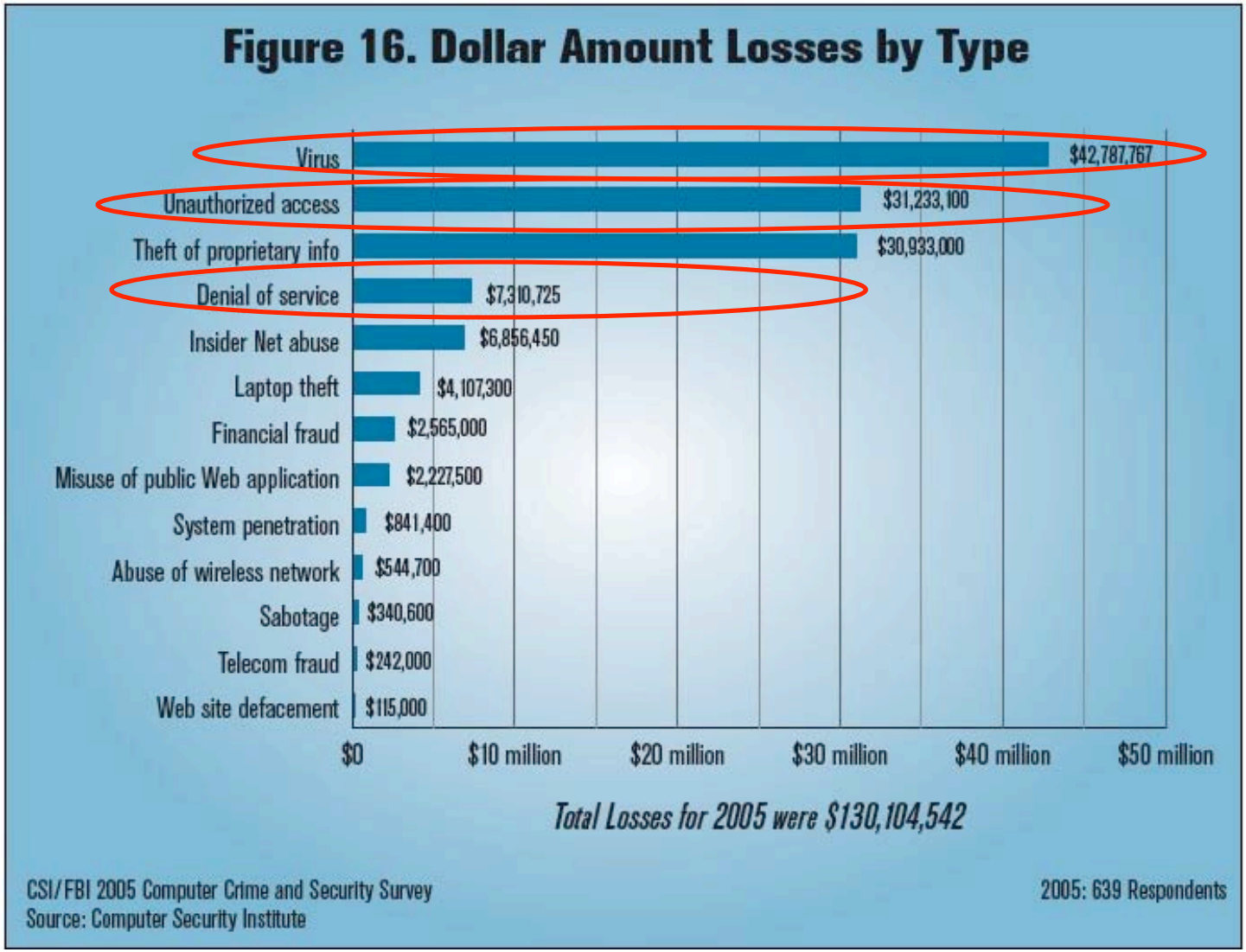
- Network/Cloud-based security services market expected to reach $560 million in 2008 - independent of associated PSS revenue opportunity



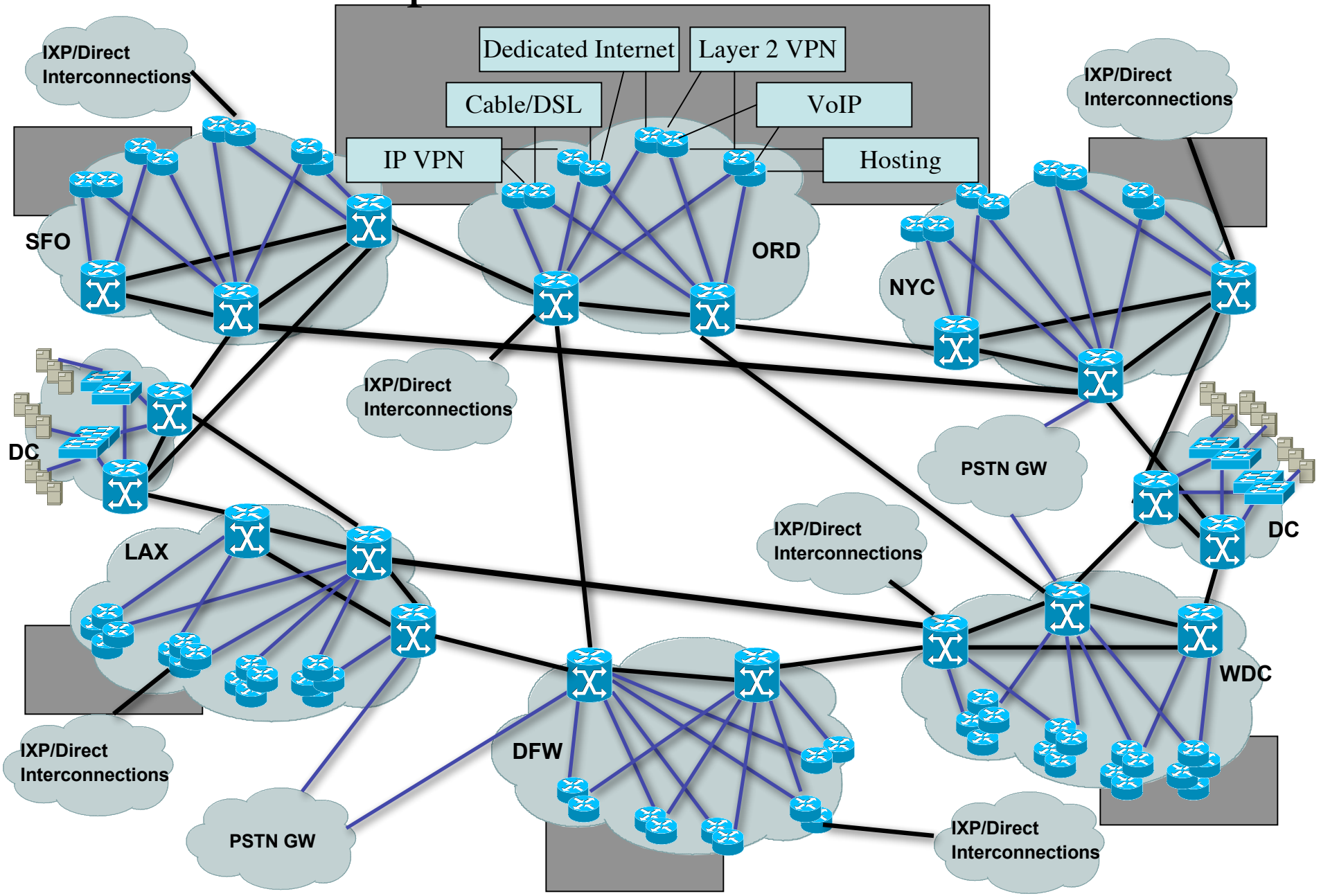
Economics Dictation (cont.)

- Network Neutrality?
  - Optimize network resources
    - Decoupling of access loops and subscriber services
    - Lack of broadband subscriber profitability
    - Peering (removing the middle man?), content distribution, traffic engineering
    - Capital life in the network - move it further out towards the edge but wait, need more features revenue generating services
- Ahh, and so too are the miscreant$ optimizing for profitability
  - Worms/Viruses evolve to less disruptive better monetized infection/compromise propagation vectors
  - Array of revenue generating service opportunities for compromised hosts, why take down the infrastructure

Cost of DoS, Worm & Viruses

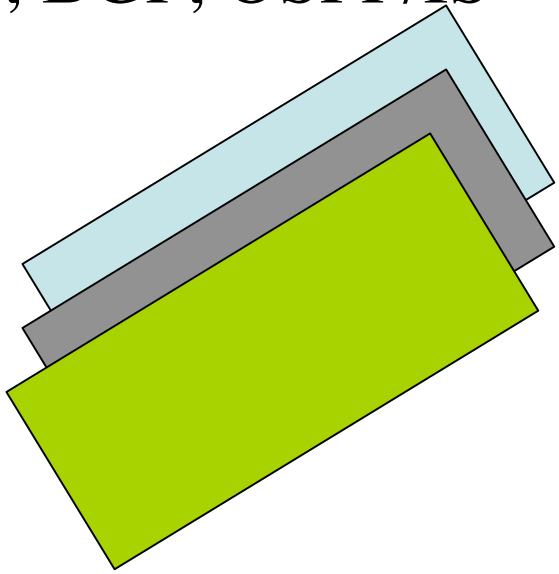


Sample Network Architecture



Compartmentalizing the Problem: Three Discrete Planes

- Management Plane
  - SNMP, Telnet, Out of Band Access, Etc..
- Control Plane
  - Routing & Signaling Protocols; BGP, OSPF/IS-IS, LDP, Etc..
- Data Plane
  - Packet forwarding functions



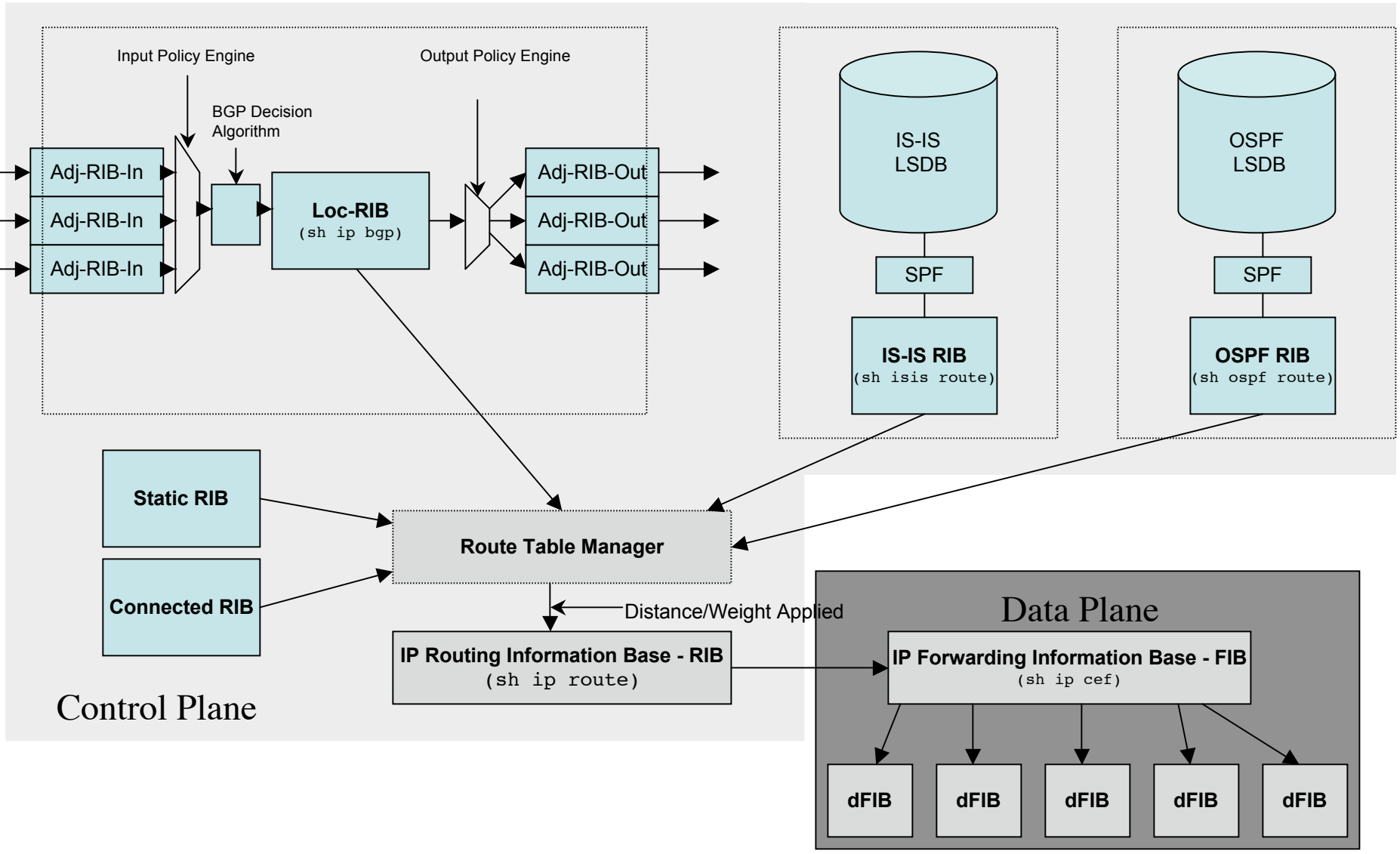
Management Plane

- Device Access & Management Functions
- Protocols include:
  - Telnet
  - SSH (Secure Shell)
  - SNMP (Simple Network Management Protocol)
  - Syslog
  - NTP (Network Time Protocol)
- Also consider console & OOBA (out of band access), etc..
- Network management
- Access to baseline network data and forensics information

Control Plane

- LDP (MPLS Label Distribution Protocol)/RSVP-TE (Traffic Engineering Resource Reservation Protocol)
- PIM (Protocol Independent Multicast)/MSDP (Multicast Source Discovery Protocol)
- BGP (Border Gateway Protocol - ‘de facto’ inter-domain routing protocol in the Internet)
- Transport protocol security (e.g., TCP)?
  - MD5 TCP Signature Option
  - IPSEC (IP Security)
  - Infrastructure ACLs (iACLs)
  - GTSM (Generalized TTL Security Mechanism)
- IGPs support MD5 for many functions
  - Neighbor discovery & adjacency establishment
  - Link State Packet (LSA/LSP/Update authentication)
- Control Plane Policing
  - filter/limit who/what/how much can gain access to a router or switch control plane/route processor

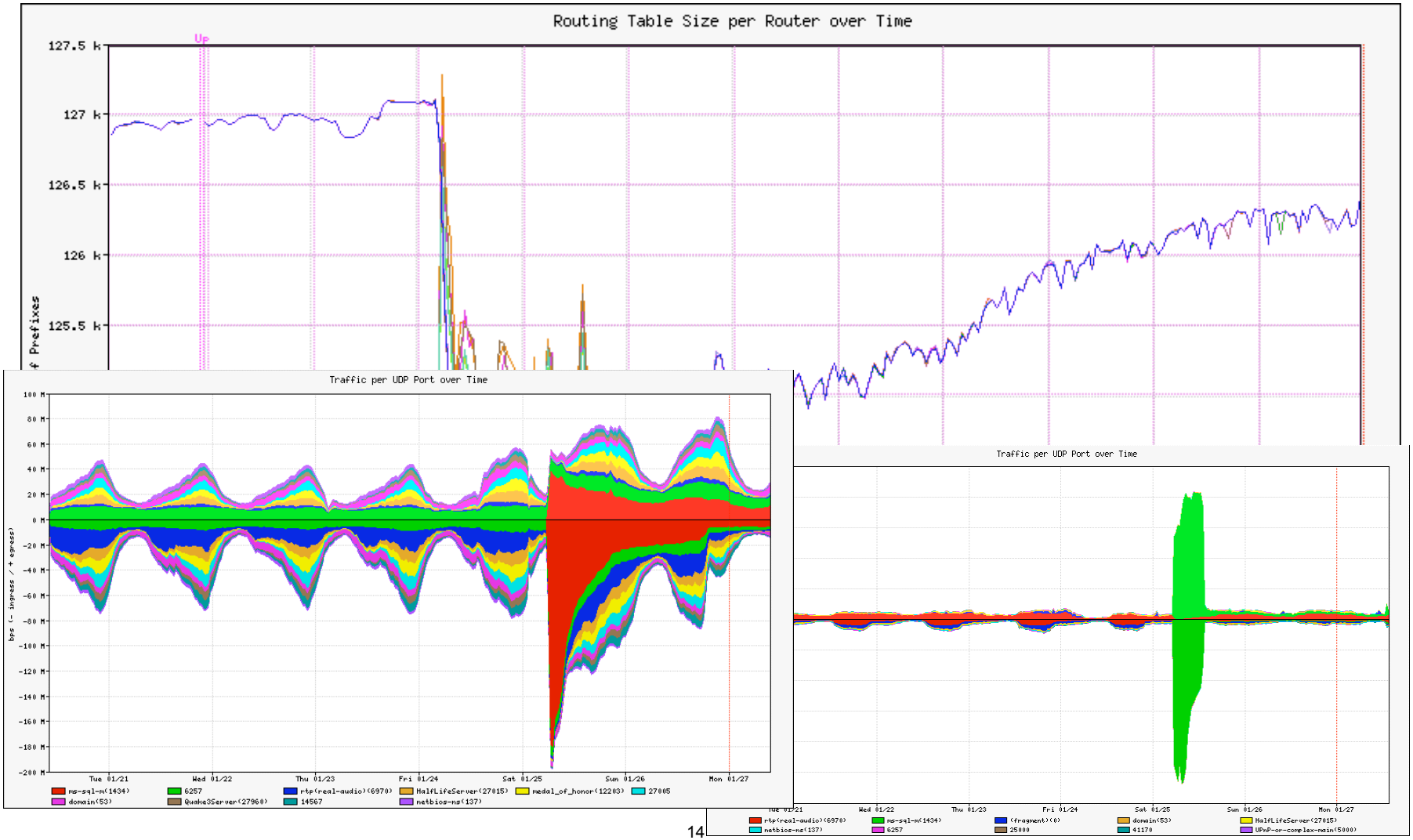
Conceptual Router Architecture: RIBs & FIBS



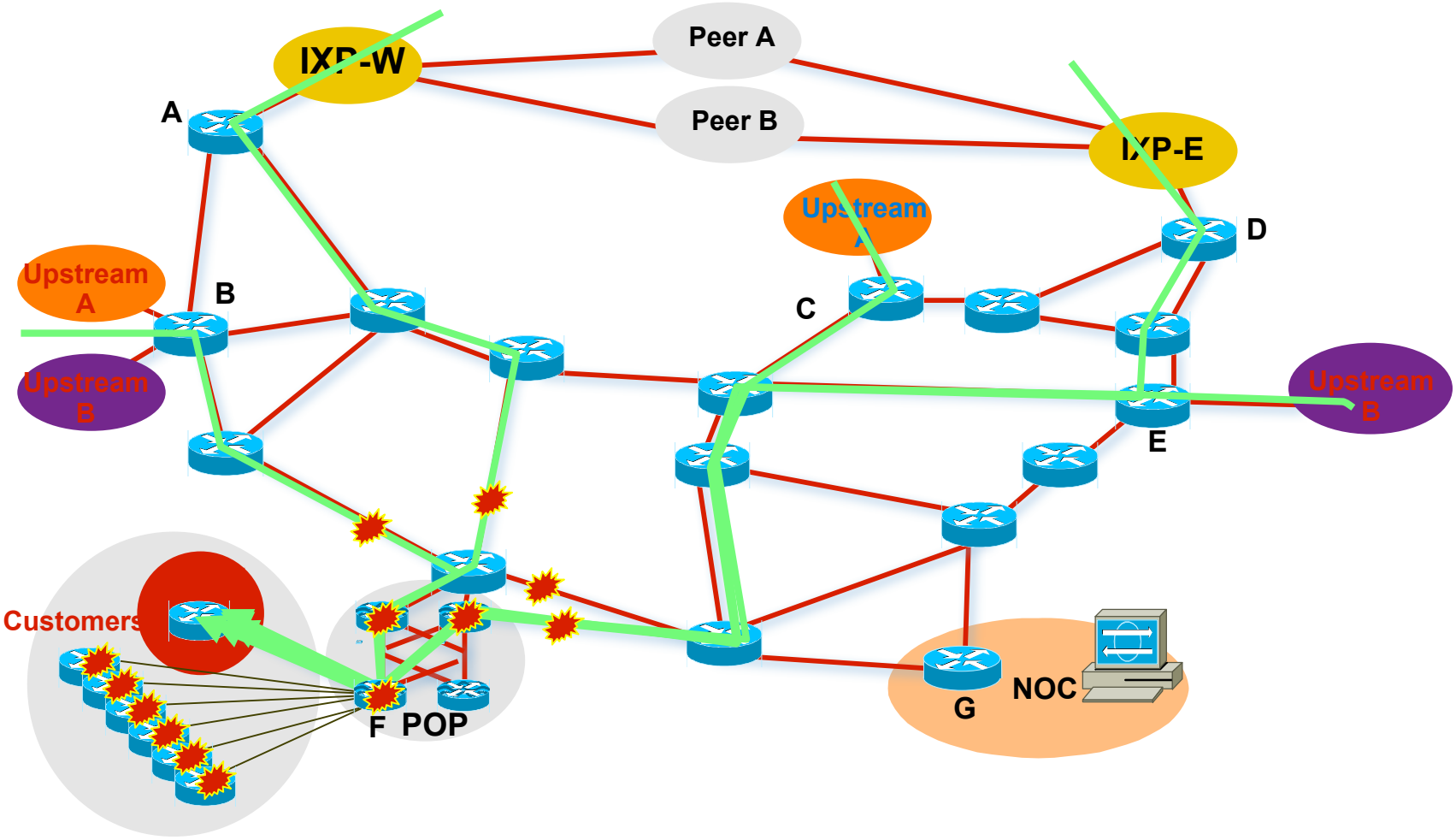
Data Plane

- Infrastructure, traceback ACLs
- Rate Limiting and service impact (e.g., PMTU discovery breakage)
- Spoofing prevalence & prevention/BCP 38/uRPF (reverse path forwarding)
- Mitigation - array of mitigation options, need accounting and forensics data
- Abstracting control plane data without widening DoS vulnerability
- Forwarding performance: latency, jitter, packet loss
- Minimizing collateral damage

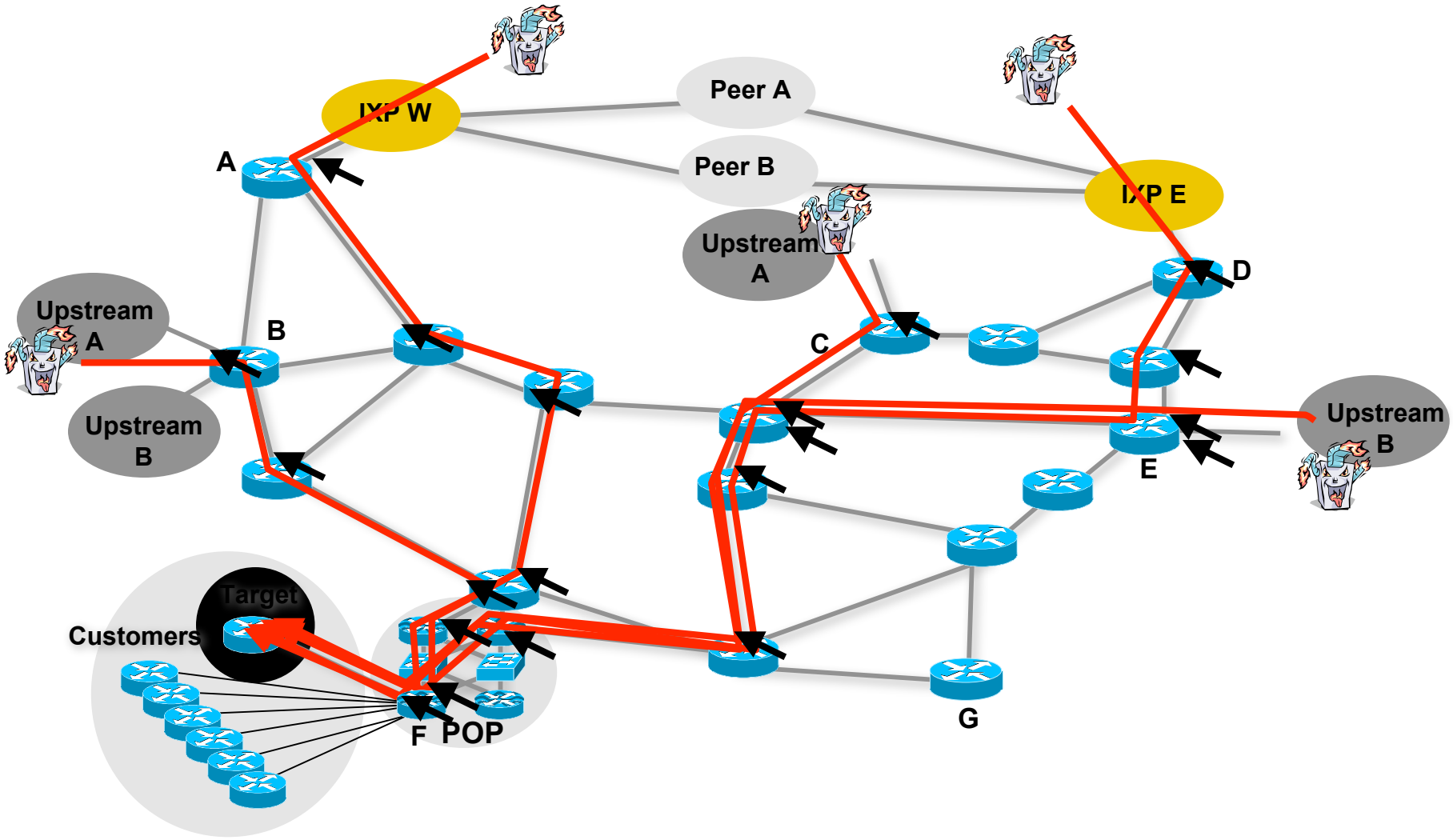
Slammer Control Plane Impact – THE BGP PICTURE



DDoS: Mitigating Collateral Damage



DDoS Traceback: Manual

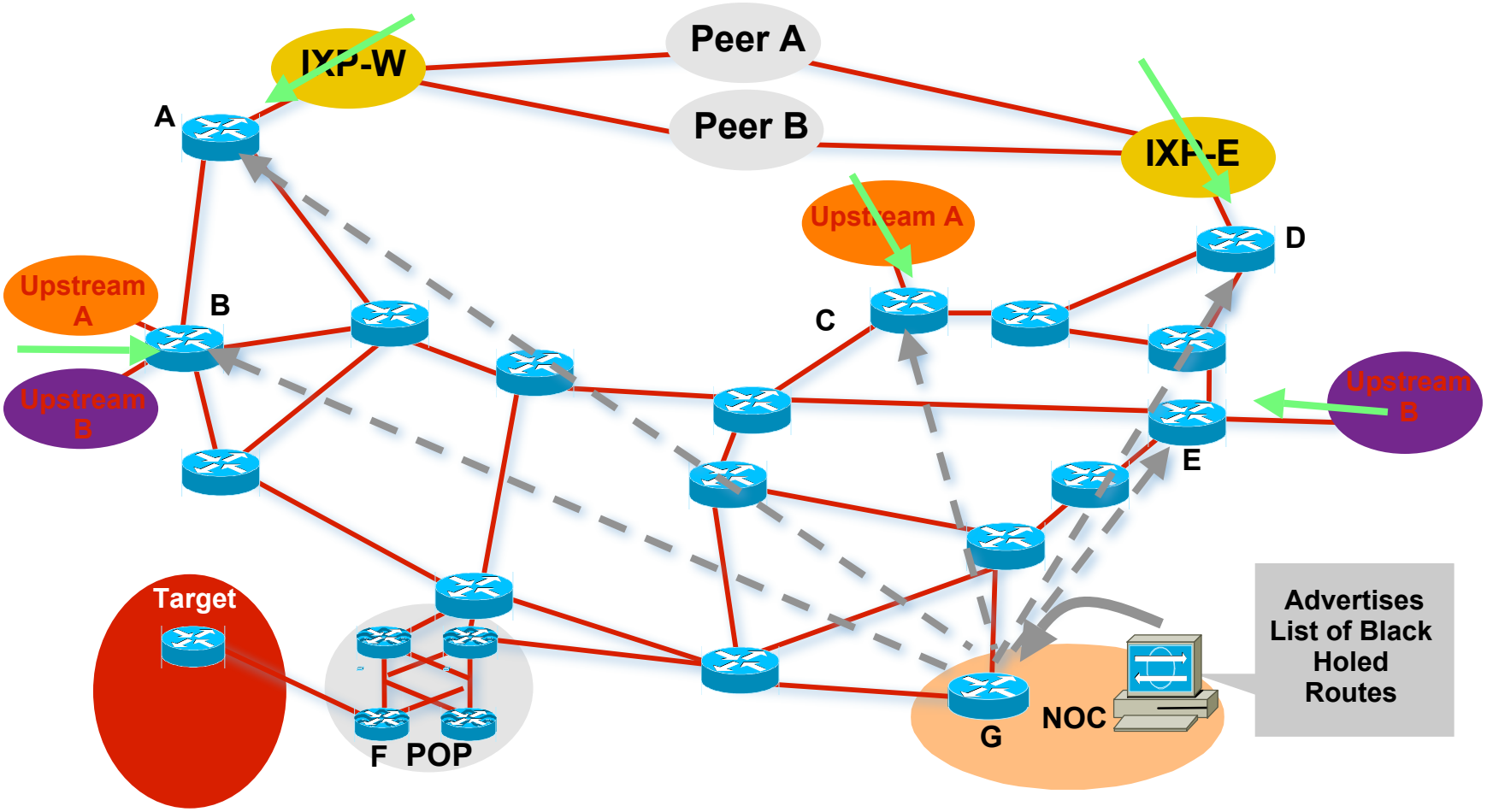


Potential Mitigation Options

- Do Nothing

- Actively respond:
  - Packet filters (e.g., ACLs) or rate-limit (e.g., CAR)
  - BGP remote-triggered drop
    - Blackhole (dst == Null 0/discard interface)
    - uRPF loose check (src == Null 0/discard interface) /Slide 74-78
    - Customer-performed
  - Intelligent filtering (e.g. divert to CloudShield, Cisco Guard)
  - Peer/upstream filtering
  - CPE filtering firewall, IDS or similar
  - New directions (BGP Flow Specification)

BGP-based Real Time Blackhole Routing (RTBH)

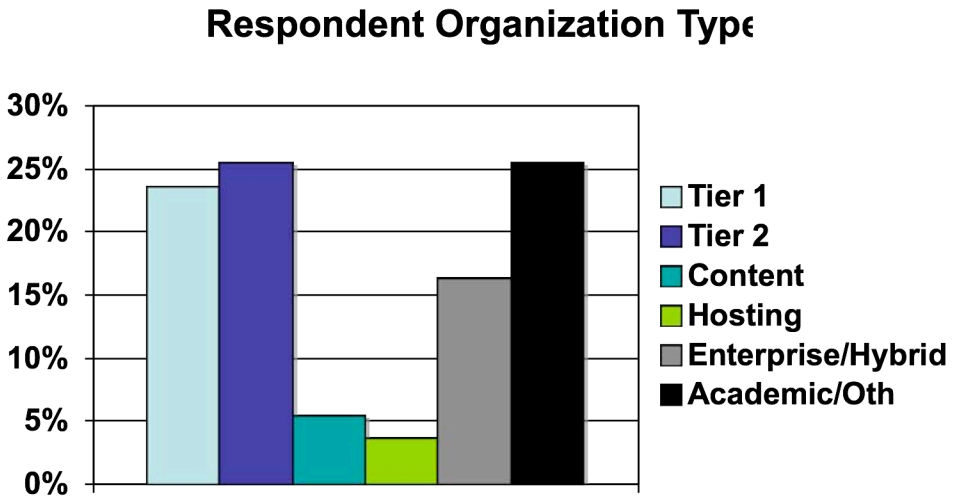


Security Survey Overview

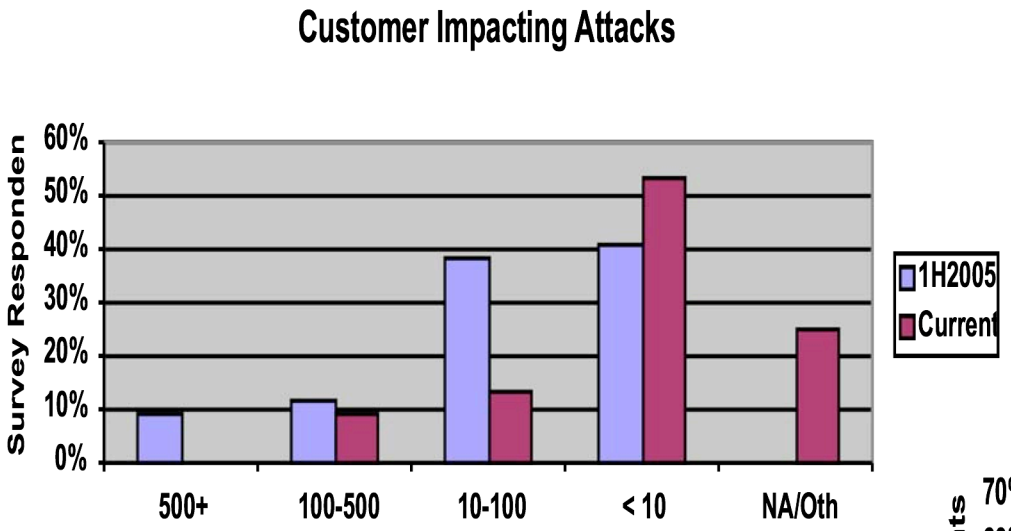
What's in a DOS Attack?

Overview

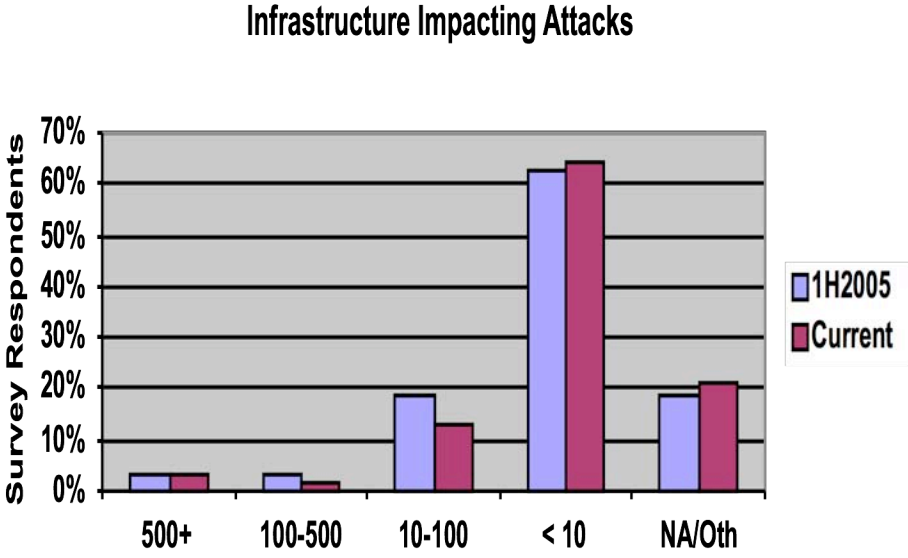
- Bi-annual survey, second edition representing 2H2005
- 55 respondents from network security operators - 65% increase from previous edition
- Respondents distributed across Tier-1, Tier-2, Large Content, Hosting, Academic & Enterprise networks - self categorized



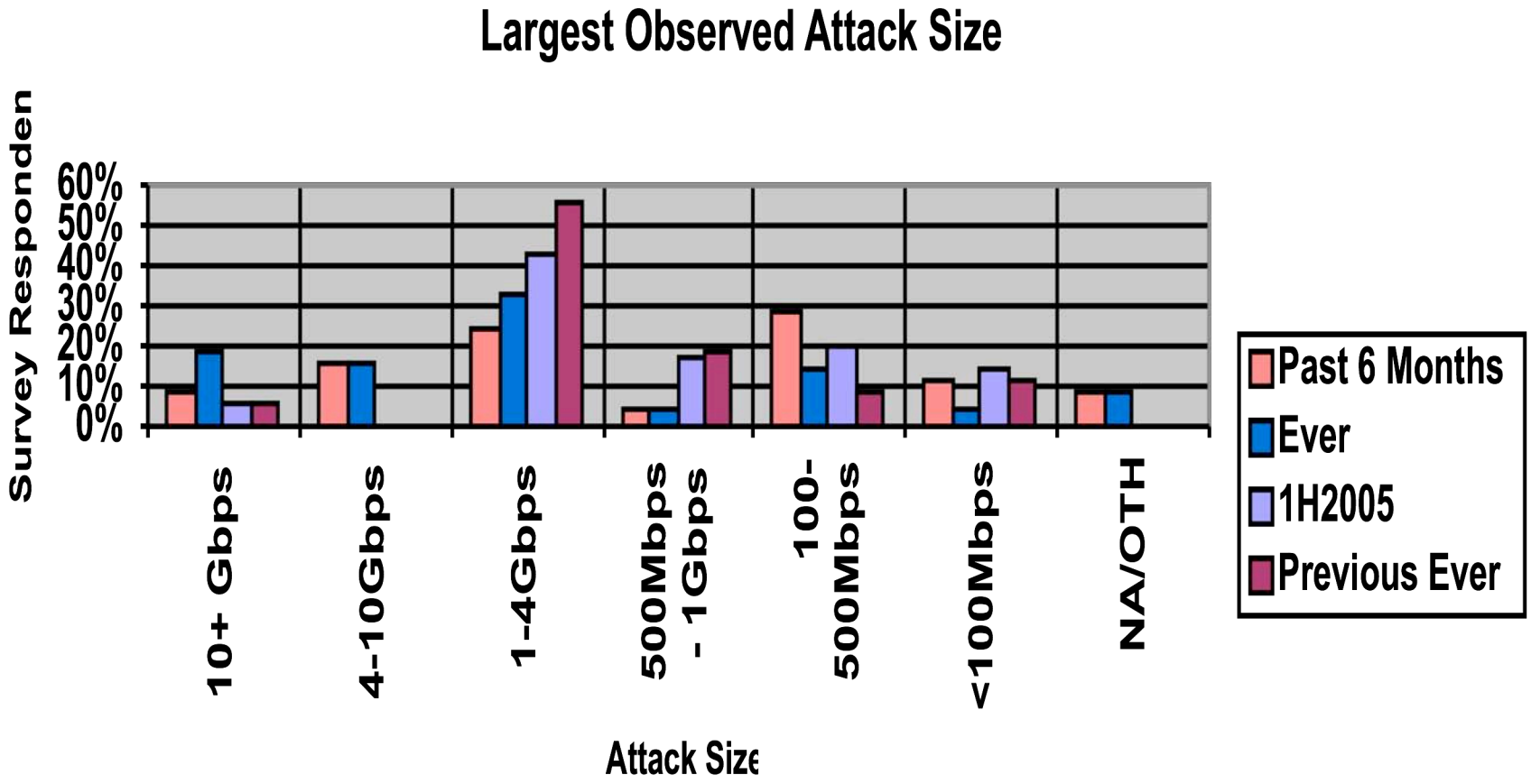
Impacting Attacks



Actionable attacks only, infrastructure attacks may have been resultant of collateral damage



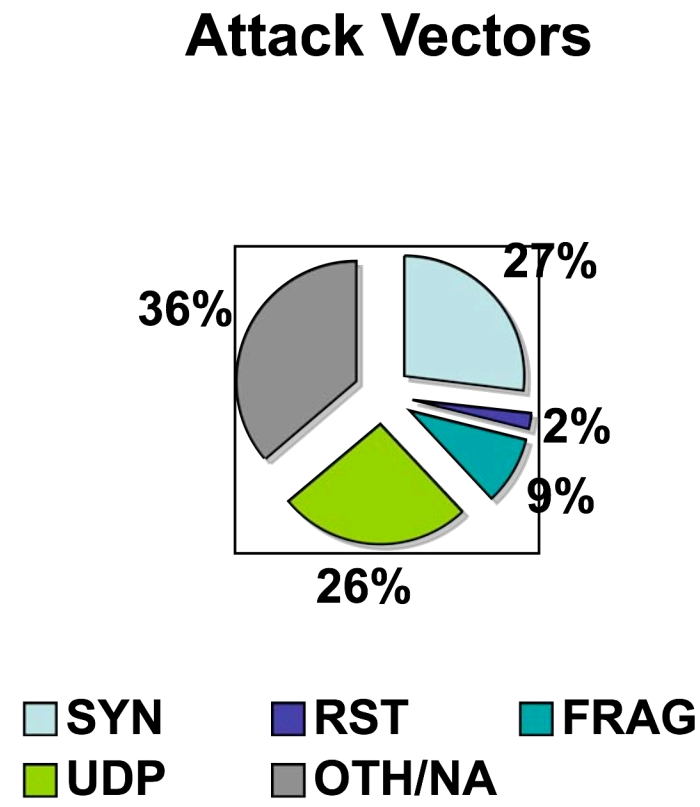
Largest Attacks Observed



10 respondents have observed attacks greater than 10 Gbps sustained - an additional 25 from 1 - 10Gbps. Largest attack reported at 17 Gbps sustained!

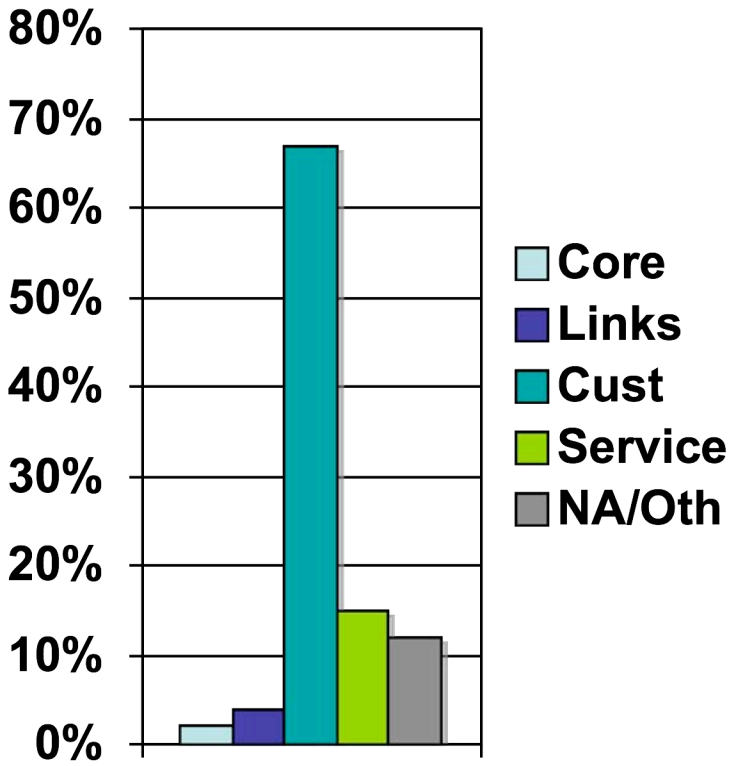
Attack Vectors

- Simple misuse “brute force” attacks still dominant
- Attacks of 14Mpps (SYN) and 22Mpps (UDP Flood) reported, also 17Gbps attack reported



Attack Targets

- Core infrastructure and customer links rarely targeted - specific customers primary target
- Services such as DNS second target of choice



Attack Targets

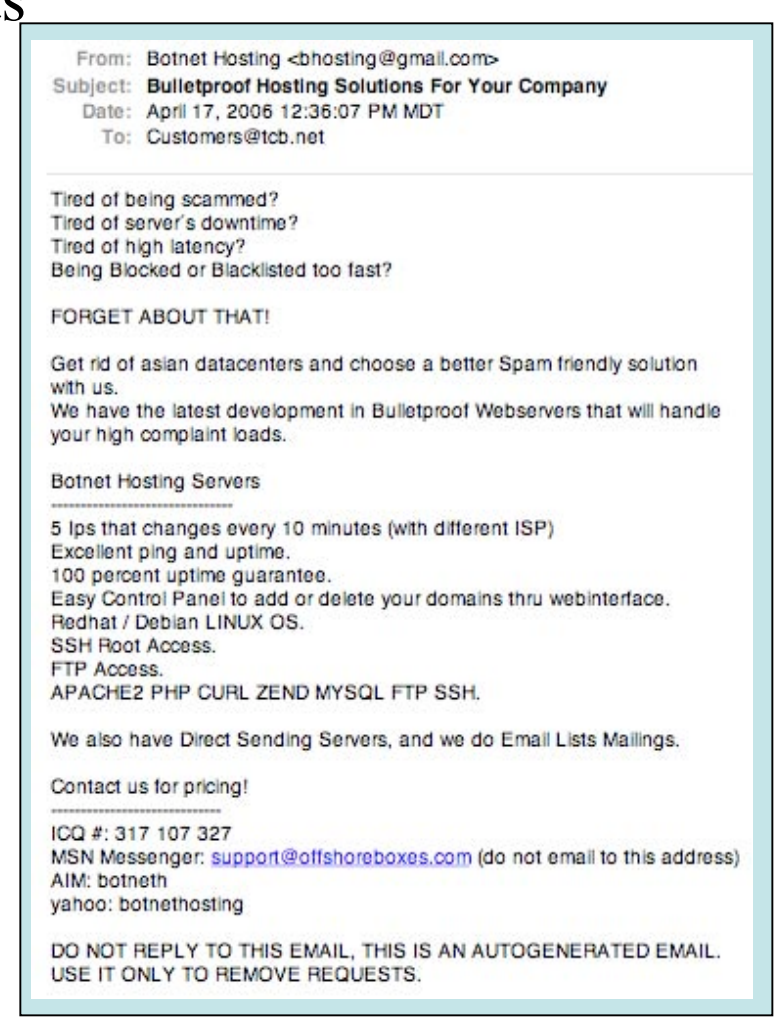
- IRC/chat most common response
- Gaming servers
- Adult entertainment sites
- Gambling/Online bookmakers
- Religious/Political

- *"The kind that pay protection :-)"*

Trends in botnets

- Commonly observe 150K node botnets
- Smaller & better organized
- Better obfuscated
- More capabilities
- Using public IRC servers now
- More difficult to monitor
- More botnets - more firepower

- *"Better marketing by botherders"*



From: Botnet Hosting <bhosting@gmail.com>
Subject: **Bulletproof Hosting Solutions For Your Company**
Date: April 17, 2006 12:36:07 PM MDT
To: Customers@tcb.net

Tired of being scammed?
Tired of server's downtime?
Tired of high latency?
Being Blocked or Blacklisted too fast?

FORGET ABOUT THAT!

Get rid of asian datacenters and choose a better Spam friendly solution with us.
We have the latest development in Bulletproof Webservers that will handle your high complaint loads.

Botnet Hosting Servers
---
5 Ips that changes every 10 minutes (with different ISP)
Excellent ping and uptime.
100 percent uptime guarantee.
Easy Control Panel to add or delete your domains thru webinterface.
Redhat / Debian LINUX OS.
SSH Root Access.
FTP Access.
APACHE2 PHP CURL ZEND MYSQL FTP SSH.

We also have Direct Sending Servers, and we do Email Lists Mailings.

Contact us for pricing!

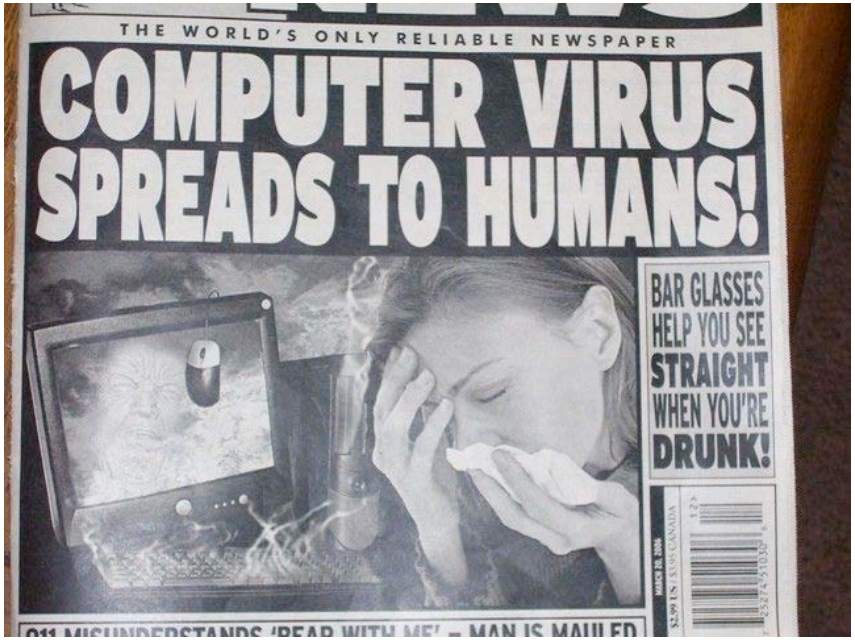
ICQ #: 317 107 327
MSN Messenger: support@offshoreboxes.com (do not email to this address)
AIM: botneth
yahoo: botnethosting

DO NOT REPLY TO THIS EMAIL, THIS IS AN AUTOGENERATED EMAIL.
USE IT ONLY TO REMOVE REQUESTS.

Botnet Employment

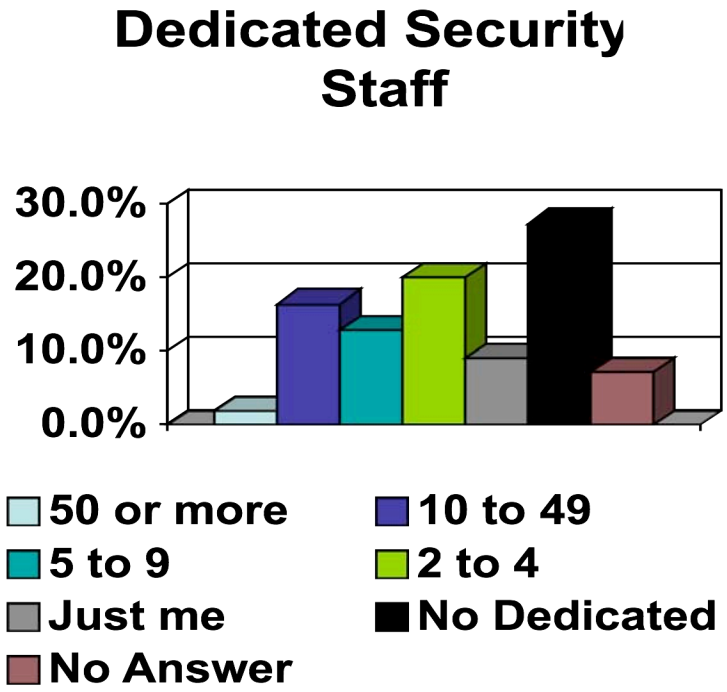
- Spamming (&& services marketing)
- [spear] Phishing
- DDOS
- ID Theft
- Form & keystroke logging
- Proxy
- Click Fraud
- Scanning
- SSH brute force attacks
- Recursive DNS/DDOS

- 1.5M node botnet observed in the wild

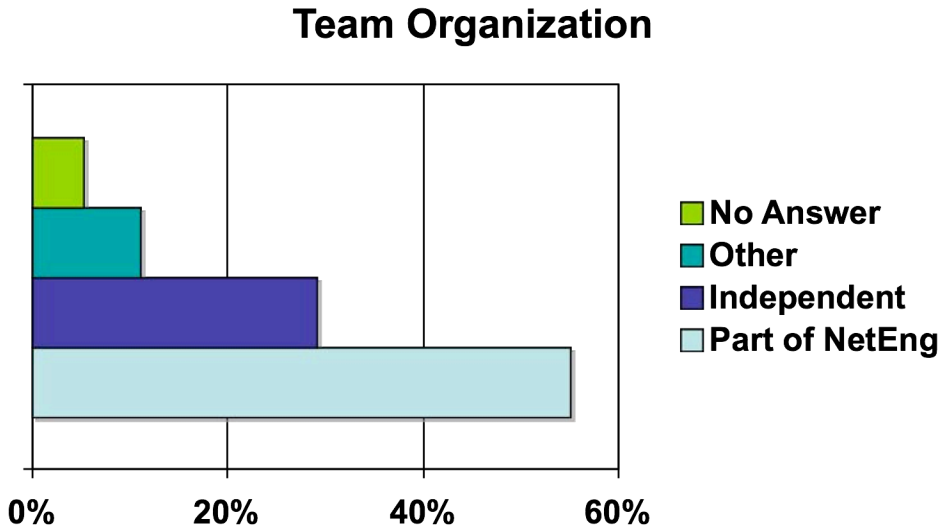


Think of the possibilities!

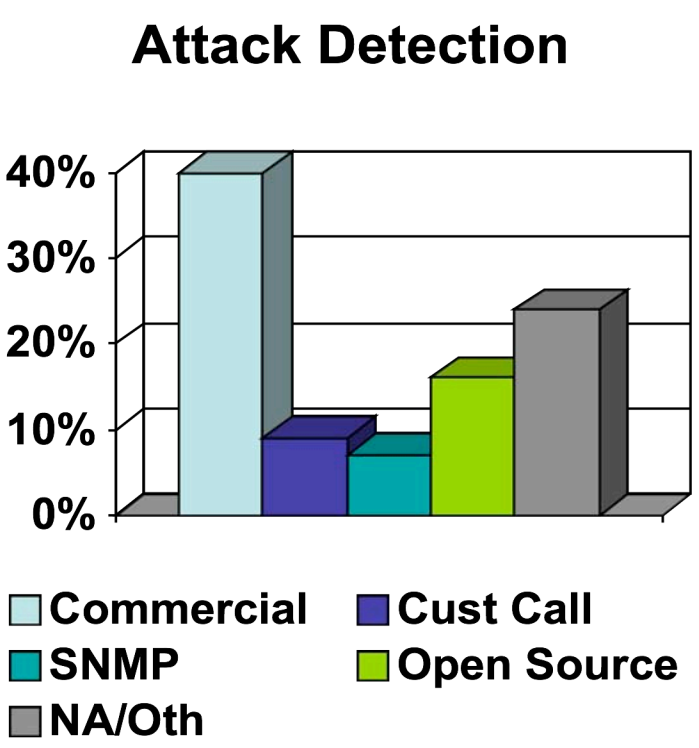
Security Organizations

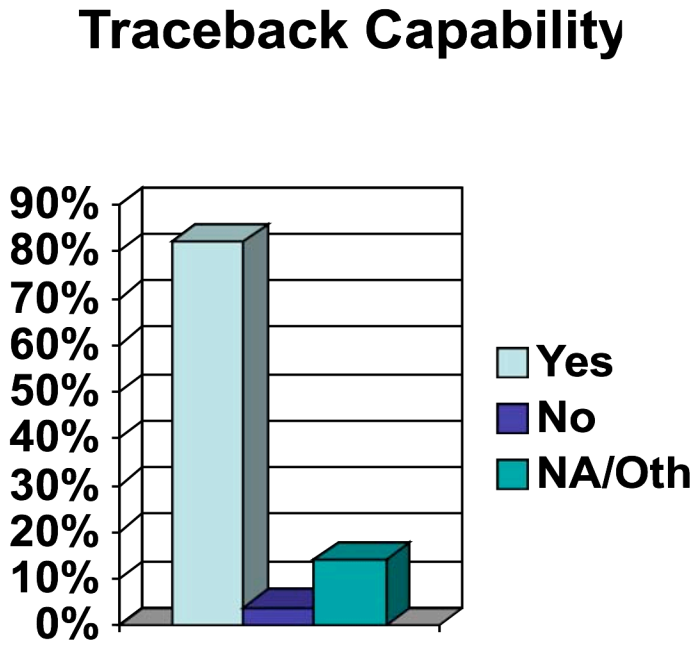


Large dedicated staff indicative of large user pool; e.g., dial-up and residential broadband services



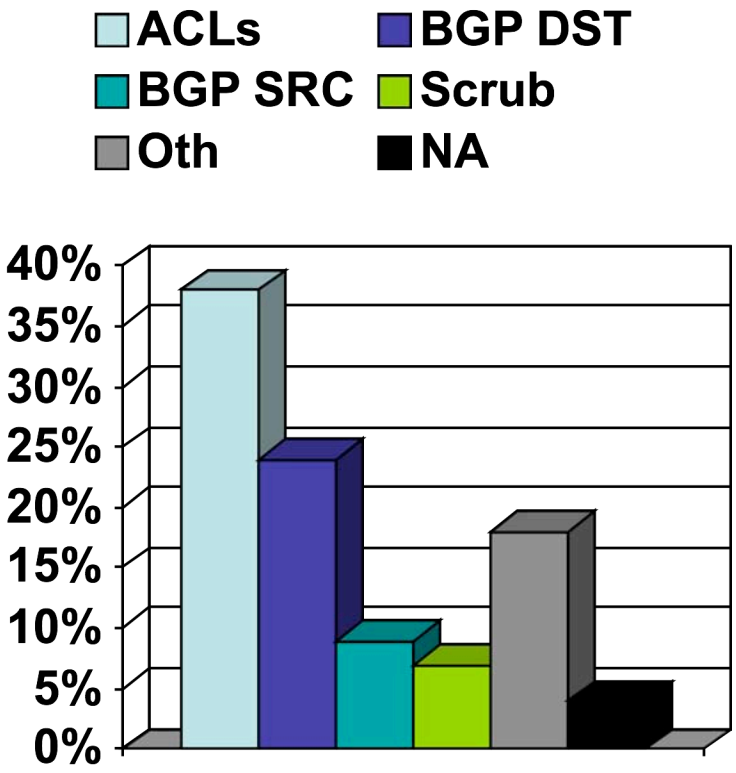
Attack Detection & Traceback





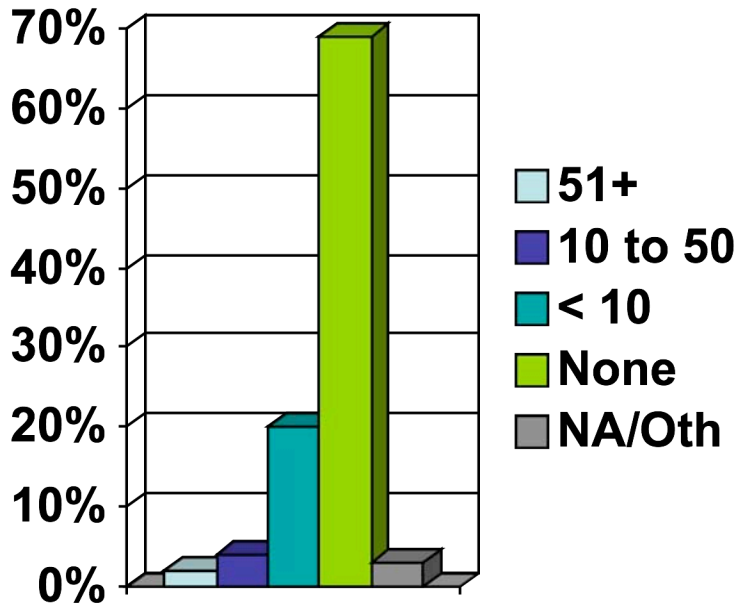
Mitigation

- ACLs are primarily destination-based with Network & Transport Layer policies
- **Number 1 & 2 techniques effectively complete DOS attack!**



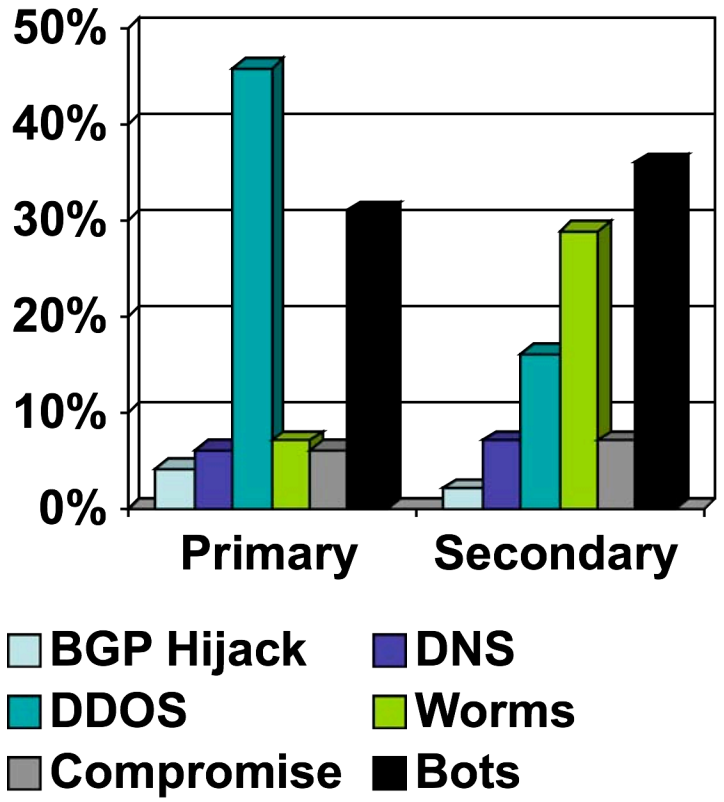
Law Enforcement Referrals

- Referrals limited by:
  - Lack of forensics detail
  - Belief in utility
  - Customer privacy request
  - Too many attacks to bother
- Only 29% of respondents believe LEOs have the power and means to act upon information provided about attacks



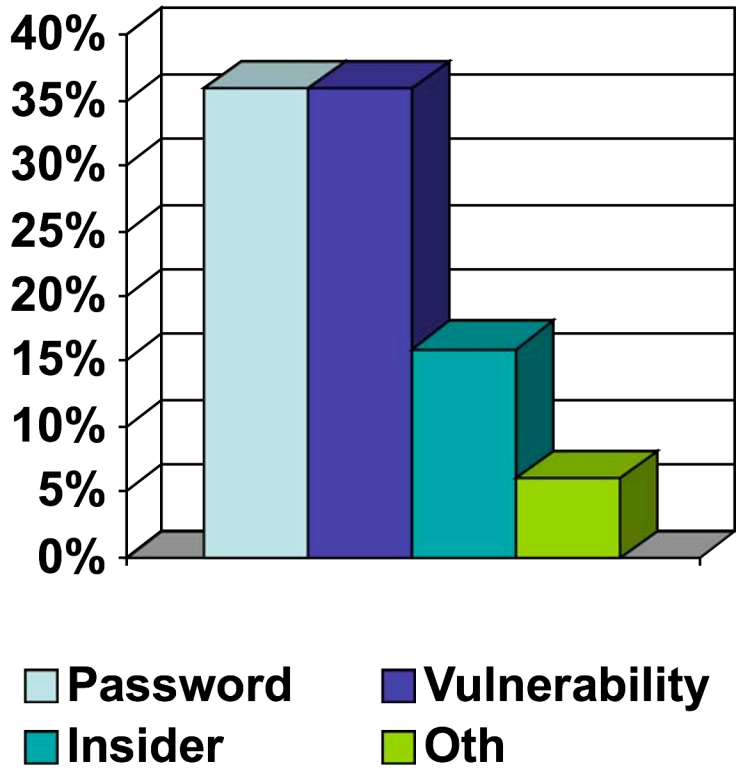
Primary Concerns

- Bots new category - most threats executed by bots
- Worm concern was implicit DDOS attributes (e.g., network congestion and control plane state)

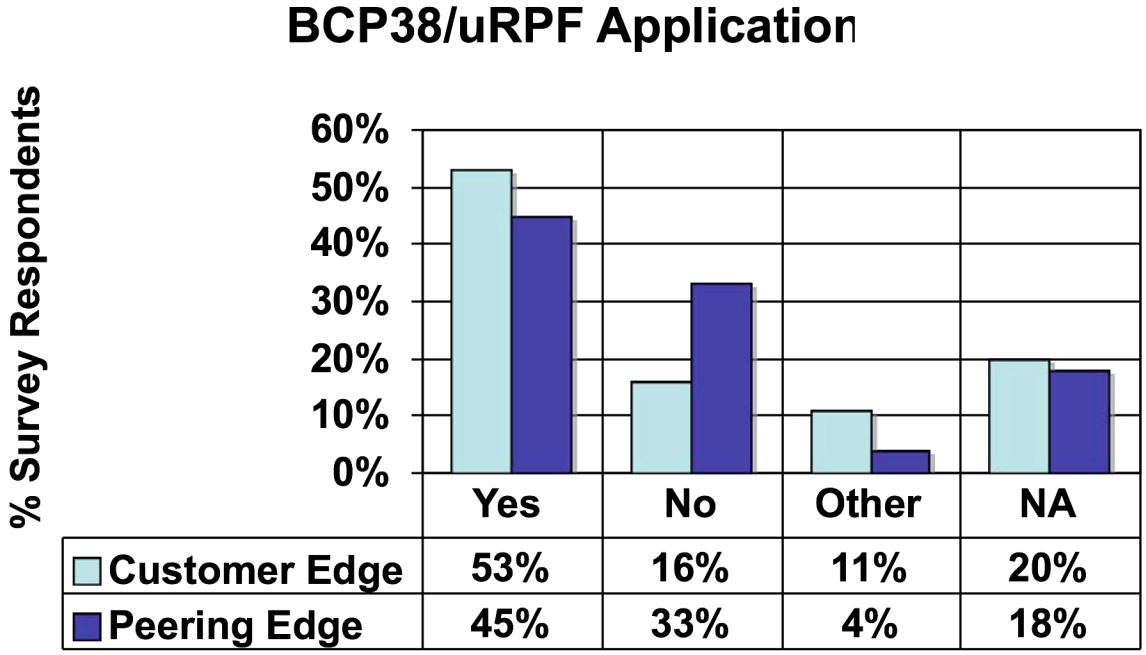


Infrastructure/OSS Attacks

- Of those respondents that have experienced internal compromise, what was the source:
  - Lack of BCP implementation
  - SNMP walk
  - Poor security practices
  - Social Engineering



Ingress Filtering Employment



Some concern uRPF loose mode introduces false sense of protection

Note: Assume more-clueful operators replied so “YES” number is likely much lower. Also, uRPF (loose mode) allows spoofing of “real hosts”(e.g., permits DNS amplification attacks)

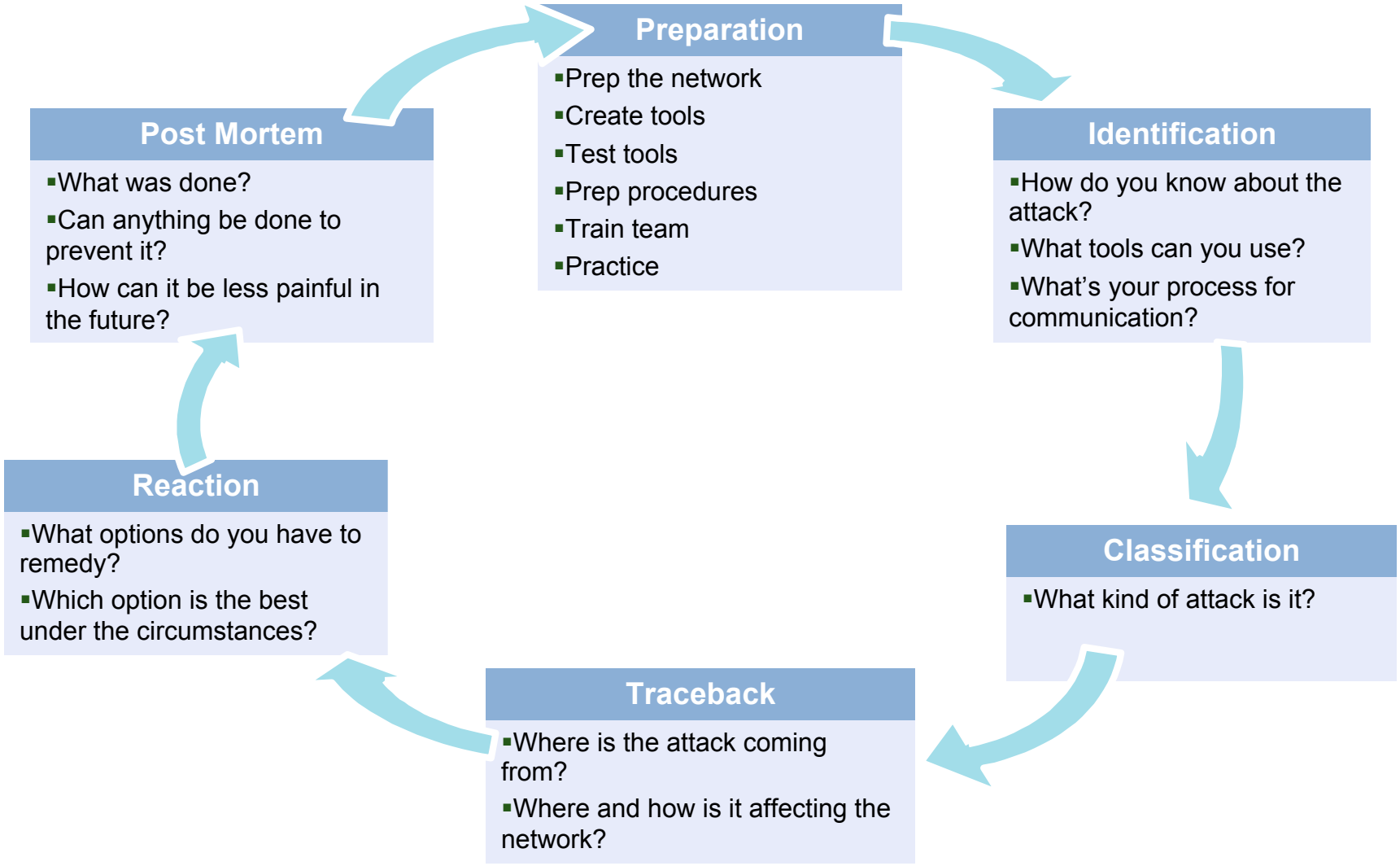
ISPs and Future Threats

- 31% believe ISPs are NOT in a position to mitigate future Internet threats
- 69% believe they are, but:
  - "Only in limited deployment for MS customers"
  - "Who else can do it - customers can't!"
  - "Yes - but cost model is VERY tough!"
  - "Not with today's margins!"
  - "$$$!"
  - "Position, yes, paid to do so - NO!"

Network-based Security Offerings

- Shared infrastructure allows SPs to provide services at a fraction of the cost of CPE-based models (from purely capital and full OPEX perspective)
- Bandwidth is a commodity - SP managed services provide Internet Service Providers a means for additional revenue opportunity, upsell and customer lock-in
- Fueled by broadband and wireless access, as well as subsequent botnet proliferation
- Infrastructure may also be employed to protect SPs themselves
- Services themselves include:
  - Email filtering
  - DoS prevention (**required**)
  - Intrusion Detection Service (IDS)
  - Intrusion Prevention Service (IPS)
  - Quality of Service (QoS)
  - Content Filtering

Six Phases of Infrastructure Security



Finally….

"Everybody's got a plan - until they get hit!"

--Mike Tyson

.. Or should I say "bit"

Questions?