SANOG 7

Security for SPs
including-
DDOS Prevention
Wireless Security

Pravin Mahajan, pmahajan@cisco.com
Mumbai
22 Jan 2006
Agenda

• Challenges
• Trends
• Threats
• The first step - Telemetry
• Next Steps –
  Techniques
  Modular Application to SP infrastructure
• Wireless Security
• Case Study
Security Challenges
Introduction: Emerging Threats
Today’s Reality…
Evolution of Network Availability Threats

Source: Arbor Networks

- **FEB 2000**: Amazon, CNN, Takasago, eBay, and ETrade downed by DDoS attacks
- **JAN 2001**: Several Microsoft sites taken down by DDoS attacks targeting a router
- **SUMMER 2001**: Code Red and Nimda worm propagation enables automated zombie collection
- **JAN 2002**: European service provider Cloud Nine closes due to DDoS-related losses
- **FEB 2002**: CERT/CC advisory warning of widespread multivendor SNMP vulnerabilities that create basis for router compromise

**Infrastructure Attacks**

**Events**
- **1999**: Researchers discuss DoS attacks
- **1999**: DoS attack tools emerge
- **FEB 2000**: Advent of mainstream DDoS attacks
- **2000**: Researchers discuss routing attacks
- **FEB 2002**: Router attack tools emerge

**Attack Source**
- Computers
- Routers

**Attack Target**
- Computers
- Network
- Internet

**Impact**
- Local
- Global
Economic Impact of DDoS

Dollar Amount of Losses by Type:

DoS is 2nd in Impact After Viruses!


The new Internet Economy brought new services and new players: NSPs, ASPs, etc…

- E-commerce has become part of the business model. Customers now depend on the Internet

- Attacks targeted to customers can and do affect the infrastructure.

- Availability is not just matter of duplicating gear.
Collateral Damage

Attacks targeted to a particular customer CAN and DO affect the infrastructure
Infrastructure Attacks
a wake up call

Now elements of the SP infrastructure are being directly targeted too:

- Services: DNS, DHCP, SMTP, WWW, FTP
- Routers
- Routing
- …
Role of Service Providers

- Protect their own infrastructure (from Customers and Internet)
- Help protect other peers
- Protect customers from attacks coming from the infrastructure or other customers
Security Trends
Evolution of Security Challenges

Target and Scope of Damage

- **GLOBAL Infrastructure Impact**
- **REGIONAL Networks**
- **MULTIPLE Networks**
- **INDIVIDUAL Networks**
- **INDIVIDUAL Computer**

Rapidly Escalating Threat to Businesses

- **Weeks**
  - **First Gen**
    - Macro viruses
    - Denial of Service
  - **Second Gen**
    - Macro viruses
    - Denial of Service
    - *Flash threats*
  - **Third Gen**
    - Distributed Denial of Service
    - Blended threats
    - *Massive “bot” driven DDoS*
    - *Damaging payload worms*

- **Days**
  - **1980s**
  - **1990s**
  - **Today**
  - **Future**

- **Seconds**
  - **Next Gen**

© 2003, Cisco Systems, Inc. All rights reserved.
Evolution of Security Strategies

1990s
- Basic router security
- Command line interface

2000
- Security appliances
- Enhanced router security
- Separate Mgt software

2002
- Multiple technologies
- Multiple locations
- Multiple appliances
- Little/no integration

2003
- Integrated security
- Routers
- Switches
- Appliances
- Endpoints
- FW + VPN + IDS
- Integrated management software
- Evolving advanced services

2004...
- Self-Defending Networks
- End-point posture enforcement
- Network device protection
- Dynamic/Secure connectivity
- Dynamic communication between elements
- Automated threat response
Self-Defending Network

1. Point Products → Integrated Security
2. Disparate Security Services → Collaborative Security Systems
3. Reactive Security → Adaptive Security
Self-Defending Network:
Controlling the Who, What, Where, When, Why and How

- **Who**—allows access to data only by authorized personnel
- **What**—prevents data from ever being stored, copied, or printed outside the secure environment
- **Where**—provides layers of protection and auditing to ensure that data is only stored in a controlled location
- **When**—users process data normally, but the data never “sleeps” outside of the secure area
- **Why**—only authorized personnel allowed to process data
- **How**—data access is restricted, authenticated, and audited by the Self-Defending Network
Self Defending Networks
From Point Products to Holistic System

Security as an Option
- Very complex environment
- Higher integration cost
- Security risks not mitigated
- Lower reliability

Security, INTEGRAL to the System
- Reduced complexity
- Easier deployment and management
- Security risks effectively mitigated
- Lower TCO
Threats
Introduction: The Basic Model

Types of Communication:
1) People Accessing Information Assets
2) People Communicating with One and Other
3) Machine to Machine Communication

Policy Primitives:
1) User / Service Identity
2) Machine Security Posture

Attack Targets:
1) End-points Themselves
2) Traffic Leaving
3) Traffic in Flight
4) Traffic Entering
Introduction: Appropriate Risk Mitigation

**LEVEL OF RISK AVERSION**

- **RISK TOLERANT**
- **RISK NEUTRAL**
- **RISK AVERSE**

**DEPTH OF MITIGATION STRATEGY**

**Conclusion:** Determine in advance the level of risk appropriate to the business
Worms and Viruses

- **Virus**: Malicious piece of software that typically propagates by attaching itself to some other form of communication. May exploit a vulnerability, but always requires human intervention to spread.

- **Worm**: Malicious piece of software that self-propagates. Always exploits a vulnerability to infect, and does not require human intervention to spread.
Worms and Viruses: What Happens

**Injection**
- Injection code arrives at end point
- Can either self-execute by having another process execute it, or can have a user execute it
- Some are completely self-contained, some need to pull down additional propagation and payload code to operate

**Propagation**
- Code replicates itself, and begins to propagate to other hosts
- Propagation can be multi-vector (Nimda)
- Mass propagation are typically why the casual user learns of these
- Can cause network-level Denial of Service (Blaster) due to massive consumption of resources

**Payload**
- Potential for most damaging portion of infection
- Historically, often not malicious (e.g. Slammer)
- Sometimes triggers a reboot (Nachi), often to further embed itself in the system
- Increasingly, used to install backdoors or trojans, and to patch the injection vector
Recent Trends in Worms and Viruses

• **Change in *Purpose***
  
  Shift from fame to profit
  
  Shift from being noisy to developing an asset with economic value

• **Change in *Expected Behavior***
  
  Less Noisy
  
  More Sophisticated
  
  More Variants, smaller scope of each
A Birthday Message for You!!!

You are the king today!
Hope U have a
R-O-A-R-I-N-G time
on your Birthday!

©123Greetings.com
Anatomy of a Trojan

- Troj/LdPinch-BD is a password-stealing Trojan for Windows platforms
- Troj/LdPinch-BD steals information, including passwords, from various applications. Information stolen may include:
  - computer details (OS version, memory, CPU etc.)
  - available drives (drive letter, type and free space)
  - hostname and IP address
  - Windows folder volume information
  - Passwords and confidential information from 'Protected Storage'
  - POP3 and IMAP server information, usernames and passwords
  - FTP usernames and passwords
  - RAS dial-up settings
- The Trojan may steal information relating to applications including the following:
  - Mirabilis ICQ
  - Opera
  - CuteFTP
  - WS_FTP
  - Windows Commander
  - Total Commander
- The Trojan attempts to download and run further malicious code.

Source: http://sophos.com/virusinfo/analyses/trojldpinchbd.html
Harvesting and Asset Development

MACHINE HARVESTING

- Creation of “bot-net” networks of thousands of compromised machines
- Used as:
  - Launch points for other attacks
  - Spam-nets (sold or rented to spammers)
  - DDoS For Hire networks (sold or rented to attackers)

INFORMATION HARVESTING

- Harvesting identity information (account names, numbers, passwords, personal information, etc)
- Used for:
  - Direct sale on the open market
  - Compromise other networks
  - Trust-enablement for fraud (traditional cons and new cons such as phishing)
BotNet Operation

Zombies

Hacker

Masters

Control Traffic

Attack Traffic

ISP Edge Router

Customer’s Premises: Server/FW/Switch/Router

Flooded Pipe

Victim (Web Server)
A New Class of Threat: Spyware

**SPYWARE**: malware that obtains or transmits personal information with intent to defraud*

**ADWARE**: Spyware’s slightly more reputable cousin

- Recently, Spyware has exploded as a significant security threat
- Can be thought of as a “drive up” virus – skip the propagation step and cut out the middle-man!
- Enhanced Concern: Threat to control of Confidential Information

* From most recent draft of US Federal I-SPY act
How Spyware/Adware Gets Installed

- Bundled in freeware/shareware
- Social Engineering
  - Pestering pop-ups until user clicks “yes”
  - Confusing or buried EULA terms
  - User doesn’t read EULA
- Drive-by Download
- Remote installation – no physical access necessary
- Via Virus or Trojan
Denial of Service: A Refresher

- Denial of Service (DoS) attacks’ goal is to make service unavailable
- The method may target:
  - A server
  - A network device
  - A network
- Can be associated with:
  - Source IP spoofing
- Collateral Damage includes:
  - Saturation of network forwarding tables
  - Exhausting processing power
  - Clogging links
Denial Of Service: What’s Going On

• Basic Denial of Service
  Often L3/L4 based; SYN attacks common; spoofing common
  Relatively easy to block sources and stop

• Distributed Denial of Service
  Similar to a basic DoS in approach, but sources appear “random”
  Tens of thousands of broad-band connected machines in a bot-net make it extremely difficult to track
  Often stopped by closing down control channels

• Emerging Threats: Application-layer Denial of Service
  Email DoS
  Web Front-end DoS
  Web-Services and XML DoS
  IP Telephony DoS
DDoS For Hire, and DoS Extortion

- **DDoS For Hire**: Criminal service in which for a nominal fee, a site of your choosing can be taken offline.

- **DoS Extortion**: Criminal enterprise in which websites must pay a protection fee to avoid being taken offline, typically during a critical business period.

**US credit card firm fights DDoS attack**

US credit card processing firm Authorize.Net is fighting a sustained distributed denial of service (DDoS) attack that has left it struggling to stay online.

Glen Zimmerman, a spokesman for Authorize.Net’s parent company, Lightbridge, told the Boston Globe that the attacks followed an extortion letter. Lightbridge said it was working with law enforcement officials to track down the attackers.

http://www.theregister.co.uk/2004/09/23/authorize_ddos_attack/

**ONLINE EXTORTION**

*How a Bookmaker and a Whiz Kid Took On an Extortionist — and Won*

Facing an online extortion threat, Mickey Richardson bet his Web-based business on a networking whiz from Sacramento who first beat back the bad guys, then helped the cops nab them. If you collect revenue online, you’d better read this.

http://www.csoonline.com/read/050105/extortion.html

---

Cisco.com
Solutions: Basic DoS and DDoS

- Real Traffic
- Attack Traffic

ISP

Router

Switch

Guard

Firewall

Anomaly Detector

ISP 2

GEnet

Guard

DDos Attack Detected

Anomaly Detector

Server Is Subject to a DDoS Attack

Internal Network

Web, DNS, Email,...
Solutions: Basic DoS and DDoS

- Real Traffic
- Attack Traffic

Routing Update Sent to Switch
Traffic Is Diverted to the Guard

Anomalous Traffic Is Detected and Dropped

Valid Traffic Continues on to Server Farm

Internal Network

Web, DNS, Email,…
Further Solutions: Denial of Service

- Denial of Service likely to continue to be a problem for a number of years
  - Economic incentives drive behavior
- Application Denial of Service a key piece of an Application Security strategy
  - Look for solutions with real DoS protective capabilities
- Partnerships are a Must
  - Enterprises must work with their Providers to set up response plans
- Incident Response a Must
  - Have a plan before your attacked. DoS attacks are very visible, very quickly. Timeliness of response is key
Messaging Security

- **SPAM / SPIM / SPIT**
  - Nuisance / Productivity Drain / DoS or Cost Imposition
  - Vector for other Frauds

- **Phishing / Pharming**

- **Solutions:**
  - IIM (Identified Internet Mail) spec
  - 2-factor auth for financials
  - Uniform policy control: Message Hygiene solutions; Endpoint Posture Compliance
SPAMity Calamity

WE HAVE A GIGANTIC DATABASE FULL OF CUSTOMER BEHAVIOR INFORMATION.

EXCELLENT. WE CAN USE NON-LINEAR MATH AND DATA MINING TECHNOLOGY TO OPTIMIZE OUR RETAIL CHANNELS!

IF THAT'S THE SAME THING AS SPAM, WE'RE HAVING A GOOD MEETING HERE.
SPAMity Calamity

- Evolution of SPAM:
  - Nuisance
  - Productivity Drain
  - Offensive Content
  - Vector for Fraud
- Dominant Source Today: Bot-nets
- SPAM is very much an unsolved problem

Associated Press

Trial Shows How Spammers Operate
LEESBURG, Va. Nov 14, 2004

Trial of Prolific Spammer Shows How He Sent 10 Million E-Mails a Day, Made $750,000 a Month

The Changing Nature of Spam

- **SPAM explosion:**
  - “Old Dog, New Tricks”
  - SPIM—Spam over Instant Messaging
  - SPIT—Spam over IP Telephony

- **Rise of Crime:**
  - Fraud as a rising threat
  - Phishing

- **Criminalization of Spam:**
  - CAN-SPAM act in US
Introduction to Phishing
Phishing Basics

From: Citi [mailto:users-support44@citibank.com]
Sent: 19 May, 2004 5:45 AM
To: @cisco.com
Subject: Citibank’s official notice

Dear client of the Citi,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.


We are grateful for your cooperation.

A member of citigroup
Copyright © 2004 Citicorp
PHISHING:
Email Schemes, Called “Phishing” or “Carding”, Are an Attempt to Trick Consumers into Disclosing Personal and/or Financial Information; the Emails Appear to Come from Companies with Whom Consumers May Regularly Conduct Business; Often Times the Email Threatens Termination of Accounts Unless Consumers Update Billing Information

Source:
www.atg.wa.gov/consumer/idprivacy/phishing.shtm

CONCLUSION: Unsolicited Email Can Be More than Just an Annoyance
New Threats: Phishing’s Cousin—Pharming

PHISHING

MUNDO-BANK.COM

172.168.1.1

Unsolicited Email

MUNDO-BANK.COM

172.168.254.254

PHARMING

MUNDO-BANK.COM

172.168.1.1

DNS Poisoning

MUNDO-BANK.COM

172.168.254.254

Hosts File:
superbank.com = 172.168.254.254

Come see us at
www.superbank.com
<172.168.254.254>
The Port 80 Problem
Opportunistic Applications Overloading Open Ports

Port Overloading enables violation of Security Policy:
Opportunistic applications tunnel through open outbound ports. Legacy firewalls cannot discern legitimate from illegitimate applications

Opportunistic Applications:
- Peer-to-peer Apps
- Instant Messaging
- Remote PC Access Apps
- Covert Channels

Some Solutions:
- Advanced firewalls can distinguish between applications by protocol semantics and enforce security policy
The Port 443 (SSL) Problem…

“Encrypted Port 80”
• Data confidentiality extends to network devices as well…
• Can verify compliance with SSL protocol spec, but beyond that, very difficult to enforce policy

Some Solutions:
• Protocol compliance checking
• Desktop application usage policy enforcement tools
• Destination filtering via domain/URL filtering
• Close 443 to all but well-defined business traffic

What is this?
Valid e-commerce?
Acceptable-use violations?
Covert channel?
Outbound attack?

We’re planning on pricing it less than $4000. I thought you’d find that interesting…

S: 10.123.234.17
D: 123.234.123.234
Port: 443
Contents: 100010111010100110010101100110101010001101011010011010111001010

oddball
Securing Web Services
Web Services and XML Security

- Exposing the application layer to external entities for the first time
- Introduces new classes of credentials for access control
- Introduces new classes of attacks: X-malware, XML DoS, XPATH injection, etc.
- Allows new services for confidentiality and integrity: Field-level encryption, document signing, transformation

Some Solutions:
- Secure Coding!
- Schema validation toolsets
- Attack prevention technologies
Social Engineering

- Social Engineering Attacks: Attacks that compromise the “human” elements of business processing
  - Assuming an identity to exploit trust relationships
- These forms of attack have been around forever
- Not an emerging threat in and of itself, but a constant “force multiplier” on new threats
The First Step - Telemetry
Holistic Approach to Patient Care

Uses a system-wide approach, coordinating with various specialists, resulting in the patient’s better overall health and wellbeing.
Holistic Approach to System-Wide Telemetry (Cont.)

Customer Edge:
- Ingress traffic [worm, attack]
- Egress traffic [spreading worms]
- Shared resources such as DNS, SMTP and such servers
- Network element health

Core:
- Network element health
- Infrastructure health
- Performance
- Packet paths

Data Center:
- Ingress / egress traffic
- Intra Datacenter traffic due to trust relationships of servers
- Availability scheme influenced traffic patterns
- Network element health

SP Peering:
- Ingress / egress traffic
- Asymmetric traffic due to peering policy & topology
- Network element health
What Is One Listening to?

- Ingress traffic flow
- Egress traffic flow
- Network element health
  Resources such as CPU, memory, etc.
  # flow to build baseline and detect anomaly
  Top talkers
  Open ports – services etc.
- Shared services
  DNS, SMTP, Availability related services, etc.
Understand the Concept of Data Gathering

Risks and threats are **NOT** prevalent in one place **ONLY**...

Need to watch everywhere to avoid being eaten by thousand turkeys...

- **Listening to a network element**
  - Per device listening
  - Local data provide information about local threats

- **Listening to Many**
  - Correlation is a **MUST**
  - Intelligent analysis is a **MUST**
Holistic Approach to System-Wide Telemetry

Data Center:
- Inter as well as Intra Data Center traffic

Customer Edge:
- Shared resources and services should be available

Core:
- Performance must not be affected

SP Peering:
- Ability to trace through asymmetric traffic

CPE/ACCESS/AGGREGATION
- CPE(s)
  - Broadband, Wireless (3G, 802.11), Ethernet, FTTH, Leased Line, ATM, Frame Relay

CORE
- L2 Agg.

DATA/SVC Center
- Data/Service Center

PEERING
- ISP / Alt. Carrier

Listen
Network Telemetry: Tools, Techniques and Protocols

How to Gather Data or Information?

- **Proactive Telemetry**
  - NetFlow
  - SNMP
  - RMON
  - Syslog
  - Network element health
  - BGP
  - DNS

- **Telemetry During the Incident**
  - Packet Capture
  - show commands
  - Network element health
  - Syslog
Netflow: What Is a Flow?

- Defined by seven unique keys:
  - Source IP address
  - Destination IP address
  - Source port
  - Destination port
  - Layer 3 protocol type
  - TOS byte (DSCP)
  - Input logical interface (ifIndex)

Exported Data
Netflow: Creating Export Packets

Enable NetFlow
Traffic
PE
Core Network

Export Packets
- Approximately 1500 bytes
- Typically contain 20-50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces
Netflow : Key Concept—NetFlow Scalability

- Packet capture is like a *wiretap*
- NetFlow is like a *phone bill*
- This level of granularity allows NetFlow to scale for very large amounts of traffic

We can learn a lot from studying the phone bill!
Who’s talking to whom, over what protocols & ports, for how long, at what speed, for what duration, etc.

NetFlow is a form of *telemetry* pushed from the routers/switches - each one can be a sensor!
NetFlow Infrastructure

Router:
- Cache Creation
- Data Export
- Aggregation

Collector:
- Collection
- Filtering
- Aggregation
- Storage
- File System Management

Applications:
- Data Presentation
- Accounting/Billing
- Network Planning
### Where to Deploy NetFlow?

#### Network Layer

- **Access**
  - Applications
    - Attack Detection
    - User (IP) monitoring
    - Application monitoring
  - Features
    - Aggregation Schemes (v8)
    - "show ip cache flow" command
    - Arbor Networks

- **Distribution**
  - Applications
    - Traffic Engineering
    - Traffic Analysis
    - Attack Detection
  - Features
    - NetFlow MPLS Egress Accounting
    - BGP Next-hop (v9)
    - Arbor Networks

- **Core**
  - Applications
    - Traffic Engineering
    - Traffic Analysis
    - Attack Detection
  - Features
    - MPLS Aware NetFlow (v9)
    - BGP Next-hop (v9)
    - Sampled NetFlow
    - Arbor Networks

- **Distribution**
  - Applications
    - Billing
    - Chargeback
    - AS Peer Monitoring
    - Attack Detection
  - Features
    - NetFlow MPLS Egress Accounting
    - BGP Next-hop (v9)
    - Arbor Networks

- **Access**
  - Applications
    - Billing
    - Chargeback
    - AS Peer Monitoring
    - Attack Detection
  - Features
    - Aggregation Schemes (v8)
    - "show ip cache flow" command
    - Arbor Networks

---

**Features**

- Aggregation Schemes (v8)
- "show ip cache flow" command
- Arbor Networks

---

**Applications**

- Attack Detection
- User (IP) monitoring
- Application monitoring

---

**Network Layer**

- Access
- Distribution
- Core
- Distribution
- Access
Principal NetFlow Benefits

**SERVICE PROVIDER**
- Peering arrangements
- SLA VPN user reporting
- Usage-based billing
- DoS/worm detection
- Traffic engineering
- Troubleshooting

**ENTERPRISE**
- Internet access monitoring (protocol distribution, traffic origin/destination)
- Associate cost of IT to departments
- More scalable than RMON
- DoS/worm detection
- Policy compliance monitoring
- Troubleshooting
Open Source Tools for NetFlow Analysis—The OSU Flow-Tools

• Open source NetFlow collection and retrieval tools
• Developed and maintained by Mark Fullmer, available from http://www.splintered.net/sw/flow-tools/
• Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
• Command-line tools allow for very display/sorting of specific criteria (source/dest IP, source/dest ASN, protocol, port, etc.)
• Data can be batched and imported into database such as Oracle, MySQL, Postgres, etc.
• Can be combined with other tools to provide visualization of traffic patterns
• Many other useful features - check it out today!
Open Source Tools for NetFlow Analysis Visualization—FlowScan

- Open source NetFlow graphing/visualization tools
- Developed and maintained by Dave Plonka, available from http://net.doit.wisc.edu/~plonka/FlowScan/
- Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
- Makes use of NetFlow data collected via flow-tools to build traffic graphs
- Top-talkers by subnet, other types of reports supported
- Makes use of RRDTool for graphing
- Add-ons such as JKFlow module allow more detailed graphing
Open Source Tools for NetFlow Analysis Visualization—FlowScan (Cont.)

Investigate the spike

Source: University of Wisconsin

An identified cause of the outage
Netflow: Coupling Control and Data Planes

Route Table Size over Time

Traffic per Peer

BGP Instability

<table>
<thead>
<tr>
<th>AS</th>
<th>Name</th>
<th>Count</th>
<th>Average</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>UPDATE</td>
<td>125</td>
<td>1.55</td>
<td>3.00</td>
</tr>
<tr>
<td>✓</td>
<td>AS486</td>
<td>317</td>
<td>590</td>
<td>16.646</td>
</tr>
<tr>
<td>✓</td>
<td>AS486</td>
<td>140</td>
<td>750</td>
<td>19.322</td>
</tr>
<tr>
<td>✓</td>
<td>AS25</td>
<td>75</td>
<td>212</td>
<td>99</td>
</tr>
<tr>
<td>✓</td>
<td>AS25</td>
<td>54</td>
<td>208</td>
<td>529</td>
</tr>
<tr>
<td>✓</td>
<td>AS19</td>
<td>54</td>
<td>208</td>
<td>929</td>
</tr>
<tr>
<td>✓</td>
<td>AS19</td>
<td>2</td>
<td>4</td>
<td>500</td>
</tr>
</tbody>
</table>
SNMP

- SNMP = Simple Network Management Protocol
- Canonical method of obtaining real-time information from network devices
- **SNMPv3** provides authentication, encryption
- MIBs support polling of statistics ranging from interface bandwidth to CPU utilization to chassis temperature, etc.
- Both a ‘pull’ model for statistical polling and a ‘push’ model for trap generation based upon events such as link up/down
- Many open-source and commercial collection systems, visualization tools
- Easiest way to get into profiling of general network characteristics
Displaying SNMP Data with MRTG

- MRTG—the Multi Router Traffic Grapher
- Open source SNMP visualization toolset developed by Tobi Oetiker, available from http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Long track-record - (in general use since 1995)
- Can be used to graph router/switch data, host performance info from systems running SNMP agents, etc. (generates HTML w/PNG images)
- Runs on Linux, FreeBSD, Mac OS/X, Solaris, other *NIX, Windows
- Written in Perl, has its own SNMP implementation
Powerful Visualization of SNMP with MRTG

Source: mrtg.org
Powerful Visualization of SNMP with MRTG (Cont.)

Various type of statistics gathering and display

Source: mrtg.org
Other Visualization Techniques Using SNMP Data with RRDTool

- RRDTool—the Round Robin Database Tool
- Another open source SNMP visualization toolset developed by Tobi Oetiker, available from http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- Improved graphing performance, new types of graphs
- Can be used in conjunction with MRTG - does not do its own SNMP collection (can also be used w/NetFlow via OSU flow-tools & FlowScan)
- Runs on Linux, FreeBSD, Mac OS/X, Solaris, other *NIX, Windows
- Many nice HTML/PHP front-ends such as Cacti, Cricket, Big Sister, etc.
Other Visualization Techniques Using SNMP Data with RRDTool (Cont.)

Anomaly for DNS Queries

- Throughput Spike
- RTT Spike

Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
Displaying SNMP Data with NMS Station

- Can be considered as “Local telemetry”
- Network Management Systems (NMS) can serve as SNMP consoles, among other things
- Many can use SNMP traps and/or other forms of telemetry as triggers for paging, scripted actions, etc.
- Pulling information together can be useful for NOCs, operations teams
- Commercial systems such as HP OpenView, Micromuse NetCool, IBM Tivoli, CA Unicenter
- Several open source systems - Big Brother (http://bb4.com/), Big Sister (http://bigsister.graeff.com/), Nagios (http://www.nagios.org/), and others
Displaying SNMP Data with NMS—Nagios

Source: http://www.nagios.org
RMON—Remote MONitoring

- RMON is a standard defining how remote probes or agents relay network traffic information back to a central console.
- Not as prevalent as SNMP or NetFlow - supported mainly by commercial network management systems.
- Cisco Network Analysis Module-2 (NAM-2), ntop (http://www.ntop.org) are examples of RMON probes.
- Most RMON probes look at raw packets via SPAN/RSPAN and generate statistics from observed traffic.
- Mini-RMON statistics available on Catalyst 6500/NAM-2, provides detailed stats from layer-2 access ports.
Displaying RMON—ntop Examples

Source: http://www.ntop.org

Detailed Analysis i.e. TTL
Value of RMON: Utilizing NAM-2 Gathered Data

- IETF Standard
- Provides great analysis with NAM-2 collected data
- Mini-RMON available as well

Source: Cisco Systems, Inc.
BGP—Why Do We Care?

- Large-scale network security events such as worms, DDoS attacks, etc. often produce side-effects visible in the global routing table.

- **Correlating** BGP information with other forms of telemetry (NetFlow, SNMP, RMON, etc.) can be effective in determining the true impact of incidents.
BGP Example—SQL Slammer
Correlating NetFlow and Routing Data

Matching data collected from different tools

Route Table Size over Time

Traffic per Router

Prefix | Current | Daily Max | Daily Average
-- | ------- | -------- | --------------
/24   | 65,900  | 68,497   | 67,259        
/23   | 9,904   | 10,157   | 10,027        
/22   | 9,053   | 9,211    | 9,110         
/21   | 6,035   | 6,106    | 6,045         
/20   | 8,485   | 8,560    | 8,487         
/19   | 8,175   | 8,221    | 8,161         
/18   | 3,007   | 3,031    | 3,005         
/17   | 1,693   | 1,705    | 1,690         
/16   | 7,293   | 7,396    | 7,326         
/15   | 473     | 473      | 469           
/14   | 263     | 263      | 262           
/13   | 98      | 98       | 97            
/12   | 55      | 55       | 54            
/11   | 12      | 12       | 11            
/10   | 6       | 6        | 5             
/9    | 4       | 4        | 3             
/8    | 19      | 19       | 18            

Current_Total: 120,475
Max_Total: 123,814
Average_Total: 122,029
Current v. Average: 98.73% (1554 prefixes)
How to Deploy BGP?

- Start with open source tools: Zebra and Quagga
- Zebra (http://www.zebra.org) and Quagga (http://www.quagga.net) are two open source BGP daemons which can log BGP updates for further analysis
- Arbor Peakflow SP Traffic provides BGP visualization, trending, NetFlow traffic correlation, additional functionality (http://www.arbornetworks.com/products_sp.php)
Syslog

- De facto logging standard for hosts, network infrastructure devices, supported in all routers and switches
- Many levels of logging detail available—choose the level(s) which are appropriate for each device/situation
- Logging of ACLs is generally contraindicated due to CPU overhead—NetFlow provides more info, doesn’t max the box
- Can be used in conjunction with Anycast and databases such as MySQL (http://www.mysql.com) to provide a scalable, robust logging infrastructure
- Different facility numbers allows for segregation of log info based upon device type, function, other criteria
Configuring Syslog on a Router

- Syslog data is invaluable
  - Attack forensics
  - Day to day events and debugging
- To log messages to a syslog server host, use the logging global configuration command
  - `logging host`
  - `logging trap level`
- To log to internal buffer use:
  - `logging buffered size`
- Ensure timestamps
  - `service timestamps log...`
Benefits of Deploying Syslog

- Syslog data can be available from a centralized SysLog server(s) as well as router’s local buffer
- Deploy on routers, switches, firewall, IPS sensors and other network elements to get a holistic picture
- Analysis tools available such as Cisco MARS, SEC, ModLogAn and others
- SysLog Server such as Kiwi and syslog-ng
Network Time Protocol

• Synchronize time across all devices

• When security event occurs, data must have consistent timestamps

  From external time source
  
  Upstream ISP, Internet, GPS, atomic clock

  From internal time source

  Router can act as *stratum 1* time source

  ntp source loopback0

  ntp server 10.1.1.1 source loopback0
Benefits of Deploying NTP

- Very valuable on a global network with network elements in different time zones
- Easy to correlate data from a global or a sizable network with a consistent time stamp
- NTP based timestamp allows to trace security events for chronological forensic work
- Any compromise or alteration is easy to detect as network elements would go out of sync with the main ‘clock’
Packet Capture

- Sometimes, there’s just no substitute for looking at the packets on the wire
- SPAN/RSPAN/ERSPAN allow packet capture from Catalyst switches; ip packet export allows packet capture from routers
- Open source tools such as tcpdump, snoop, Ethereal (http://www.ethereal.com) on free *NIX or Windows allow inexpensive packet-capture solutions to be built and deployed
- Commercial tools such as Cisco NAM-2, NAI Sniffer/Distributed Sniffer, Wandel and Goltermann available
- Use macroanalytical telemetry such as SNMP, NetFlow, RMON to guide your use of microanalytical telemetry (i.e., packet capture)
Packet Capture Examples

Wealth of information, L1-L7 raw data for analysis

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH</td>
<td>Ethernet II, Src: 00:00:00:00:00, Dst: 00:00:00:00:00</td>
<td>VLAN 802.1Q Virtual LAN</td>
<td>IP</td>
</tr>
</tbody>
</table>

Packet Details:
- Protocol: HTTP
- Source: eth0: 192.168.6.2
- Destination: 192.168.6.2
- Port: 12345
- Length: 1219 bytes

How to Use Packet Capture

• Mainly a **reactionary** tool
  
  Generally a reaction after finding out that there is an anomaly

• Used in telemetry **during** the security event
  
  Need to know where to capture the packet.
  
  Sometimes, the same packet needs to be captured in multiple places

• **Wealth of information**
  
  Informs what type of outbreak one is observing on the network
  
  Provides raw data for further analysis
  
  Helps by providing information on how to bring the safeguards for short term and long term mitigation
Okay—Tell Me Where to Start From?

1. NetFlow enablement on the network elements
2. NetFlow data correlation and analysis
3. SNMP / RMON [SNMP more prevalent]
   1. CPU / Memory util
   2. Link usage and display with MRTG
4. SysLog collection and analysis
5. Monitoring to Routing, DNS queries, etc. [BGP, DNS]
6. Local and remote packet capture facility [Most have it today with sniffer, ethereal]
The Next Steps-
Best Practice Techniques
SP network security system cycle

Stage 1: Secure
Stage 2: Monitor
Stage 3: Test
Stage 4: Improve
Security Best Practices - Overview

• Define a Security **Policy** and the required procedures to enforce it
  
  this should include roles, responsibilities, customer contacts, etc.

• Create an Incident Response **Team**
  
  should work in conjunction with the NOC/SOC

• Establish a **Relationship** with other relevant organizations
  
  PSIRTs, CERTs, NSPs, and peering SPs
Security Best Practices – Overview (cont’)

• Design and Implement Services with Security in mind

• Secure the infrastructure following a **Modular** design

  Focus on the most critical areas first

• Define a solid incident handling **Procedure**

  Preparation
  Identification
  Classification
  Traceback
  Reaction
  Post Mortem
Procedure: Preparation

- **Know the enemy**
  - Understand what drives the miscreants
  - Understand their techniques

- **Create the security team and plan**
  - Who handles security during an event? Is it the security folks? The networking folks?
  - A good operational security professional needs to be a cross between the two: silos are useless...

- **Harden the devices**

- **Prepare the tools**
  - Network telemetry
  - Reaction tools
  - Understand performance characteristics
Prepare Response Teams

- Identify key individuals/groups and create an incident response team
- Participate in and communicate to incident response forums and organizations
  
  FIRST
  
  NSP-SEC
  
  NANOG
  
  PSIRT
- Monitor emerging threats
  
  http://packetstormsecurity.org
  
  http://isc.sans.org
  
  Many others…
Preparing the Network

• Understanding your network is critical to preparation

• What is normal? What is healthy?

• Monitor important indexes
  Bandwidth—peer, router, interface, application
  Routing—hijacking, instability
  CPU—punted traffic, “show ip traffic”
  Traffic patterns—by AS, prefixes, ports
Preparing the Network

Harden the Network

- Secure the control plane
  Routing protocol authentication, BGP TTL check, prefix-filtering
- Secure the management plane
  Disable unnecessary services
  Secured and authenticated device access – AAA, VTY/SNMP
  ACL’s, Out-of-band management
- Secure the data plane
  Anti-spoofing via strict/loose uRPF, infrastructure ACL’s
- Auditing
  Logging, AAA records, SNMP traps
The Old World: Network Edge

- Core routers individually secured
- Every router accessible from outside
The New World: Network Edge

- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside
The Old World: Router Perspective

- Policy enforced at process level (VTY ACL, SNMP ACL, etc.)
- Some early features such as ingress ACL used when possible
Central policy enforcement, prior to process level

Granular protection schemes

On high-end platforms, hardware implementations
ASIC-Based Platform: Main Components

- **Ingress Packets**
- **Forwarding/Feature ASIC Cluster**
- **Forwarded Packets**
- **To Fab to Other Line Cards**
- **Punted Packets**
- **Packets Bound for the LC CPU or RP**
- **Receive Path Packets**

**ASIC’s Supporting CPU**

**RAW Queue(s)**
- Also Called CPU Queue(s) and Punt Queue(s)

**Route Processor CPU**
Data Plane

Forwarding/Feature ASIC Cluster

Ingress Packets

Data Plane

All Packets Forwarded Through the Platform

Punted Packets

ASIC’s Supporting CPU

Receive Path Packets

Forwarded Packets

To Fab to Other Line Cards

Route Processor CPU

Preparation
Control Plane

Ingress Packets

Forwarding/Feature ASIC Cluster

Forwarded Packets

To Fab to Other Line Cards

Control Plane

ARP, BGP, OSPF, and Other Protocols that Glue the Network Together

Ingress Packets

Control Plane

Route Processor CPU

Most Control Plane Packets Go to the RP

Receive Path Packets

Preparation
Management Plane

Ingress Packets

Forwarding/Feature ASIC Cluster

Forwarded Packets

To Fab to Other Line Cards

Management Plane

Telnet, SSH, TFTP, SNMP, FTP, NTP, and Other Protocols Used to Manage the Device

Management Plane

Receive Path Packets

All Management Plane Traffic Goes to the RP

ASIC's Supporting CPU

Route Processor CPU

Preparation
Preparing the Network—Infrastructure Protection

- Techniques to secure your transit networks
  Infrastructure ACLs, Receive ACLs, Control Plane Policing
Packet Filtering Viewed Horizontally

Spoofed Source Addresses

Targeting the Infrastructure

Application Filters—Policy Enforcement

Targeting the Customer

Customer Traffic
Packet Filtering
Remember to Filter the Return Path

Spoofed Source Addr.
Targeting the Infra.
Application Filters—Policy Enforcement
Targeting the Customer
Permitted Customer Traffic

Spoofed Source Addresses
Denied Apps Out
Infrastructure Protection Tools

- **Infrastructure ACLs (iACLs)—Originally, the only approach**
  
  Create policies (ACLs or MQC) for control plane traffic to block all unwanted IP traffic destined to the core.
  
  Applied to ALL ingress port—affects ALL traffic (control and data plane).

- **Receive Path ACLs (rACLs)—The first step…**
  
  Create ACLs to block unwanted IP traffic destined to the core.
  
  Global (single) configuration affects all “receive path” packets.
  
  Only affects control plane traffic.
  
  Only available for Cisco 12000 and Cisco 7500 routers.

- **Control Plane Policing (CoPP)—The newest approach**
  
  Extends rACLs by adding Modular QoS CLI (MQC) policing.
  
  Modify input path to “split” control and data plane traffic prior to input feature application.
Control Plane Policing Deployment Policies

Define Service Policy

- Start with a simplistic policy that will not disrupt network operations
  - For critical, important, and normal traffic types, conform actions are “transmit”
  - For undesirable traffic, all actions are unconditionally “drop” regardless of rate
  - For default traffic, rate-limit the amount of traffic permitted above a certain bps

- Modify the policy over time as more confidence is gained in traffic rates—particularly for “critical” traffic
  - A very low rate might discard necessary traffic, whereas a high rate might allow the Route Processor to be inundated with a flood of non-critical packets
  - The appropriate rates are dependent on platform capabilities and CPU capacity
  - The appropriate rates are typically site-specific as well, depending on local topology and routing table size

- Strive for constant improvement to keep pace with new attacks, and to cover new services

---

### Basic Control Plane Policing Service Policy

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Rate (bps)</th>
<th>Conform Action</th>
<th>Exceed Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>N/A</td>
<td>Transmit</td>
<td>Transmit</td>
</tr>
<tr>
<td>Important</td>
<td>125,000</td>
<td>Transmit</td>
<td>Transmit</td>
</tr>
<tr>
<td>Normal</td>
<td>15,000</td>
<td>Transmit</td>
<td>Transmit</td>
</tr>
<tr>
<td>Undesirable</td>
<td>8,000</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>Default</td>
<td>8,000</td>
<td>Transmit</td>
<td>Drop</td>
</tr>
</tbody>
</table>

### Hybrid Control Plane Policing Service Policy

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Rate (bps)</th>
<th>Conform Action</th>
<th>Exceed Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>N/A</td>
<td>Transmit</td>
<td>Transmit</td>
</tr>
<tr>
<td>Important</td>
<td>125,000</td>
<td>Transmit</td>
<td>Drop</td>
</tr>
<tr>
<td>Normal</td>
<td>15,000</td>
<td>Transmit</td>
<td>Drop</td>
</tr>
<tr>
<td>Undesirable</td>
<td>8,000</td>
<td>Drop</td>
<td>Drop</td>
</tr>
<tr>
<td>Default</td>
<td>8,000</td>
<td>Transmit</td>
<td>Drop</td>
</tr>
</tbody>
</table>
Prepare the Tools

Sinkholes

• Sinkholes are a versatile function of routing topology and hardened infrastructure

• Infrastructure protection
  
  Sinkhole your core address space to minimize attack

• Identification/classification
  
  Monitor dark IP space for attack noise and worm/botnet scanning
  Redirect attacks for analysis

• Traceback
  
  Use backscatter to trace spoofed hosts

• Reaction
  
  Divert attacks from the victim
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 scrubbers
Sinkholes: Worm Detection

Customer

May Also Use NetFlow Data from Edge Routers for This Purpose...

Computer Starts Scanning the Internet

SQL

Sinkhole Advertising Bogon and Dark IP Space

SINKHOLE NETWORK
Backscatter Analysis of Attack Noise

Other ISPs → Ingress Routers → Other ISPs

RANDOM DESTINATIONS

RANDOM SOURCES

Target

Sink Hole Router

Preparation
Sink Hole Routers/Networks

172.168.20.1 is attacked
172.168.20.0/24 - target’s network
172.168.20.1 is attacked

Sink Hole Network

Target of Attack

Preparation
Sink Hole Routers/Networks

Target of Attack
172.168.20.0/24 - target’s network
172.168.20.1 is attacked

Router advertises 172.168.20.1/32

Sink Hole Network
Identifying Attacks

- Proactively monitor internal and “dark IP space”
- Build baselines for all traffic to expose anomalous behavior
- Utilize tools that enable network-wide correlation of control and data planes (e.g., CPU utilization, route stability, Netflow, etc..)
- Notify your customers before they notify you—be proactive!
Changes to Network Baselines

- SNMP data
- Unexplained changes in link utilization
  - Worms can generate a lot of traffic, sudden changes in link utilization can indicate an attack or a worm
- Unexplained changes in CPU utilization
  - Attack/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/worm!

Need to know what’s normal to identify abnormal behavior
Ways to Identify DoS Attacks

- Customer/End User call
- SNMP: Line/CPU overload, drops
- NetFlow: Counting flows
- ACLs with logging
- Backscatter
- Sniffers
- Anomaly Detector
Identification Examples

BGP Flaps

Packet Size

CPU
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 a router?
Classification

• What type of attack has been identified?
• Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  What type of attack has been identified?
  What’s the effect of the attack on the victim(s)?
  What next steps are required (if any)?
Ways to Classify DoS Attacks

- NetFlow: Flow information
- ACLs (maybe with logging)
- Backscatter
- Sniffers
- Anomaly Detector
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

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

Looks Like Smurf Attack
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
Traceback

- Traceback to network perimeter
  - Netflow
  - Backscatter
  - Packet accounting
  - IP Source
- Retain attack data
  - Use to correlate inter-domain traceback
  - Required for prosecution
  - Deters future attacks
  - Clarify billing and other disputes
  - Post Mortem Analysis
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
The Internet Routing Registry (IRR): Network Info

madrid% whois -h whois.arin.net 64.103.0.0

<table>
<thead>
<tr>
<th>OrgName:</th>
<th>Cisco Systems, Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrgID:</td>
<td>CISCOS-2</td>
</tr>
<tr>
<td>Address:</td>
<td>170 West Tasman Drive</td>
</tr>
<tr>
<td>City:</td>
<td>San Jose</td>
</tr>
<tr>
<td>StateProv:</td>
<td>CA</td>
</tr>
<tr>
<td>PostalCode:</td>
<td>95134</td>
</tr>
<tr>
<td>Country:</td>
<td>US</td>
</tr>
<tr>
<td>NetRange:</td>
<td>64.100.0.0 - 64.104.255.255</td>
</tr>
<tr>
<td>CIDR:</td>
<td>64.100.0.0/14, 64.104.0.0/16</td>
</tr>
<tr>
<td>TechHandle:</td>
<td>CAH5-ARIN</td>
</tr>
<tr>
<td>TechName:</td>
<td>Huegen, Craig</td>
</tr>
<tr>
<td>TechPhone:</td>
<td>+1-408-526-8104</td>
</tr>
<tr>
<td>TechEmail:</td>
<td><a href="mailto:chuegen@cisco.com">chuegen@cisco.com</a></td>
</tr>
<tr>
<td>OrgTechHandle:</td>
<td>DN5-ORG-ARIN</td>
</tr>
<tr>
<td>OrgTechName:</td>
<td>Cisco Systems, Inc.</td>
</tr>
<tr>
<td>OrgTechPhone:</td>
<td>+1-408-527-9223</td>
</tr>
<tr>
<td>OrgTechEmail:</td>
<td><a href="mailto:dns-info@cisco.com">dns-info@cisco.com</a></td>
</tr>
</tbody>
</table>

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

```
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

Victim
Trace-Back in One Step: ICMP Backscatter

iBGP Updates:
“Drop Packets to Target”
Trace-Back in One Step: ICMP Backscatter

- **Target**
- **Sink Hole Router with Logging**
- **ICMP Unreachables**
- **iBGP Updates:**
  - “Drop Packets to Target”
- **Ingress Routers**
- **Other ISPs**

Diagram shows network traffic flow and traceback process.
1. Don’t Panic!

2. Use A Mitigation Methodology.

3. Do not make drastic changes to the network while the attack/worm is rampant.
ISP Security Incident Response

- Given that ISPs are transit networks, the way incident response happens is slightly different from other networks.
- More effort is made to mitigate the effects of the attack 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.
Capacity as a Solution

- To many sorts of attacks, a common solution is to add **more capacity**
- Not every problem gets solved this way
  Think about collateral damage
- Challenge is to solve all the problems in the most economically feasible way
Using IP Routing as a Security Tool

• ISPs use **routing** to get packets from customers to the Internet

• ISPs use routing to engineer traffic through their network

• ISPs manipulate traffic to get the most out of their available bandwidth

• What is the problem with manipulating bad traffic to get the most out of available bandwidth?
Using IP Routing as a Security Tool

- IP Routing can be used to manipulate traffic on the ISPs network to:
  - Null0 (Black Hole)
  - Shunts
  - Sink Hole
  - Analysis Devices
  - Clean up Devices
  - Rate-Limit
And it is all done via BGP....

Uses a BGP “trigger router”

One router on the network connected via an iBGP route reflector that injects “trigger update”

The BGP Update packet
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!
Customer Is DOSed—Before

Reaction
Customer Is DOSed—After

- **IXP-W**
- **Peer A**
- **Peer B**
- **Upstream A**
- **Upstream B**
- **IXP-E**
- **Target**
- **POP**
- **F**
- **G**
- **NOC**
- **Reaction**

iBGP Advertises List of Black Holed Prefixes based on SOURCE ADDRESSES
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
Re-Directing Traffic from the Victim

Sink Hole Router: Announces Route “target/32”

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

Other ISPs
Ingress Routers

Target
Guard: Packet Scrubbing

1. Detect
   Anomaly Detector, IDS, NetFlow...


3. Divert Only Target’s Traffic

Non-Targeted Servers

Target
Guard: Packet Scrubbing

4. Identify and Filter the Malicious

5. Forward the Legitimate Traffic Destined to The Target

6. Non Targeted Traffic Flows Freely

Non-Targeted Servers

Anomaly Detector, IDS, NetFlow,…

Target
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?
Post Mortem

- Analyze data, trends and discuss attack
- Fully history of attack(s), trends, etc..
- Determine what, if anything, could have been done to be better prepared—make appropriate modifications if necessary
Post Mortem Activities

• Assess Incident Response Team Role
  Full Representation?
  Single/centralized Point of Contact?
• Review and Update Technical AND Operational Functions and Procedures
• **Quantify** impact of downtime
  Financial
  Operational
• What can we do better next time?
The Next Steps-
Modular Application of Techniques to SP Infrastructure
SP Functional Blocks

Module 4

Network Operation Center
Security Operation Center

Customer Premises

CPE

Core Infras. POP

POP Border

ISP Backbone

To POPs

Peering

Distribution

Data Center

Data Center Edge

Infrastructure Services

Dedicated Server-Farm

Shared Server-Farm

Module 2

Module 1

Module 3
Why and the benefits of Modular Design

- Systematic approach where security is implemented throughout the network rather than point products
- Multiple layers of control provides higher security
- It allows you to focus on the most critical areas first
- Facilitates the enforcement of the security policy
- Contains the effects of attacks
- More flexible to adapt to keep up with the always changing threats
Module I - Typical POP & Core Infrastructure

**POP Border (Medium Speed):**
- 64K and nx64K circuits
- Mixture of channelised T1/E1, 56/64K and nx64K circuits
- Channelised T1/E1

**POP Border (High Speed):**
- Channelised T3/E3
- T1 and E1 circuits
- Mixture of channelised T3/E3 and T1/E1 circuits

**ISP Backbone:**
- 3640/7206/7507
- Mixture of channelised T3/E3 and T1/E1 circuits

**Distribution:**
- 3600/7200/7500
- Mixture of channelised T1/E1, 56/64K and nx64K circuits

**Network Operations Center:**
- Data Center

**Peering:**
- Other POPs

**Other ISPs:**
- Other ISPs
• Network Reconnaissance
• Denial of Service
• Viruses and Worms
• IP Spoofing
• Direct Exploits
• Routing Disruption
• .......

Module 1
Securing POP & Core Infrastructure Module

- **Harden routers and switches**
  Prevents DoS and Direct attacks to routers and switches

- **Secure Dynamic Routing Exchange**
  Route Authentication, Route Filters prevent attacks on the Dynamic Routing

- **Deploy packet filters**
  Mitigates DoS attacks, spoofed attacks, reconnaissance, viruses/worms and direct attacks

- **Attack detection, traceback and containment**
Securing POP & Core Infrastructure Module

Harden routers and switches

• **IOS hardening**
  - Set strong passwords
  - Enable secure access
  - Configure banners
  - Disable unnecessary global and interface services
  - Autosecure
  - ......

• **Selective Packet Discard (SPD)**
  - Prioritize control packets

• **Control ICMP Unreachable**
  - ......
Secure Dynamic Routing Exchange

- **Secure Routing Route Authentication**
  - Plain text
  - HMAC-MD5

- **Control Routing Updates**
  - Dynamic Routing Filter on Customers
  - Dynamic Routing Filter to Peers
  - Dynamic Routing Filter from Peers

- ............
Securing POP & Core Infrastructure Module
Deploy packet filters

• Packet Filters
  – RFC 2827 BCP 38 Packet Filtering (source address spoofing)
  – BCP 38 Ingress Packet Filtering
  – Static BCP 38 Filtering
  – Unicast RPF (strict mode)
  – ………
Securing POP & Core Infrastructure Module

Attack detection, traceback and containment

- Netflow
- Intrusion Detection System alerts
- Sink hole routers/networks
- Unusual CPU load – reported via SNMP
- Circuits Saturated
- BGP Session Flapping
- Customer calls
- .......
The IDS uses Netflow to collect data on the flows through the network, looking for matches to known attacks while watching for new anomalies in the data flow.
Securing POP & Core Infrastructure Module
Attack detection, traceback and containment

1. Apply temporary ACLs with log-input and examine the logs
2. Query Netflow’s flow table
   • No changes to the router while the network is under attack; passive monitoring
   • Scripts can be used to poll and sample throughout the network
   • IDS products can plug into Netflow
   • Working on a MIB for SNMP access
3. Backscatter Traceback Technique
   • Reduced Operational Risk to the Network while traceback is in progress.
   • Speedy Traceback
   • Ability to hand off from one ISP to another - potentially tracing back to it’s source.
Securing POP & Core Infrastructure Module
Attack detection, traceback and containment

Backscatter Traceback Technique

1. Dos Attack starts
2. Sink Hole configured with route to the /32 under attack with next-hop equal to the Test-Net
3. Router Advertises Bogus and unallocated networks
4. Edge Routers start dropping packets to the /32
5. All edge routers with static route Test-Net (192.0.2.0/24) to null

BGP Propagates the update
ICMP Unreachable backscatter will start sending packets to bogus/unallocated nets

171.68.19.1
Victim

Cisco.com
Securing POP & Core Infrastructure Module

Attack detection, traceback and containment

• ACLs—Manual upload/dynamic upload
• uRPF—Remote trigger via BGP
• CAR—Manual upload or remote trigger via BGP
• ........
Remote Triggered uRPF

• Same as Backscatter Traceback Technique but with uRPF loose check on all border routers
• If source = null then drop
• static to null also drops on destination
Remote Triggered CAR

- Quality Policy Propagation with BGP (QPPB) empowers CAR to use updates triggered by BGP. This enables a network protocol to trigger the rate limits on source/destination.
Module II - Secure Customer Premises

- Secure deployment and provisioning
- Secure management and configuration
- Integrated Security at the CPE
Secure Provisioning and Deployment

Provisioning and deployment are the phases in which the devices are the most vulnerable:

- Not all devices come with secure defaults
- Initial configurations may include more items than needed for initial setup (i.e. unnecessary services)
- The protocols and applications used for initial configuration may not be secure
- Deployment may not include the authentication of the new device
- Pre-configure the new device with a secure configuration prior to its deployment (consider even before shipping)
- Once connected, use secure access for initial setup
- For high volume deployments use a hierarchical management solution
- Access Control\Authorization Using AAA
Module III - Secure Data Center

ISP Backbone

ISP Edge Distribution

Shared Compartment

Dedicated Compartment

Services Module

Content switch

Content Engine

SSL
IDC Security Highlights

• Core, Distribution, Access model
• Resilience at layer 2 and 3
• Uses Scaling Modules
• Provides Baseline Content Services
• Access: Layer 2 VLAN separation
• Distribution: Aggregate VLANs, routing and layer 3 filtering
• Core: Provides L3 connectivity
Secure Data Center Design

Spoof Mitigation
(D)DoS Rate-Limiting

Stateful Packet Filtering
Basic Layer 7 Filtering
DoS Mitigation

Host IDS Local Attack Mitigation

Infrastrucure Services

Stateful Packet Filtering
Basic Layer 7 Filtering
Host DoS Mitigation

Server farms

Stateful Packet Filtering
Basic Layer 7 Filtering
Private VLANs
Host DoS Mitigation
IDS Layer 4-7
Module IV - Secure NOC/SOC module

• Protect the NOC
  Separate physical networks (NOC vs. campus)
  Separate address space (192.168.25x.xxx)
    - Not routed anywhere else
  Firewall between management subnet and rest of SP campus
    - Chokepoint to protect NOC functions
  NIDS and HIPS on the management subnet
  One-Time Passwords (OTPs) for authentication of administrators
  IPSec for remote administrative access to the NOC
Module IV - Secure NOC/SOC module - cont’d

- Secure remote management of CPE devices
  
  Consider Out-Of-Band (OOB) management network

  Dedicated physical management interfaces on all remote managed devices

  Alternatively a high availability backup option

Secure transport

- IPsec for always-up SNMP\MIB\syslog access

  SNMP read-only

  Pre-shared keys (no wildcard) or PKI

  SSL, SSH, or IPsec RA for troubleshooting
Secure NOC/SOC module Design

- Two-Factor Authentication
- AAA Services
- Read-Only SNMP
- Network Log Data
- SSH Where Possible
- Config and Content Management
- OTP Server
- Access Control Server
- Network Monitoring
- IOS Director
- Syslog 1
- Syslog 2
- System Admin
- IPS Services Lockdown
- Comprehensive Layer 4-7 Analysis
- Stateful Packet Filtering
- IPsec Termination for Management
- Campus/Edge
- FW
Wireless Security
A Quick Glance
Wireless LAN Security Hierarchy

Open Access
- No Encryption, Basic Authentication
  - Public “Hotspots”

Basic Security
- 40-bit or 128-bit Static WEP Encryption
  - Home Use

Enhanced Security
- WPA, 802.1X, TKIP Encryption, Mutual Authentication, Dynamic Keys
  - Business

Remote Access
- Virtual Private Network (VPN)

Business Traveler, Telecommuter
Basic Wireless LAN Security
802.11 Security Vulnerabilities

- **Shared, static Wired Equivalent Privacy (WEP) keys**
  - No centralized key management
  - Poor protection from variety of security attacks
- **No effective method to deal with lost or stolen client adapters**
  - Possessor of client adapter has access to WLAN and any network resource for which no network logon is required
  - Re-keying of all WLAN devices is required
- **Lack of integrated user administration**
  - No central authentication entity
  - Potential to identify user by MAC address, not username
  - No usage accounting and auditing. No means to detect unusual activity
- **Lack of effective message integrity**
  - Management and data frames use ineffective CRC for integrity check.
Wireless LAN Security
Authentication and Encryption

• Authentication
  - IEEE 802.11 Authentication: Open or shared-key – Not secure
  - Static WEP Keys – Unable to send or receive without correct keys. Device can be stolen. Keys can be cracked
  - MAC Address Authentication – Device-based. Address can be spoofed
  - IEEE 802.1X: EAP Types – LEAP, EAP-FAST, PEAP and EAP-TLS, EAP-TTLS. Component of new standard for WLAN security. Supports mutual authentication and dynamic, per-user, per-session encryption keys
  - Wi-Fi Protected Access (WPA) - 802.1X is a required component of the WPA standard. WPA is tested with EAP-TLS but works with all EAP types including Cisco LEAP.

• Encryption
  - IEEE 802.11 WEP - Standard for encryption
    • Uses RC4 algorithm - known vulnerabilities
    • Keys can be static and shared among many clients or, as with 802.1X, keys can be dynamic and unique for each client
  - Temporal Key Integrity Protocol (TKIP): Enhancements to RC4-based WEP
    • Cisco TKIP and WPA TKIP available
    • Key Hashing or Per-packet keying, Message Integrity Check (MIC) and Broadcast Key Rotation
  - Advanced Encryption Standard (AES)
Enhanced Wireless LAN Security
802.1X Protocol in WLAN Environment

EAP Authentication Types: LEAP, PEAP, EAP-TLS, EAP-FAST:
1. User requests access; AP prevents wired network access
2. Encrypted credentials sent to authentication server
3. Authentication server validates user, grants access rights
4. AP Port enabled and dynamic encryption keys are assigned to client (encrypted)
5. Wireless client can now access general network services securely
Enhanced Wireless LAN Security
802.1X for 802.11 Benefits

- Open, extensible and standards based solution
- Leverages existing standards: EAP (Extensible Authentication Protocol), RADIUS
- Strong authentication with support for a variety of authentication types
- User-based identification
- Dynamic key management
- Better multicast capability
- Centralized policy control - authentication, authorization and accounting
- Session timeout triggers re-authentication and new encryption key
New Security Enhancements
Mitigate Network Attacks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Open</td>
<td>Static WEP</td>
<td>Cisco LEAP, EAP-FAST, EAP-TLS or PEAP</td>
<td>Dynamic WEP</td>
<td>Cisco LEAP, EAP-FAST, EAP-TLS or PEAP</td>
<td>Cisco TKIP, WPA-TKIP, AES</td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Protected**</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
</tr>
<tr>
<td>Authentication Forging</td>
<td>Vulnerable</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
</tr>
<tr>
<td>Weak Key Attacks</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
</tr>
<tr>
<td>Packet Forgery</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
</tr>
<tr>
<td>Brute Force Attacks</td>
<td>40-bit WEP</td>
<td>Protected *</td>
<td>Protected *</td>
<td>Protected</td>
<td>Protected</td>
<td>Protected</td>
</tr>
</tbody>
</table>

*Cisco LEAP requires strong passwords

**PEAP vulnerable when used with legacy authentication

Protected from War Driving
Protected from Script Kiddies
Protected from Professionals
Protected from War Driving
Case Study
Example Customer Profile

• Major US Service Provider

• Services:
  – Broadband Internet Access
  – IP VPNs
  – VoIP
  – Web Hosting

• Incident Response Team deals with 1 DoS a day in average
Example Customer Network Topology

Customer Premises

Data Center

Other POPs

Other ISPs
Example Customer Security Modular Design

Route Authentication
- uRPF
- Ingress/Egress Filters
- Netflow/IDS

Data Center
- Ingress Filters
- IDS Sensors
- Stateful Firewall
- Encrypted Access

ISP Backbone
- Peering
- POP Border

Distribution
- Other POPs
- Other ISPs

Sink Hole for:
- Backscatter traceback
- Remote Triggered uRPF/CAR

Route Authen.
- uRPF
- Ingress Filters

Route Authen.
- uRPF loose mode
- Ingress Filters
- Egress Filters
What have they done to improve?

Attack Detection

Before:
- check resources such as CPU, input queues
- Backscatter analysis using tools such as snoop and tcpdump
- Use ACLs to confirm attacks.

Now:
- Netflow at border routers.
- IDS Sensors at Data Center and aggregation points

Results:
- More attacks are being detected
- Attack detection and mitigation times have been significantly reduced
What have they done to improve?

Traceback source of attacks

Before:
- Hop by hop using ACLs with logging.

Now:
- Backscatter Traceback Technique

Results:
- Traceback in minutes
- Works under large scale attacks
- Easy to hand over to peer SPs
Conclusions

• What we covered-
  Challenges, Trends, Threats
  Telemetry, Techniques, Application

• SP Security is a real issue, need an integrated system

• Integrate security throughout the network, not point products

• Define Security Policies and related Procedures

• Telemetry – Get a grip on what’s going on

• Modularize – Break the tasks into layered items
The Last Word…

- New threats enter, old threats leave, but the core risk mitigation strategies stay the same
- However, the shift from **Fame to Profit** as the dominant motivation is changing the paradigm of threat management
- Tomorrow’s threats will be different than today's—plan ahead to maintain flexibility