



# Security Best Practices for Service Providers

Chuck Sellers, CISSP

Sr. Product Engineer

NTT Comm. - Global IP Network US

**NAv6TF/ARIN XV IPv6 Conference**

**Orlando, Florida**

**April 17 – 21, 2005**





# Agenda

---

- Systems Security
- Backbone
- Provider Edge/Customer Premise Equipment
- ISP Supporting Activities
- IPv6 Specific
- IPv6 – m2m-x



# Systems Security Overview



# ISP Security = Systems Security

- ISP Security needs to be looked at from a systems perspective:
  - Hardware: Routers, servers, switches, firewalls, etc.
  - Software: Applications, tools, scripts, databases, etc.
  - Documentation: Policies, procedures, best practices
  - Access Control: Authentication, Authorization, Accounting
  - Forensics, preservation of evidence
  - Data privacy protection
  - Business and Legal (SOX, HIPPA, GLB, etc)
  - Business Continuity
- Applies to medium and large Enterprises as well



# Security Points to Remember

- Security is a continuous process
- Every network device is either a potential target or weapon from which to launch an attack
- Operational simplicity sometimes means topological complexity
- Avoid security through obscurity – have peers review design and implementation
- Seek to minimize risk while maximizing security without breaking the bank
- Disgruntled (ex)employees – prime candidates for inside jobs
- Defense in depth / security in layers



# Breaking the System Into Components-ISP

---

- Backbone/core
  - Device integrity
  - Route authentication
- Aggregation/Distribution
  - Device integrity
  - Route authentication
  - Stateful/stateless firewall
  - Crypto
  - L3 filtering, L3 DDoS mitigation, L3 spoof mitigation



# Breaking the System Into Components - Customer

---

- CPE Access/Perimeter
  - L3 filtering, L3 DDoS mitigation
  - L2 security (Firewall, AAA, device integrity)
  - URL filtering
  - IDS (Host/Network based)
- Endpoints
  - Device integrity
  - Device and user AAA
  - Hosts: firewall (i.e. Black Ice), OS patches, AV, hardening
  - File system encryption
  - Vulnerability scanning



# Threat Overview

- Types of Attacks:
  - Layer 1: (Primarily physical) Wiretapping, Fiber tapping, console access, Rogue devices, etc.
  - Layer 2 attacks: VLAN "hopping"; MAC, DHCP, ARP, Spoofing; Others
  - Layer 3: IP Spoofing, DoD/DDoS, routing, Smurf, Tunneling, Translation, Transition
  - Layer 4-7: Viruses, Worms, Application, Rogue software, Man in the Middle
- Multiple Layers
  - Reconnaissance, unauthorized access
  - Sniffing
- Daily Probes and Attacks (60 days)
  - Low: 83, Average: 529, High: 4355\*



\* 60 Days of Basic Naughtiness, Rob Thomas, <http://www.cyrmu.com>



# Backbone Security Overview



# Best Practices – Device Integrity

- Secure ALL administrative interfaces!
  - 16,815 out of 115,466 non-rfc1918 routers probed were reachable\* of at least one admin interface (14.5% of probed routers total)
  - US average: 14.22% of publicly accessible routers
- Maintain equipment in:
  - A locked room / restrict access
  - Environmentally controlled environment
  - Include all hardware: routers, switches, hubs, hosts, servers, RPCs, modems, terminal servers, etc.
- Helps to prevent rogue devices being installed in sensitive locations

\*Based only on receipt of SYN-ACK





# Best Practices - BGP

- Unicast RPF (RFC 2827 Filtering)
  - Ingress Access Lists
  - Strict Reverse Path Forwarding
  - Feasible Path Reverse Path Forwarding
  - Loose Reverse Path Forwarding
  - Loose Reverse Path Forwarding ignoring default routes
- Ingress and Egress Prefix Filters (with max prefix length limit and bogon filtering)
- Bogon route filtering (<http://www.cymru.com/Bogons/>)
- Route Flap Dampening
- BGP Network ACLs at all borders / gateways / peers
- TCP MD5 (with strong passwords)



# Best Practices – BGP (Continued)

---

- Static ARP for Ethernet peering
- Static CAM entries and port security [20] for IXP Ethernet switches
- AS Path Filtering
- Implementing Security
  - BGP – MD5 authentication
- TCP Spoofing is required to inject data, DoS
  - Especially important in 6to4 translations



# Best Practices – OSPFv3 IPv6

- ACLs to allow peers/links to talk to each other
- Authentication has been removed from OSPF packet header (AuType, Authentication)
- Utilize IPsec AH (RFC 2402) and ESP (RFC 2406) for OSPFv3 to ensure integrity and authentication/confidentiality of routing exchanges
- Each v6 router interface has a single metric, representing the cost of sending packets out the interface.
- Accidental data corruption is provided by the standard IPv6 16-bit one's complement checksum
- Very important for the implementation to check the IPSEC SA, and local SA database to make sure that the packet originates from a source THAT IS TRUSTED FOR OSPF PURPOSES.
- ISIS - Optional password protected checksums - RFC 3358



# Provider Edge/ Customer Premise Equipment (CPE)



# Aggregation and Customer Sites

- Customers have issues (v4 and v6) - and want ISP's help at the CPE:
- Managed Router
  - Configuration change management
  - ACLs (IP / TCP / UDP specific)
- Managed Security
  - Firewall
  - IDS
  - URL Filtering
- Black hole filters (RFC 3882, other)
- E-mail: Spam and Phishing



# Top TCP and UDP Attacks

	TCP	UDP
1	3663 (DDoS Attack)	137 NETBIOS
2	0 Reserved (DDoS Attack)	53 DNS
3	6667 IRC (DDoS Attack)	27960
4	81 (DDoS Attack)	500 ISAKMP
5	21 FTP-control	33480 (likely UNIX traceroute)



# ISP Supporting Activities





# Internet Services (v4 and v6)

---

- DNS, HTTP, SMTP, NTP
- Don't implement IPv6 and not implement security on these platforms
- DNSSEC and Dynamic DNS available now
- Don't forget to lock down v6 host security



# Application Level Security

---

- Software Applications
  - Where most exploits/compromises occur
  - Application software itself, Databases, scripts, etc.
  - Glue software (scripts, hacks, etc.)
- Types of Attacks
  - Buffer overflows
  - Remote exploits
  - Virus and trojan programs delivered various ways



# Vulnerable Application Software

- Estimated bugs in software is between 5 to 50 per 1,000 LOC (Lines of Code)

System	Lines of Code	Estimated Bugs
Solaris 7	400,000	2k – 20k
Linux	1.5 million	7.5k – 75k
Netscape	17 million	85k – 850k
Boeing 777	7 million	1.4k – 4k
Space Shuttle	10 million	50k – 500k
Space Station	40 million	200k – 2 mn
Windows 95	< 5 million	25k – 250k
NT5	35 million	175k – 1.75mn
Windows XP	40 million	200k – 2 mn



# ISP Supporting Activities

---

- Route registry (IPv4 and IPv6)
- Internal tools platforms
  - Office/Enterprise network
  - Security Policies and Procedures
  - Bringing in Law Enforcement
- Intellectual Property (router configs, tool configs & data are "Company Confidential")
- Network management & monitoring systems



# IT Systems

---

- Internal systems necessary to run the business:
  - Sales
  - Legal
  - Human Resources
  - Supply Chain
  - Billing & Collections
- Backup storage (Tapes, SANs, other media)
- Disposal of old equipment



# Economic Impact Example

- Satellite Pay Per View (PPV)
  - 100,000 in signal theft
  - \$9.95 PPV = potential \$1 million loss
  - \$29.95 PPV event = potential \$3 million loss
- Free Web for 30 days Deal
  - 10,000 perps/month globally
  - \$50 account = potential \$500k/month loss
  - Favored by phishers – too fast for ISP / LEA



# IPv6 Specific





# IPv6 Specific - IPSec

- IPSec Mandatory in IPv6 protocol
- Utilization optional
- IPSec Issues same as in IPv4
  - Configuration Complexity
  - Key Management
  - More complexity when adding wireless/mobile
- No commercial application for IPv6 Security
- Not specifically addressed here is MIPv6 or wireless



# IPv6 – Architectural Changes

---

- More address space - recon harder
  - Ping sweep useless
- IPv6 restores true end-to-end connectivity
- Privacy extensions complicate troubleshooting & trace backs
- Various potential “private” networks possible
  - Secure just like a public network
- Unknown attacks – little broad-based operational experience with IPv6



# IPv6 Security Threats

- Most IPv4 recon techniques & threats
- Tunnels (6 in 4, i.e. GRE, ipip, VPNs) can bypass firewall/perimeter security
- Tunneling mechanisms are susceptible to packet forgery and DoS attacks
- Neighbor Discovery attacks
- Hosts security for IPv6 missing/inadequate
- Example: Key systems can be ID'ed using multicast – (i.e. NTP)



# IPv6 Specific Security Procedures

- Implementation Recommendations:
  - Applicable BCPs in IPv4 into IPv6
  - Routing protocol security as described previously
  - Static neighbor entries for critical systems (eliminates ND attacks)
  - Drop all fragments < 1280 octets (IPv6 MTU=1280 octets)
  - Dual-stack (preferred) when migrating (removes translation security issues)
  - Static tunneling between endpoints + ACLs
  - Outbound filtering to allow only authorized tunnel endpoints
    - Deny IP protocol 41 out (6to4)
    - Deny UDP port 3544 (Teredo)



# IPv6 Specific Security Procedures

---

- Filter internal-use IPv6 addresses at organization border routers
- Use standard, but nonobvious static addresses for critical systems (i.e. ::DEA1 vs ::10, ::20)
- Filter unneeded services at the firewall, CPE and other places as needed
- Remember to use a trust model for tunneling and translation mechanisms



# The Future



# Emerging Technologies

- Apply what has been presented to fixed network
- Adapt security strategies for IPv6 with mobile capability
  - IPv6 Mobile networks (cell phones, PDAs)
  - IPv6 peer-to-peer (Fixed and mobile wireless)
  - Ad hoc connections
- IP TV - Direct Video Broadcast (DVB)
- IP radio (Sirrus, XM)
- RF ID (DoD, Wal\*Mart, Delta Airlines)
- Embedded Systems – how to secure?

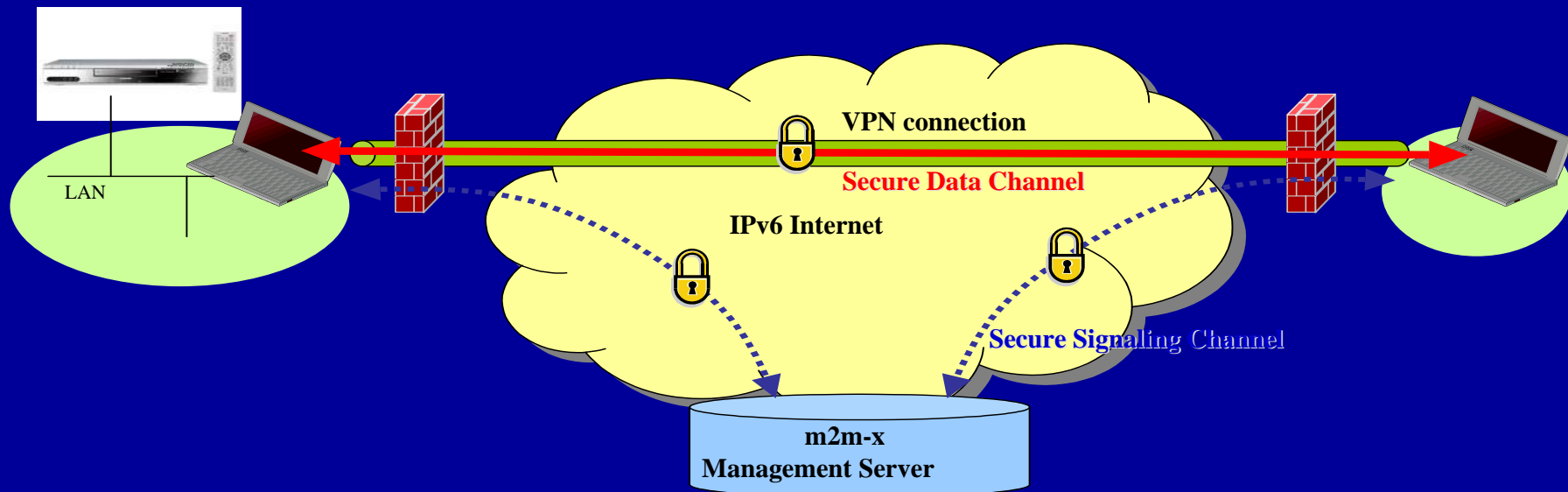


m2m-x





# NTT Communications m2m-x Technology



- m2m-x = machine to machine security (authentication and encryption) anytime, anywhere
- Designed to facilitate secure communications between appliances, computers, and any other device
- Based on IPsec and SIP
- Authentication, connection management, and configuration is controlled by a central m2m-x management server
- After necessary connection management by m2m-x server, data communications between devices is conducted peer-to-peer with IPsec encryption with no intervention by the m2m-x server



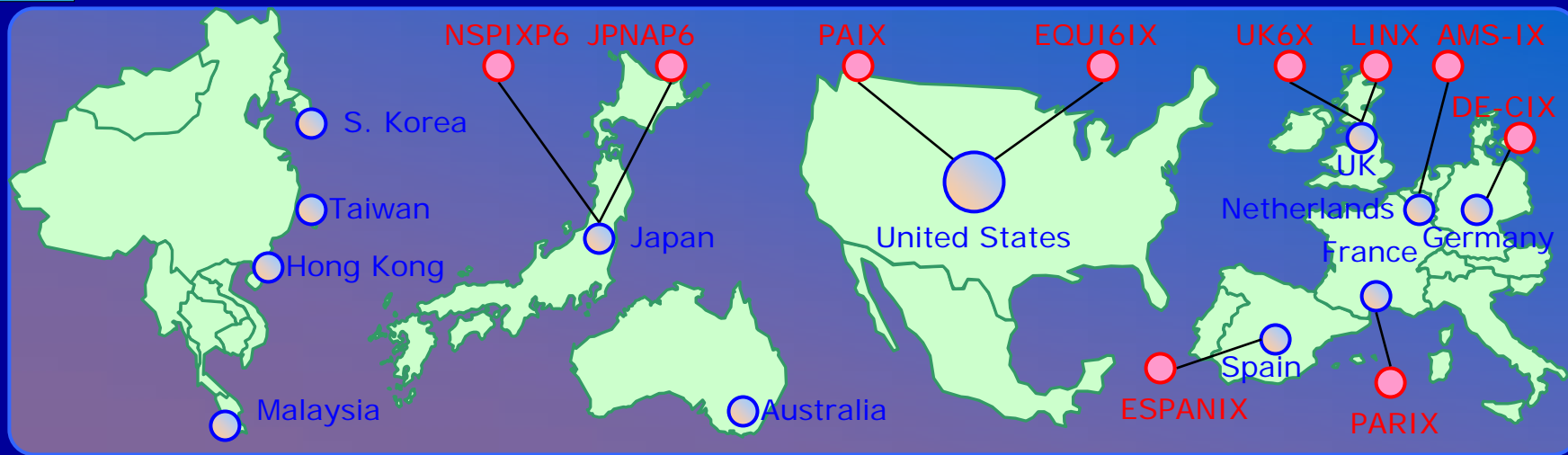
# m2m-x - IPv6 Product Development Example

---

- - Cyber conferencing system - secured end to end
- 8 sites deployed
  - Denver, CO
  - Hong Kong, China
  - London, UK
  - Malaysia
  - Redmond, WA
  - Tokyo, Japan
  - Taiwan
  - Washington, DC
- m2m-x technology promotion



# NTT/VERIO Global IPv6 Backbone and Services



## NTT/VERIO IPv6 Backbone

- : IPv6 Exchange Point
- : NTT/VERIO Global IPv6 Service Availability

## Our Strength

- Global IPv6 networks covering Asia, Australia, the United States and Europe
- Providing commercial IPv6 transit services:
  - Since April 2001 in Japan
  - Since February 2003 in Europe
  - Since June 2003 in the United States and many of the Asia Pacific countries
- More than 3 years of operational experience
- 24x7 monitoring and operations by NTT/VERIO dual NOC in Japan and the United States
- Main IPv6-IX Connection:
  - Japan: NSPIXP6, JPNAP6 (Tokyo)
  - United States: PAIX (West Coast), EQUI6IX (West Coast, East coast)
  - Europe: LINX, UK6X (London), AMS-IX (Amsterdam), PARIX (Paris), DE-CIX (Frankfurt), ESPANIX (Madrid)
- Optimal IPv6 routes



# References

---

- BGP
  - <http://www.nanog.org/mtg-0306/pdf/franz.pdf>
- IPv6 Style
  - <http://www.ipv6style.jp/en/index.shtml>
- IPv4/IPv6 Threat Comparison and Threat Evaluation
  - [http://www.cisco.com/security\\_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf)
- Books
  - Stealing the Network: How to Own a Continent, Ryan Russell, et al
- Best Common Practices (BCPs)
  - <http://www.rfc-editor.org/bcp-index.html>