IPv6-Enabled (Cyber-) Security
The Shifting Security Paradigm

Joe Klein CISSP CISM CISA NSA-IAM/IEM IA-CMM 6Sigma …

Day Job – SME Security Architecture, SRA International

My Research - Scientific Hooligan, Longboat LLC

Cyber Security SME, North American IPv6 Task Force
Cyber Security SME, IPv6 Forum
Cyber Security SME, IPv6 Cyber Security Task Force
Contributor to: NIST SP-119, NIST SP-123, DoD MO2, MO3.x,
“Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government 2012”

JSKlein@gmail.com  Voice: +1-703-594-1419  #JoeKlein

Blog: http://scientifichooligan.me/

© 2013, Joe Klein, Longboat LLC  Podcast Guest: Healthy Paranoia
Growth of Endpoints

Internet Growth History

- Host Computers
  - 10,000,000
  - 1,000,000
  - 100,000
  - 10,000
  - 1,000
  - 100
  - 10

- Year
  - 1970
  - 1975
  - 1980
  - 1985
  - 1990
  - 1995

- Doubling Time, months
  - 30
  - 16
  - 8
  - 12

- ARPAnet, NSF, .edu, All
Growth via Technology Cycles

New Major Technology Cycles = Often Support 10x More Users & Devices, Driven by Lower Price + Improved Functionality

Computing Growth Drivers Over Time, 1960 – 2020E

KPCB

© 2013, Joe Klein, Longboat LLC
Growth of Non-Traditional IT

Internet of Things
More Machines Than Humans

<table>
<thead>
<tr>
<th>World Population</th>
<th>6.3 Billion</th>
<th>6.8 Billion</th>
<th>7.2 Billion</th>
<th>7.6 Billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Devices</td>
<td>500 Million</td>
<td>12.5 Billion</td>
<td>25 Billion</td>
<td>50 Billion</td>
</tr>
</tbody>
</table>

Source: Cisco IBSG, April 2011

© 2013, Joe Klein, Longboat LLC
Two Paths To Save the Internet

IPv4

~2018 - 50%
~2013 - 2%
~2012 - 0.75%
~2011 - 0.6%
~1997-2006
~1999
~1998
~1995
~1993
~1992

IPv6

Shipping
Global Test
Test Devices & Networks
First RIR
Stable Spec
First IPv6 Spec
IPNG - Protocol Design Begins

NAT BYPASS
CIDER, DHCP
RFC 1918, NAT

© 2013, Joe Klein, Longboat LLC
Impact of Technology Growth

Past the Tipping Point:
Regional Internet Registries (RIRs) manage the allocation and registration of Internet number resources for 5 regions in the world and some of them are already out of IPv4 addresses, with the rest soon to follow.

- Already out of IPv4 addresses
- Projected to run out soon

- **AMERICAS (ARIN)**
  - APRIL 2014
- **LATIN AMERICAN (LACNIC)**
  - AUG 2014
- **EUROPE AND MIDDLE EAST (RIPE NCC)**
  - SEP 2012
- **AFRICA (AFRINIC)**
  - AUG 2020
- **ASIA PACIFIC (APNIC)**
  - APRIL 2011

© 2013, Joe Klein, Longboat LLC
Current IPv4 Security Strategy
Security Vulnerabilities Exist Everywhere!

- Envisioning, Design, Prototype, Architecture Phase
  - RFC, IEEE, WC3, ITU, vendors, etc.
- Development Phase (Coding)
  - Libraries, coding style, code examples, assumptions & ‘business’ decisions
- Architecting, Implementation and Deployment
  - Staff, Procedures, Governance, Processes, etc.
- Management
  - Patching, Configuration Management, Processes, etc.
- End of Life, Refresh & Replacement
- Leaked Information
- Buzz Word Technology
- Security Parity with existing Protocol

Complexity is Good For Attackers, Bad For Defenders!

© 2013, Joe Klein, Longboat LLC
Current Security Model is Broken
Humans Are Too Slow...
NAT* is Evil!

* Network Address Translation
What is the Impact of IPv4 Security Model & ‘Man in the Loop’?

“The best companies aren’t the ones who stop attacks, – that’s important – it’s the companies that can spot intrusions quickly and respond to them in ways that limit the damage.”

“This idea that you can stop intrusions… just isn’t going to hold up against certain kinds of threats,”

- Richard Bejtlich – TaoSecurity Blog
Result: Current State of Internet Security
What are the Nation-State approaches to cyber attack mitigation?

<table>
<thead>
<tr>
<th>Type</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>IPv6 (IPSec + Good Crypto)</td>
</tr>
<tr>
<td>Military</td>
<td>Sun Tzu’s Art of War</td>
</tr>
<tr>
<td>Military / Political</td>
<td>Cyber attack deterrence</td>
</tr>
<tr>
<td>Political / Technical</td>
<td>Cyber arms control</td>
</tr>
</tbody>
</table>

**Used:** Decision Making Trial and Evaluation Laboratory (DEMATEL)

**Developed:** Battelle Memorial Institute

**Provides:** Solve scientific, political and economic problems that contain a complex array of important factors, which may involve many stakeholders.
Two Models of Survivability

Fortress (traditional)
- Impenetrable (hopefully)
- Monolithic
- Single Layer
- Rigid
- Immobile

Organism
- Many partial barriers
- Heterogeneous
- Defense in depth & Self Healing
- Adapts, Learns, Evolves
- Mobile

© 2013, Joe Klein, Longboat LLC
Survivability Model | Resilience/Agility

Cost of Mitigating an Attack

Low

High
IPv6 Resiliency Engineering
Recon Detection
IPv6 Resiliency Engineering
Deception
IPv6 Resiliency Engineering Maneuvering
IPv6 Resiliency Engineering
Topology Hiding
IPv6 Resiliency Engineering
Multiple Crypto Checkpoints
IPv6 Resiliency Engineering
Active Defense
Problem Space | IPv6 Protocol

- **Mindset**
  - “IPv6 is only about the addresses”
  - “No need to update to IPv6”
  - “No business value”
  - “I can implement IPv6 because it is just like IPv4”
  - “Engineering IPv6 for scarcity vs. abundant addresses”

- **Training – Not just Network Engineers!**
  - Security Engineering and Architects
  - Auditors, Assessors and Penetration Testers
  - Defenders
  - Programmers

- **Product Vendors**
  - Use of Old RFC’s, Partial Implementation
  - Problems exists at layer 2 – 7, Management

- **Procurement**
  - Organizations don’t require default IPv6 to a standard (FAR)
  - Vendors are not pushed to support security needs
Security Problem Space | IPv6 Protocol

- **Address Allocation** - Static Addresses | Autoconfiguration | DHCPv6
- **Host/Domain Lookup** - Host Tables | Unicast DNS[Sec] | Multicast [ UPNP | Auto Discovery]
- **Device Inventory** - Neighbor Cache | First Hop Scan | Enterprise Scan | Address Allocation & Host/Domain Lookup/Address Management
- **First Hop** - Discovery | [ Host | Router ] Spoofing | DOS | [ Address | CPU ] Exhaustion | Bypass Layer 2 Controls | Host Control bypass | NC Poison | SEND/CGA
- **Network Topology** - Discoverable | Non-Discoverable
- **Tunnels** - On First Hop | Between two endpoints [ Inside | ISP
- **Extension Headers** - RH0 | Fragmentation | Non-existent
- **Number of Protocols** - IPv4 Only | IPv4/6 with no controls | IPv4/6 + IPv6/4 Tunnelled | Dual Stack | IPv6 | IPv4-v6 Translators
- **Routing Protocol** - Core | Internet Edge | OSPF3 | BGP+RPKI+BGPSec
- **Multicast** – MLDv1/2 | PIM [ASM | SSM | SM] | MBGP | MSEC
- **End to End Security** – IPSEC (Optional) | Perfect Forward Security (PFS) | DNSSec

**Security Understands the Risk – Who is Making the Decision?**

© 2013, Joe Klein, Longboat LLC
Problem Space | Tunnels (IPv4 & IPv6)

- Types of Tunnel (+16) – How do you discover them all?
  - Layer 3: Protocol 41
  - Layer 4: [TCP | UDP | ICMPv6]
  - Layer 7: [ssh | ssl | dns]
  - Defaults [ ports | End IP | Host Name ] - but not required
  - Can be Many Levels Deep [IPv4[UDP[IPv6[GRE[IPv4[UDP[DATA]]]]]]]

- Detection Tools
  - Port & Vulnerability Scanners – Very Poor
  - SNORT and others – Signature - Poor
  - Assure6 – Signature - Good
  - Bro – Signature + Behavior + Protocol Analysis - Best!

Tunnels are a work around – Who is making this decision?
Current Security Research

Defense Tool

- **Recon + Attack Detection**
  - IPv6 attack profile [Top 5 Techniques/Tools]
  - First Hop attack identification [Top Techniques/Tools]
  - Tunnel Identification [+16]

- **Topology Hiding | Detection | Maneuvering | Active Defense**
  - Real-time [ < 1000ms ]

IPv6 Standards | Internet of Things (IoT)

- Cognitive Radio - IEEE 802.22.2011 – MAC to IPv6 Layer
- Automobile – [C-C][C-I] - 1609.2/4 & IETF security service review

Security Engineering Standard

- NIST System Security Engineering standard
## Bonus Slide: Assumptions

<table>
<thead>
<tr>
<th>Features</th>
<th>IPv4 Expert</th>
<th>IPv6 Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses per Interface</td>
<td>1</td>
<td>Link-Local, ULA (n-1), Global (n-1), Privacy Address, MultiCast, Scoping</td>
</tr>
<tr>
<td>Outbound initiated traffic = Inbound</td>
<td>Yes</td>
<td>Depending on interface configuration</td>
</tr>
<tr>
<td>External Address</td>
<td>Public Address</td>
<td>Global Address (n-1) &amp; Privacy Address (n-1)</td>
</tr>
<tr>
<td>Internal Address</td>
<td>NAT, mapped to NAT/PAT Pool, RFC1918</td>
<td>Scoped Addresses (Link-Local, ULA, Global)</td>
</tr>
<tr>
<td>Attacker scans system and it does not responding</td>
<td>Perform additional Scans to see if crashed or blocked. Return later to see if rebooted.</td>
<td>Outbound - Privacy Address Change Inbound – ULA and Global can Change</td>
</tr>
<tr>
<td>Address Density</td>
<td>Very Dense, Fast and easy to find</td>
<td>Very Sparse, Hard to find unless you make it easy!</td>
</tr>
<tr>
<td>Discover Topology</td>
<td>Traceroute</td>
<td>Scoped Address Hides Topology</td>
</tr>
</tbody>
</table>
IPv6-Enabled (Cyber-) Security
The Shifting Security Paradigm

Joe Klein CISSP CISM CISA NSA-IAM/IEM IA-CMM 6Sigma …

Day Job – SME Security Architecture, SRA International
My Research - Scientific Hooligan, Longboat LLC

Cyber Security SME, North American IPv6 Task Force
Cyber Security SME, IPv6 Forum
Cyber Security SME, IPv6 Cyber Security Task Force
Contributor to: NIST SP-119, NIST SP-123, DoD MO2, MO3.x,
“Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government 2012”

JSKlein@gmail.com Voice: +1-703-594-1419 #JoeKlein
Blog: http://scientifichooligan.me/

© 2013, Joe Klein, Longboat LLC Podcast Guest: Healthy Paranoia

ISD2013 - 9-24-13
References:

PHOTOS & GRAPHICS

- Redcoats Battle of Quatre Bras 1815, https://imaginausten.wordpress.com/2012/02/03/red-coats/
- Xwing Box Set, http://2.bp.blogspot.com/-mhZoCkhBB8g/UFkk8fQyItI/AAAAAAAAYNo/z2q5CNGNaG4/s1600/Xwing+Box+Set+%252817%2529.JPG
References:

Papers, Videos, Books, etc.