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,

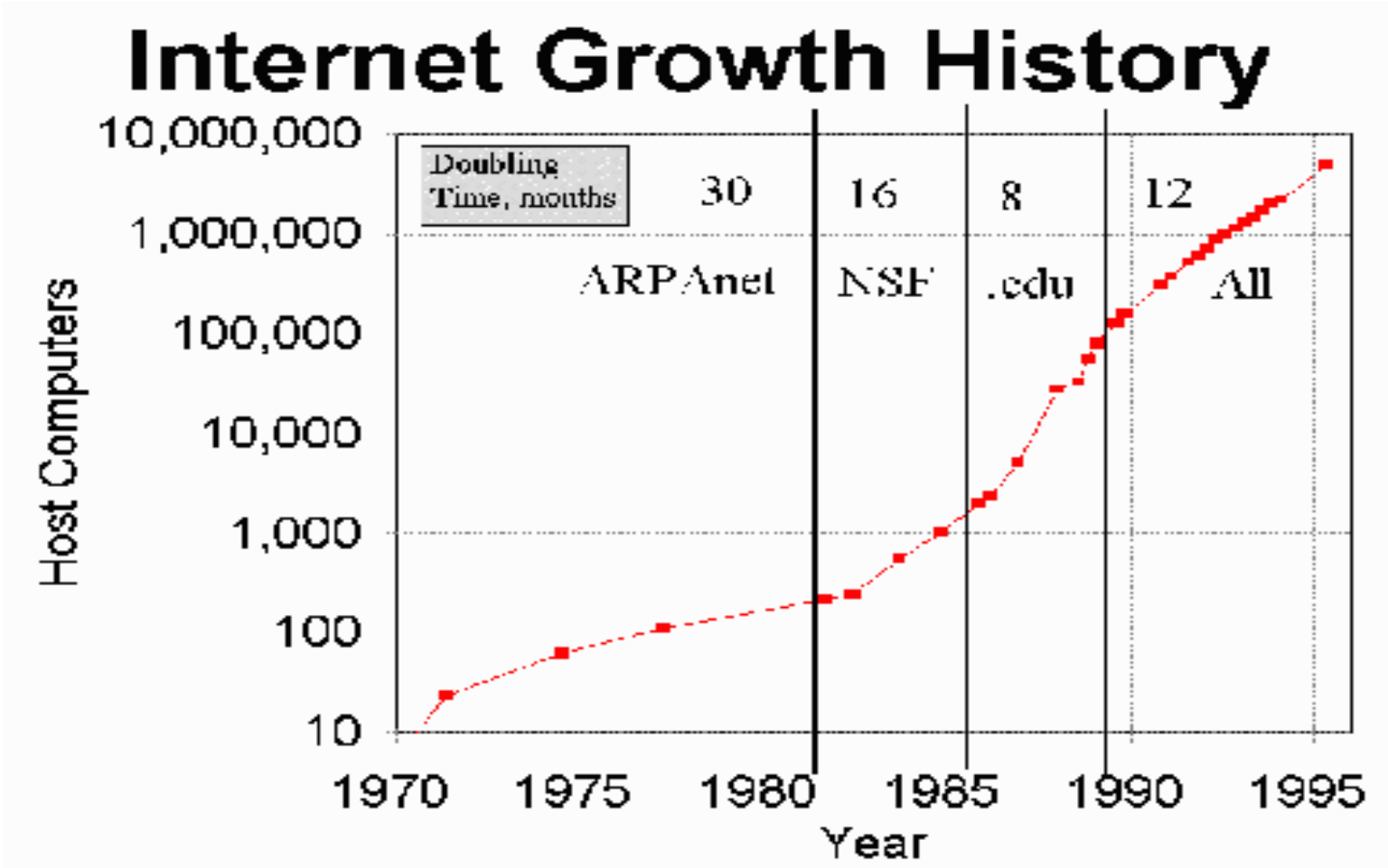
"Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government 2012"

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

Blog: http://scientifichooligan.me/

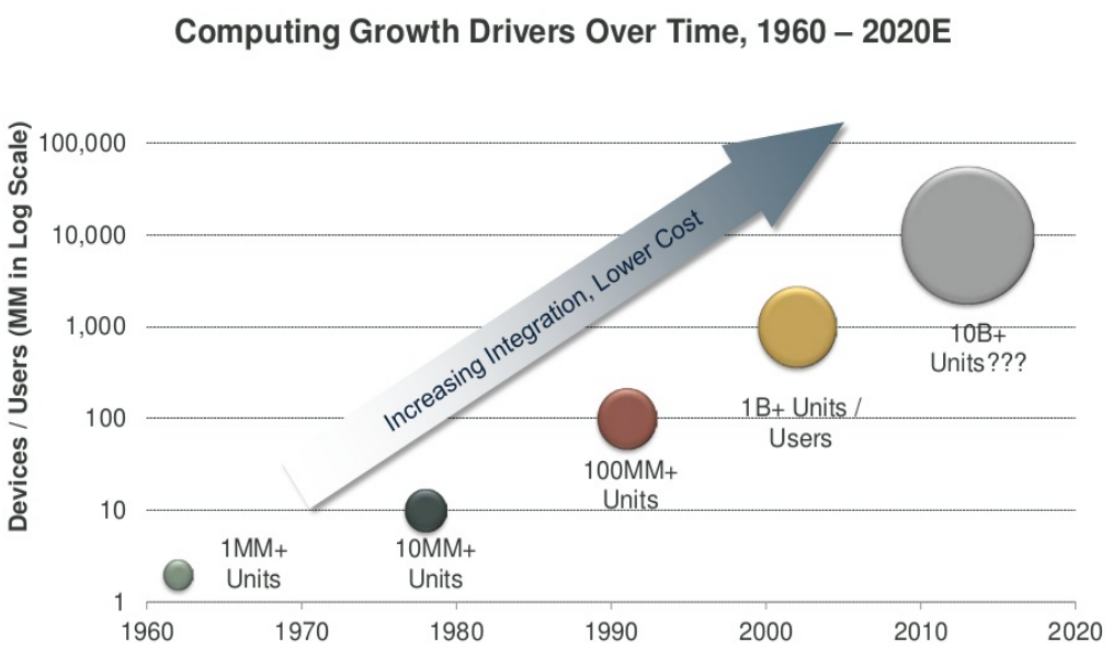
Podcast Guest: Healthy Paranoia

Growth of Endpoints



Growth via Technology Cycles

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

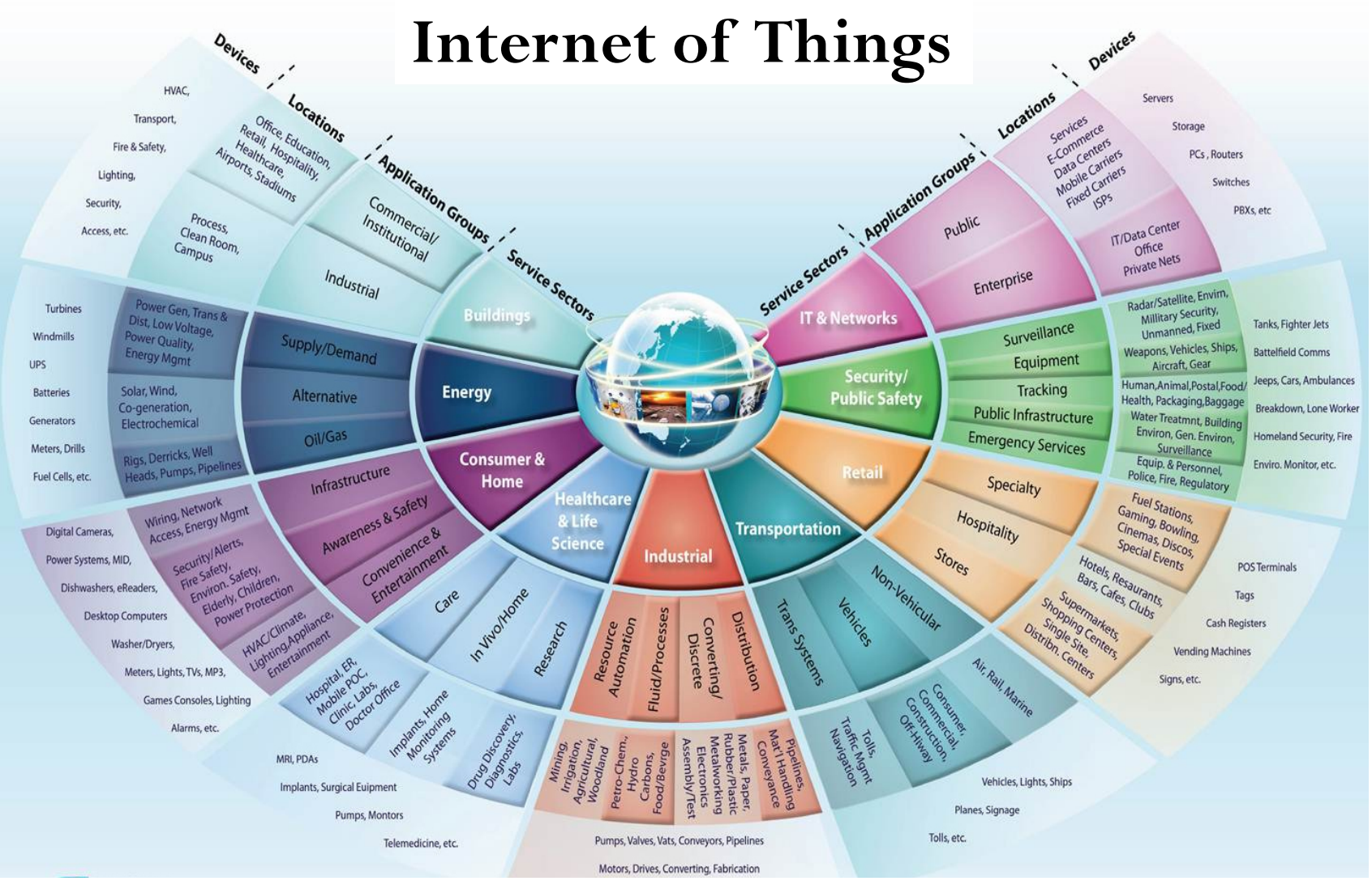


KPCB

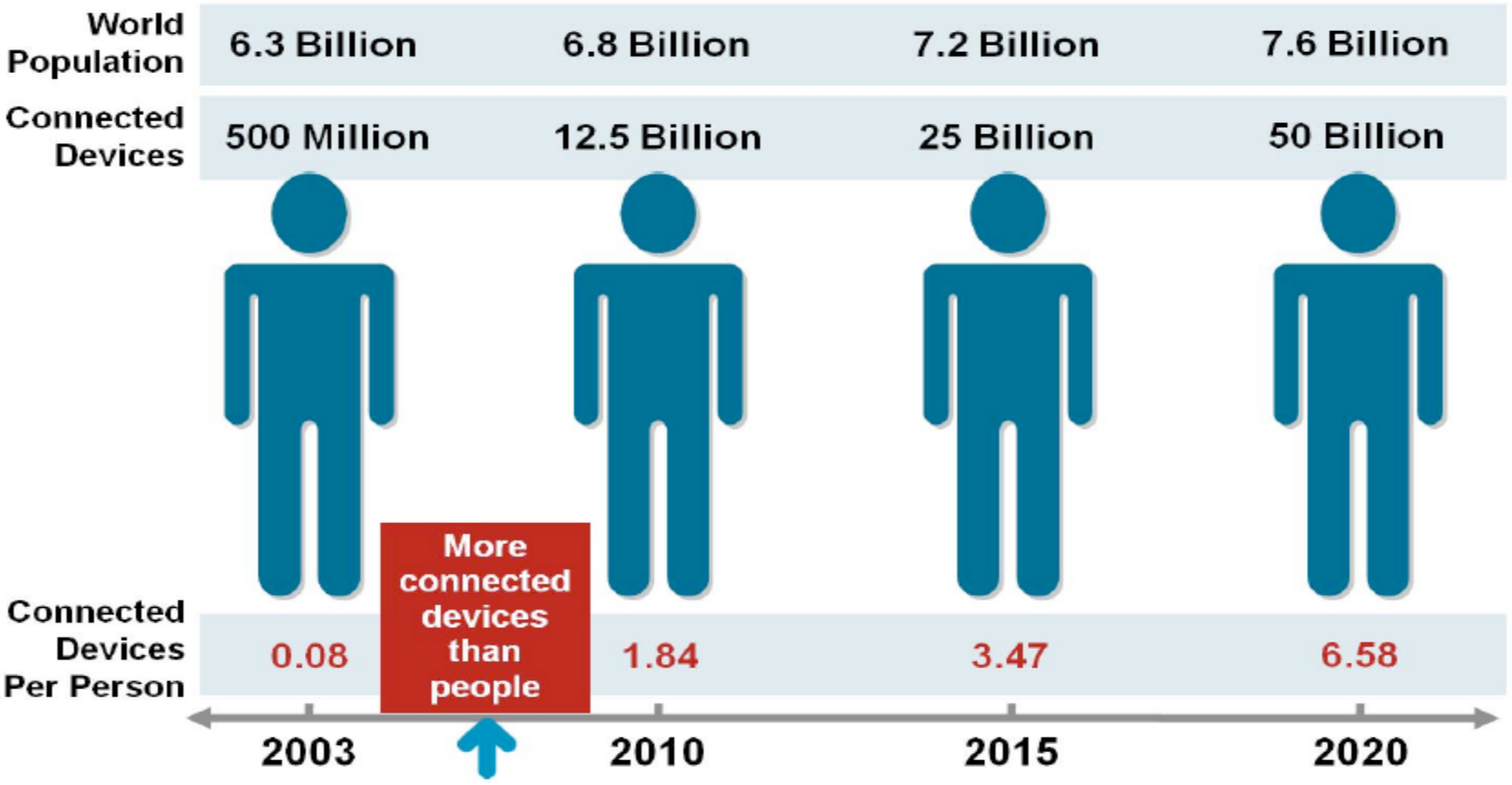
Note: PC installed base reached 100MM in 1993, cellphone / Internet users reached 1B in 2002 / 2005 respectively; Source: ITU, Morgan Stanley Research.

50

Growth of Non-Traditional IT



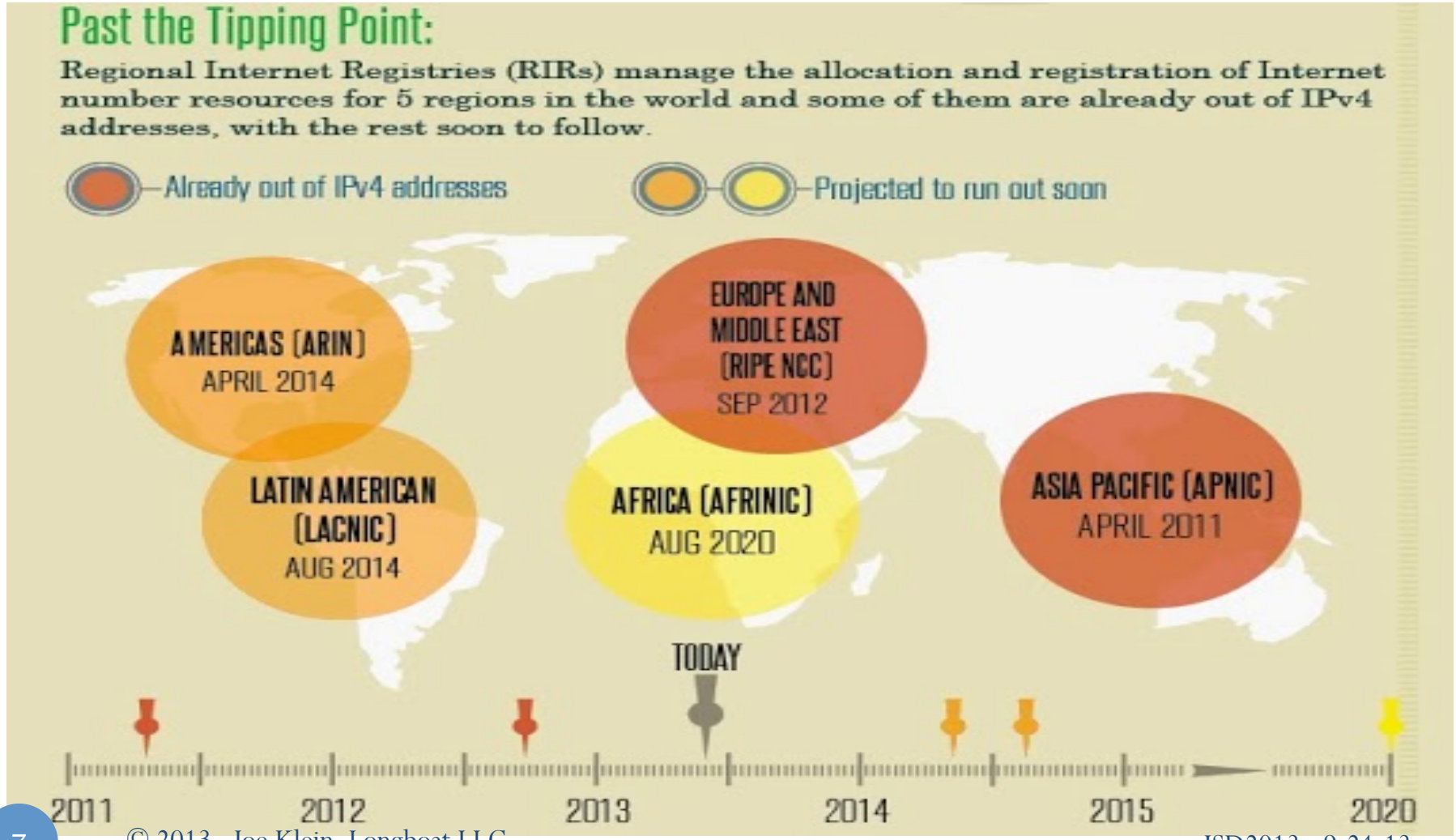
More Machines Than Humans



Source: Cisco IBSG, April 2011

Two Paths To Save the Internet

Impact of Technology Growth



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!

Current Security Model is Broken

Source: http://www.photographersdirect.com/buyers/stockphoto.asp?imageid=2249700

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."

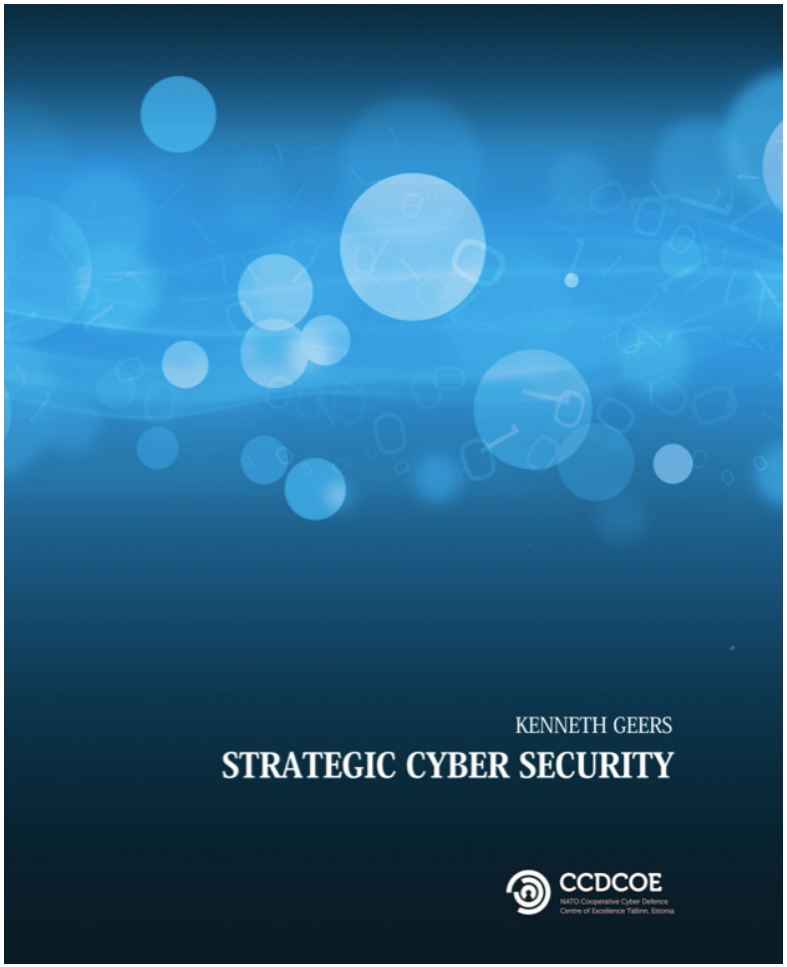
"This idea that you can stop intrusions… just

isn't going to hold up against certain kinds of threats,"

- Richard Bejtlich – TaoSecurity Blog

Result: Current State of Internet Security

Strategic Cyber Security
by Dr. Kenneth Geers



What are the Nation-State approaches to cyber attack mitigation?

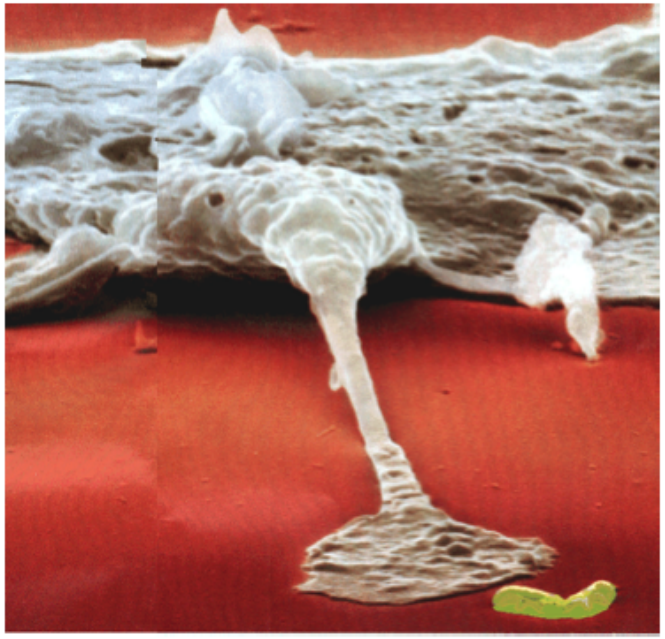
Technical	IPv6 (IPSec + Good Crypto)
Military	Sun Tzu's Art of War
Military/ Political	Cyber attack deterrence
Political/ Technical	Cyber arms control

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

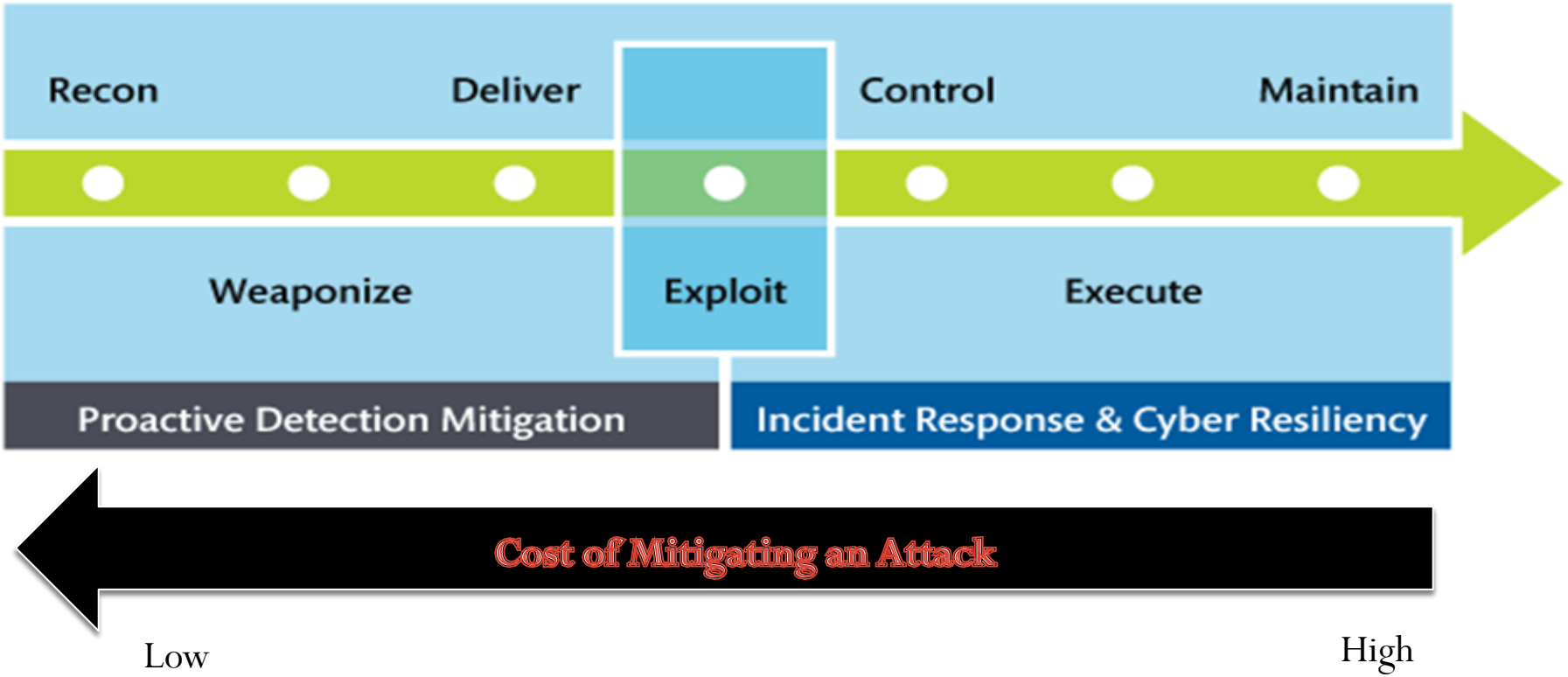


Organism

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

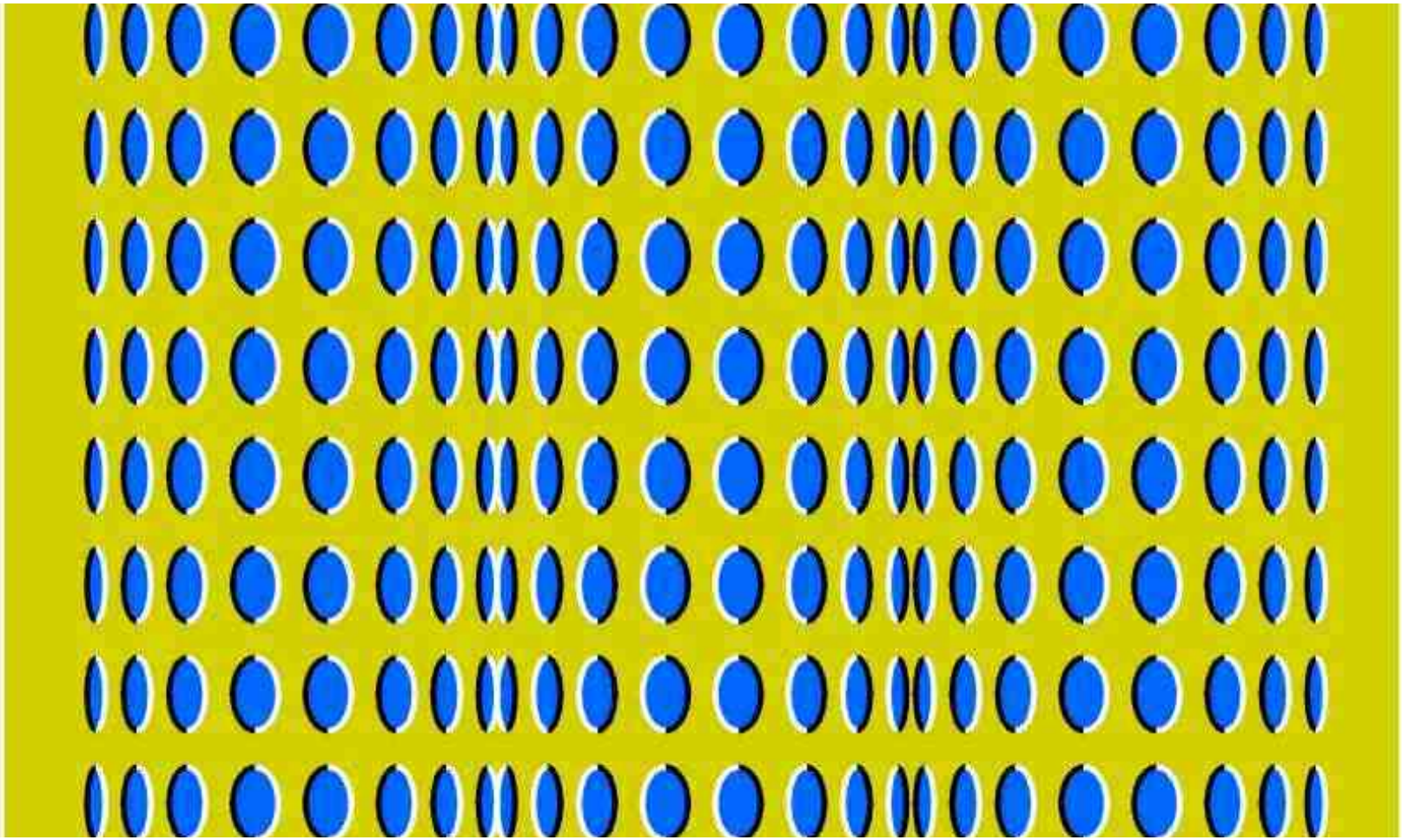
"**What If We Got A "Do-Over?" an Overview of CRASH and MRC**", Howard Shrobe Program Manager, DARPA I2O, 2012

Survivability Model | Resilience/Agility

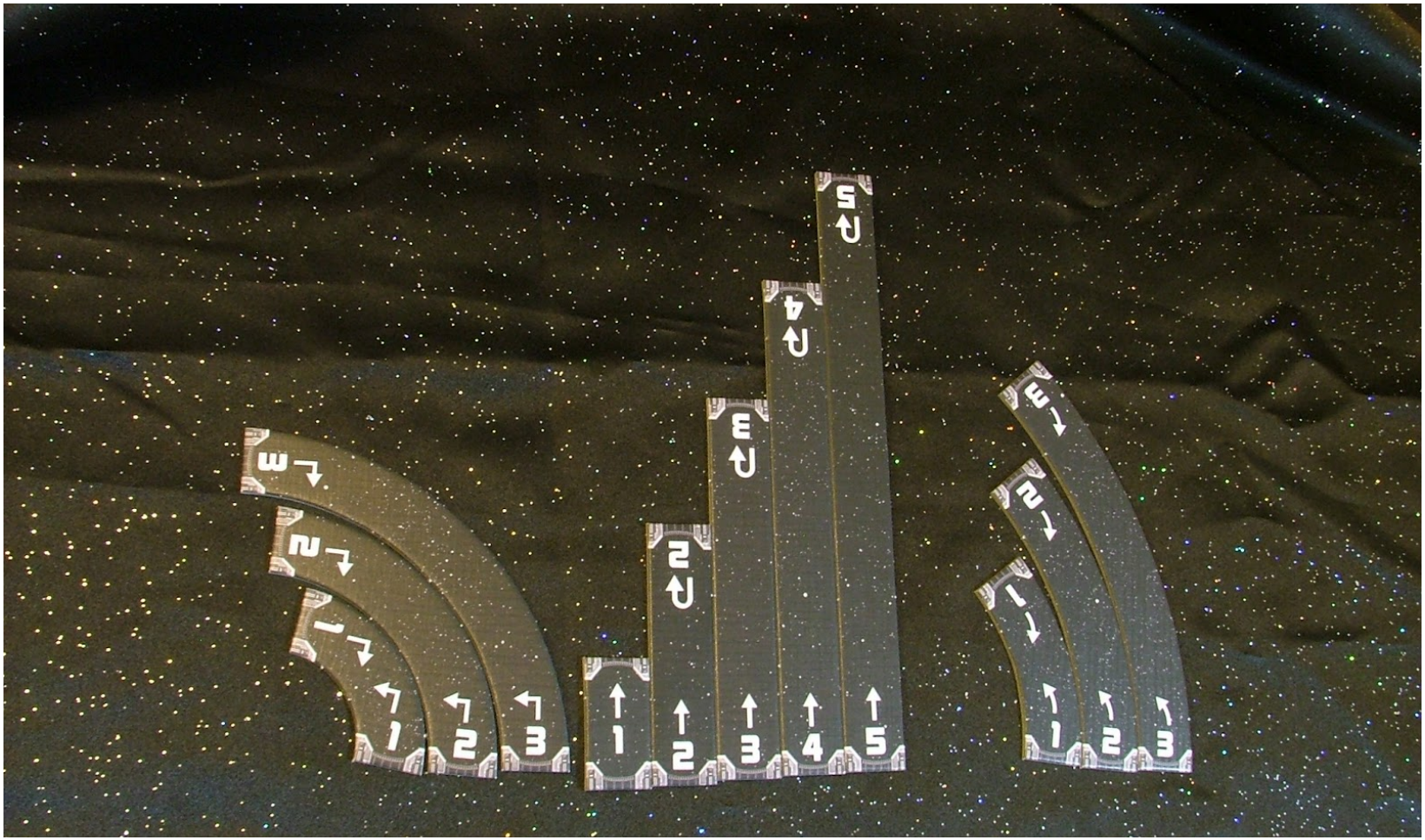


IPv6 Resiliency Engineering
Recon Detection

IPv6 Resiliency Engineering Deception

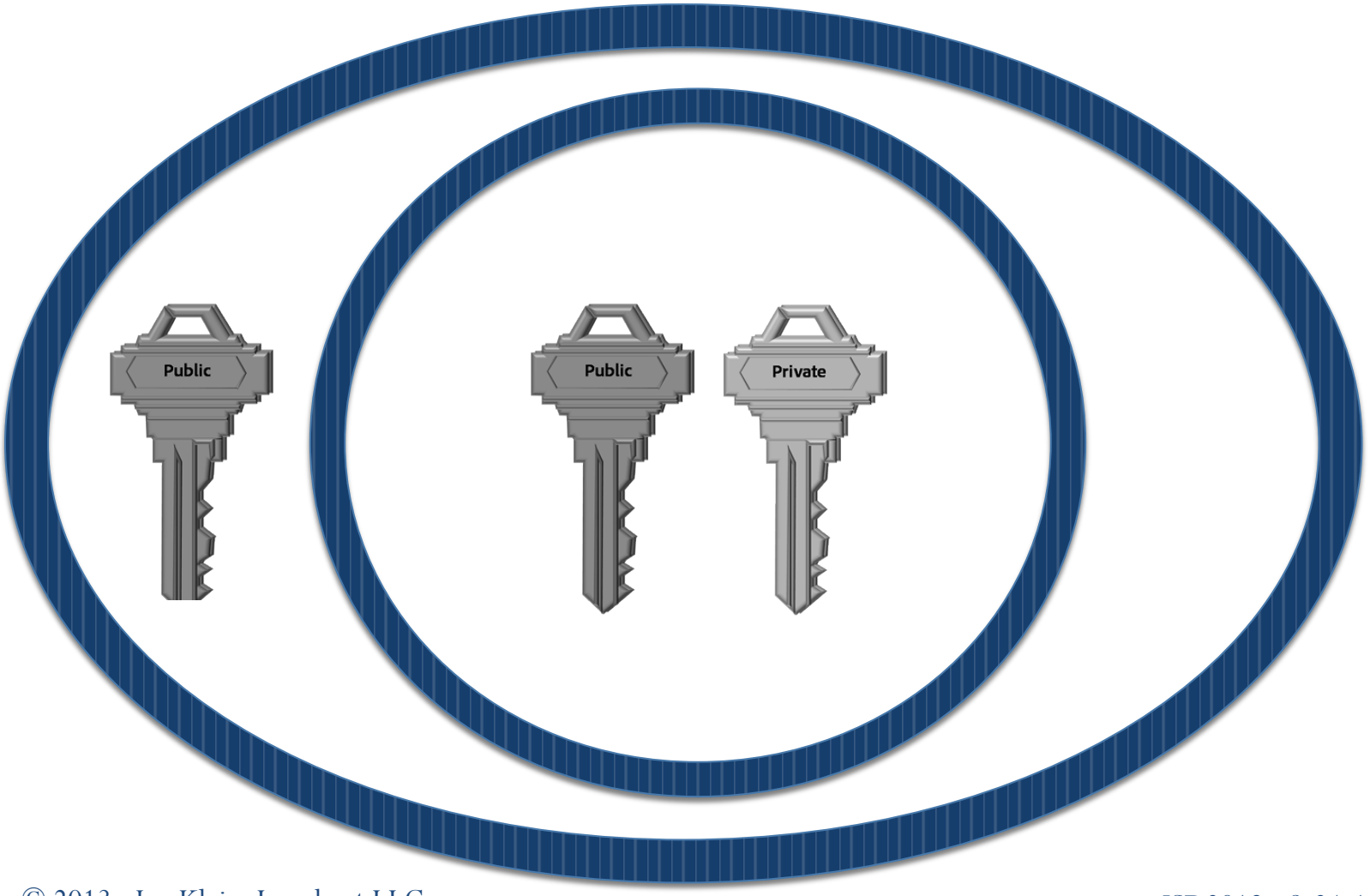


IPv6 Resiliency Engineering Maneuvering



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 Tunneled | 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?

Problem Space | Tunnels (IPv4 & IPv6)

- **Types of Tunnel (+16) – How do you discover them all?**
  - [IPv4|IPv6] over [IPv4|IPv6] over …
  - 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

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

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/

Podcast Guest: Healthy Paranoia

References:

PHOTOS & GRAPHICS

- Talk for the Canadian Society of Civil Engineers: The Internet, Roy Brander, P.Eng. 1995, http://www.cuug.ab.ca/~branderr/csce/growth.gif
- KPCB Internet Trends 2013, Pg 50, http://www.slideshare.net/kleinerperkins/kpcb-internet-trends-2013
- BEECHAM RESEARCH, http://www.beechamresearch.com/article.aspx?id=4
- Cisco IBSG, April 2011, https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- Two Paths, http://www.newcumberlandhomes.com/careers/
- IPv6 Implementation Series, Wolfgang Kandek, Sep 5, 2012, https://community.qualys.com/blogs/laws-of-vulnerabilities/2012/09/05/ipv6-implementation-series
- Redcoats Battle of Quatre Bras 1815, https://imaginausten.wordpress.com/2012/02/03/red-coats/
- Castle, http://www.photographersdirect.com/buyers/stockphoto.asp?imageid=2249700
- Man vs. plane: Who will win the race?, http://www.news.com.au/travel/news/man-vs-plane-who-will-win-the-race/story-e6frfq80-1226689411886
- Whisper Down the Lane, Ginny Huo, 2011, http://soho20gallery.com/ginny-huo/
- Trailer Park Taj Mahal in Zeba, Mich., http://i41.photobucket.com/albums/e267/xcstaylor/trailer-park-taj-mahal.jpg
- Positive Affirmations and Incantations for Abundance, http://www.empowernetwork.com/alaska303/files/2013/06/abundance.jpg
- Moving Wave, A.Kitaoka, 2004, http://www.grand-illusions.com/images/articles/opticalillusions/oblong_wave/mainimage.gif
- Xwing Box Set, http://2.bp.blogspot.com/-mhZoCkhBB8g/UFkk8fQyltI/AAAAAAAAYNo/z2q5CNGNaG4/s1600/Xwing+Box+Set+%252817%2529.JPG
- Hiding_in_the_Haycocks_(1881)_by_William_Bliss_Baker, http://upload.wikimedia.org/wikipedia/commons/thumb/f/fd/Hiding_in_the_Haycocks_(1881)_by_William_Bliss_Baker.jpg/640px-Hiding_in_the_Haycocks_(1881)_by_William_Bliss_Baker.jpg
- Sword, http://e-cgb.com/wp-content/uploads/2013/05/sword.jpg
- Worm Hole, http://www.dlconsulting.com/wp-content/uploads/2012/12/wormhole-235x176.jpg

References:

Papers, Videos, Books, etc.

- "Talk for the Canadian Society of Civil Engineers: The Internet", Roy Brander, P.Eng, 1995, http://www.cuug.ab.ca/~branderr/csce/Ihistory.html
- KPCB Internet Trends 2013, Mary Meeker and Liang Wu, May 2013, http://www.slideshare.net/kleinerperkins/kpcb-internet-trends-2013
- ITU Internet Reports 2005: The Internet of Things, ITU, Nov 2005, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf
- The Internet of Things, How the Next Evolution of the Internet Is Changing Everything, Dave Evans, 2011, https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- The Jericho Forum and Challenge - Defcon, Paul Simmonds, et el, Aug 2006, https://www.youtube.com/watch?v=n29P824H-NY
- "Abrupt rise of new machine ecology beyond human response time",
- Neil Johnson, Guannan Zhao, Eric Hunsader, Hong Qi, Nicholas Johnson, Jing Meng & Brian Tivnan, Scientific Reports 3, Article number: 2627 doi:10.1038/srep02627, 11 September 2013, http://www.nature.com/srep/2013/130911/srep02627/full/srep02627.html
- "NATs are Evil - Well, Maybe just Bad for You", Randy Bush, et el, 26 Feburary, 2004, http://archive.apnic.net/meetings/17/docs/sigs/policy/addrpol-pres-randy-nats.pdf
- "Cyber Security Monitoring, Network Visibility – Interview: Richard Bejtlich", Defense News TV, 4 Sept 2012, http://blog.endace.com/2012/09/defense-news-tv-see-it-quick-deal-with-it-quick/
- "TaoSecurity Blog", Richard Bejtlich, http://taosecurity.blogspot.com/
- "The 2013 Data Breach Investigations Report", February, http://www.verizonenterprise.com/DBIR/2013/
- "Strategic Cyber Security", Kenneth Geers, NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, July 2011, https://www.ccdcoe.org/278.html
- "Suppose We Got a Do-Over: A Revolution for Secure Computing," Howard Shrobe (DARPA), Daniel Adams, IEEE Security & Privacy, vol. 10, no. 6, pp. 36-39, Nov.-Dec. 2012, doi:10.1109/MSP.2012.84, https://www.computer.org/csdl/mags/sp/2012/06/msp2012060036-abs.html
- "Intended Effects of Cyber Resiliency Techniques On Adversary Activities", Deborah Bodeau, Richard Graubart, The MITRE Corporation, June 2013, http://www.mitre.org/sites/default/files/pdf/13_1952.pdf