Observations from the lab, field & executive suite

Joe Klein, CISSP
Cybersecurity Fellow, IPv6 Forum
Consultant, Researcher & Trainer, Longboat, LLC

May 2018

About me: Joe Klein <many certs>

- **Spoken at:** DefCon, Black Hat, Torcon, SecTor, Security Days, Hackers on Planet Earth, SANS, IEEE, IoT,…
- **Roles:** Photographer, Electronics Engineer, Robotics Engineer, Entrepreneur, CEO, CTO, CSO, ISP, Security Architect, Developer, Pentester, Incident Handler, Professor, Policy Writer, Auditor, Assure, Firewall/Network Engineer, Integrator, Data Scientist, ML experimenter, Threat Intel, Computer Scientist, Hacker
- **Timeline:**
  - **70's:** Electronics, Radios, Gamer, Magic, Mainframe & Micro Computers, First 'Hack'
  - **80's:** BBS's, Game Hacker, Robots, Unix/c/FORTH/Basic/ COBOL/LISP/c++, DEC, SNA Networks, Internet connected, CyberForensics, Routers/Switches
  - **90's:** ISP, IPv6, Penetrations Testing, Network Defender, Web Developer, Teaching Internet/Web Dev, IETF
  - **2000's:** CSO, Linux, Audits, Assessments, Car/IOT/ Building Controls, SCADA Hacking, Teaching Cybersecurity + SANS, Patents, International Speaking
  - **2010's:** DARPA, Policies, Startup, Honeypots, Deception Networks, IPv6 Fellow, GoLang, IEEE, Sprint Triathlon

Recent Focus: Attacked Forced Time Scoped D&D

How to Prepare To Implement IPv6!
It’s Complex…

Observation 1 - Establish your IPv6 Standard for all Procurement!

- Why?
  - Establish a baseline of technology standards, during technology refresh
  - Ensure you are ready to move to IPv6, without big purchases!
- How?
  1. Can the Product vender support IPv6? *“Eating their own dog Food!”*
     - Internet Facing Services (Dual Stack) https://ip6.nl/#
     - IPv6 only clients behind 6xlt & NAT64/DNS64 https://nat64check.ipv6-lab.net/v6score

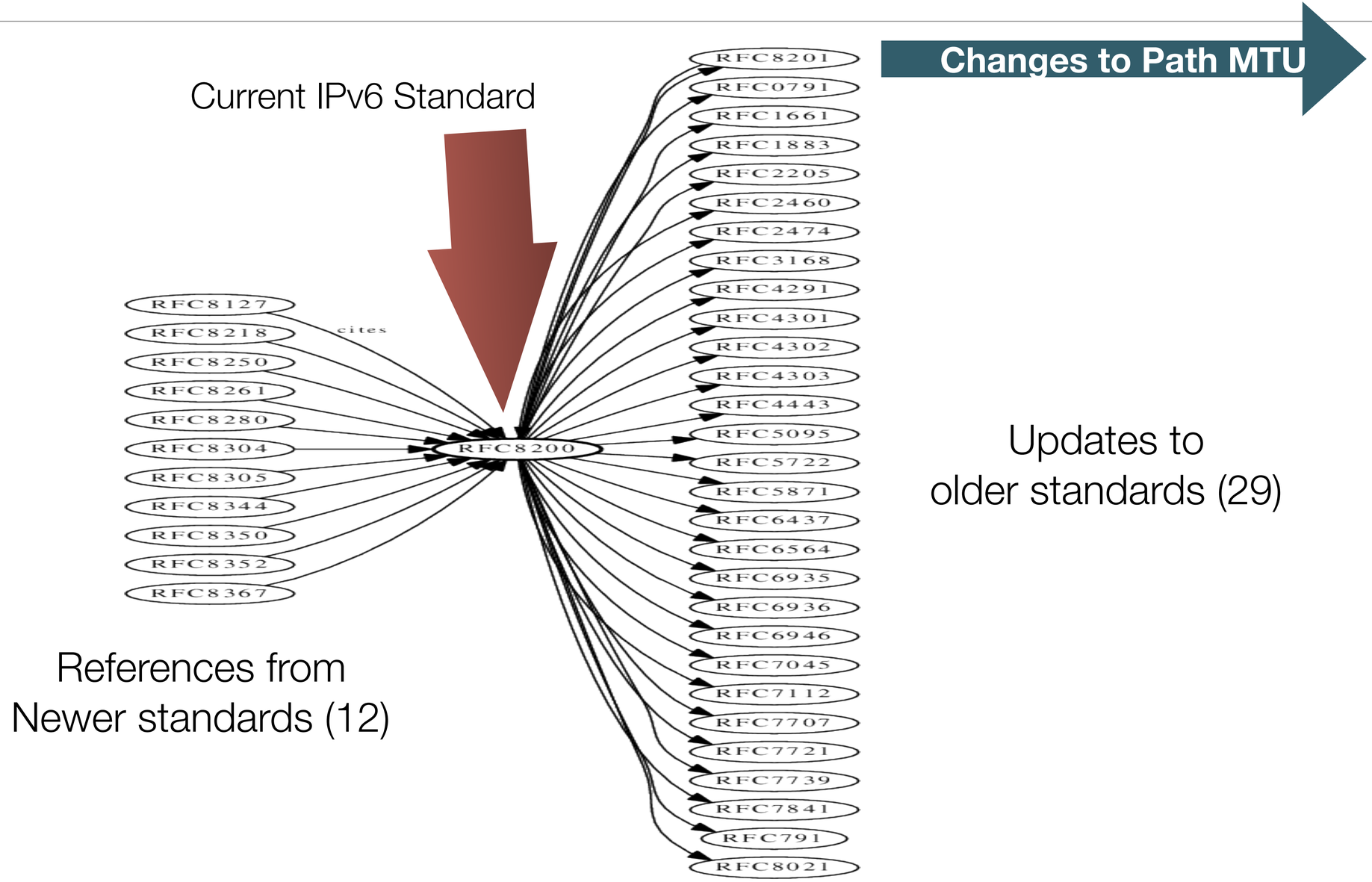
LONGBOAT cybersecurity

Observation 1 - Establish your IPv6 standard for all Procurement!

- How?
  1. The Supplier's Declaration of Conformity (SDOC)
     - Product suppliers declare product capabilities to buyers, as advertised
       - Buyer is responsible for providing specifications
       - Seller is responsible to fix, if it does not meet specifications
       - https://www-x.antd.nist.gov/usgv6/sdoc.html

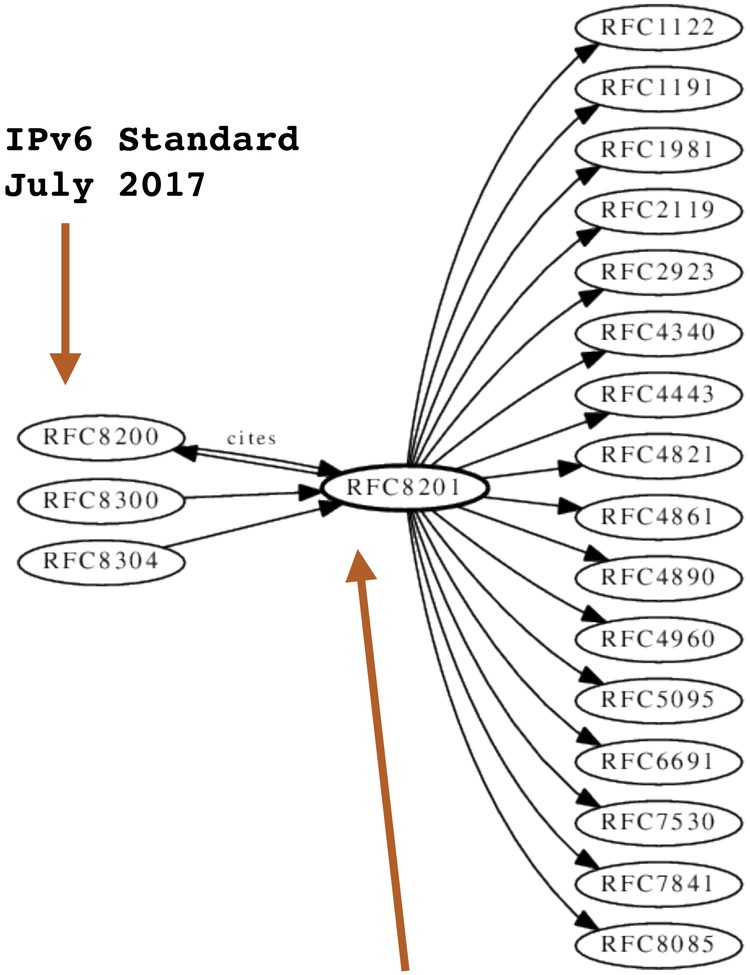
IPv6 Standards Touch Every Protocol!

What does IPv6 compliant mean to me?
IPv6 Standard 86 (RFC 8200) First Order Dependencies



IPv6 Standard 86 (RFC 8200)
First & Second Order Path MTU Dependencies

IPv6 Standard
July 2017



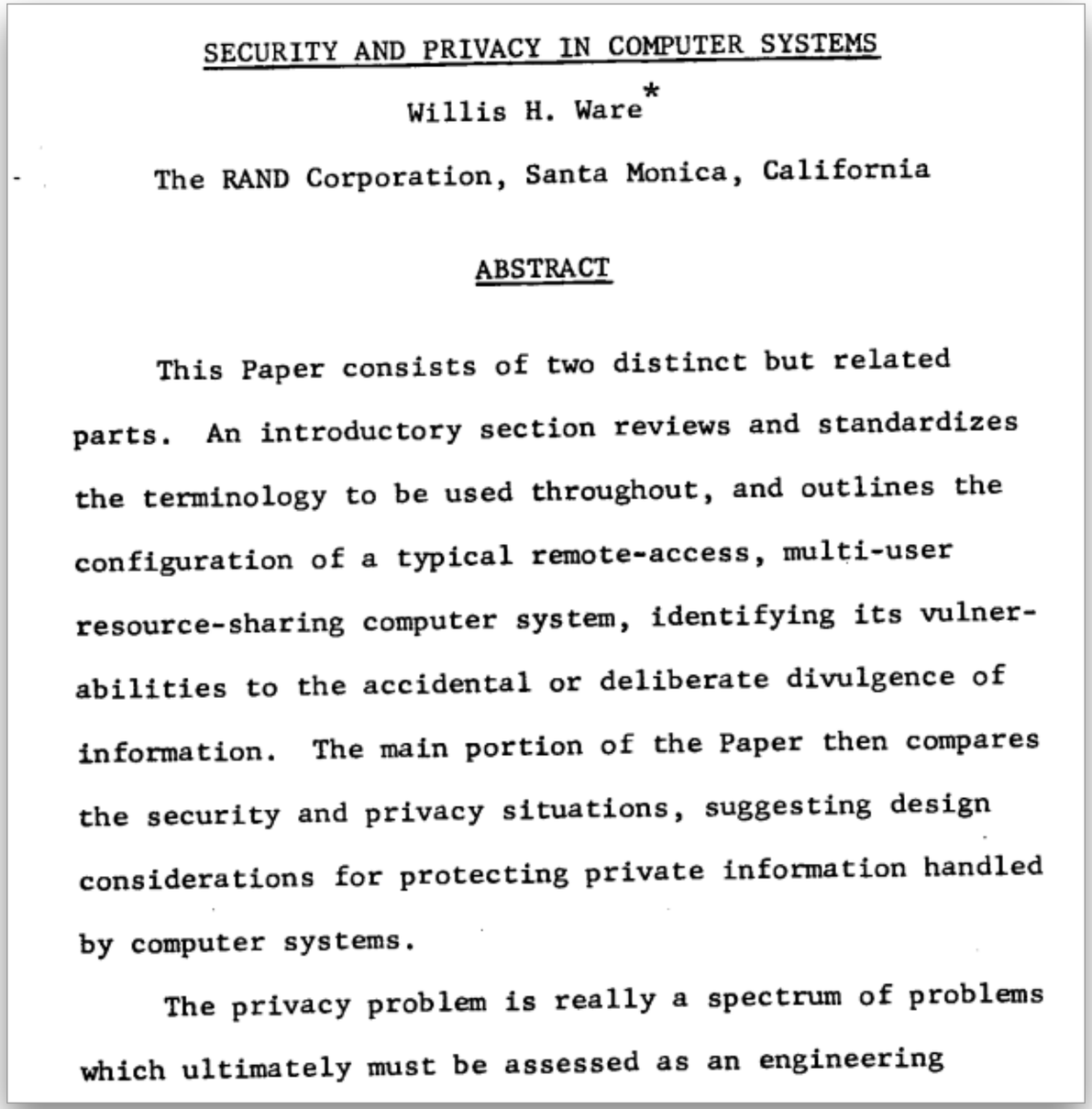
- October 1989 - Updated - Requirements for Internet Hosts -- Communication Layers
- November 1990 - Path MTU Discovery
- November 1996 - Path MTU Discovery for IP version 6 - **Obsoleted by 8201 July 2017**
- November 1997 - Key words for use in RFCs to Indicate Requirement Levels
- September 2000 - TCP Problems with Path MTU Discovery
- March 2006 - Datagram Congestion Control Protocol (DCCP)
- March 2006 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification - **Obsoletes RFC 2463**
- March 2007 - Packetization Layer Path MTU Discovery
- September 2007- Neighbor Discovery for IP version 6 (IPv6)- **Obsoletes 2461**
- May 2007- Neighbor Discovery for IP version 6 (IPv6)- **Obsoletes 2461**
- September 2007 - Stream Control Transmission Protocol- **Obsoletes 2960. 3309**
- December 2007 - Deprecation of Type 0 Routing Headers in IPv6 - **Obsoletes 2960**
- July 2012 - TCP Options and Maximum Segment Size (MSS)
- March 2015- Network File System (NFS) Version 4 Protocol- **Obsoletes 3530**
- May 2016- RFC Streams, Headers, and Boilerplates - **Obsoletes 5741**
- March 2017 - UDP Usage Guideline - **Obsoletes 5405**
- March 2017 - **Path MTU Discovery for IP version 6 - Obsoletes 1981**

Updates to
older standards (17))

IPv6 will not solve cybersecurity problems, right?

Fundamental of Cyber Security & Privacy

- “Remote-access, multi-user resource- sharing computer system”
- Attackers Exploit
  - Systems
    - Hardware | Software | Data
  - Networks
  - People
    - Users
    - Operators
    - Systems Programmers
    - Maintenance Man (Person)



SECURITY AND PRIVACY IN COMPUTER SYSTEMS

Willis H. Ware*

The RAND Corporation, Santa Monica, California

ABSTRACT

This Paper consists of two distinct but related parts. An introductory section reviews and standardizes the terminology to be used throughout, and outlines the configuration of a typical remote-access, multi-user resource-sharing computer system, identifying its vulnerabilities to the accidental or deliberate divulgence of information. The main portion of the Paper then compares the security and privacy situations, suggesting design considerations for protecting private information handled by computer systems.

The privacy problem is really a spectrum of problems which ultimately must be assessed as an engineering

April 1967

Reference: https://www.rand.org/pubs/authors/w/ware_willis_h.html

LONGBOAT cybersecurity

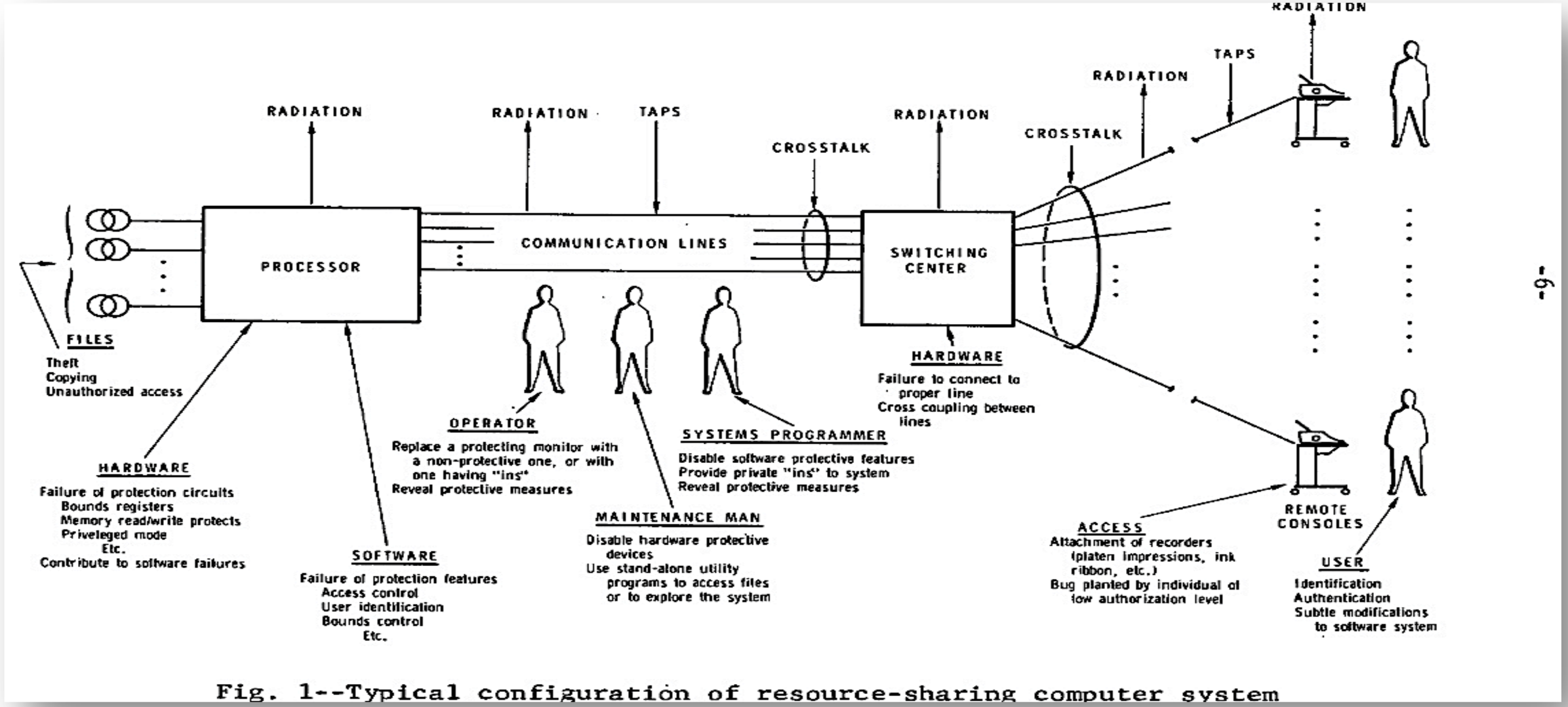


Fig. 1--Typical configuration of resource-sharing computer system

First Cybersecurity Threats Diagram

Willis H. Ware, RAND Corporation
April 1967
Reference: https://www.rand.org/pubs/authors/w/ware_willis_h.html

SO why is this happening?
Technical Supply-Chain Debt —
The real problem!

Technical Debt Powerpoint

What Does Winning Defender Look Like?

Defender's Dilemma

“The intruder only needs to exploit one of the victims in order to compromise the enterprise.”

Intruder's Dilemma

“The defender only needs to detect one of the indicators of the intruder’s presence in order
to initiate incident response within the enterprise.”

Reference: https://taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html

The Intruder Game

Tactic - Technical goal of the intruder
Technique - How intruder achieves the goal

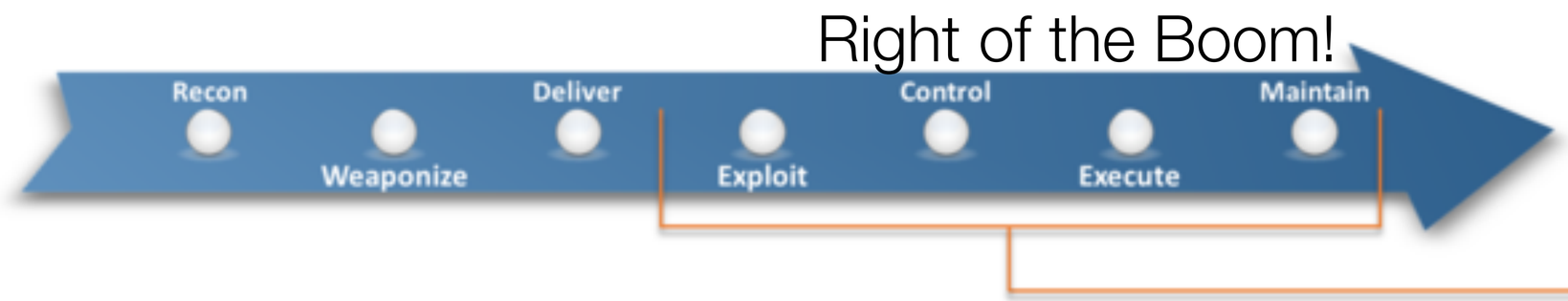
The Intruder Chooses Time and Goal, Not You!
The Defender Choose Confidence level of the Detection!

How do I Remove the Noise to Find the Attackers and increase confidence levels?

Reduce False Positives and Negatives!

Defenders Game: ATT&CK: Deconstructs the Lifecycle

Right of the Boom!



- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Freely available, curated knowledge based on observed adversary behavior

MITRE

Higher fidelity on right-of-exploit, post-access phases

Describes behavior and not adversary tools

Built for the “Public Good”

LONGBOAT cybersecurity

MITRE Pre-ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

Priority Definition
- **Planning, Direction**

Target Selection

Information Gathering
- **Technical, People, Organizational**

Weakness Identification
- **Technical, People, Organizational**

Adversary OpSec

Establish & Maintain Infrastructure

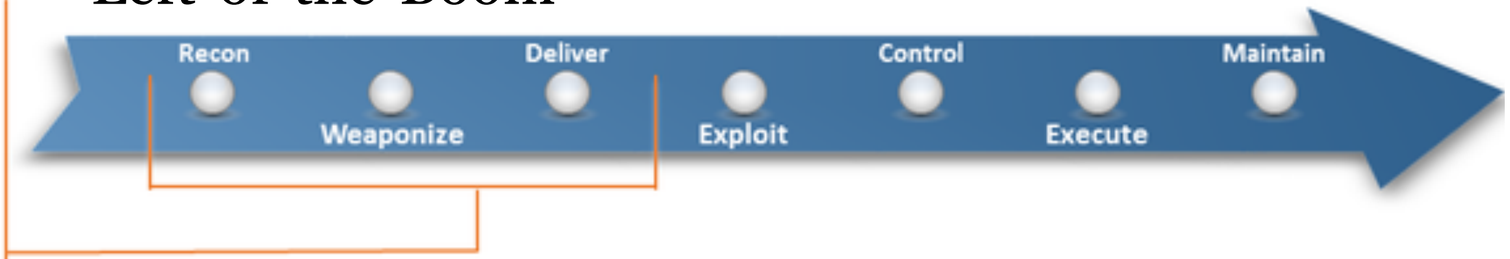
Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

Left-of-the-Boom



- Blacklist IP, Hash Domains are fungible, quickly replaceable
- Pre-compromise activities are largely executed outside the enterprise's field of view
  - Data Brokers (Free and for pay),
  - Websites (Partners, Yours, Government),
  - Search Engines and Bots
  - Social Network Bots

LONGBOAT cybersecurity

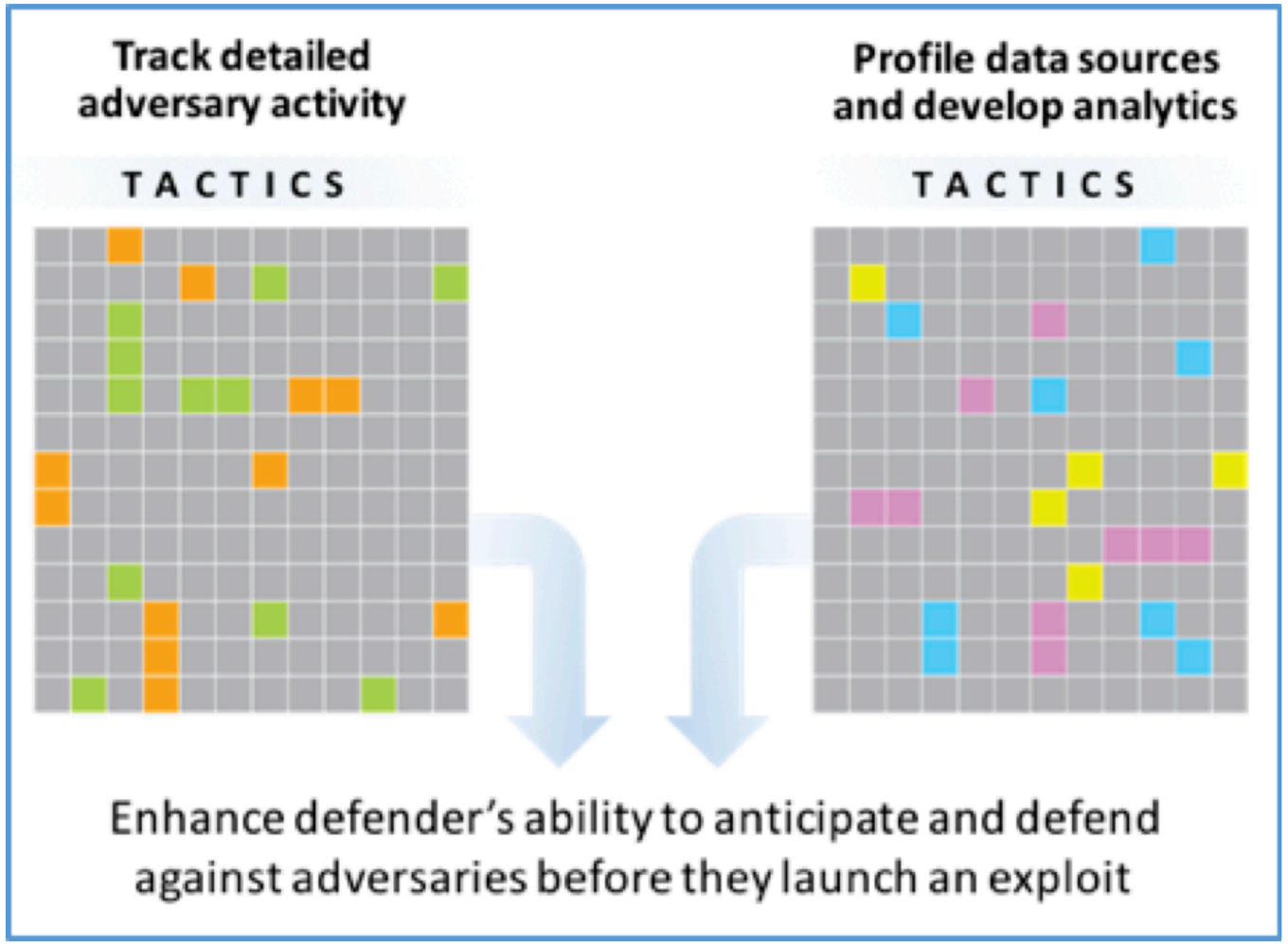
MITRE ATT&CK Enterprise Perimeter Defense

- Items in yellow are the only attributes detectable by tuned perimeter security
- Items in red, address requirements on hosts and first hop networks.

- Conclusion:
  - Perimeter security has minimal visibility into attackers insider your environment
  - IT slows the attacker, but this is not measurable
  - Tuning the security perimeter security to detect and alert on pre & post attack items are critical to catch attackers.

The Defenders Goal

- Strong trusted alerts
- Behavior tracking
- Automated response



More Detail?

Open Source - MITRE Resources

- Interactive Attack Navigator:
  - ATT&CK Enterprise: https://mitre.github.io/attack-navigator/enterprise/
  - ATT&CK Mobile: https://mitre.github.io/attack-navigator/mobile/
  - Source Code: https://github.com/mitre/attack-navigator
- Attacker Groups: https://attack.mitre.org/pre-attack/index.php/Groups
- Attacker Group Tactics: https://attack.mitre.org/pre-attack/index.php/Tactics
- Unfetter Project - Discover and analyze gaps in your security posture
  - https://nsacyber.github.io/unfetter/ https://github.com/unfetter-discover/unfetter
- Caldera - An automated adversary emulation system (validate alerts)
  - https://github.com/mitre/caldera

LONGBOAT cybersecurity

I understand there is no way of scanning the IPv6 Internet, is that true?

History of Scanning Internet-Facing IPv6 Devices

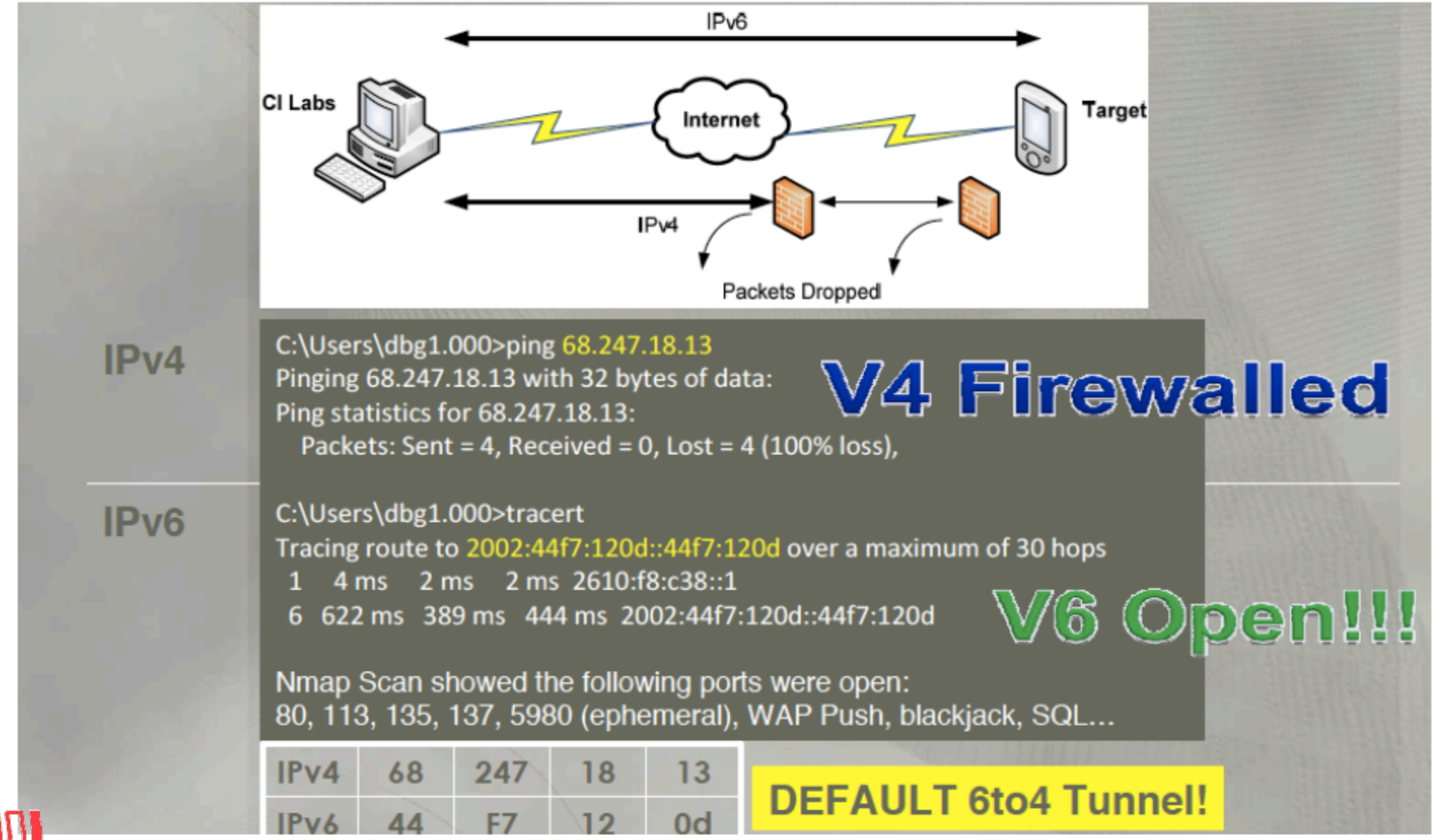
- 2^64 or 2^128 - Brute Force - Fails in IPv6!
- **May 2005**, Marc “van Huser” Heuse, Attacking the IPv6 Protocol Suite, THC-IPv6 toolkit (1)
- **May 2007**, Joe Klein, “Scanning and Microsoft Mobile compromise via 6to4 on SPRINT”, Responsible Disclosure Notice to Microsoft, Sprint and US CERT, HOPE 2008 (2)
- **March 2008**, IETF, RFC 5157, “IPv6 Implications for Network Scanning” (3)
- **May 2012**, NMAP for IPv6, version 6 (4)
- **March 2016**, IETF, RFC 7707, “Network Reconnaissance in IPv6 Networks” (5)
- **December 2018**, Joe Klein, “Outbound Initiated Requests for Passive Scanning of IPv6” (6)
- **December 2018**, Joe Klein, “Passive IPv6 Scanning using Certificate Transparency process” (7)

So we are safe? Attackers have not used IPv6 in the past?

Attacks on IPv6

Year	Issue
2001	Review of logs, after Honeynet Project announcement
2002	Honeynet Project : Lance Spitzner: Solaris Snort : Martin Roesch : Added then removed IPv6
2003	Worm : W32.HLLW.Raleka : Download files from a predefined location and connect to an IRC server - MALWARE
2005	Trojan : Troj/LegMir-AT : Connect to an IRC server CERT : Covert Channels using IPv6 Teredo Mike Lynn : Blackhat : IOS' handling of IPv6 packets
2006	CAMSECWest : THC IPv6 Hacking Tools RP Murphy : DefCon : IPv6 Covert Channels
2007	Rootkit : W32/Agent.EZM!tr.dldr : TCP HTTP SMTP James Hoagland : Blackhat : Teredo/IPv6-related flaw in Vista
2008	HOPE : IPv6 Mobile Phone Vulnerability
2011	IPv6 THC & SCAPY Updated, Use of Teredo as APT, Metasploit IPv6

Microsoft Phones are not on IPv6 in 2007



Attacks on IPv6

Year	Issue
2007	Ghost in the Machine/Cell Phone – Wired Blog
2009	Router Header o -Vendor Router Header o , **Botnet C&C** -Honeypot
2010	Malware Analysis , **First DDOS**
2011	New Data Center

Are their engineering things I can do, to improved detection and reduce operational complexity?

It's not just 96 more bits

Features	IPv4	IPv6
Addresses per Interface	1 (sometimes more)	Link-Local, ULA (n-1), Global (n-1), Privacy Address, MultiCast, Scoping
Outbound initiated - Inbound	Yes	See Above
External Address – Inbound Initiated	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)
System not responding	Perform additional Scans to see if crashed or blocked. Return later to see if rebooted.	Static or 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

It's not just 96 more bits

Features	IPv4	IPv6
Precedence	IPv4	IPv6 [Tunnel | IPv4] Unpatched MS [IPv4 | Tunnel] Patched MS/Linux
Address Allocation	Static, DHCP | 1 address	Static, Neighbor Discovery, DHCPv6
- Segment Address	CIDER Mask, unallocated bits	Self Allocated (/64): MAC Address or Random or Crypto Generated
- Next Hop Address	Default Route	Static Neighbor Discovery - IP Only (No DNS) - IP + DNS - Initial Address + DHCPv6 DHCPv6
MTU	68 – 1,500 – 9,216	1,280 to 4,000,0000
OSPF Routing	MD5	IPSec (Except with Cisco)

How long have systems
been compromise via IPv6?

Published 2008

Operating System	Capable	On by Default
Microsoft 2000 (2000)	Yes	No
Microsoft XP (2002)	Yes	No
Microsoft Vista (2007)	Yes	Yes
Solaris 2.10	Yes	Yes
Linux 2.4 Kernel	Yes	No
Linux 2.6 Kernel	Yes	Yes
OpenBSD / NetBSD / FreeBSD ('96)	Yes	Yes
Linux 2.1.6 Kernel ('96)	Yes	No
AIX 4.2 ('97)	Yes	No
AIX 6	Yes	Yes
Solaris 2.8 (2000)	Yes	Yes
IBM AS/400 (2002)	Yes	Yes
HP-UX 11iv2 (2007)	Yes	Yes
Open VMS (2007)	Yes	Yes

OS	Capable	On by Default
Macintosh OS/X Current	Yes	Yes
Cisco IOS (12.x and Later) (2001)	Yes	No
Juniper (5.1 and Later) (2002)	Yes	Mostly
Linksys Routers (2006)	Yes, Upgrade to DD-WRT	No
Apple Airport Extreme (2007)	Yes	Yes
Window 95/98/ME/NT 3.5/NT 4.0 (2000)	Yes, Add on	No
IBM z/OS (2002)	Yes	Yes
Apple OS/10.3 (2002)	Yes	Yes
Cell Phone – Many (2006)	Yes	Yes
Cell Phone – BlackBerry	No	No

The opportunity to re-engineer our part of the Global Internet only happens once in a lifetime!

Ensure it is operational and security!

Joe Klein

jsklein@gmail.com

@joeklein