Check Point
SOFTWARE TECHNOLOGIES LTD

IPv6, Internet Security, and the Internet of Insecure Things

Bob Hinden / Check Point Fellow

WELCOME TO THE FUTURE OF
CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION

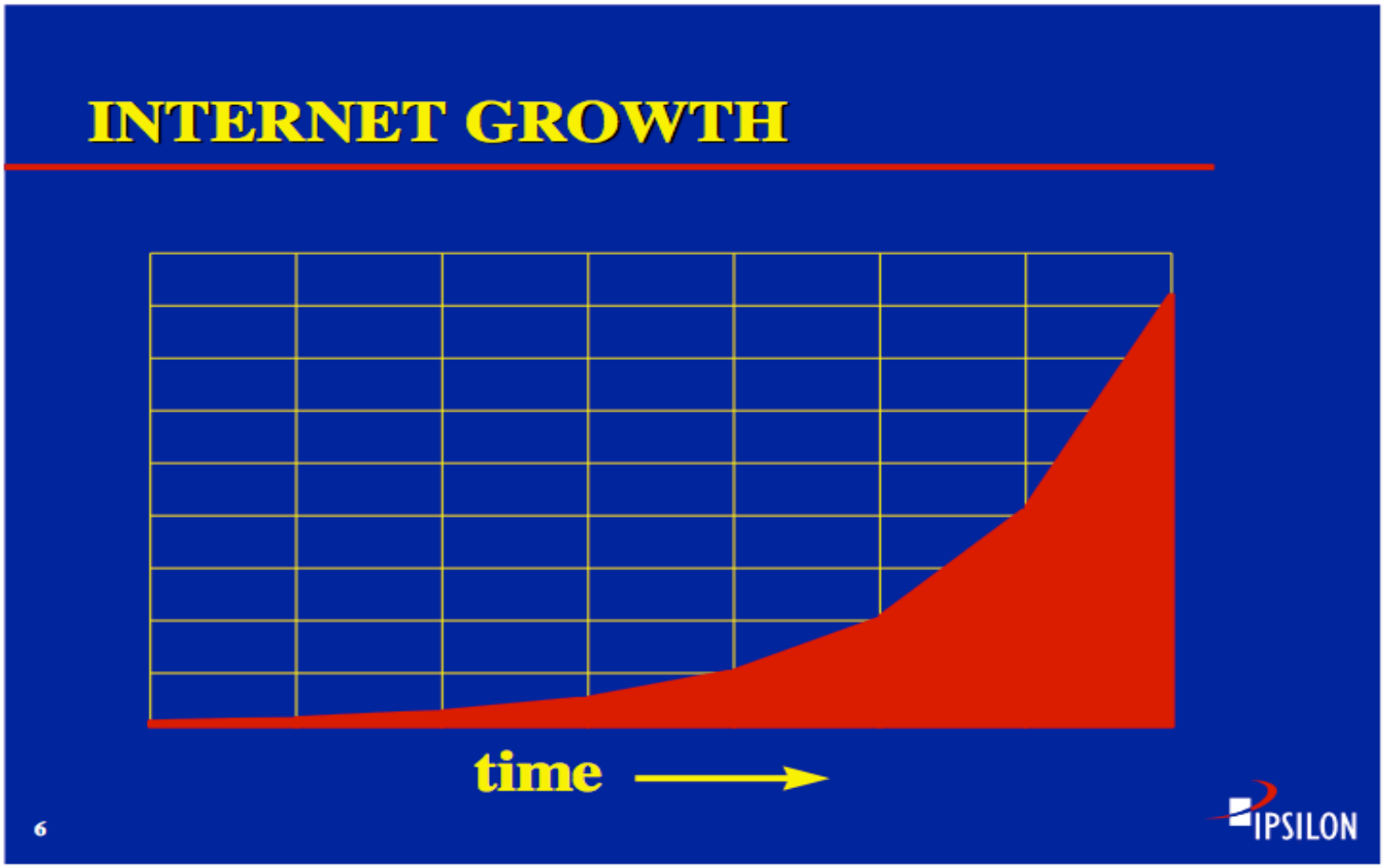
INTERNET PROTOCOL VERSION 6 (IPV6)

Bob Hinden – May 2018

IPv6 Background

- In the early 1990s it was not clear that TCP/IP was going to be successful
- There were many competitors
  - OSI CLNP, ATM, AT&T Business, etc.
- Predictions of Internet melt downs
- The IETF was not considered to be an official standards organization
- Not having a plan for what follows IPv4 was a real issue

Some Old Slides from ~1995

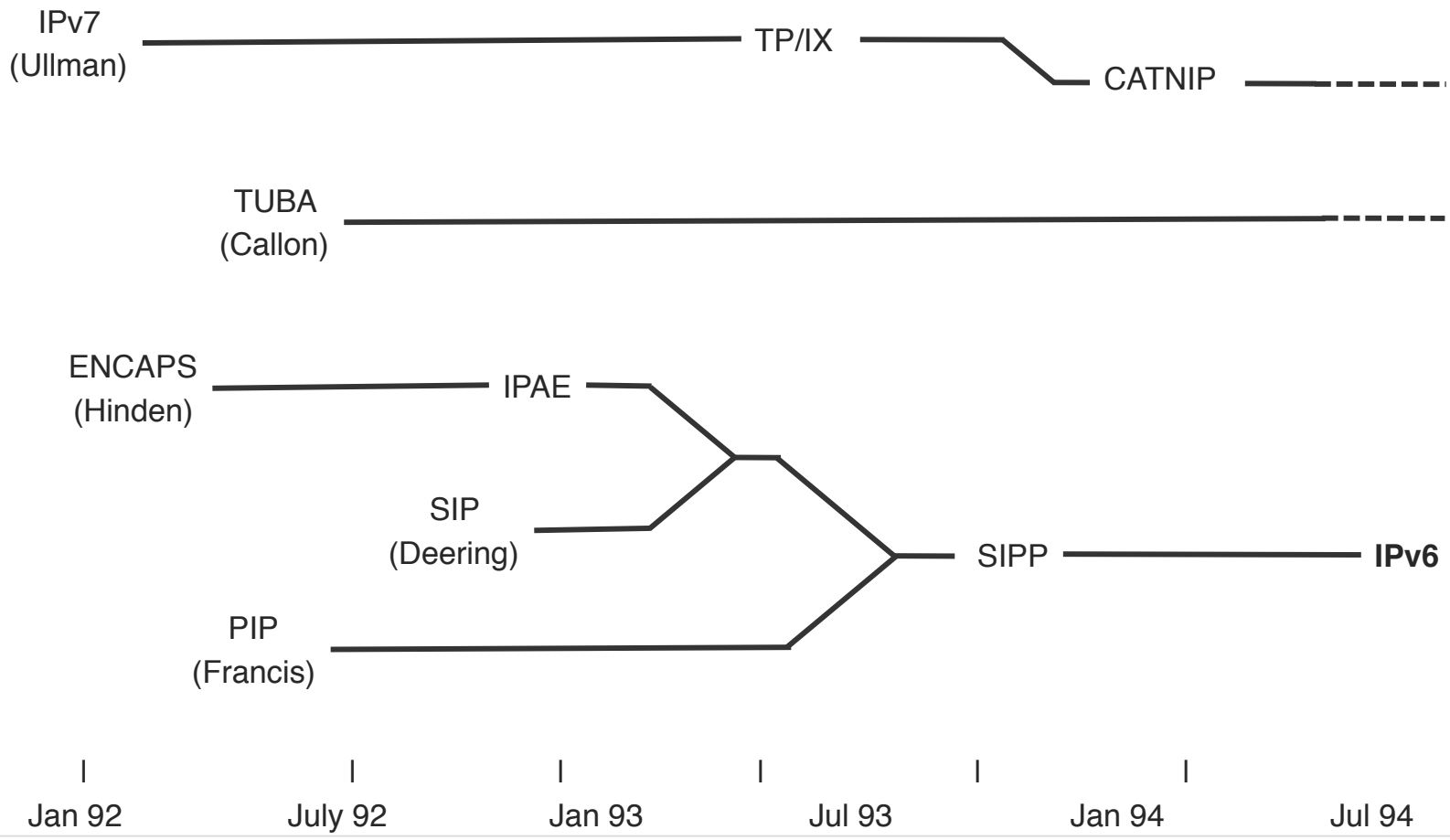



FACTORS CAUSING GROWTH
More of what we have Today
– All Computers on Internet
– Real Commerce / Advertising
New Users
– Large Countries (China, India, ...)
– New Industries (cable, mobile, ...)
Networked Everything
– All Information Devices (FAX, Printers, ...)
– Energy Management (meters, controllers, switches....)
7
IPSILON

IETF IPng Time Line

- ~1990
  - Internet growing exponentially and started looking like running out of IP addresses
  - Projected exhaustion of Class B Address space
- 1991
  - Routing and Addressing (ROAD) group formed
    - Recommended implementing CIDR and develop IP Next Generation (IPng)
- 1992
  - IAB issues “IP Version 7”
    - This came to be known as the “Kobe Incident”
- 1992 (cont)
  - IETF issues call for IPng proposals
- 1993
  - IESG took on IPng responsibility
  - IPng Area formed
    - Scott Bradner & Allison Mankin area directors
  - RFC1550 Call for IPng Solicitation published
- 1994
  - IPng Recommendation

IPng Candidates



IP Version Numbers

Version	Name
0-3	Unassigned
4	Internet Protocol (current IPv4)
5	Stream Protocol (ST) (not an IPng)
6	SIP – SIPP – IPv6
7	IPv7 – TP/IX – CATNIP
8	Pip
9	TUBA
10-15	unassigned

Classless Inter-Domain Routing (CIDR)

- Relaxed fixed boundaries in IP address allocation
  - Original IP allocation strategy was “flat”
- Allocate blocks of IP addresses to Providers
  - Now called prefixes
  - Routing protocols changed to aggregate all routes to a single provider
- CIDR made address utilization more efficient and greatly improved core routing scaling

TUBA

- TCP/UDP Over Bigger Addresses
  - Chairs: Peter Ford & Mark Knopper
  - Documented in RFC1347

- Approach was to run TCP/UDP over the ISO Connection-Less Network Protocol (CLNP)
  - Leveraged the ISO work

- Strength was CLNP, weakness was CLNP

CATNIP

- Common Architecture for Next-generation Internet Protocol (CATNIP)
  - Chair: Vladimir Sukonnik
  - Documented in RFC1707
- Based on work of TP/IX working group
  - Goal was to find common ground between OSI and Novell protocols, and to increase the scale and performance
- Not well specified, interesting ideas, but not a complete proposal

SIPP

- Simple Internet Protocol Plus (SIPP
  - Chairs: Steve Deering, Paul Francis, Bob Hinden
  - Documented in RFC1710
- Based on merger of ENCAPS into IPAE, merged with SIP, and with PIP
  - New version of IP designed to be an evolutionary step from IPv4. Designed to work over a range of speeds and network types.
- Clean design from SIP, addresses too small, extended addresses too complex.

The Address Size Debate

- Fixed length 64-bit addresses (SIP)
  - Met requirements by 3 orders of magnitude, 10^{12} sites, 10^{15} nodes at .0001 allocation
  - Minimizes growth of packet
  - Efficient for software processing
- Variable length addresses, up to 160-bits (TUBA)
  - Compatible with OSI NSAP address plans
  - Large enough for auto-configuration using IEEE 802 addresses
  - Could start with short addresses and grow later
- Compromised on fixed length 128-bit addresses

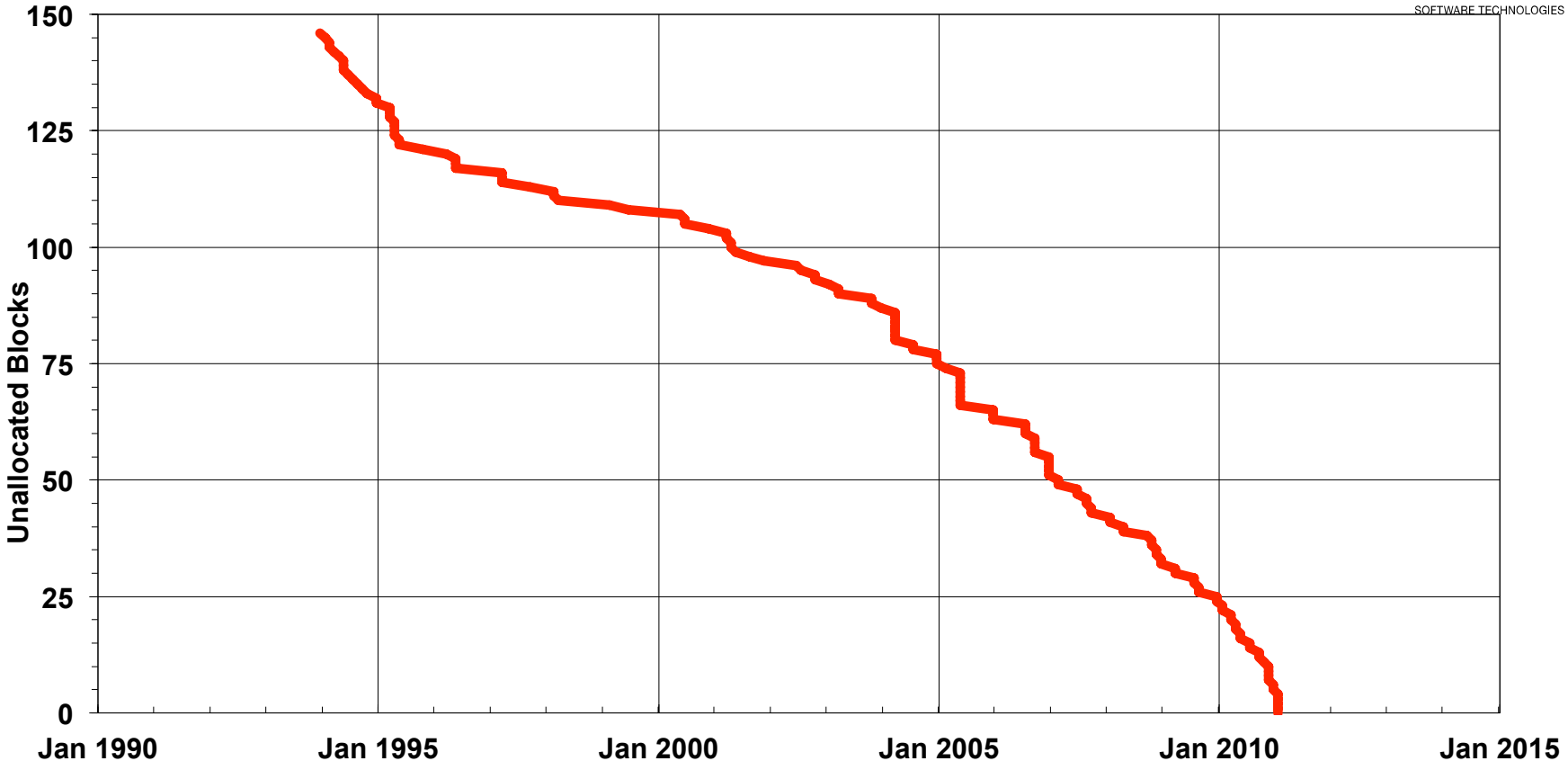
IPng Recommendation

- IPng based on SIPP with 128-bit addresses

- IPng working group created to create specifications and standardize IPv6
  - Chairs: Steve Deering, Ross Callon
  - Document editor: Bob Hinden

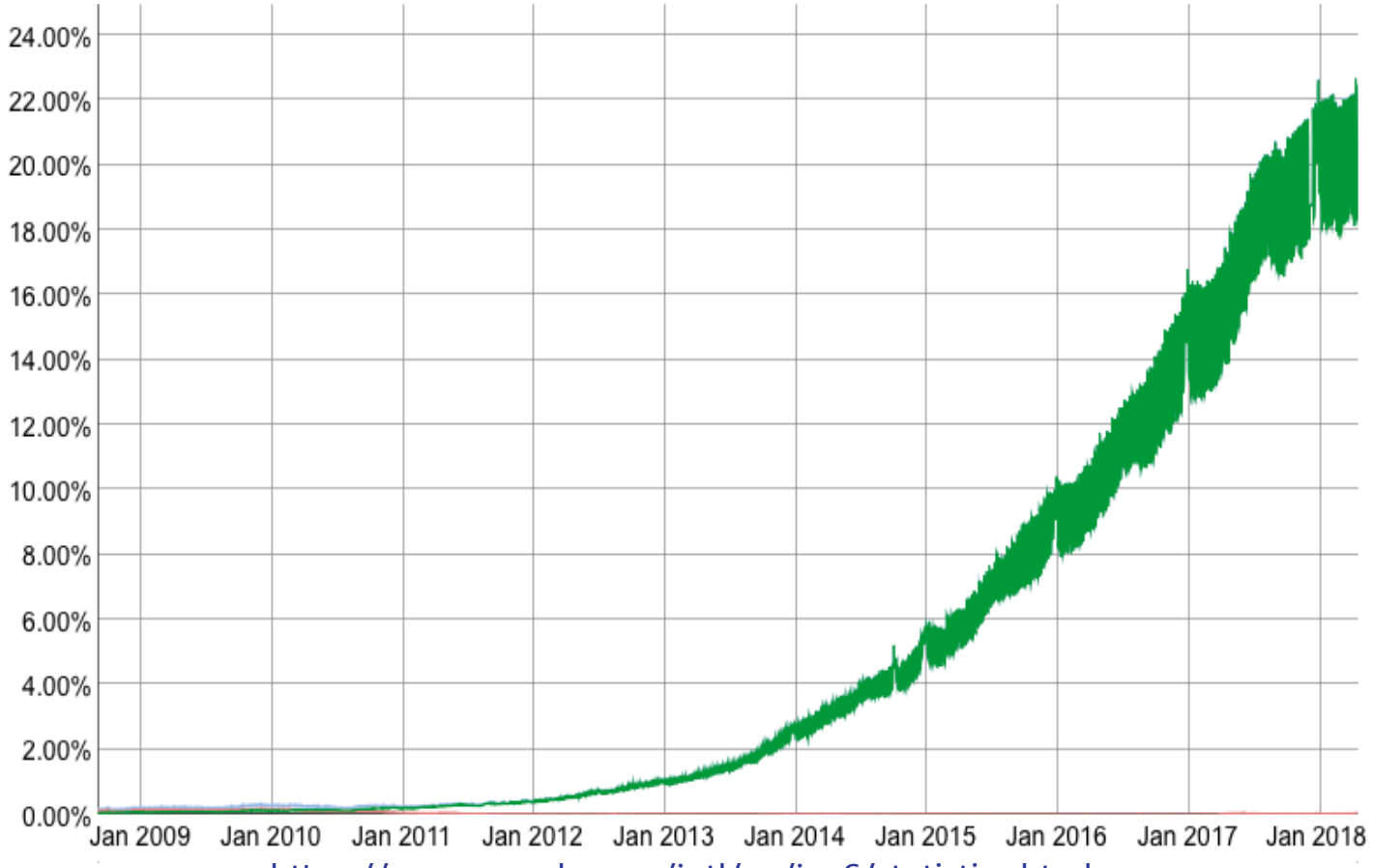
- Goal to resolve remaining issues, complete unfinished work, move to Proposed Standard
  - IPv6 first published as RFC1883 December 1995

We did Run Out of IPv4 Addresses



(Last allocation to RIRs from the IANA free pool 31 Jan 2011)

22% of User Access to Google is with IPv6



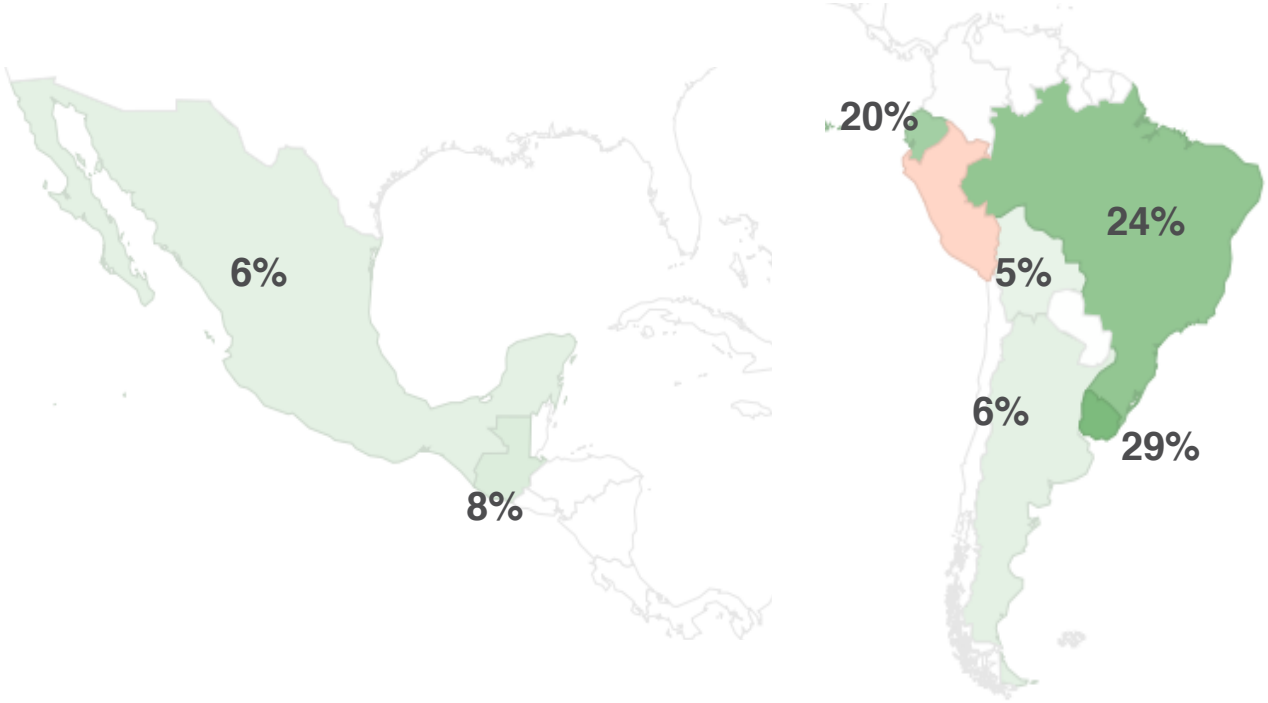
https://www.google.com/intl/en/ipv6/statistics.html

North America ISP Status

ISP	Percentage
Comcast	65%
AT&T	65%
Charter Communications	31%
Cox Communications	48%
T-Mobile USA	93%
Verizon Wireless	84%
Rogers Communications	49%
Sprint Wireless	70%

http://www.worldipv6launch.org/measurements/

IPv6 Deployment by Country LATNIC Region



https://www.google.com/intl/en/ipv6/statistics.html

IPv6 is now an Internet Standard

- The IETF published the IPv6 as an Internet Standard in July 2018
  - Internet Standard is the last step in the IETF Standards Process

STD 86
RFC 8200
Title: Internet Protocol, Version 6 (IPv6) Specification
Author: S. Deering, R. Hinden
Status: Standards Track
Date: July 2017
Obsoletes: RFC 2460

IPv6 State Today

- Major platforms all support IPv6
  - MacOS, Windows 10, Linux, Android, iOS, …
  - Routers, Switches, Firewalls, …
- Major content providers support IPv6
  - Google, Netflix, Facebook, LinkedIn, YouTube, …
- Large ISPs support IPv6
- CDN provide IPv6 access to IPv4 only sites
- AWS now supports IPv6
- Some large Enterprise are going IPv6 only

Challenges going Forward

Check Point
SOFTWARE TECHNOLOGIES LTD

- Mid size sites
  - Banks, Commerce, ….
- Enterprises are mostly IPv4 today
- Smaller ISPs
- IoT Devices
- Some new networks products still come IPv4 only
  - IPv6 is on the roadmap, but…

We have come a long way, but more to do

IPv6 Conclusions

- We were right about running out of IPv4 addresses
  - But did not understand the impact of NAT

- We were not right about
  - How long it would take to develop IPv6
  - When IPv4 addresses would run out
  - How hard and long to deploy

- We made IPv6 happen by building a broad community of motivated and dedicated people around the world

Conclusions (2)

Check Point
SOFTWARE TECHNOLOGIES LTD

- We did not anticipate how Internet would change
  - No longer “build it and they will come”
  - Now there has to be a business case
- A lot of the industry was in denial for a long time
- No one has done this before

The Internet Today

- It's very hard to deploy anything that requires global deployment before it becomes useful
  - Anything new needs immediate return
  - It has to solve a local problem, before it can solve a global problem

- The good news is that IPv6 deployment has become a local problem

INTERNET SECURITY

Sometime I Wonder Why People

- <RANT>
  - Choose the platform with the most exploits?
  - Don't upgrade to the latest version of the Operating System?
  - Don't apply patches and updates?
  - Don't run AV, Anti-Malware, etc.?
  - Run systems with no support?
- </RANT>

They must WANT to run Malware!

Internet Security is a Problem

- Making systems secure is hard
- Openness and Secure are opposites
- General purpose computing platforms are close to impossible to secure
- Isolation from the Internet does not protect systems
- There is no inside or outside
- Open Source doesn't mean secure
- https: doesn't protect you from bad actors
- Motivations for attacks include:
  - State Sponsored
  - Financial
  - Political
- It doesn't seem to be getting better….

Trust on the Internet

- The Snowden NSA revelations have reduced trust in the Internet
  - Everyone was surprised by how extensively Internet traffic is being monitored
- It has made it much harder for the “West” to speak for an Open Internet
- Calls for more regulation of the Internet

What is being done

- The IETF and other standards organizations are moving to make protocols have encryption on by default
- Content providers are enabling encryption
  - Google reports that 93% of their access traffic is https !
- Browsers are flagging non secure sites
- This won't stop Pervasive Monitoring, but it will make it harder to see all of the traffic all of the time
  - Selected individuals will always be vulnerable
- However, some bad actors are now encrypting their traffic
  - Just because it's a secure connection, doesn't mean it is safe

Making Platforms more Secure

- Platforms modeled like Apple's iOS Apps may be the future
  - Vendor controlled applications
  - Only verified applications are allowed
  - Vendor has the ability to remove or disable applications
  - Windows 10 S is the latest example
- This is a loss for everyone in many ways, but may be the only approach that works
  - I doubt most consumers will care
- We need to have platforms that are more secure
- What do we do about the installed base of old systems?

The Internet Of Insecure Things (sometimes call IoT)

We Have Problem

- Most IoT Devices are not secure
- Numerous Security Weaknesses
  - Default login/passwords, fix firmware login/passwords, no software updates, no vendor security support, …
- Gartner says 6.4 Billion IoT Devices now
  - Forecasts 20.8 Billion in 2020

Initial IoT Based DDoS Attacks

- **KrebsOnSecurity** attacked 13 Sept 2016
- Published a series of articles about vDOS (a DDoS for hire service)
  - Article stated that vDOS made $600K in two years, knocking sites offline
- Two weeks after articles were published, Krebs site was attacked with 620 Giga bits/sec of traffic
  - Akamai was providing pro-bono DDoS protection, but they couldn't continue to handle the traffic load
  - Google Project Shield is now protecting his site
- **OVH** (large international web hosting provider) attacked early October 2016
- Attacked by botnet comprised of more than 145k compromised IP cameras and DVRs
- Attack peaked at 1 Tera bits/sec
- OVH was able to withstand it

IoT Devices Involved

DYN Attack

- DYN (large DNS provider) attacked late October 2016
- Attacked by millions of source IP addresses, attack attributed to Mirai IoT malware
- Attack peaked at 1.2 Tera bits/sec
- Attack affected Amazon, CNN, NYT, Netflix, PayPal, Twitter, WSJ, etc.

IoT Botnet Malware

- **Mirai**
  - Used in attack on KrebsOnSecurity
  - Works by scanning the internet for vulnerable devices
  - Looks for systems with factory default usernames and passwords
  - Installs software turning devices into "bots" used to launch DDoS attacks

- **Bashlight**
  - Similar to "Mirai" – it infects IoT devices via default usernames and passwords

- **New Variants**
  - Brickerbot – March 2017
    - Kills IoT devices
  - Persirai – May 2017
  - IoT Malware continues to evolve

We Should be Worried

- Scale of the attacks – everyone is vulnerable
- The number and growth of IoT devices
- The nature of most IoT devices makes this much harder to fix than laptop/desktops/servers and iOS/Android

It's Going to be a Challenge to Fix

Check Point
SOFTWARE TECHNOLOGIES LTD

- Technically some of the problems are easy
  - Don't allow default login/passwords
  - No fixed firmware login/passwords
  - Automatic updates on software
- Other problems are much harder
  - How to provide support for low cost IoT devices?
  - How long will they be supported?
  - What happens when they are not supported?
  - How are attacks detected and contained?
  - How do we fix current deployed base of IoT devices?
  - Does the owner/seller of the IoT devices even care?

Economics are Challenging

- Who is responsible? Is there any liability?
  - User
  - Retail Supplier
  - Manufacturer
  - Component Vendor
- Role of the Internet Service Provider?
- How do you provide long term support for very low cost devices?
  - What do you do when support ends?

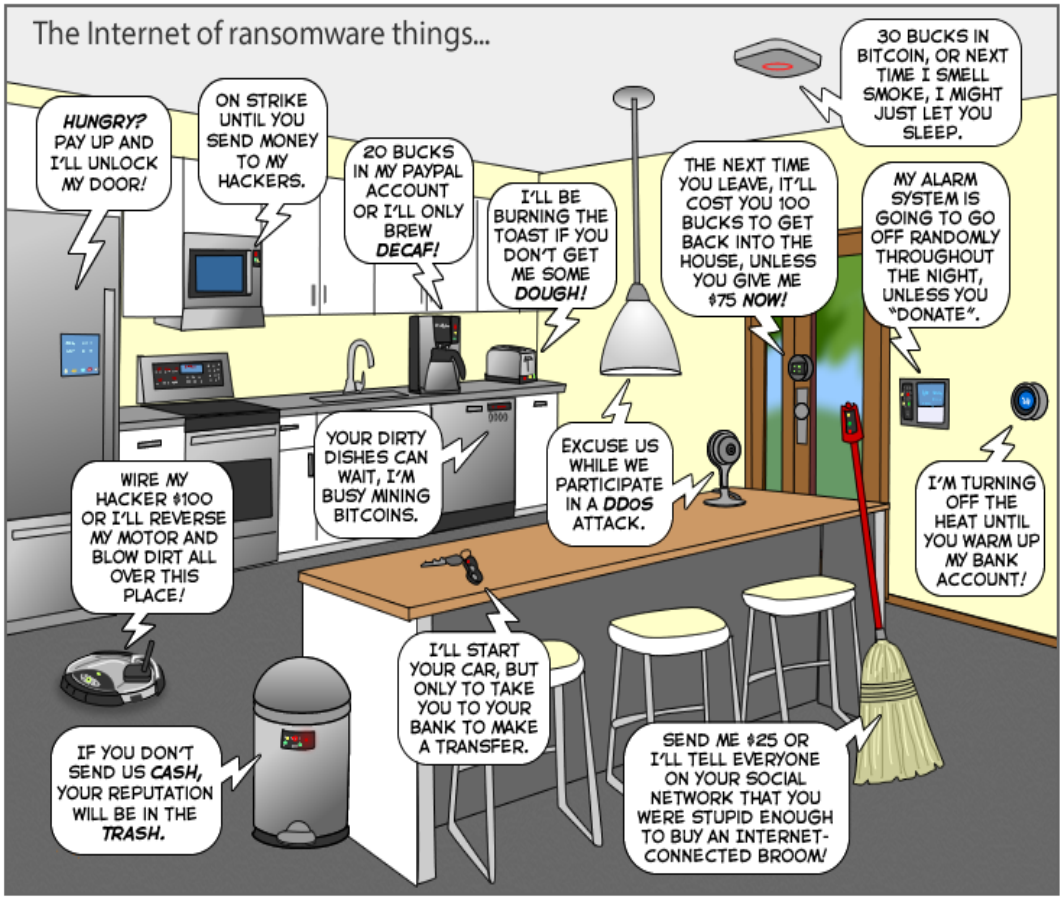
How Can This be Fixed?

- Can the market fix the problem?
- Is there an alternative to government regulation?
- It is an worldwide problem
- My view is that we need to treat this as a product safety issue
  - Vendors and retail channel need to have some form of liability for security failures

Check Point
SOFTWARE TECHNOLOGIES LTD

Bob Hinden, *The Internet of Insecure Things*, Internet Protocol Journal, March 2017, Volume 20, Number 1, page 12

http://ipj.dreamhosters.com/wp-content/uploads/issues/2017/ipj20-1.pdf



The Internet of Ransomware Things

FOR EXTRA CREDIT

RFC 6921

Check Point
SOFTWARE TECHNOLOGIES LTD

- Title: *Design Considerations for Faster-Than-Light (FTL) Communication*
- Date: 1 April 2013
- Abstract:
  - We are approaching the time when we will be able to communicate faster than the speed of light. It is well known that as we approach the speed of light, time slows down. Logically, it is reasonable to assume that as we go faster than the speed of light, time will reverse. The major consequence of this for Internet protocols is that packets will arrive before they are sent. This will have a major impact on the way we design Internet protocols. This paper outlines some of the issues and suggests some directions for additional analysis of these issues.
- https://tools.ietf.org/html/rfc6921

Check Point®
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION