Business and Security Justification For IPv6 Only IoT Networks

Joe Klein, CISSP
Founder & CTO, Disrupt6
Fellow, IPv6 Forum

www.Disrupt6.com | @JoeKlein | Joe.Klein@Disrupt6.com

DISRUPT6

IPV6 BUSINESS CASE

Decrease OPEX/CAPEX,
Increase Competiveness & Agility

The business reality – OPEX/CAPX : Wells Fargo

- Greater space for growth
- Reduced requirement for readdressing duplicate address space in mergers/acquisitions
- Support for low-functionality end-points that may lack DHCP and static addressing capabilities (IoT, even Android devices)
- Reduce reliance on NAT (and associated logging complexity)
- More universally geo-locate address space (assuming ULA usage is reduced compared to RFC1918)
- Simplification of routing tables through improved summarization
- International Commerce

Source: http://www.ntia.doc.gov/files/ntia/publications/wellsfargo_10_3.pdf

The business reality – OPEX/CAPX : Microsoft

- Improved peer-to-peer networking for communications
  - Personalized user experience using IP-based location services
- We see minor performance benefits as address translators are removed and implementations are improved NAT64 & NAT 444 (CGN) obscure location data, and cause service failures
- Market opportunities increase when customers mandate IPv6 support
- IPv6 allows faster infrastructure growth for services experiencing rapid customer usage
- *"Microsoft corporate IT efforts are based on a belief that IPv6 support is a cost of business, with returns on investment to be seen only over a very long time frame"*. Source: https://www.ntia.doc.gov/files/ntia/publications/microsoft_10_4.pdf

The business reality – OPEX/CAPX : FACEBOOK

- Easier management of networks:
  - Flatter, simpler, and more manageable.
- End-to-end connectivity integrity:
  - Direct addressing is possible, due to vast address space
  - Shortest path, no additional latency (middle boxes).
- Improved User Experience & Higher Engagement:
  - One address per user (or household), no additional latency (10-15% faster).
- Improved interoperability and mobility capabilities (which are already widely embedded in network devices)

Reference: https://code.facebook.com/posts/1192894270727351/ipv6-it-s-time-to-get-on-board/

The business reality – OPEX/CAPX : COMCAST

- Reduce costs based on depleted IPv4 addresses
  - USD 9.50/IPv4 address (In Bulk) – USD 35.00/IPv4 address in cloud
- Reduce operational complexity
  - One IPv6 address per user/household sensor/floor
- Increase service offerings and become more competitive
  - IoT wireless and analytics

IPV6 MOBILE CUSTOMERS

"Better Use Experience"
"10% to 40% faster mobile (LTE) users applications"

In 201

"Improved interoperability and mobility capabilities"

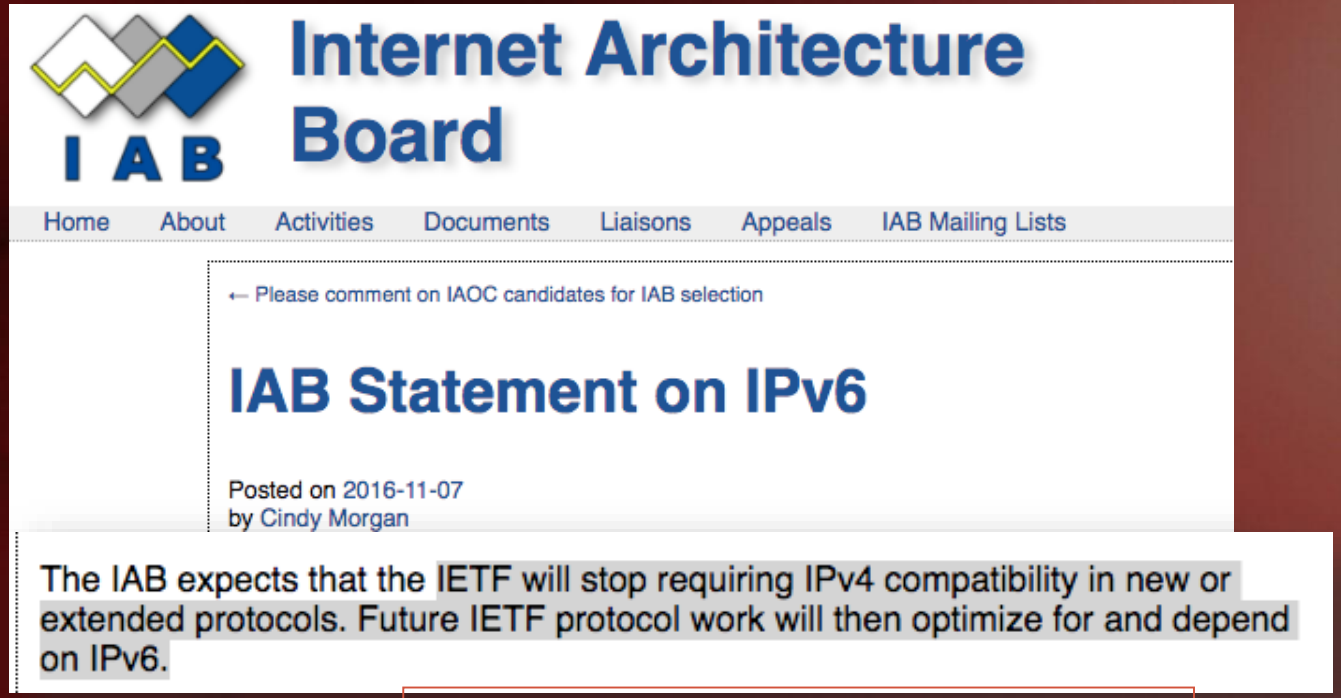
, US

IN WITH THE NEW – Impact on competition
The business reality – OPEX/CAPX : IPv6 only

- Foundational Wireless:
  - High Bandwidth
    - 4G LTE NG Wireless & 5G Wireless
  - Low Bandwidth – Low Power
    - Cognitive radio (TV Whitespace) & IoT Networks (LoRaWan)
- IoT & IoTT (Internet of Trusted Things)
  - 6LowPan (IPv6 for low power systems)
  - Car-toCar/Car-to-Infrastructure Communications
- Many New Wireless networks already exist
  - Cellular infrastructure does not exist
  - Many international 'smart cites', 'smart buildings', 'smart transportation system'

OUT WITH THE OLD

The business reality – OPEX/CAPX : IPv4 End of Life



Internet Architecture Board

Home About Activities Documents Liaisons Appeals IAB Mailing Lists

← Please comment on IAOC candidates for IAB selection

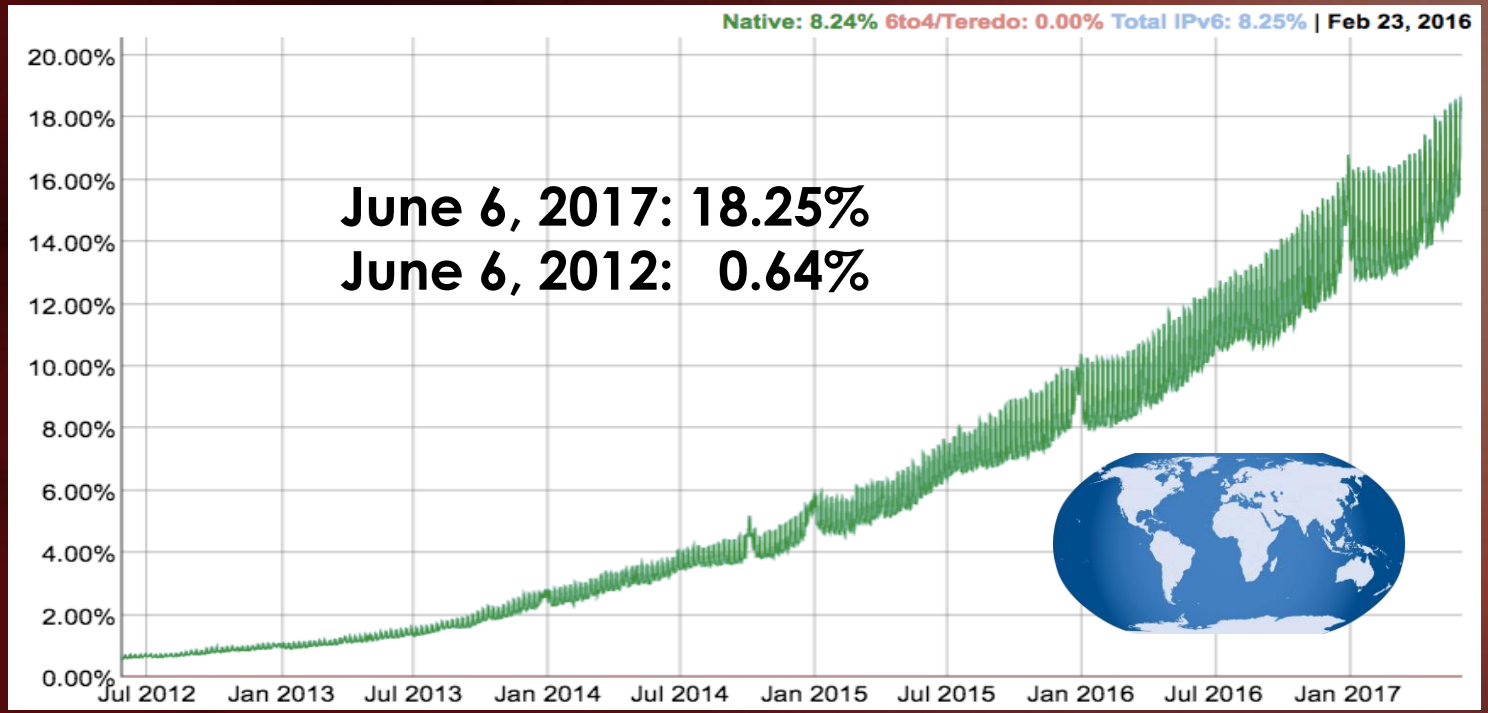
IAB Statement on IPv6

Posted on 2016-11-07
by Cindy Morgan

The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6.

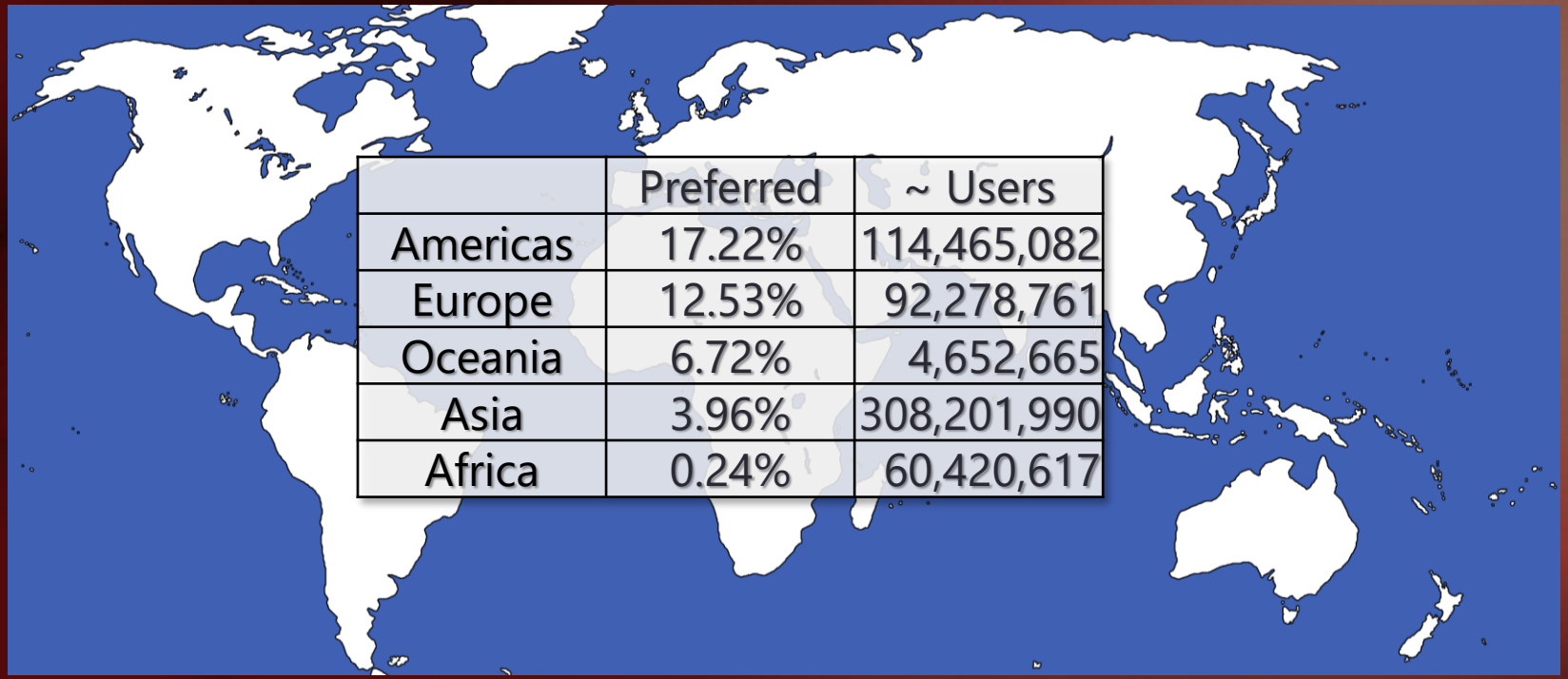
Source: https://www.iab.org/2016/11/07/iab-statement-on-ipv6/

DID I MENTION THE WORLD GROWTH?



Reference: https://stats.labs.apnic.net/ipv6/XA

EVERYONE IS DOING IPV6!



	Preferred	~ Users
Americas	17.22%	114,465,082
Europe	12.53%	92,278,761
Oceania	6.72%	4,652,665
Asia	3.96%	308,201,990
Africa	0.24%	60,420,617

Reference: https://stats.labs.apnic.net/ipv6/

SUMMARY

IPV6 IS NOW A BUSINESS DISCUSSION
NOT A TECHNICAL DISCUSSION!

NEW SECURITY FEATURES

INCREASE THE COSTS TO THE ATTACKERS!

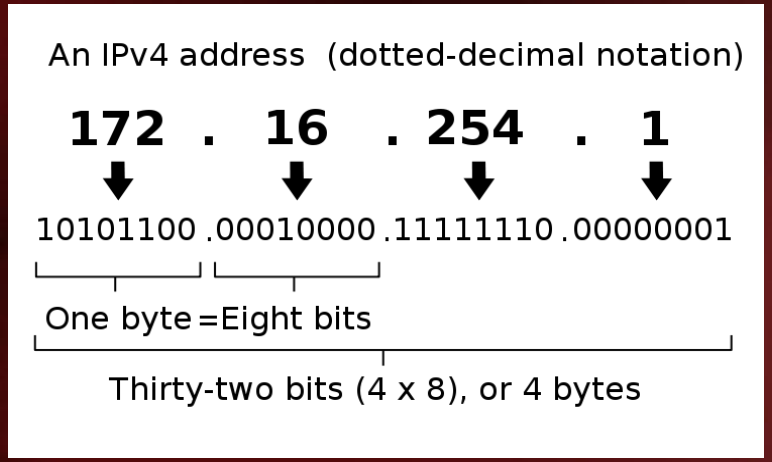
REDUCE COSTS TO DEFENDERS!

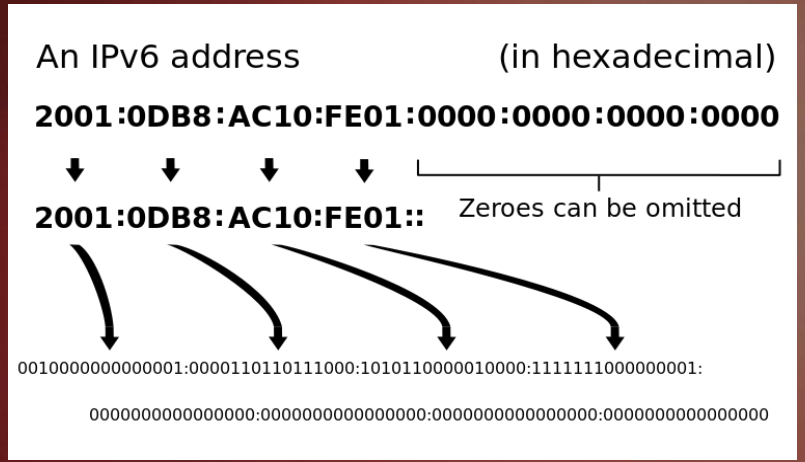
REMOVE THE IPV4 WARTS

IPV6 KILLS SPAM/PHISHING - IMPROVED TRUST

- **Basic Level**
  - **Trust between email servers (MTA)**
    - Associate IP address and valid domain (FCrDNS)
    - Validate email is from expected domain (SPF)
  - **Trust email sent between servers**
    - Source Validates trust before sent (DKIM)
    - E-Mail Authentication (DMARC)
  - **Block bad domains not IP addresses**
    - Spamhaus Domain Block List (SURBL) or Newly Observed Domains (NOD)
- **Advanced Level**
  - Encrypt all email (TLS/valid certificate)
  - Validate Certificate (DNSSEC)
  - User Validating E-Mail Server (DANE)
  - Scanning Detection (use /118 from a /64)
  - Allow connections from only registered blocks (BOGON List)

LAW OF SMALL VS. LARGE NUMBER





45 Min	Scan all Internet IP's (no DNS)	500,000+ Years
/24 < 1 Min	Scan smallest range (no DNS)	/64 < 500 Years
/24 < 1 Min	Reverse DNS Scan	/64 < 500 Years

Simplifies identification of Bots, C&C, active attacks

NAT VS. END-TO-END PRINCIPLE

	IPv4	IPv6
Addresses	Overlapping	Unique
Routers	Anyone can insert	Quickly Identify
End-Devices	Anyone can connect	Quickly Identify
Renumbering	Manual	Automatic
Addressing	Static/DHCP	Auto-configuration/DHCPv6 (Static)
Trust	Disassociated	End-to-End

NAT STATEFULNESS IMPACTS POWER

IPv4

- Hosts
  - Keep Alive =
    - (# Applications) * (Connections Per Application)
- Firewall/Routers with NAT on path
  - Keep Alive =
    - (# Devices) * (# Applications) * (Connections Per Application)

IPv6

- Hosts
  - No Keep Alive needed
- Firewall/Router
  - No Keep Alive needed

3-14% power reduction & battery savings

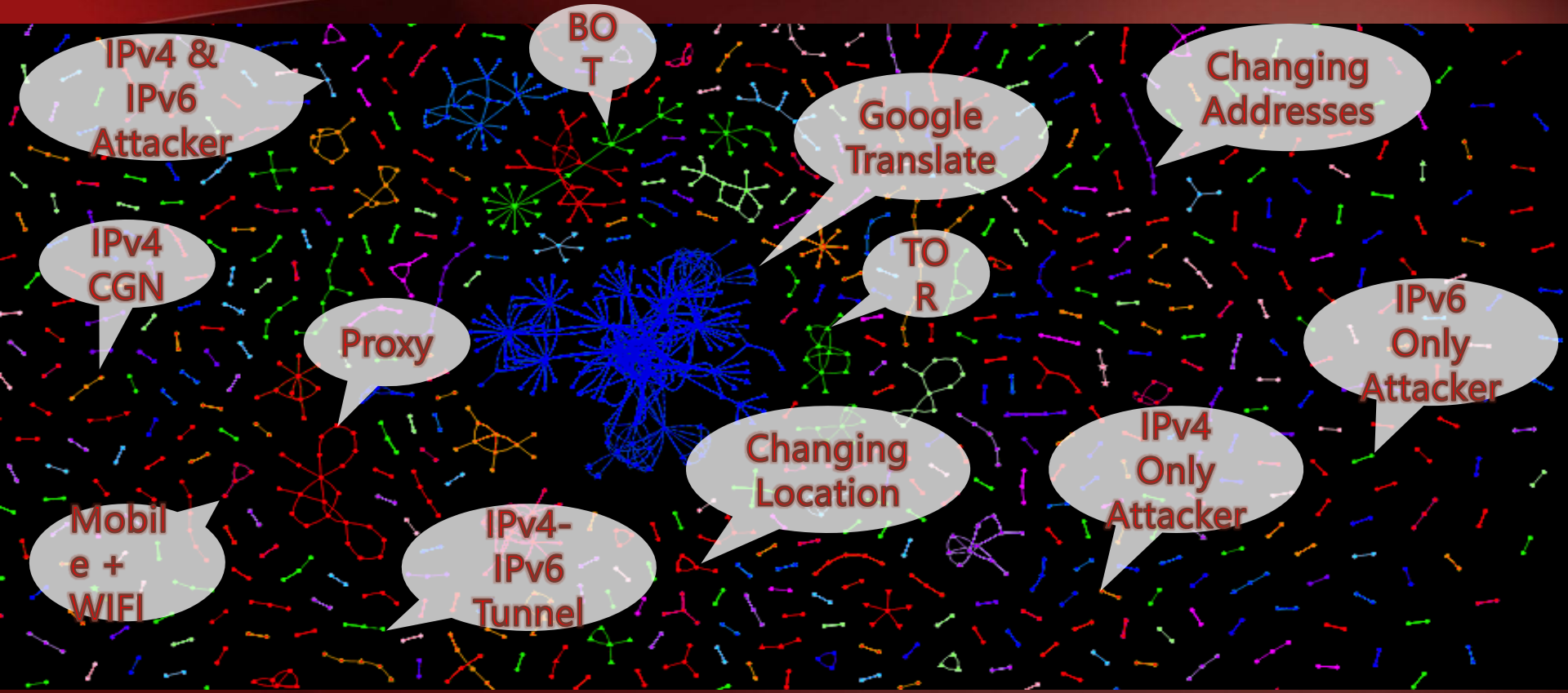
SUMMARY

INCREASING THE COSTS TO THE ATTACKERS!
REDUCE COST TO DEFENDERS!

NEXT STEPS

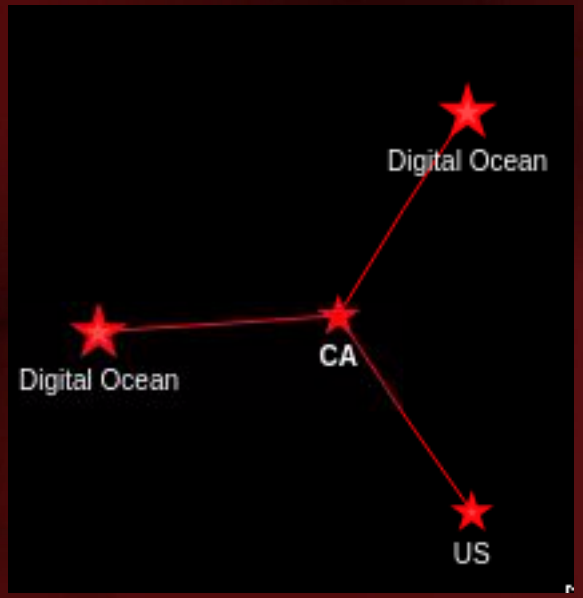
Disrupt6 Research?

ADVANCED SECURITY IPV6 FEATURES



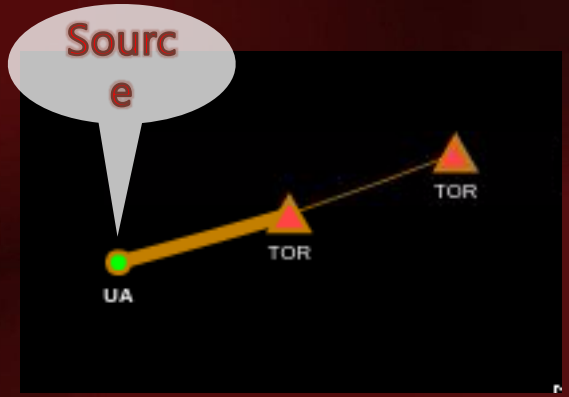
INDICATORS OF INTENT (IOI)

TRACKING THROUGH CYBERSPACE & TIME



Tracked address changes:
2015-08-19 23:07:27 GMT: **142.167.242.21** (Prohibited content)
2015-08-20 00:14:51 GMT: 107.170.136.239 (Digital Ocean)
2015-08-20 00:15:08 GMT: 107.170.144.142 (Digital Ocean)
2015-08-20 00:15:51 GMT: 162.217.133.104 (Prohibited content)

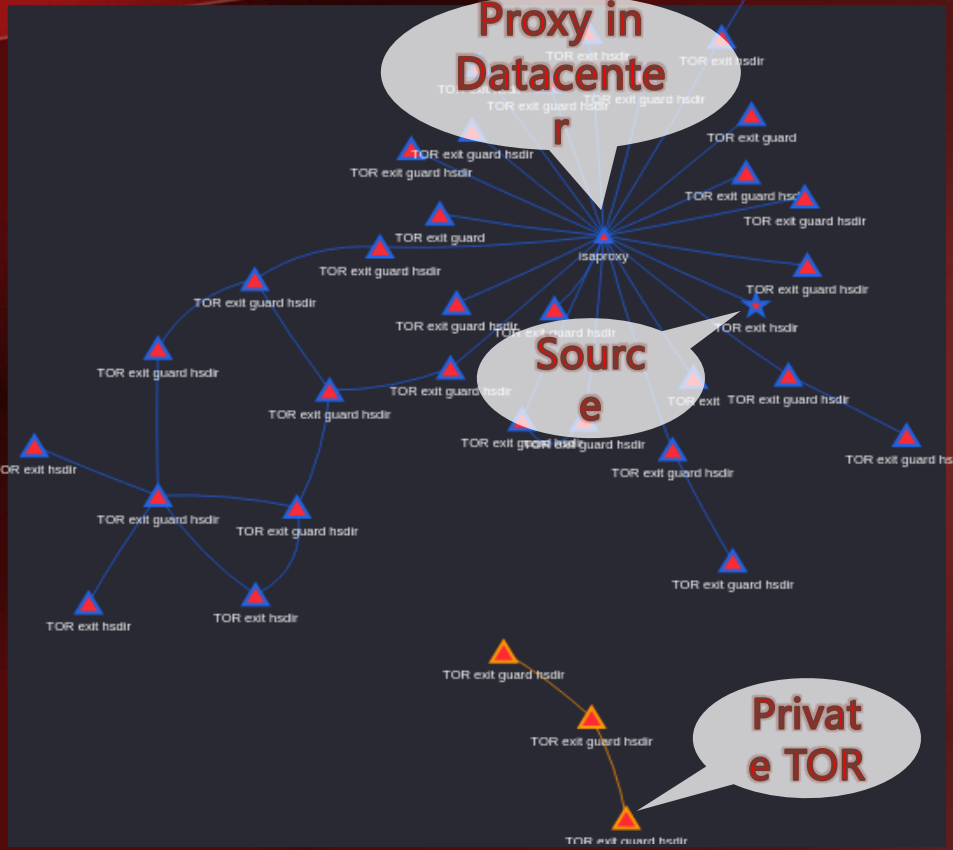
ATTRIBUTION THROUGH TOR



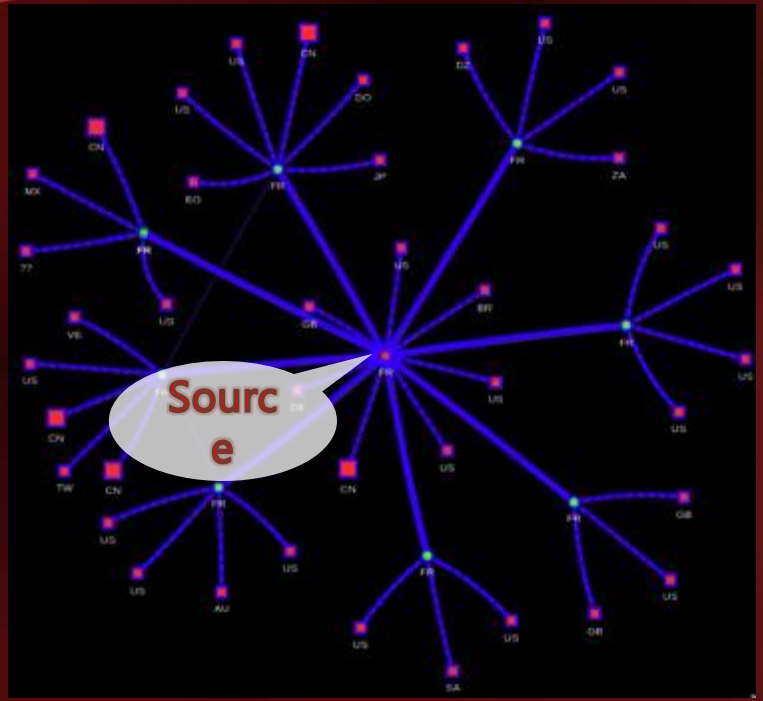
Tracked address changes:
2015-08-26 19:37:16 GMT: **77.247.181.162** (TOR)
2015-08-26 19:37:19 GMT: **77.247.181.162** (TOR) =
2a02:27a[redacted]2b:34ff:fe45:eda3 (UA)
2015-08-26 19:48:33 GMT: 46.165.221.166 (TOR)

NIC MAC:	902b3445eda3
NIC Vendor:	GIGA-BYTE TECHNOLOGY CO.,LTD.

A VISIT FROM ANONYMOUS



IPV4 & IPV6 DECOYS



Tracked address changes:

2015-08-26 11:18:09 GMT: 2a01:e35:8a13: d918:91c4:5cd2 (FR)
2015-08-26 12:36:25 GMT: **2a01:e35:8a13** **:da3a:1482:171** (FR)
2015-08-26 12:36:25 GMT: **2a01:e35:8a13** **:da3a:1482:171** (FR)
= 134.208.167.95 (TW)
2015-08-26 12:36:25 GMT: **2a01:e35:8a13:** **:da3a:1482:171** (FR)
= 186.164.65.135 (VE)
2015-08-26 12:36:25 GMT: **2a01:e35:8a13:** **:da3a:1482:171** (FR)
= 222.63.11.106 (CN)
2015-08-26 12:36:25 GMT: **2a01:e35:8a13:** **:da3a:1482:171** (FR)
= 88.161.51.89 (FR)
2015-08-26 12:36:29 GMT: **2a01:e35:8a13:** **da3a:1482:171** (FR)
2015-08-26 12:36:29 GMT: **2a01:e35:8a13:** **:da3a:1482:171** (FR)
= 199.131.99.62 (US)
2015-08-26 13:42:29 GMT: **2a01:e35:8a13:** **:da3a:1482:171** (FR)
= 114.2 196 (CN)
2015-08-26 13:56:29 GMT: 2a01:e35:8a13: 3c3e:fb3:647 (FR)

ATTACKER & BROKER ATTRIBUTION RESULTS

- Privacy vs. Attribution:
  - Privacy to Users
  - Deny Privacy and Attribute Attacker, Bots & Brokers
- Additional Findings:
  - Location Intelligence (Geo-location)
  - Network & Device Intelligence
    - Browser type, Networks, Operating Systems, Tunnels, VPN's, TOR, etc.
  - Statistical validation of other attributed including:
    - Identified Data Brokers which scan and provide ($) vulnerability to others

Business and Security Justification For IPv6 Only IoT Networks

Joe Klein, CISSP
Founder & CTO, Disrupt6
Fellow, IPv6 Forum

www.Disrupt6.com | @JoeKlein | Joe.Klein@Disrupt6.com

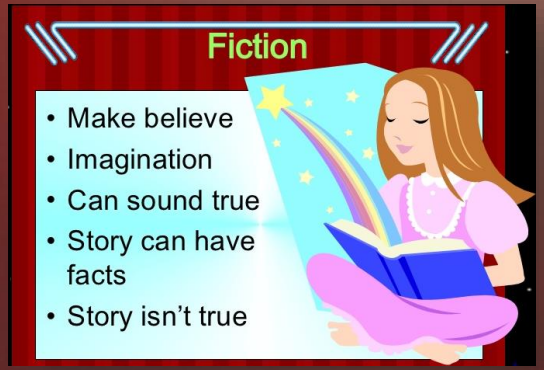
DISRUPT6

OTHER RESOURCES

- Report of the DoC Task Force on the New Internet Protocol (IPv6) - NIST, 2016, https://www.nist.gov/document-17789
- National Telecommunications & Information Administration, Additional IPv6 Resources, https://www.ntia.doc.gov/page/additional-ipv6-resources

I LIKE A GOOD IPV6 FICTION

- Running IPv4 & IPv6 in parallel increases CAPEX/OPEX – 2x
- Deployment will take years
- My gear does not support IPv6
- My Customers & Partners don't use or want IPv6
- IPv6 is slower because of the larger header
- We don't need that many addresses
- IPv6 is just a fad – waiting till IPv9
- Many, Many more…



Source: https://github.com/detobate/ipv6excuses.com/blob/master/excuses

THIRD INDUSTRIAL REVOLUTION

- Power
  - Renewable, Efficient, Effective
- Communications
  - Wide frequency range to choose
  - Low to High speed transports
  - Real-time and stored
- Manufacturing
  - Multitude of designer materials
  - 3D Printing at scale

Smart*

- Buildings
- Energy
- Consumer & Home
- Healthcare. Life & Science
- Industry
- Transportation
- Retail
- Security/Public Safety
- IT & Networks