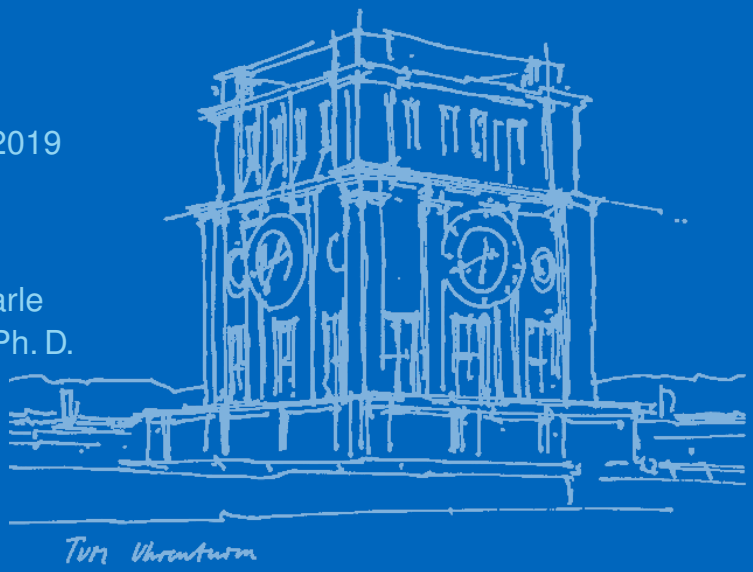
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Evaluating Network Security Using Internet-wide Measurements

Oliver Gasser

Ph. D. Defense, Friday 24th May, 2019

Chairman: Prof. Dr. Jörg Ott
Examiners: Prof. Dr.-Ing. Georg Carle
Prof. Anja Feldmann, Ph. D.



Motivation

SYDNEY, Australia, August 15, 2018

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

Detection, Response and Privacy Driving Demand for Security Products and Services

Motivation

TLS Certs Outliving Domain Ownership Open Door to MitM and DoS

By Ionut Ilascu August 21, 2018 11:04 AM 0

SYDNEY, Australia, August 15, 2018

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

Detection, Response and Privacy Driving Demand for Security Products and Services

Motivation

TLS Certs Outliving Domain Ownership Open Door to MitM and DoS

By Ionut Ilascu August 21, 2018 11:04 AM 0

SYDNEY, Australia, August 15, 2018

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

Detection, Response and Privacy Driving Demand for Security Products and Services

Memcached DDoS: The biggest, baddest denial of service attacker yet

Distributed denial of service attacks just got turned up to 11 with Memcrashed, an internet assault that can slam a website with over a terabyte of bad traffic.

By Steven J. Vaughan-Nichols for Networking | March 1, 2018 -- 23:38 GMT (23:38 GMT) | Topic: Security

Motivation

The Internet

- Internet measurements can be leveraged to empirically assess security of
  - protocols,
  - devices,
  - implementations, and
  - configurations
- Vast IPv6 address space poses big challenge for Internet measurements

Motivation

The Internet

- Internet measurements can be leveraged to empirically assess security of
  - protocols,
  - devices,
  - implementations, and
  - configurations
- Vast IPv6 address space poses big challenge for Internet measurements

Goals

- Improve measurement methodology for Internet-wide security measurements
  - IPv4 and IPv6
- Empirically assess security of three different protocols
  - HTTPS
  - BACnet
  - IPMI

Research questions

Research questions

RQ I

RQ II

RQ III

RQ IV

RQ V

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements?

ZMapv6 goscanner

RQ II

RQ III

RQ IV

RQ V

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements?

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists?

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III

RQ IV

RQ V

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements?

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists?

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Certificate security HTTPS security

RQ IV

RQ V

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements?

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists?

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Certificate security HTTPS security

RQ IV: Are BACnet devices vulnerable to amplification attacks?

Deployment Amplification Notification

RQ V

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements?

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists?

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Certificate security HTTPS security

RQ IV: Are BACnet devices vulnerable to amplification attacks?

Deployment Amplification Notification

RQ V: Are IPMI devices vulnerable to MitM attacks?

Deployment TLS security

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements? Chapter 3

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists? Chapter 4

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks? Chapter 5

Certificate security HTTPS security

RQ IV: Are BACnet devices vulnerable to amplification attacks? Chapter 6

Deployment Amplification Notification

RQ V: Are IPMI devices vulnerable to MitM attacks? Chapter 7

Deployment TLS security

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements? Chapter 3

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists? Chapter 4

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks? Chapter 5

Certificate security HTTPS security

RQ IV: Are BACnet devices vulnerable to amplification attacks? Chapter 6

Deployment Amplification Notification

RQ V: Are IPMI devices vulnerable to MitM attacks? Chapter 7

Deployment TLS security

RQ II: How biased are address sources for IPv6 hitlists?

RQ II: How biased are address sources for IPv6 hitlists?

Motivation

- IPv6 address space too large to perform brute-force measurements
- Assemble lists of IPv6 target addresses: IPv6 hitlists

RQ II: How biased are address sources for IPv6 hitlists?

Motivation

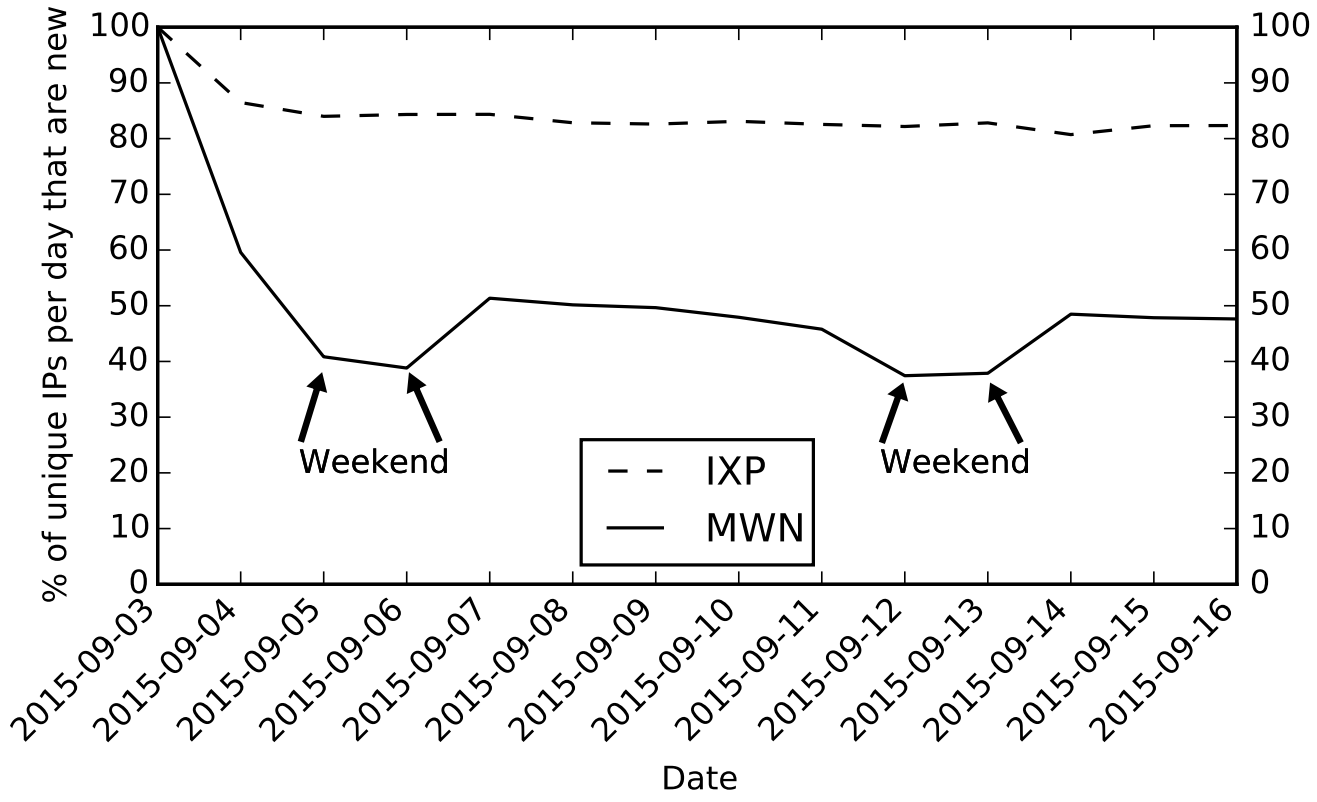
- IPv6 address space too large to perform brute-force measurements
- Assemble lists of IPv6 target addresses: IPv6 hitlists

Measurements & analyses

- Passive and active measurements
- Empirical analysis of different types of biases
  - Weekly patterns
  - Different host populations
  - Different number of addresses
  - Over-representation of certain prefixes

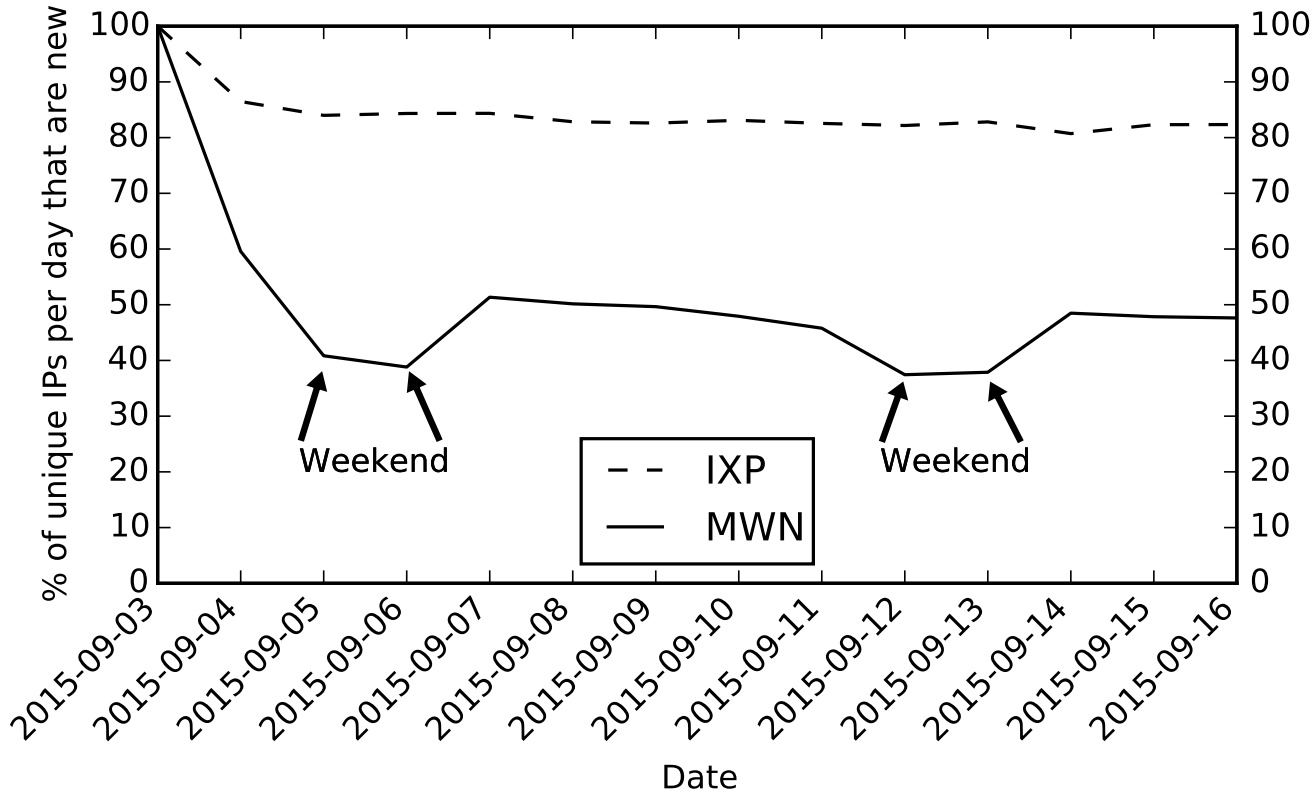
RQ II: How biased are address sources for IPv6 hitlists?

IPv6 hitlist passive sources: new IPv6 addresses per day



RQ II: How biased are address sources for IPv6 hitlists?

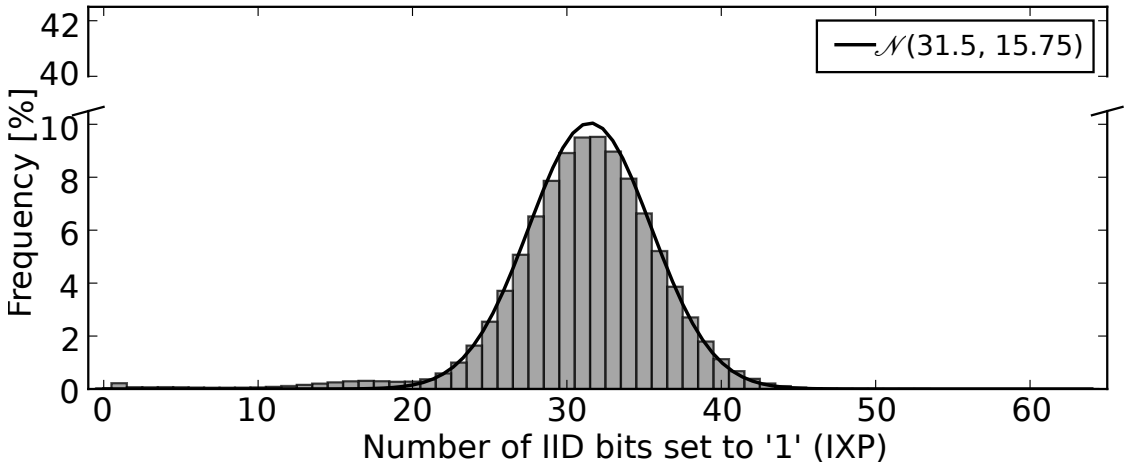
IPv6 hitlist passive sources: new IPv6 addresses per day



- Large share of new addresses each day hints at privacy extensions

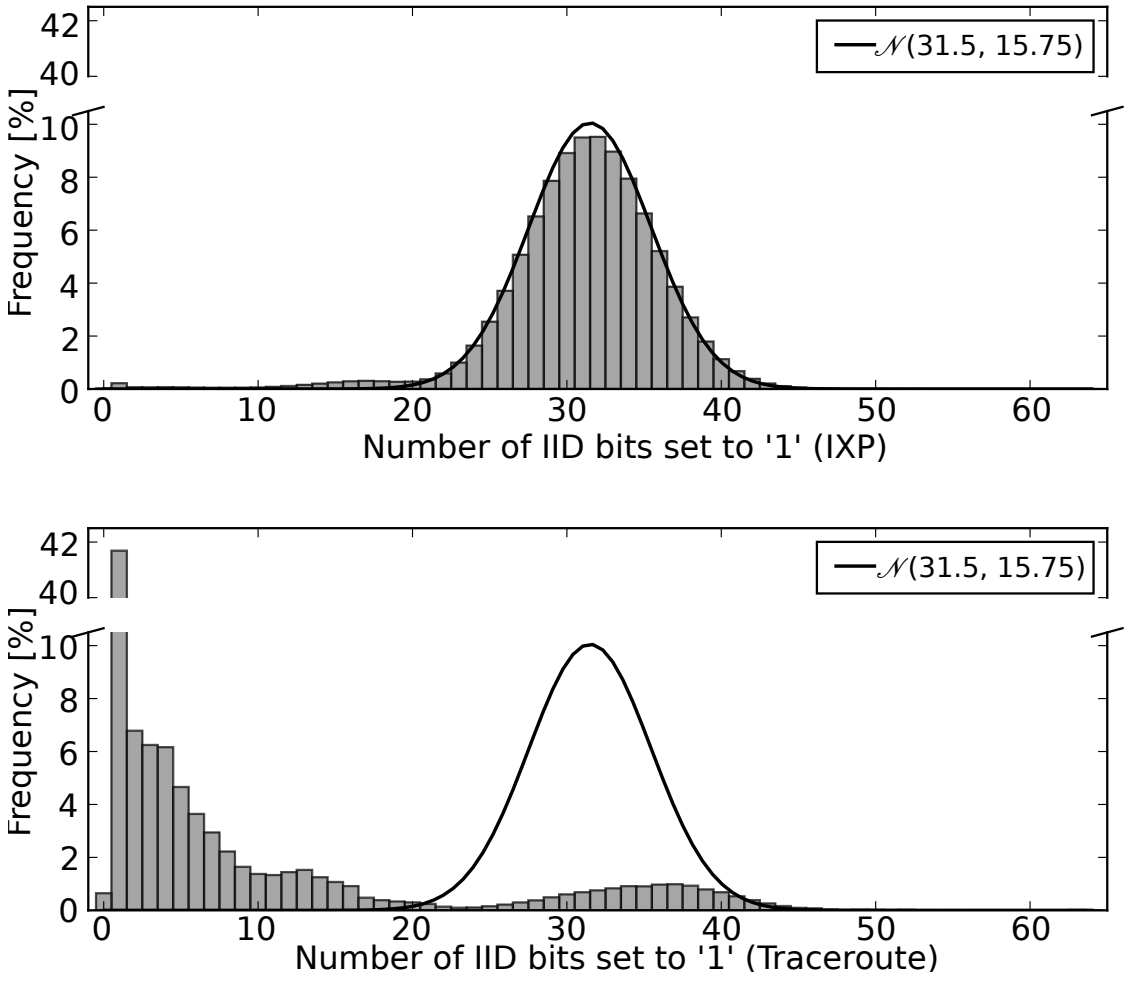
RQ II: How biased are address sources for IPv6 hitlists?

IPv6 hitlist passive vs. active sources: Hamming weight distribution



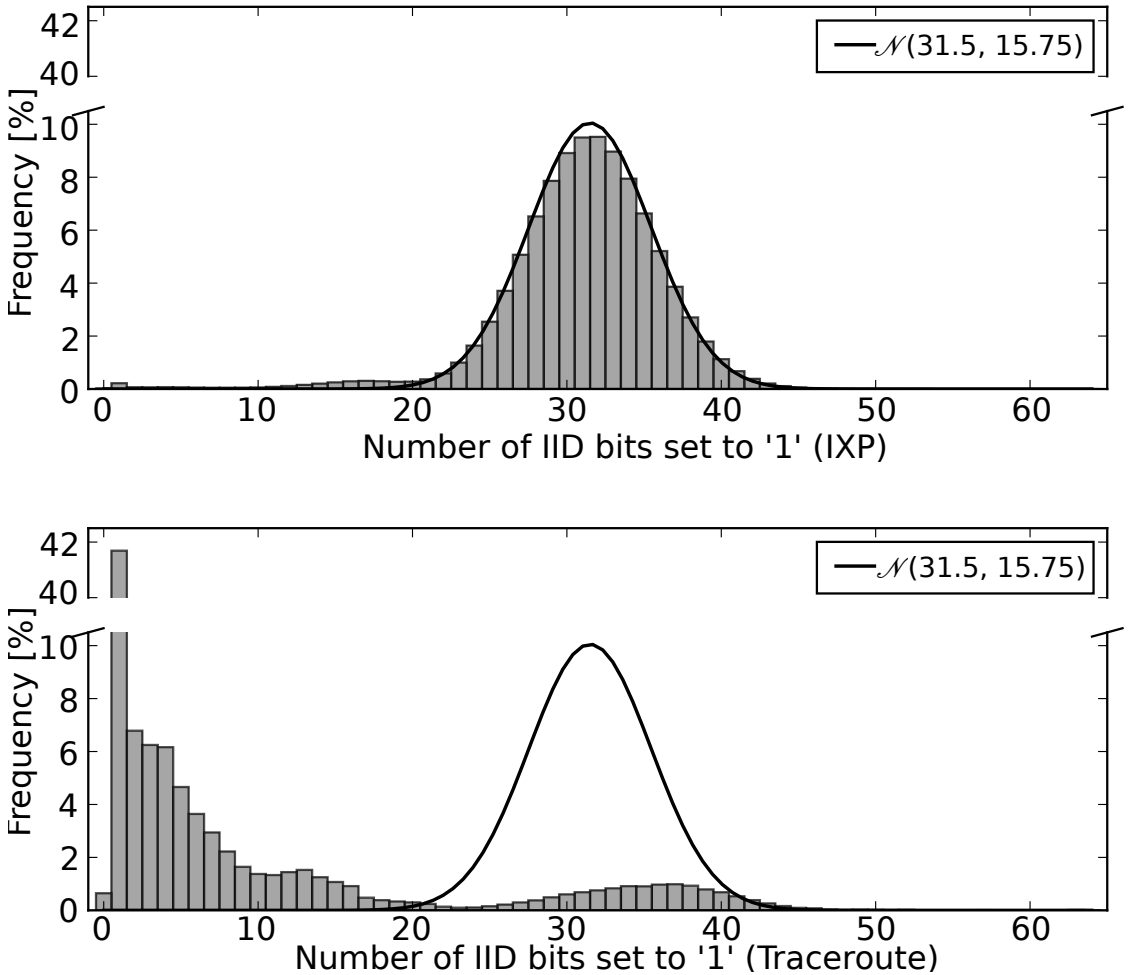
RQ II: How biased are address sources for IPv6 hitlists?

IPv6 hitlist passive vs. active sources: Hamming weight distribution



RQ II: How biased are address sources for IPv6 hitlists?

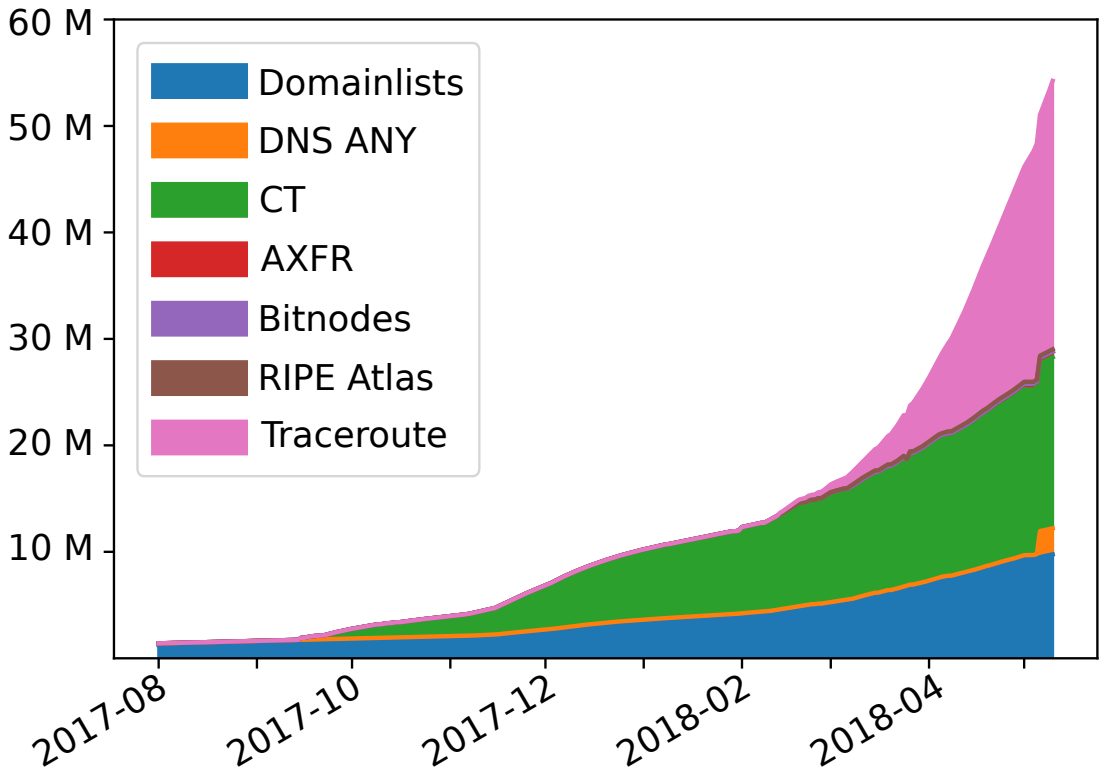
IPv6 hitlist passive vs. active sources: Hamming weight distribution



- Different host populations: clients at IXP (privacy extensions) vs. routers (manually assigned addresses)

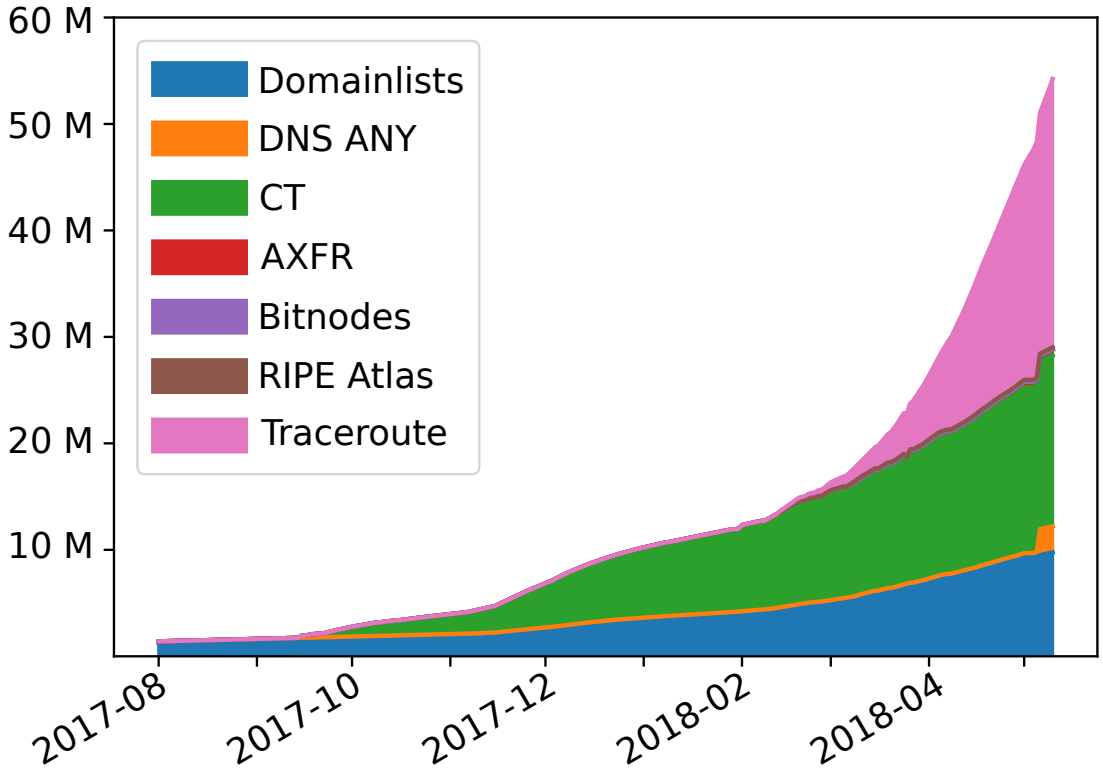
RQ II: How biased are address sources for IPv6 hitlists?

IPv6 hitlist active sources: Cumulative address runup



RQ II: How biased are address sources for IPv6 hitlists?

IPv6 hitlist active sources: Cumulative address runup



- Many addresses from domainlists, CT, and traceroutes
- Rapid increase of traceroute addresses due to CPE routers

RQ II: How biased are address sources for IPv6 hitlists?

Taxonomy

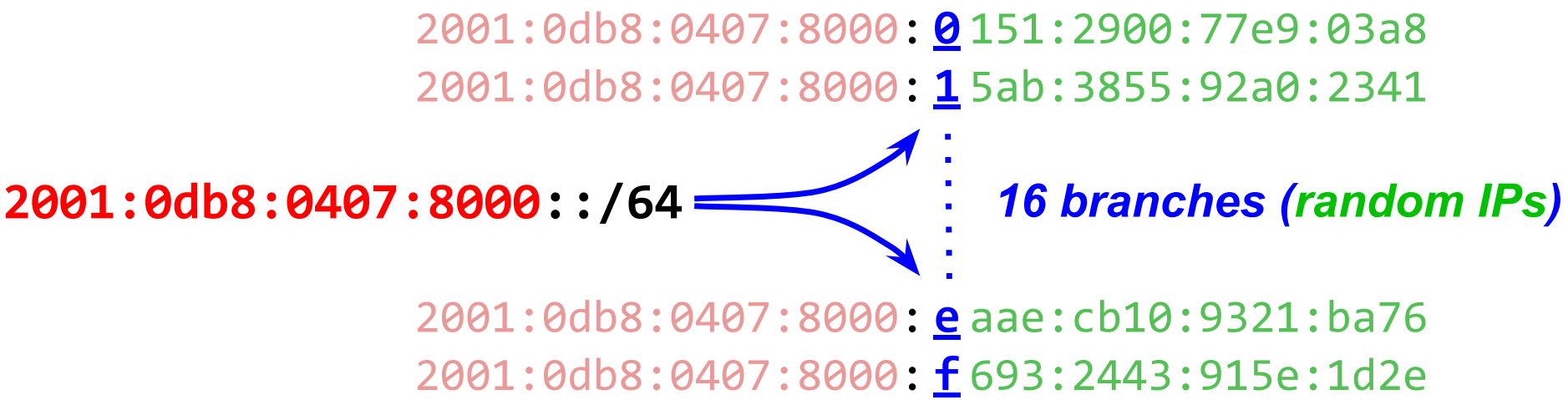
- Alias: another address of the same host
- Aliased prefix: whole prefix bound to the same host
- Bias: some hosts overrepresented due to aliased prefixes

RQ II: How biased are address sources for IPv6 hitlists?

Taxonomy

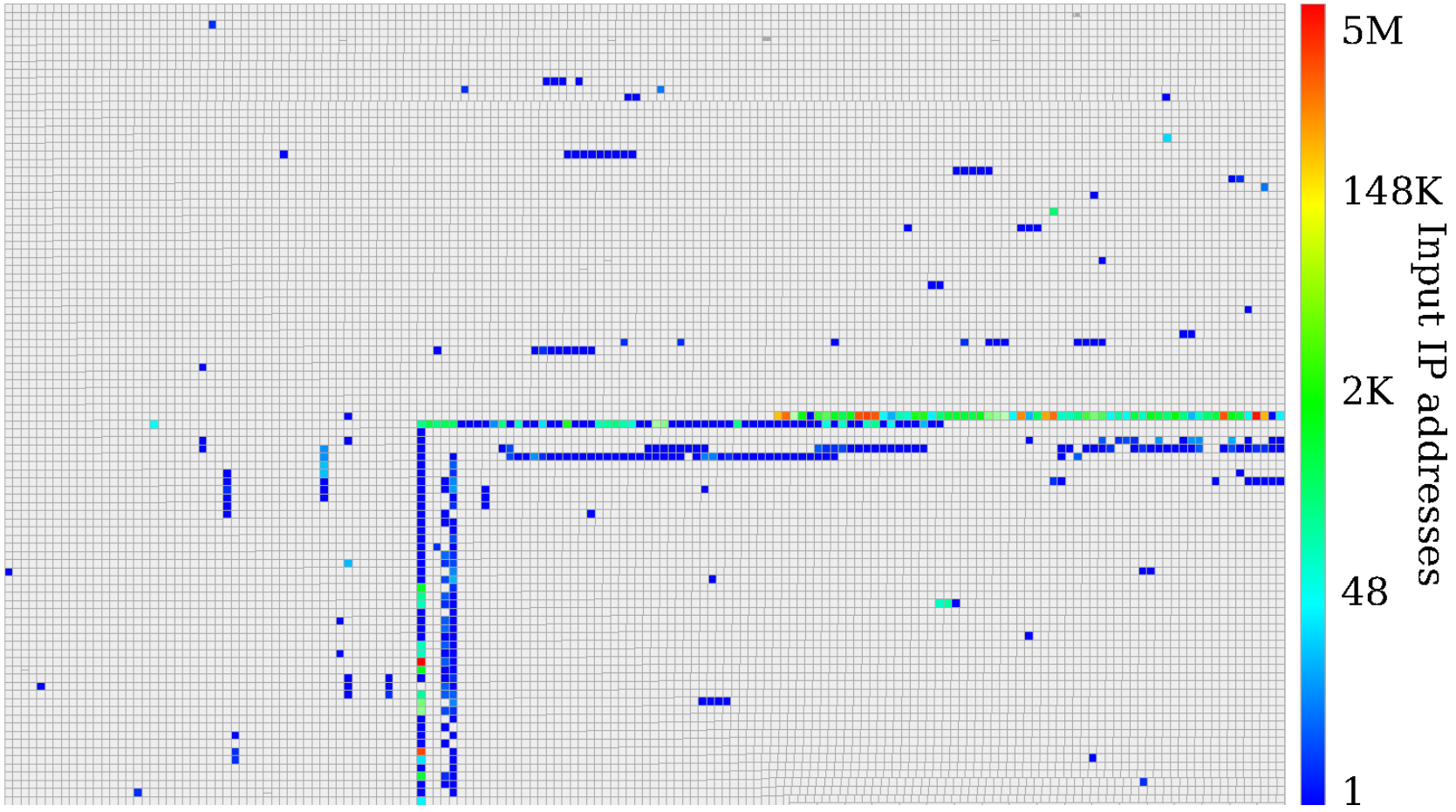
- Alias: another address of the same host
- Aliased prefix: whole prefix bound to the same host
- Bias: some hosts overrepresented due to aliased prefixes

Aliased prefix detection



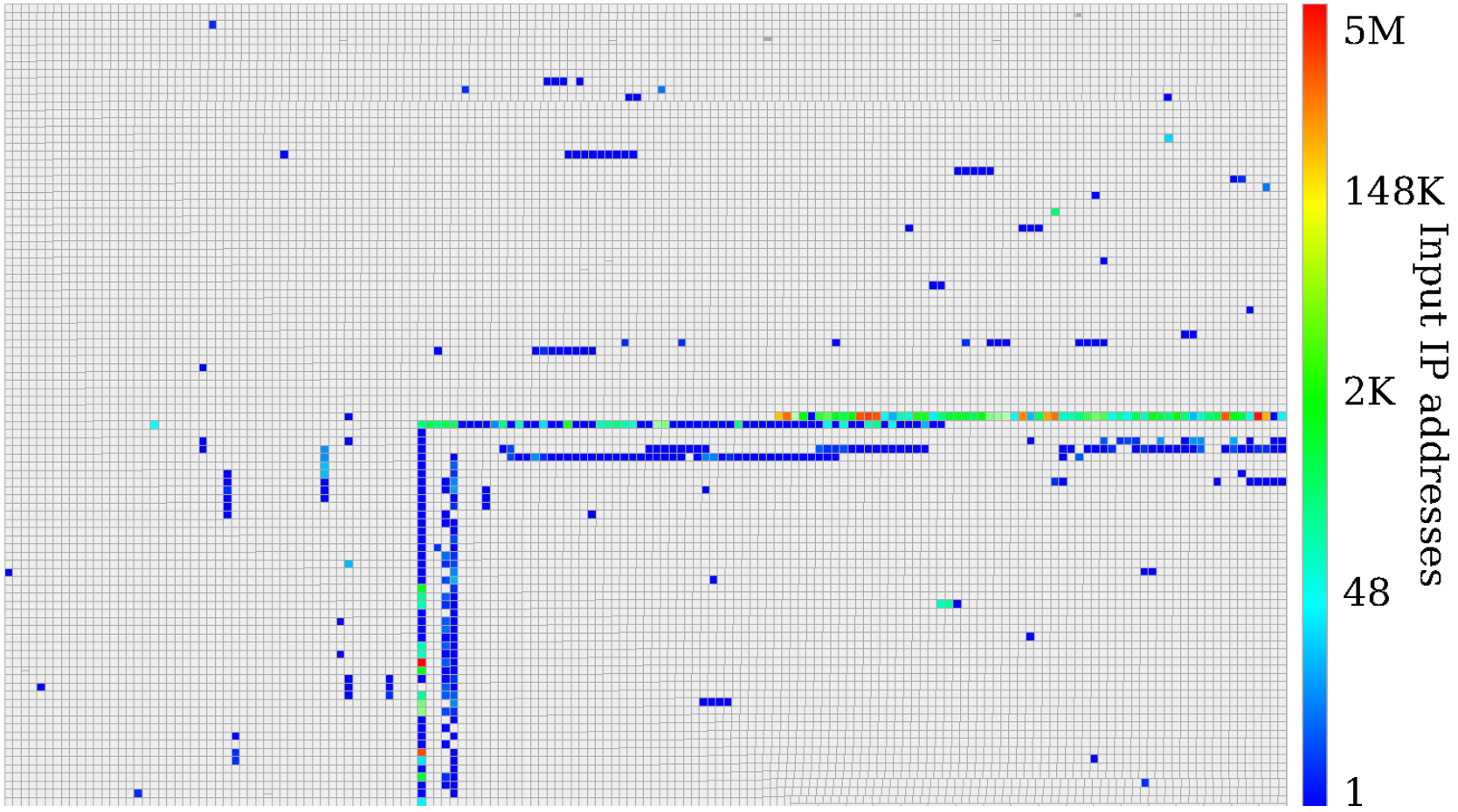
RQ II: How biased are address sources for IPv6 hitlists?

Detected aliased prefixes



RQ II: How biased are address sources for IPv6 hitlists?

Detected aliased prefixes

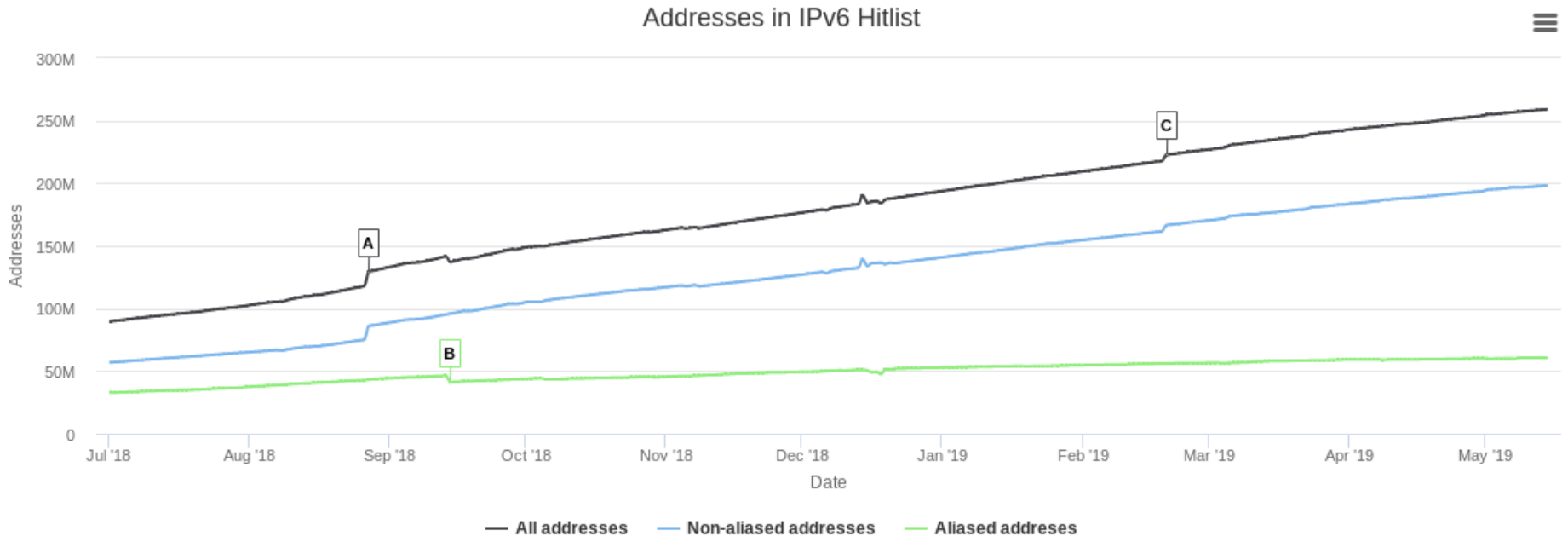


- Only 3.2 % of prefixes are aliased
- But 46.6 % of addresses are in aliased prefixes → bias

RQ II: How biased are address sources for IPv6 hitlists?

IPv6 Hitlist Service

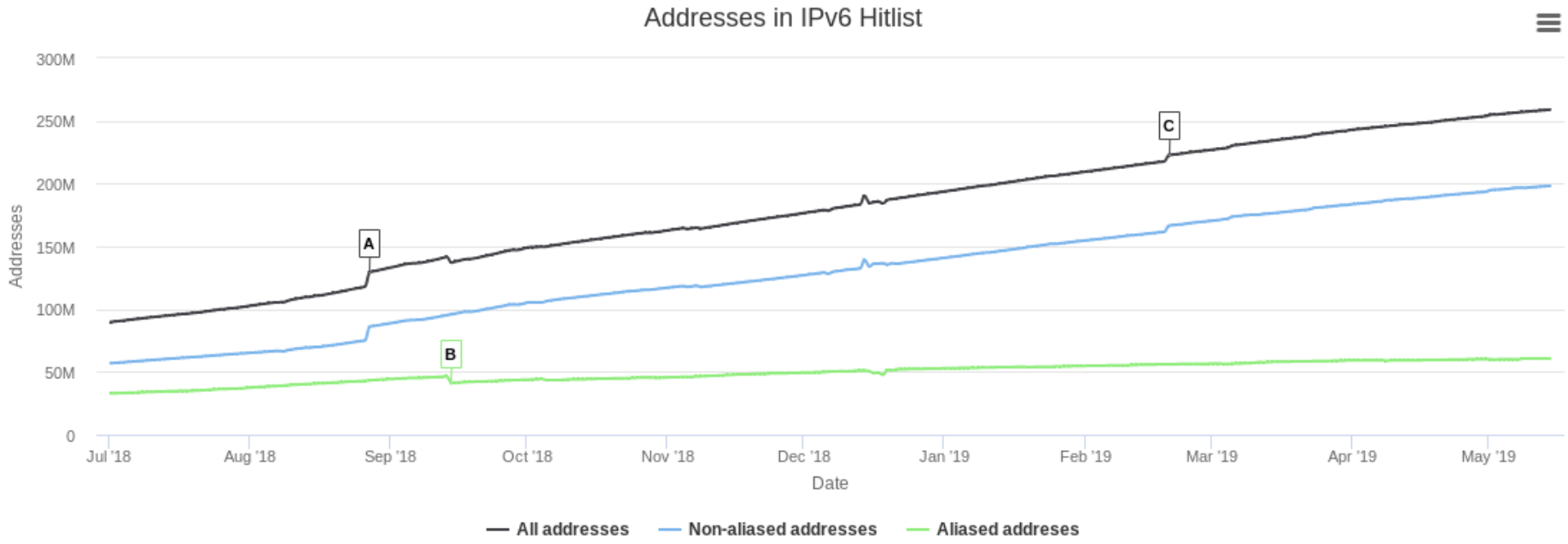
We provide an IPv6 Hitlist Service where we publish **responsive IPv6 addresses, aliased prefixes, and non-aliased prefixes** to interested researchers. The IPv6 Hitlist Service consists of an openly accessible one and a registration-first service.



RQ II: How biased are address sources for IPv6 hitlists?

IPv6 Hitlist Service

We provide an IPv6 Hitlist Service where we publish **responsive IPv6 addresses, aliased prefixes, and non-aliased prefixes** to interested researchers. The IPv6 Hitlist Service consists of an openly accessible one and a registration-first service.



- Daily publication
  - Responsive IPv6 addresses for 5 protocol-port combinations
  - Aliased and non-aliased IPv6 prefixes
- Dozens of fellow researchers have access

RQ II: How biased are address sources for IPv6 hitlists?

Summary

- Identified different types of biases in IPv6 hitlist sources
  - Distort targets by almost 50 %
  - Biases can be detected
- IPv6 Hitlist Service provides fellow researchers with access to daily IPv6 address data

Publications (this research question)

- *Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczynski, Stephen D. Strowes, Luuk Hendriks, and Georg Carle*, “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”, **IMC’18**.
- *Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle*, “Scanning the IPv6 Internet: Towards a Comprehensive Hitlist”, **TMA’16**.

Research questions

RQ I: How can we perform Internet-scale IPv6 measurements? Chapter 3

ZMapv6 goscanner

RQ II: How biased are address sources for IPv6 hitlists? Chapter 4

Passive sources Active sources Biases in sources IPv6 Hitlist Service

RQ III: Are HTTPS servers still vulnerable to MitM attacks? Chapter 5

Certificate security HTTPS security

RQ IV: Are BACnet devices vulnerable to amplification attacks? Chapter 6

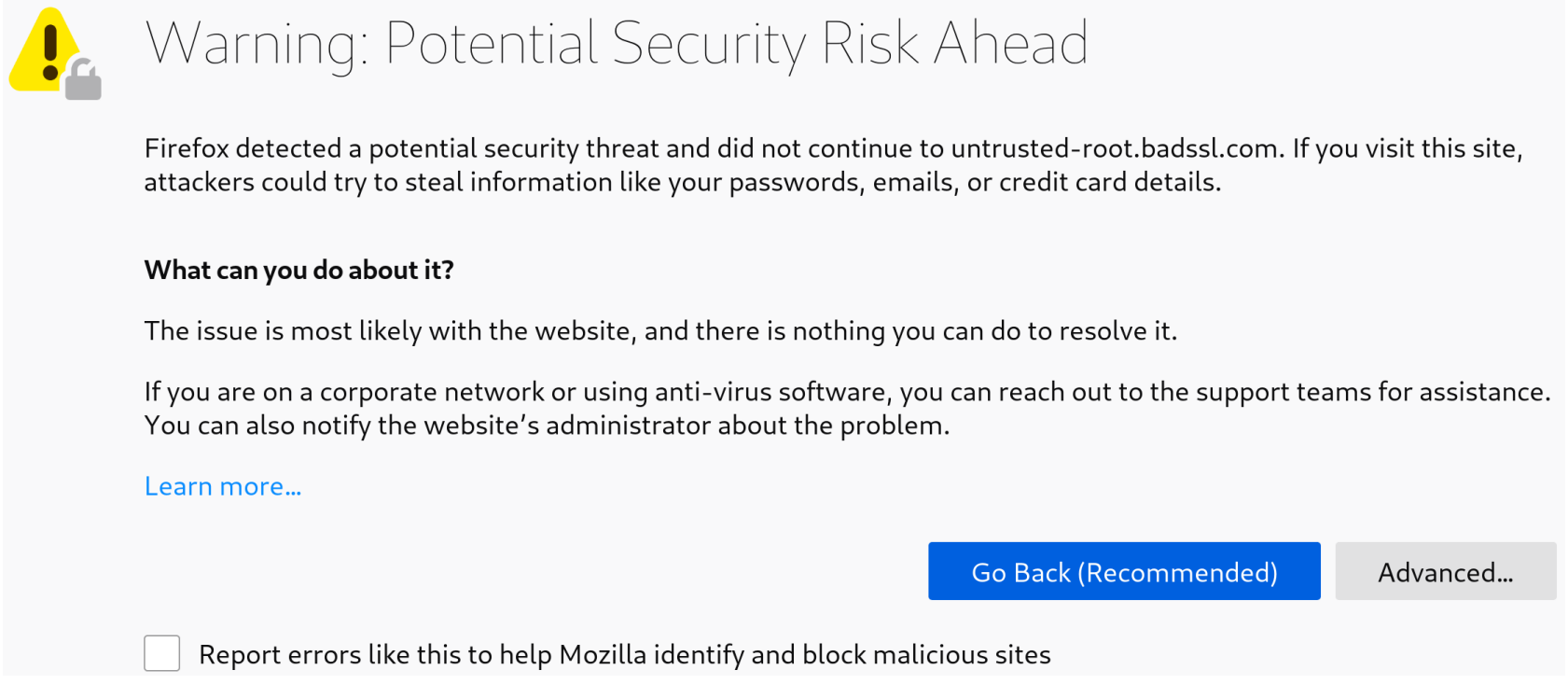
Deployment Amplification Notification

RQ V: Are IPMI devices vulnerable to MitM attacks? Chapter 7

Deployment TLS security

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

RQ III: Are HTTPS servers still vulnerable to MitM attacks?



RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Motivation

- HTTPS ecosystem experienced many security issues which allow for MitM attacks (e.g., misissued certificates, weak keys, CA breaches)
- A number of HTTPS security extensions have been proposed to make the HTTPS ecosystem more secure

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Motivation

- HTTPS ecosystem experienced many security issues which allow for MitM attacks (e.g., misissued certificates, weak keys, CA breaches)
- A number of HTTPS security extensions have been proposed to make the HTTPS ecosystem more secure

Measurements & analyses

- Active measurements
- Empirical analysis of different HTTPS ecosystem weaknesses
  - Insecure certificates
  - Downgrade from HTTPS to HTTP
  - Misissued certificates

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Baseline Requirements (BRs)

- Rules regarding certificates and issuing processes which CAs adhere to
- Devised within the CA/Browser Forum
- Each requirement has an enforcement date

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Baseline Requirements (BRs)

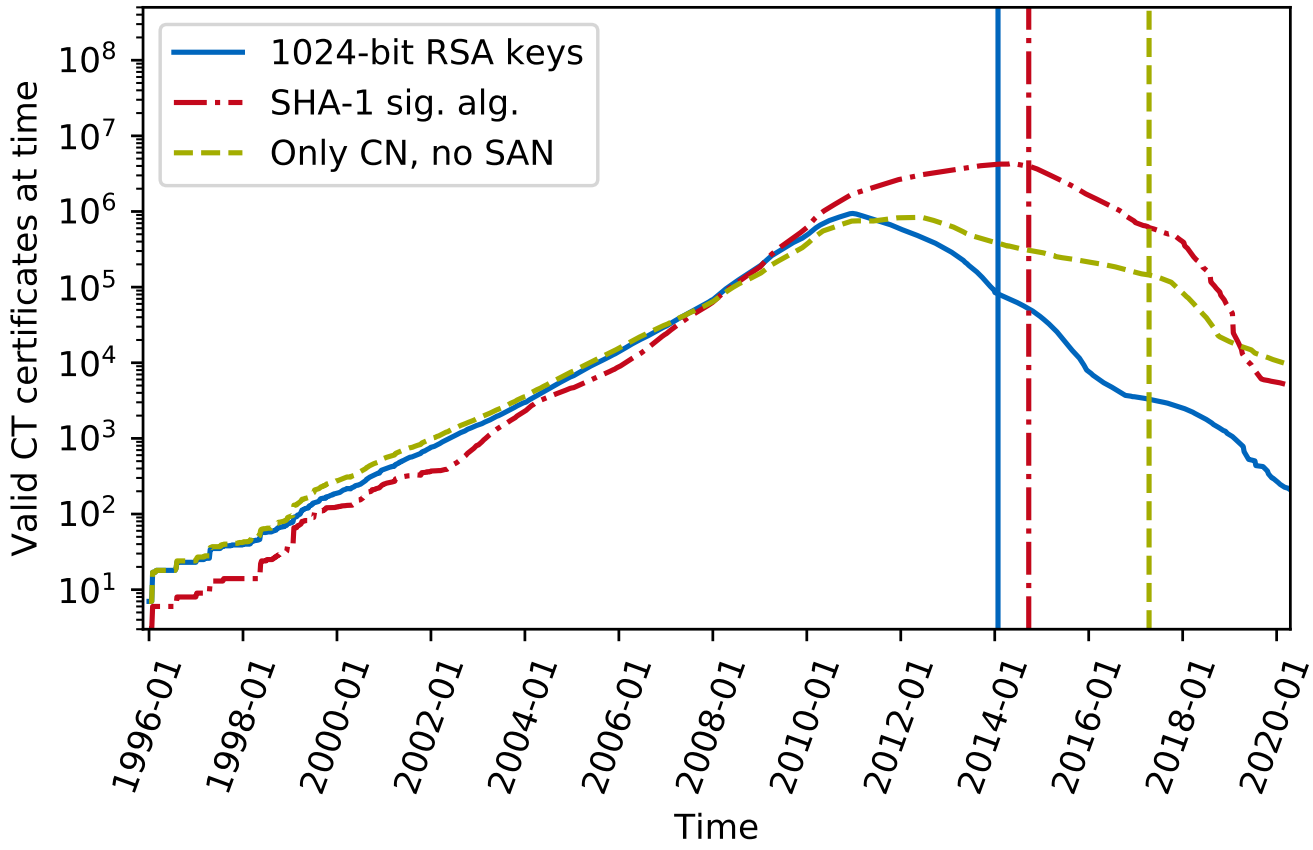
- Rules regarding certificates and issuing processes which CAs adhere to
- Devised within the CA/Browser Forum
- Each requirement has an enforcement date

Analyze BR adherence of all certificates in Certificate Transparency (CT) logs

- Must not use 1024 bit keys
- Must not use SHA-1 signature algorithm
- Must contain SAN in addition to CN

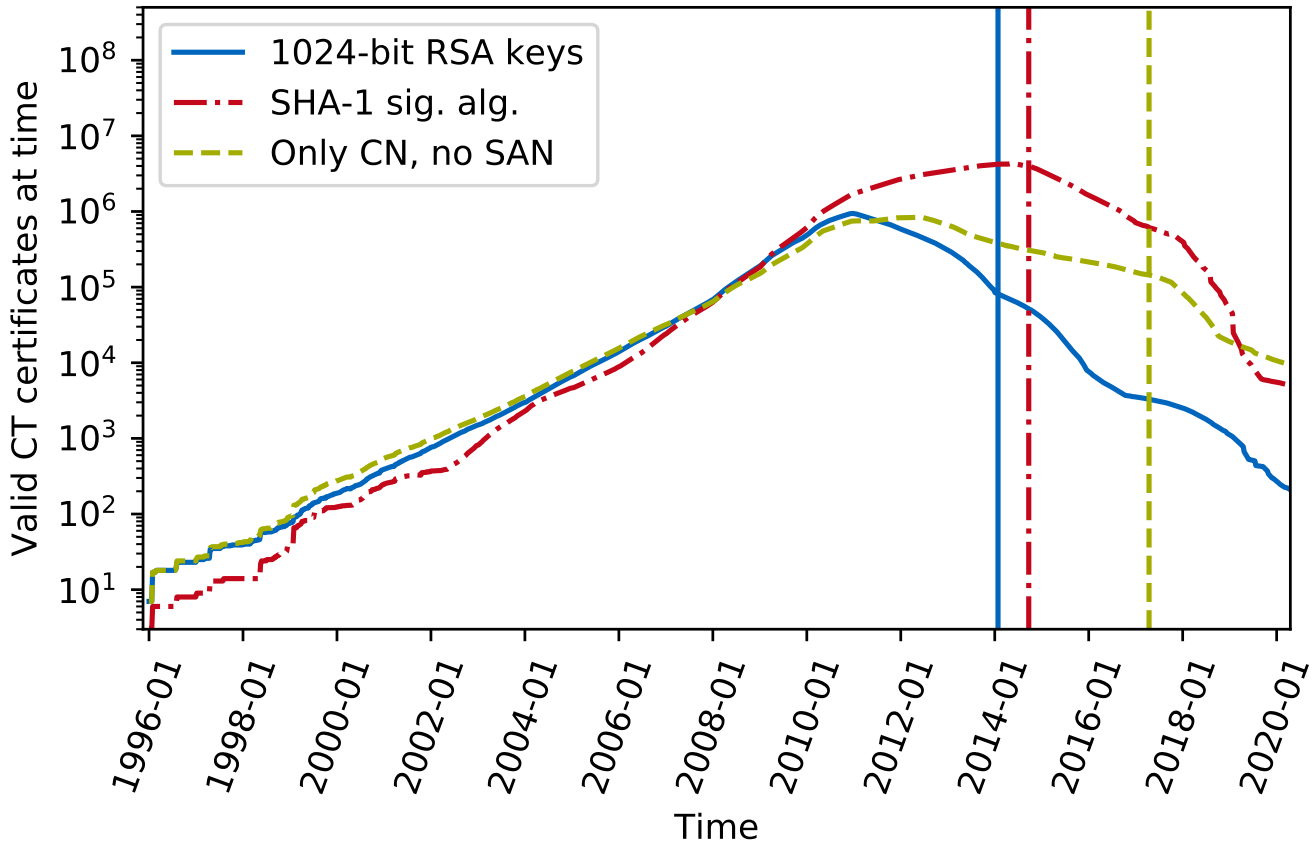
RQ III: Are HTTPS servers still vulnerable to MitM attacks?

BR violations of certificates in CT logs



RQ III: Are HTTPS servers still vulnerable to MitM attacks?

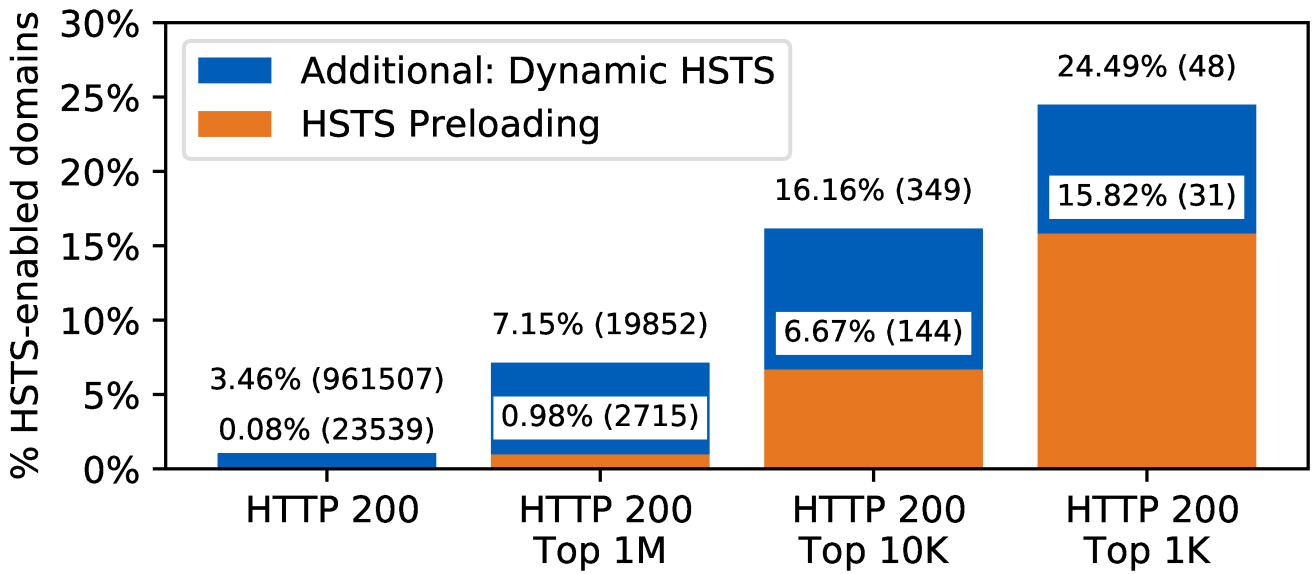
BR violations of certificates in CT logs



- Enforcement of stricter rules helps curb the number of insecure certificates
- But: Many valid insecure certificates are found in CT logs

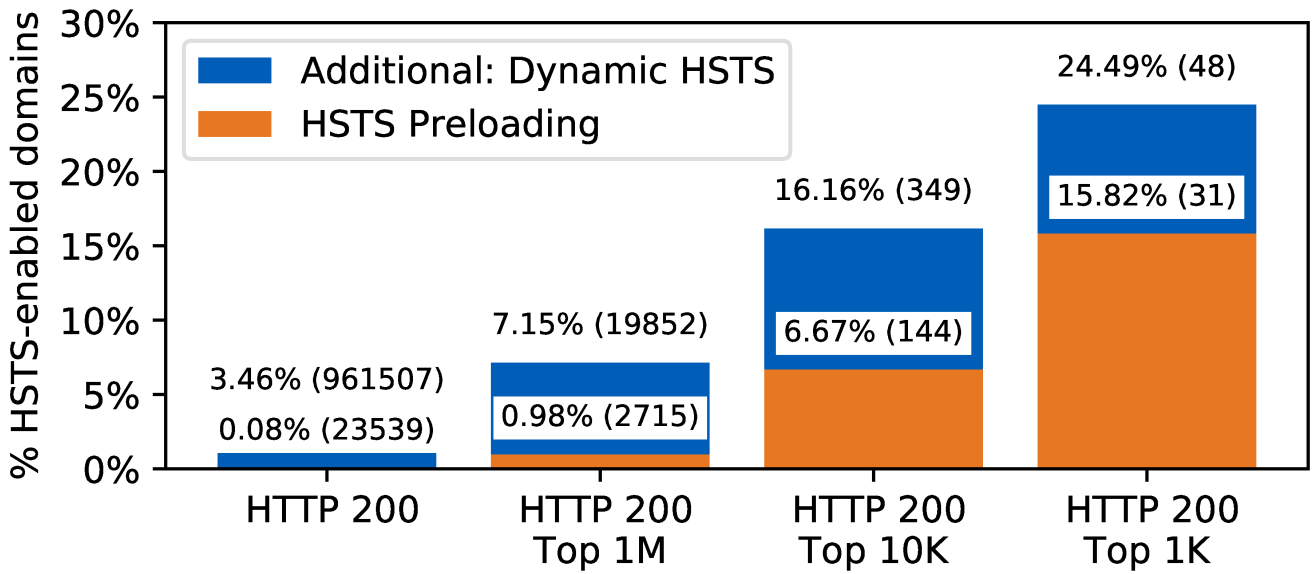
RQ III: Are HTTPS servers still vulnerable to MitM attacks?

HTTP Strict Transport Security (HSTS) deployment



RQ III: Are HTTPS servers still vulnerable to MitM attacks?

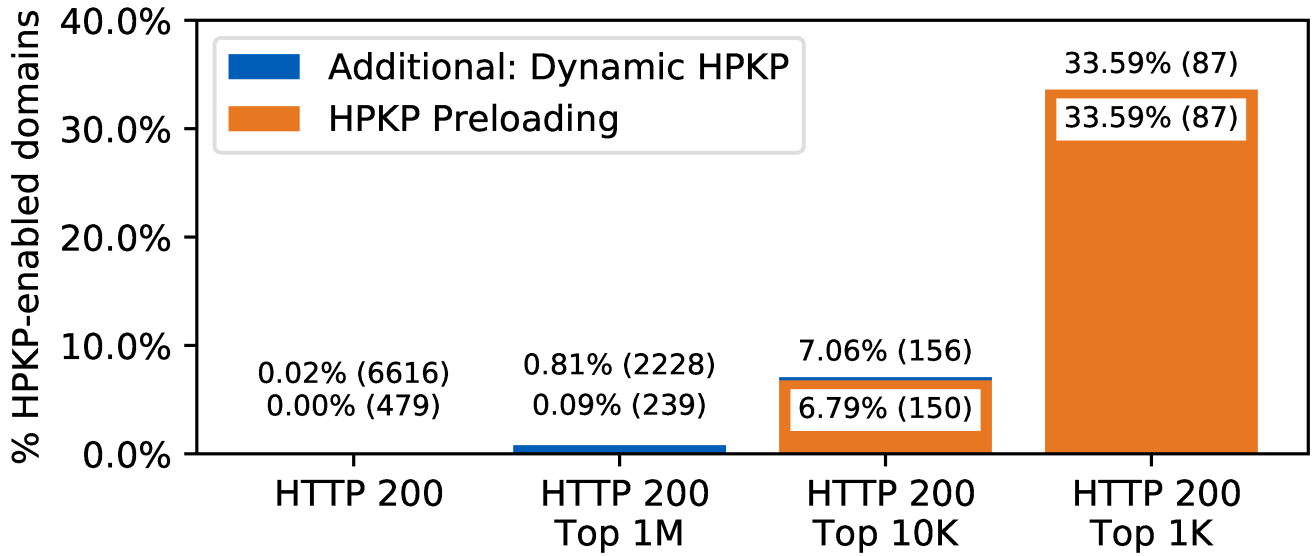
HTTP Strict Transport Security (HSTS) deployment



- Significant usage among top domains
- Preloading highly used among top domains, smaller usage among general population

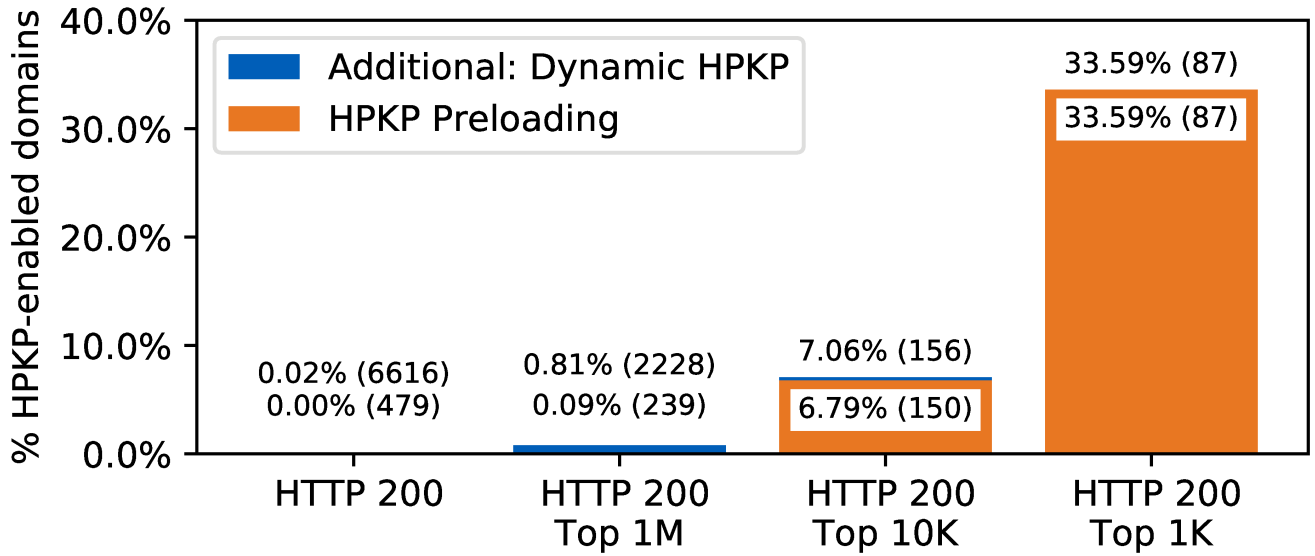
RQ III: Are HTTPS servers still vulnerable to MitM attacks?

HTTP Public Key Pinning (HPKP) deployment



RQ III: Are HTTPS servers still vulnerable to MitM attacks?

HTTP Public Key Pinning (HPKP) deployment



- Low usage among general population
- High usage through preloading among top domains

RQ III: Are HTTPS servers still vulnerable to MitM attacks?

Summary

- Thousands of insecure certificates are still valid
- High usage of HSTS and HPKP among top domains, mostly due to preloading
- Insecure certificates and lack of HTTPS security techniques make hosts vulnerable to Man-in-the-Middle attacks

Publications (this research question)

- *Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle*, “In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements”, **PAM’18**.
- *Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch*, “The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem”, **IMC’18**.
- *Johanna Amann, Oliver Gasser, Quirin Scheitle, Lexi Brent, Georg Carle, and Ralph Holz*, “Mission Accomplished? HTTPS Security after DigiNotar”, **IMC’17**.

Comparison to related work

Comparison to related work

	Holz (2014) [8]	Durumeric (2017) [2]	Fiebig (2017) [3]	Hendriks (2019) [7]
IPv6 measurements	✗	✗	✓	✓
Bias analyses	✗	✗	✓	✗
HTTPS security analyses	✓	✓	✗	✗
Reproducibility efforts	✗	✗	✓	✗
Measurement service	✗	✓	✗	✗

Comparison to related work

	Holz (2014) [8]	Durumeric (2017) [2]	Fiebig (2017) [3]	Hendriks (2019) [7]	**This dissertation**
IPv6 measurements	✗	✗	✓	✓	✓
Bias analyses	✗	✗	✓	✗	✓
HTTPS security analyses	✓	✓	✗	✗	✓
Reproducibility efforts	✗	✗	✓	✗	✓
Measurement service	✗	✓	✗	✗	✓

Key contributions

Key contributions

- Internet measurement methodology
  - Largest IPv6 hitlist to date
  - Extensive bias analyses in hitlist sources
  - IPv6 Hitlist Service
- HTTPS security
  - Thousands of insecure certificates
  - Millions of domains lacking HTTPS security extensions
  - Man-in-the-Middle attacks still possible

Key contributions

- Internet measurement methodology
  - Largest IPv6 hitlist to date
  - Extensive bias analyses in hitlist sources
  - IPv6 Hitlist Service
- HTTPS security
  - Thousands of insecure certificates
  - Millions of domains lacking HTTPS security extensions
  - Man-in-the-Middle attacks still possible

Publications (this talk)

- *Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle*, “In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements”, **PAM’18**. **Best Paper Award**.
- *Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczynski, Stephen D. Strowes, Luuk Hendriks, and Georg Carle*, “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”, **IMC’18**.
- *Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch*, “The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem”, **IMC’18**.
- *Johanna Amann, Oliver Gasser, Quirin Scheitle, Lexi Brent, Georg Carle, and Ralph Holz*, “Mission Accomplished? HTTPS Security after DigiNotar”, **IMC’17**. **Community Contribution Award, IRTF Applied Networking Research Prize**.
- *Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle*, “Scanning the IPv6 Internet: Towards a Comprehensive Hitlist”, **TMA’16**.

Bibliography

[1] Johanna Amann, Oliver Gasser, Quirin Scheitle, Lexi Brent, Georg Carle, and Ralph Holz. “Mission Accomplished? HTTPS Security after DigiNotar”. In: IMC’17. Community Contribution Award, IRTF Applied Networking Research Prize. ACM. London, United Kingdom, Nov. 2017, pp. 325–340.

[2] Zakir Durumeric. “Fast Internet-Wide Scanning: A New Security Perspective”. PhD thesis. University of Michigan, 2017.

[3] Tobias Fiebig. “An Empirical Evaluation of Misconfiguration in Internet Services”. PhD thesis. Technische Universität Berlin, 2017.

[4] Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle. “In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements”. In: PAM’18. Best Paper Award. Springer. Berlin, Germany, Mar. 2018, pp. 173–185.

[5] Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczynski, Stephen D. Strowes, Luuk Hendriks, and Georg Carle. “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”. In: IMC’18. ACM. Boston, MA, USA, Nov. 2018. DOI: 10.1145/3278532.3278564.

[6] Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle. “Scanning the IPv6 Internet: Towards a Comprehensive Hitlist”. In: TMA’16. IFIP. Louvain-la-Neuve, Belgium, Apr. 2016.

[7] Luuk Hendriks. “Measuring IPv6 Resilience and Security”. PhD thesis. University of Twente, 2019.

[8] Ralph-Günther Holz. “Empirical Analysis of Public Key Infrastructures and Investigation of Improvements”. PhD thesis. Technical University of Munich, 2014.

Bibliography

[9] IMC'18. ACM. Boston, MA, USA, Nov. 2018.

[10] Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch. "The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem". In: IMC'18. ACM. Boston, MA, USA, Nov. 2018, pp. 343–349. ISBN: 978-1-4503-5619-0. DOI: 10.1145/3278532.3278562.