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

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

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
- gosscanner

**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?**
- ZMapv6
- goscanner

Chapter 3

**RQ II: How biased are address sources for IPv6 hitlists?**
- Passive sources
- Active sources
- Biases in sources
- IPv6 Hitlist Service

Chapter 4

**RQ III: Are HTTPS servers still vulnerable to MitM attacks?**
- Certificate security
- HTTPS security

Chapter 5

**RQ IV: Are BACnet devices vulnerable to amplification attacks?**
- Deployment
- Amplification
- Notification

Chapter 6

**RQ V: Are IPMI devices vulnerable to MitM attacks?**
- Deployment
- TLS security

Chapter 7
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?
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

% of unique IPs per day that are new

Weekend

Weekend

IXP

MWN

Date

2015-09-03
2015-09-04
2015-09-05
2015-09-06
2015-09-07
2015-09-08
2015-09-09
2015-09-10
2015-09-11
2015-09-12
2015-09-13
2015-09-14
2015-09-15
2015-09-16

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

- 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 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

- Domainlists
- DNS ANY
- CT
- AXFR
- Bitnodes
- RIPE Atlas
- Traceroute

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

```
2001:0db8:0407:8000::/64
2001:0db8:0407:8000: 0 151:2900:77e9:03a8
2001:0db8:0407:8000: 1 5ab:3855:92a0:2341
16 branches (random IPs)
```
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.

Addresses in IPv6 Hitlist

- All addresses
- Non-aliased addresses
- Aliased addresses
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)

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?

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to untrusted-root.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website’s administrator about the problem.

Learn more...

Go Back (Recommended)  Advanced...

Report errors like this to help Mozilla identify and block malicious sites
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

- 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?

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

<table>
<thead>
<tr>
<th></th>
<th>Additional: Dynamic HSTS</th>
<th>HSTS Preloading</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP 200</td>
<td>3.46% (961507)</td>
<td>0.08% (23539)</td>
</tr>
<tr>
<td>HTTP Top 1M</td>
<td>0.98% (2715)</td>
<td></td>
</tr>
<tr>
<td>HTTP Top 10K</td>
<td>6.67% (144)</td>
<td></td>
</tr>
<tr>
<td>HTTP Top 1K</td>
<td>24.49% (48)</td>
<td>15.82% (31)</td>
</tr>
</tbody>
</table>
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

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

![Graph showing HPKP deployment](image)
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)

Comparison to related work
Comparison to related work

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 measurements</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bias analyses</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HTTPS security analyses</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Reproducibility efforts</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Measurement service</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
### Comparison to related work

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 measurements</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bias analyses</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>HTTPS security analyses</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Reproducibility efforts</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Measurement service</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>
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

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.
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)


