Bamboozling Certificate Authorities with BGP

Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, Prateek Mittal
Digital certificates as a root of trust

- **Root of trust** on the internet
- Bootstraps trust on **first time connections**
- The **keys** to all web encryption
Digital certificates as a root of trust

- Root of trust on the internet
- Bootstraps trust on first time connections
- The keys to all web encryption

Border Gateway Protocol (BGP) attacks compromise this root of trust
Overview

● Domain Control Validation
● BGP Attacks
● Quantifying Vulnerability
● Countermeasures
● Takeaways
Domain Control Verification

Could I get a certificate for example.com?

(Certificate Signing Request)

Certificate Authority

Server at example.com

Owner of example.com
Domain Control Verification

Certificate Authority

Upload <content> to example.com/verify.html (Domain Control Verification Challenge)

Owner of example.com

Server at example.com
Domain Control Verification

Certificate Authority

Server at example.com

Server modifications

Owner of example.com
Domain Control Verification

HTTP GET example.com/verify.html

Certificate Authority

Server at example.com

Owner of example.com

I did it!
Domain Control Verification

Here is your certificate

Certificate Authority

Server at example.com

HTTP 200 OK: <content>

Here is your certificate

Owner of example.com
Where BGP Comes In

If an adversary can hijack this request with BGP, it can generate a response.
Overview

- Domain Control Validation
- BGP Attacks
- Quantifying Vulnerability
- Countermeasures
- Takeaways
Original BGP route to victim

Certificate Authority

AS 1

AS containing example.com

AS 2

AS 3

AS 4

Adversary
Original BGP route to victim

Certificate Authority

AS 1

I own 2.2.2.0/23

AS containing example.com

AS 3

AS 4

Adversary
BGP route to victim under sub-prefix attack

- **Certificate Authority**
- **Adversary**: I own sub-prefix 2.2.2.0/24
- **AS 1**: Certificate Authority
- **AS 2**, **AS 3**, **AS 4**: I own 2.2.2.0/23
- **AS containing example.com**: I own 2.2.2.0/23

Diagram:
- Self-loops on **AS 2**, **AS 3**, **AS 4**
- Adversary attacking AS 1
BGP route to victim under sub-prefix attack

Certificate Authority

AS 1

I own sub-prefix 2.2.2.0/24

AS 3

HTTP GET example.com/verify.html goes to adversary

AS 4

I own 2.2.2.0/23

Adversary

I own sub-prefix 2.2.2.0/24

AS 2
BGP route to victim under sub-prefix attack

Certificate Authority

Adversary

AS 1

I own sub-prefix 2.2.2.0/24

AS 2

I own sub-prefix 2.2.2.0/23

AS 3

AS 4

- Routers prefer more specific announcements
- Global visibility
- Connectivity broken
- Not very stealthy
A local (equally-specific prefix) attack

A. Gavrichenkov. Breaking HTTPS with BGP hijacking. Black Hat USA Briefings, 2015
A local (equally-specific prefix) attack

A. Gavrichenkov. Breaking HTTPS with BGP hijacking. Black Hat USA Briefings, 2015
A local (equally-specific prefix) attack

- Equally specific announcements compete for traffic
- Announcement localized
- Local broken connectivity
- Potentially stealthy

A. Gavrichenkov. Breaking HTTPS with BGP hijacking. Black Hat USA Briefings, 2015
A local (equally-specific prefix) attack

- Equally specific announcements compete for traffic
- Announcement localized
- Local broken connectivity
- Potentially stealthy
- Not all ASes can perform

A. Gavrichenkov. Breaking HTTPS with BGP hijacking. Black Hat USA Briefings, 2015
AS path poisoning

I can get to 2.2.2.0/24 through AS 4

I own 2.2.2.0/23

Certificate Authority

Adversary

AS 2

AS 3

AS 4
AS path poisoning

- Everyone sees announcement but looks less suspicious
- Connectivity preserved
- Almost any AS can perform
- Very stealthy
- Perfect setup to intercept traffic with certificate

I can get to 2.2.2.0/24 through AS 4

Certificate Authority

Adversary

AS 1

AS 2

AS 3

AS 4

I own 2.2.2.0/23

AS containing example.com
Ethical framework for launching real-world attacks

- Hijack only our own prefixes
- Domains run on our own prefixes
- No real users attacked
- Approached trusted CAs for certificates
AS path poisoning attack demonstration
## Results from real world attacks

<table>
<thead>
<tr>
<th></th>
<th>Let’s Encrypt</th>
<th>GoDaddy</th>
<th>Comodo</th>
<th>Symantec*</th>
<th>GlobalSign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to issue certificate</td>
<td>35 seconds</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
</tr>
<tr>
<td>Human interaction</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Multiple Vantage Points</td>
<td>Not yet</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Validation Method Attacked</td>
<td>HTTP</td>
<td>HTTP</td>
<td>Email</td>
<td>Email</td>
<td>Email</td>
</tr>
</tbody>
</table>

*At time of experiments Symantec was still a trusted CA*
### Results from real world attacks

<table>
<thead>
<tr>
<th></th>
<th>Let’s Encrypt</th>
<th>GoDaddy</th>
<th>Comodo</th>
<th>Symantec</th>
<th>GlobalSign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to issue certificate</td>
<td>35 seconds</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
<td>&lt; 2 min</td>
</tr>
<tr>
<td>Human interaction</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Multiple Vantage Points</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Validation Method Attacked</td>
<td>HTTP</td>
<td>HTTP</td>
<td>Email</td>
<td>Email</td>
<td>Email</td>
</tr>
</tbody>
</table>

*All studied CAs were vulnerable*

*At time of experiments Symantec was still a trusted CA*
Additional Attacks

- More targets:
  - Authoritative DNS servers
  - Mail servers
Additional Attacks

- More targets:
  - Authoritative DNS servers
  - Mail servers
- Attacking CA prefixes:
  - Reverse (victim domain -> CA) traffic also vulnerable
Overview

● Domain Control Validation
● BGP Attacks
● Quantifying Vulnerability
● Countermeasures
● Takeaways
Quantifying Vulnerability

- How many domains are vulnerable?
- How many adversaries can launch attacks?
Quantifying Vulnerability

- How many domains are vulnerable?
- How many adversaries can launch attacks?

- 1.8 million certificates via Certificate Transparency
- Common names resolved to IPs
- Recorded the BGP routes used for IPs at time of signing
Vulnerability of domains: sub-prefix attacks

- Any AS can launch
- Only prefix lengths less than /24 vulnerable
Vulnerability of domains: sub-prefix attacks

- Any AS can launch
- Only prefix lengths less than /24 vulnerable (filtering)

28% of Domains Unaffected
72% of Domains Vulnerable
Resilience to equally-specific prefix attacks

Lad et al., “Understanding resiliency of Internet topology against prefix hijack attacks”, IEEE DSN, 2007
Resilience to equally-specific prefix attacks

Lad et al., “Understanding resiliency of Internet topology against prefix hijack attacks”, IEEE DSN, 2007
Resilience to equally-specific prefix attacks

Lad et al., “Understanding resiliency of Internet topology against prefix hijack attacks”, IEEE DSN, 2007

- Probability a CA will be resilient to attacks on a domain
Resilience of domains assuming random CA
Resilience of domains assuming random CA

Median resilience is 0.57

43% chance of attack viability
Choosing an affected CA

- CA 1
  - Adversary
  - I own 2.2.2.0/23

- AS 1
  - AS containing example.com

- CA 2
  - Adversary
  - I own 2.2.2.0/23

- AS 3
  - AS 4
  - Hijacked portion
  - Unaffected portion

- • Around 100 CAs
  - • Any one can sign any for domain
Vulnerability of Domains: Equally-specific attacks

- Effective Resilience of Domains
- Average Resilience of Domains

CDF

Resilience
Vulnerability of Domains: Equally-specific attacks

Median resilience drops from .57 to .25

75% chance of attack viability
Overview

- Domain Control Validation
- BGP Attacks
- Quantifying Vulnerability
- Countermeasures
- Takeaways
Multiple Vantage Points

AS 5

AS 1

AS containing example.com

I own 2.2.2.0/23

Unaffected portion

Certificate Authority

AS 3

AS 4

Hijacked portion

I own 2.2.2.0/23

Adversary
Multiple Vantage Points

Remote Vantage Point

AS 1

I own 2.2.2.0/23

AS containing example.com

Unaffected portion

Hijacked portion

Certificate Authority

AS 3

Adversary

AS 4

I own 2.2.2.0/23
Multiple Vantage Points

- **Remote Vantage Point**
- **Certificate Authority**
- **AS 1**
- **AS containing example.com**
- **AS 3**
- **AS 4**
- **Adversary**
- **I own 2.2.2.0/23**

Unaffected portion

Hijacked portion

- Only sign certificate if all vantage points and CA agree
Multiple Vantage Points

- Key factor influencing Let’s Encrypts staging deployment
- Full deployment coming soon

3 Remote Vantage Points in AS 16509

1. 52.29.173.72 - - [29/Jul/2018 18:15:09] "GET /well-...
2. 34.213.106.112 - - [29/Jul/2018 18:15:10] "GET /well-...

Data Center in AS 13649
Resilience Improvement of Multiple Vantage Points

Resilience computed using Let’s Encrypt data center and optimally located additional vantage points.
Resilience Improvement of Multiple Vantage Points

Resilience computed using Let’s Encrypt data center and optimally located additional vantage points

Median resilience improves from .60 to .95
Other Defenses

● CAs:
  ○ BGP Monitoring
  ○ CA Prefix Length
  ○ CA Resilience

● Domains:
  ○ CAA DNS Records
  ○ DNSSEC
Overview

- Domain Control Validation
- BGP Attacks
- Quantifying Vulnerability
- Countermeasures
- Takeaways
Takeaways

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings
Takeaways

Next BGP phishing attack the malicious certificate might be trusted!
Takeaways

- CAs bootstrap trust on the internet through digital certificates
- The majority of domains and CAs are vulnerable
- CAs must implement countermeasures soon
- Secure routing (i.e., BGPsec, RPKI, SCION) is still important even with end-to-end encryption

Thanks to support from

More information at https://secure-certificates.princeton.edu/
Takeaways

- CAs bootstrap trust on the internet through digital certificates
- The majority of domains and CAs are vulnerable
- CAs must implement countermeasures soon
- Secure routing (i.e., BGPsec, RPKI, SCION) is still important even with end-to-end encryption

Questions?

More information at https://secure-certificates.princeton.edu/