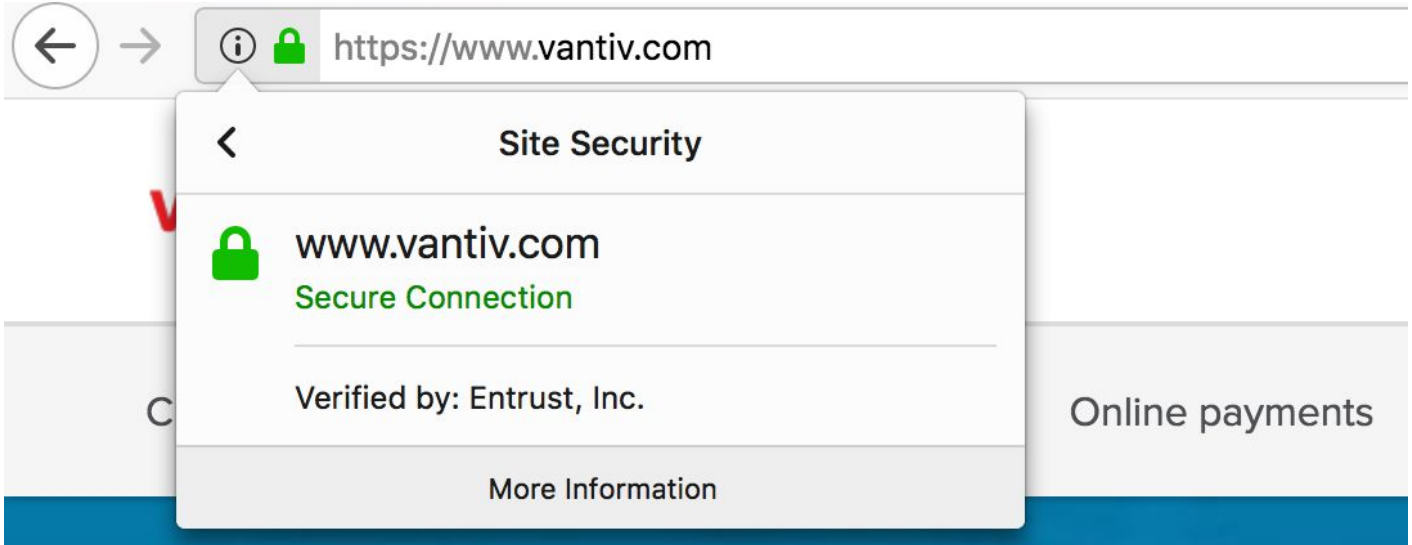
Bamboozling Certificate Authorities with BGP

Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, Prateek Mittal

PRINCETON UNIVERSITY

Digital certificates as a root of trust

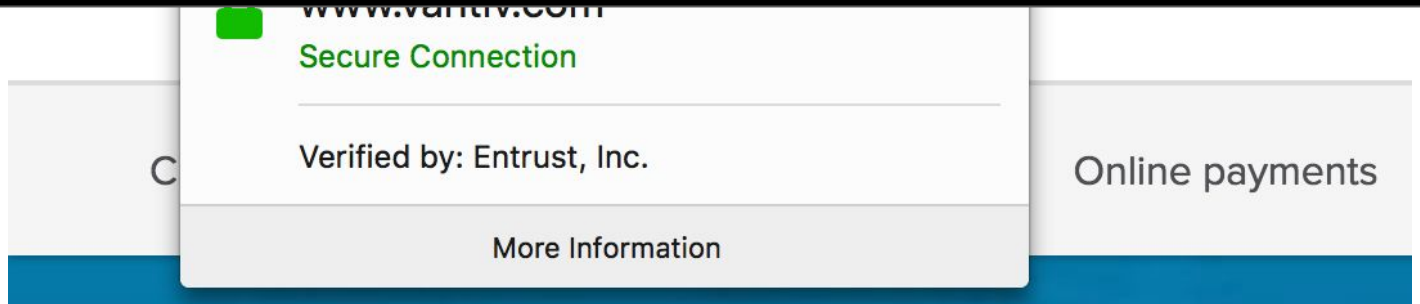
- **Root of trust** on the internet
- Bootstraps trust on **first time connections**
- The **keys** to all web encryption



Digital certificates as a root of trust

-
-
-

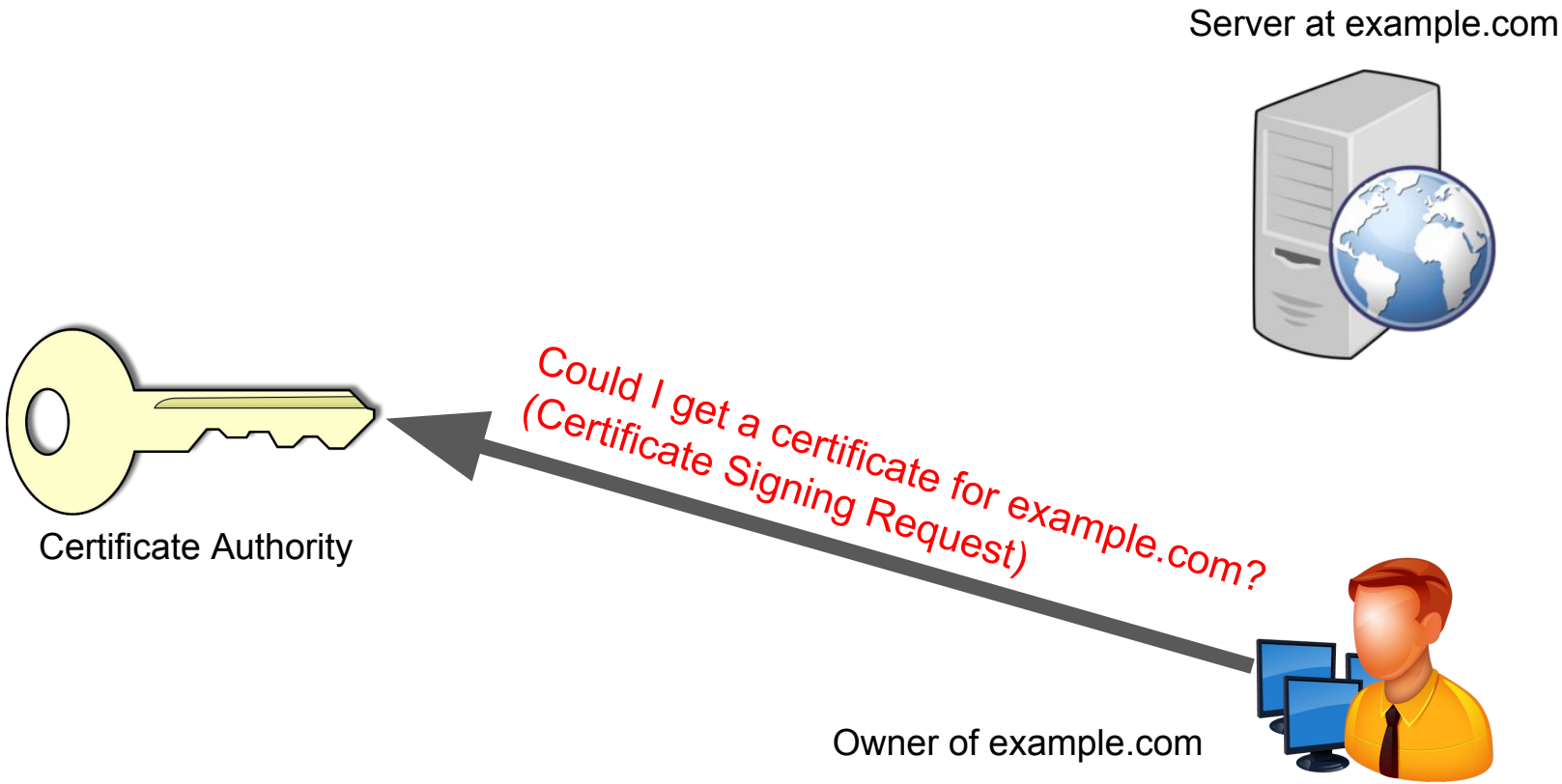
Border Gateway Protocol (BGP) attacks compromise this root of trust



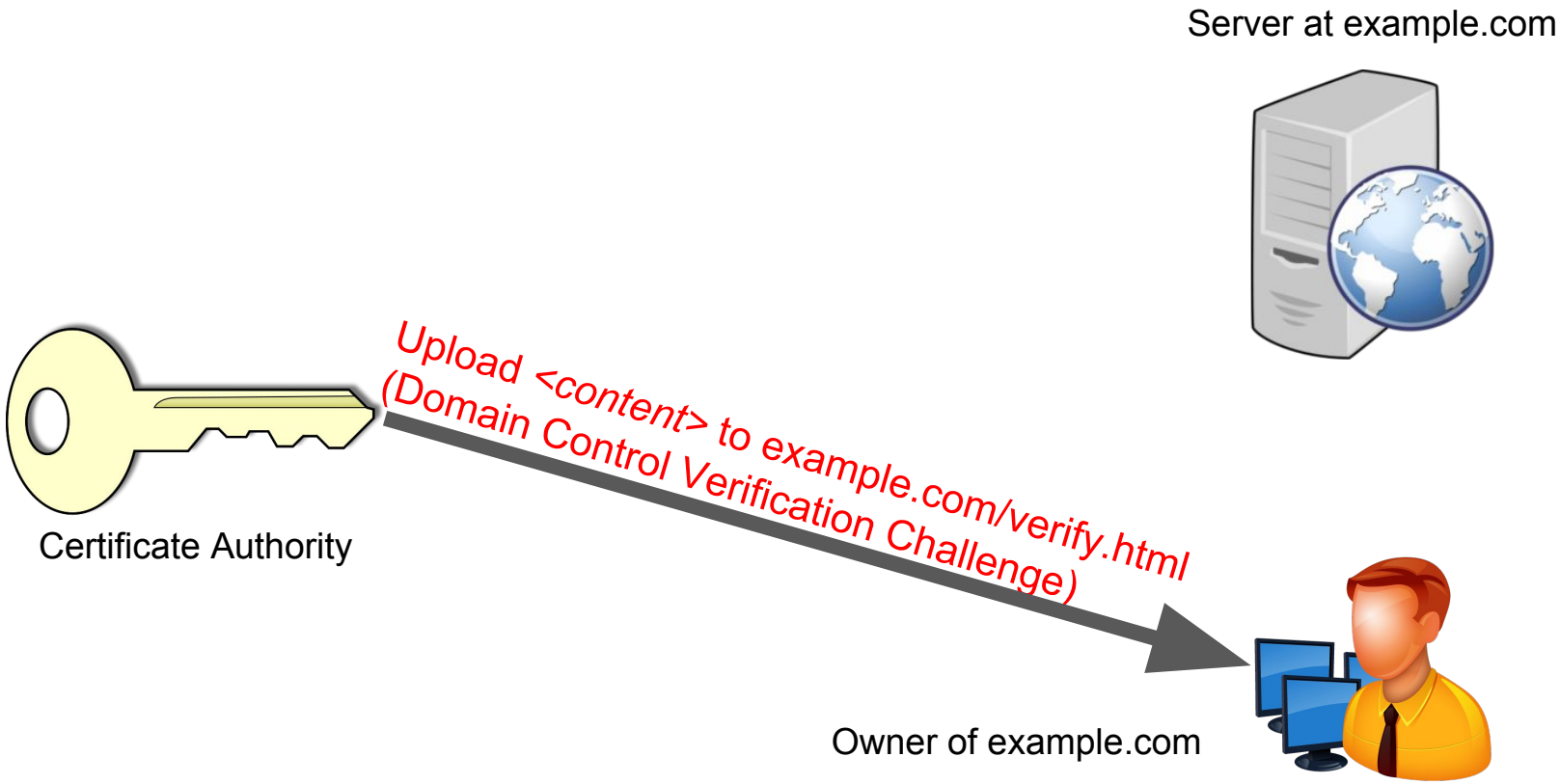
Overview

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

Domain Control Verification

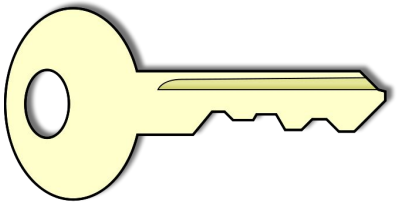


Domain Control Verification



Domain Control Verification

Server at example.com

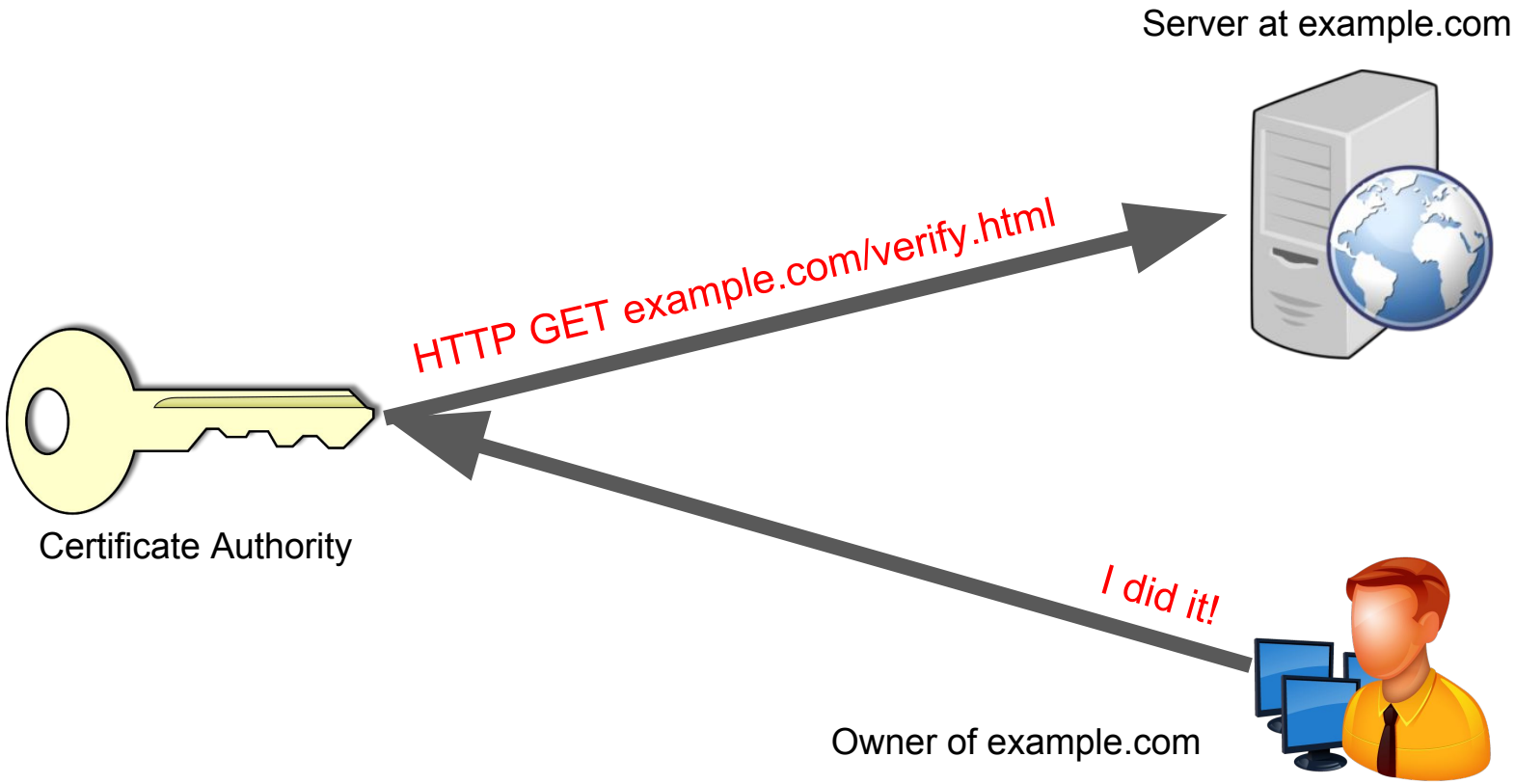


Certificate Authority

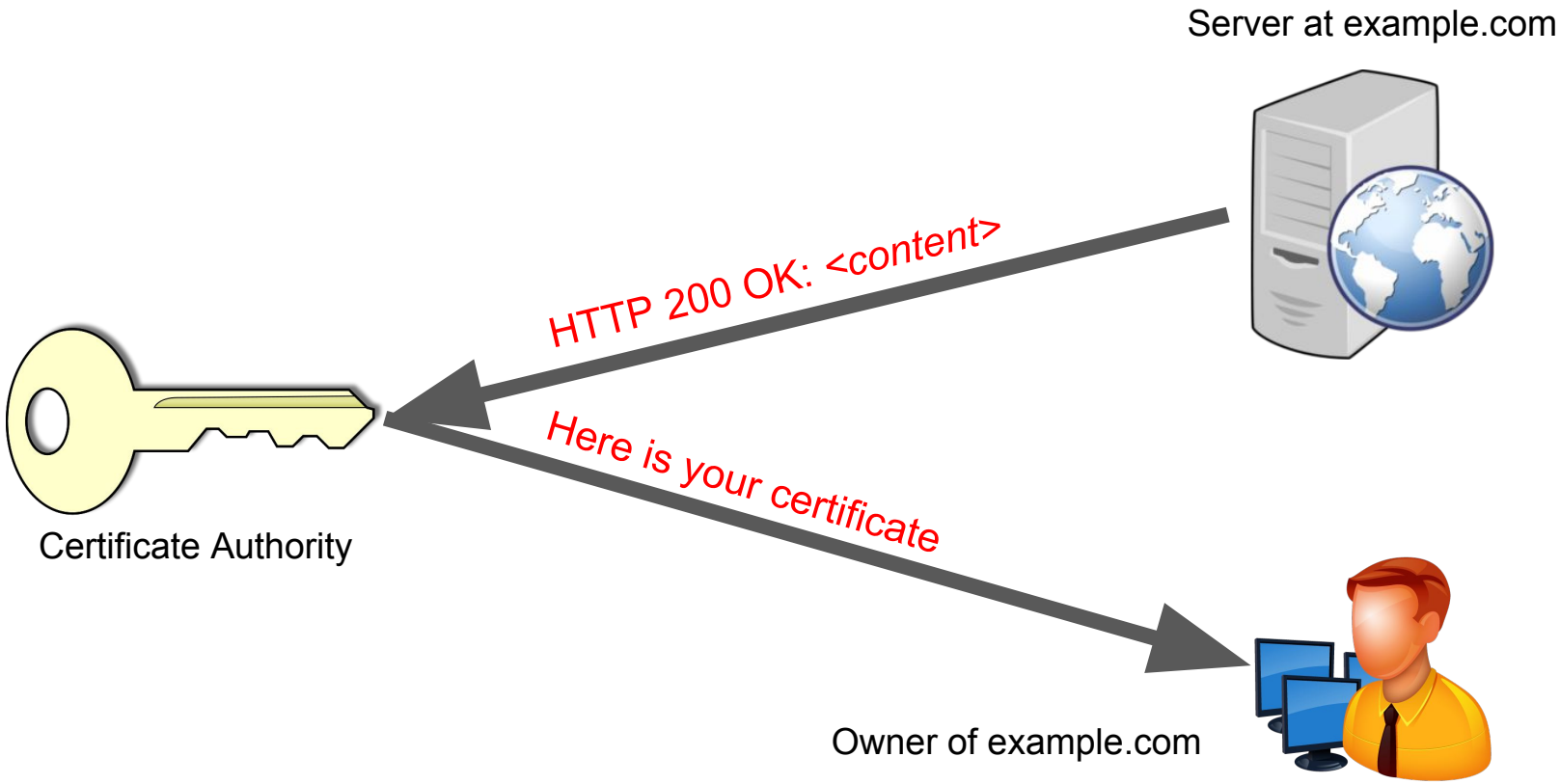
Server modifications

Owner of example.com

Domain Control Verification

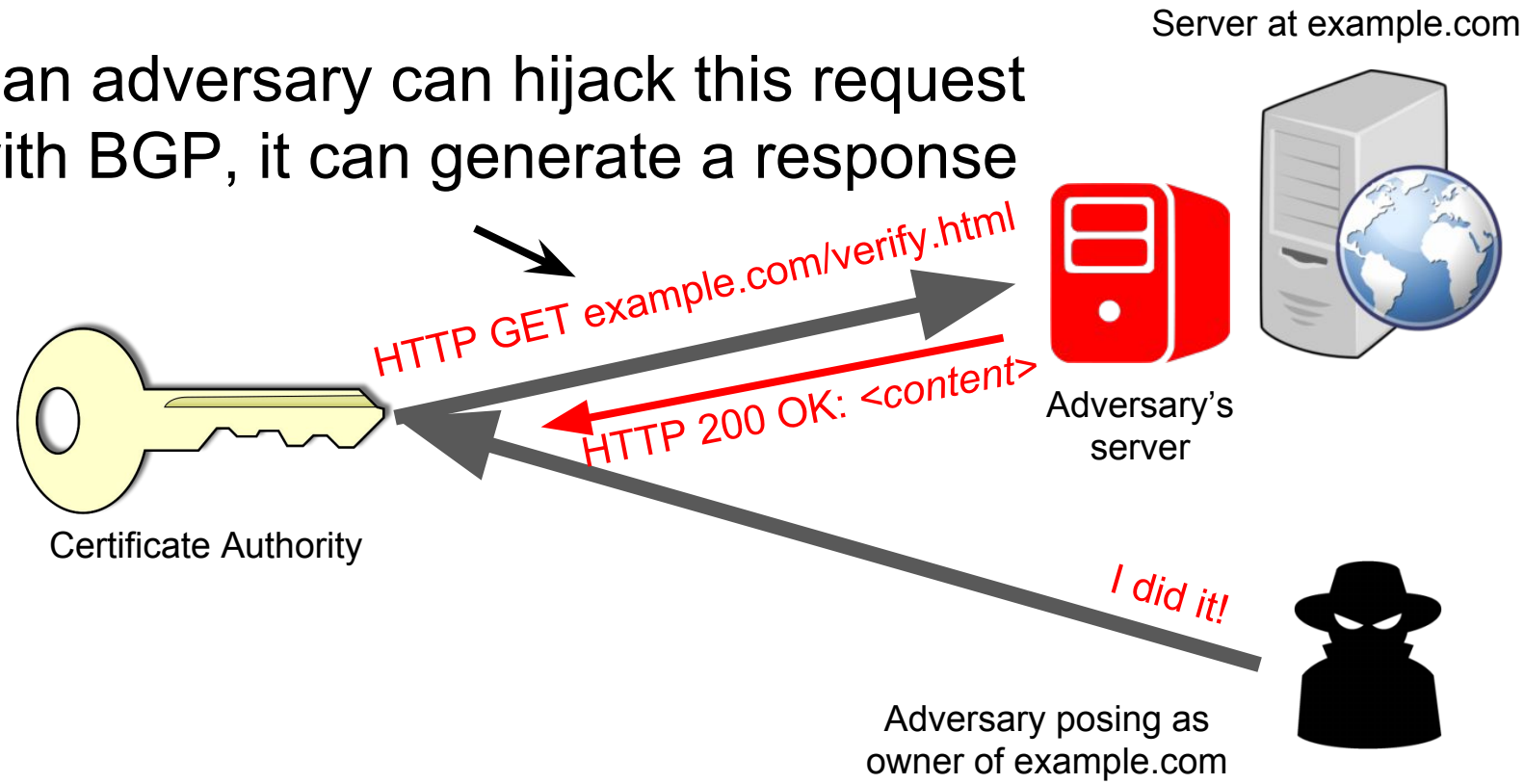


Domain Control Verification



Where BGP Comes In

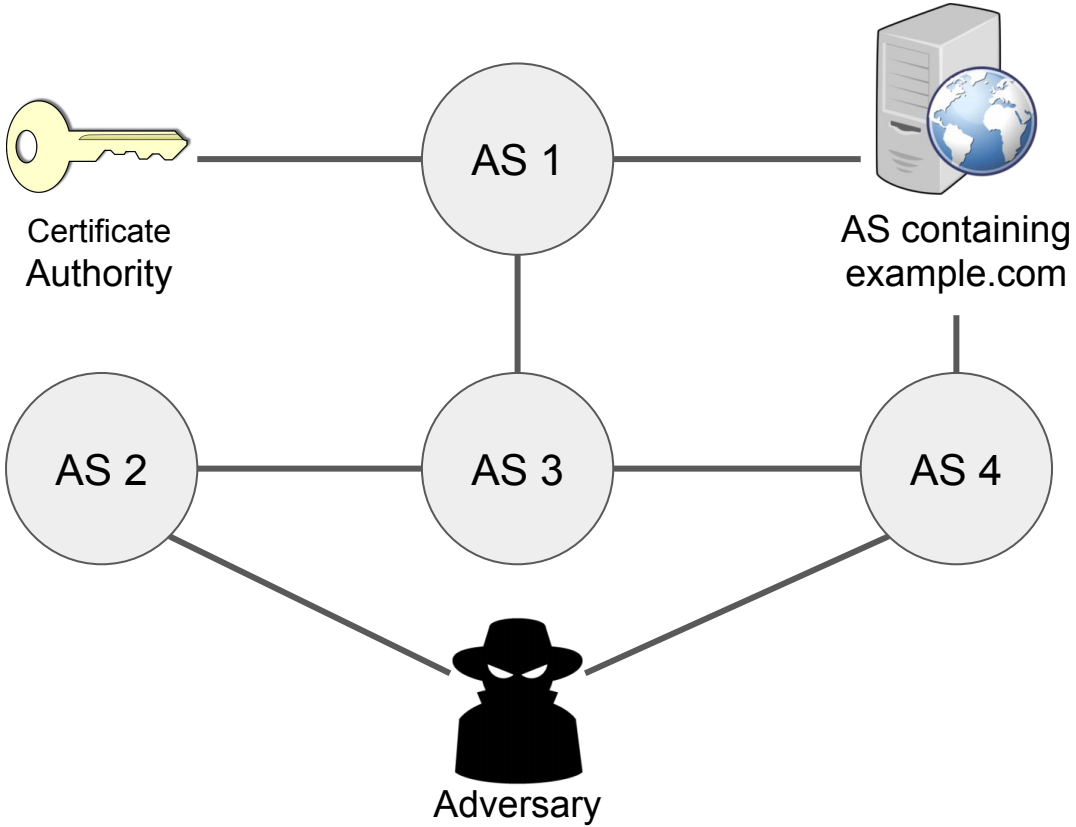
If an adversary can hijack this request with BGP, it can generate a response



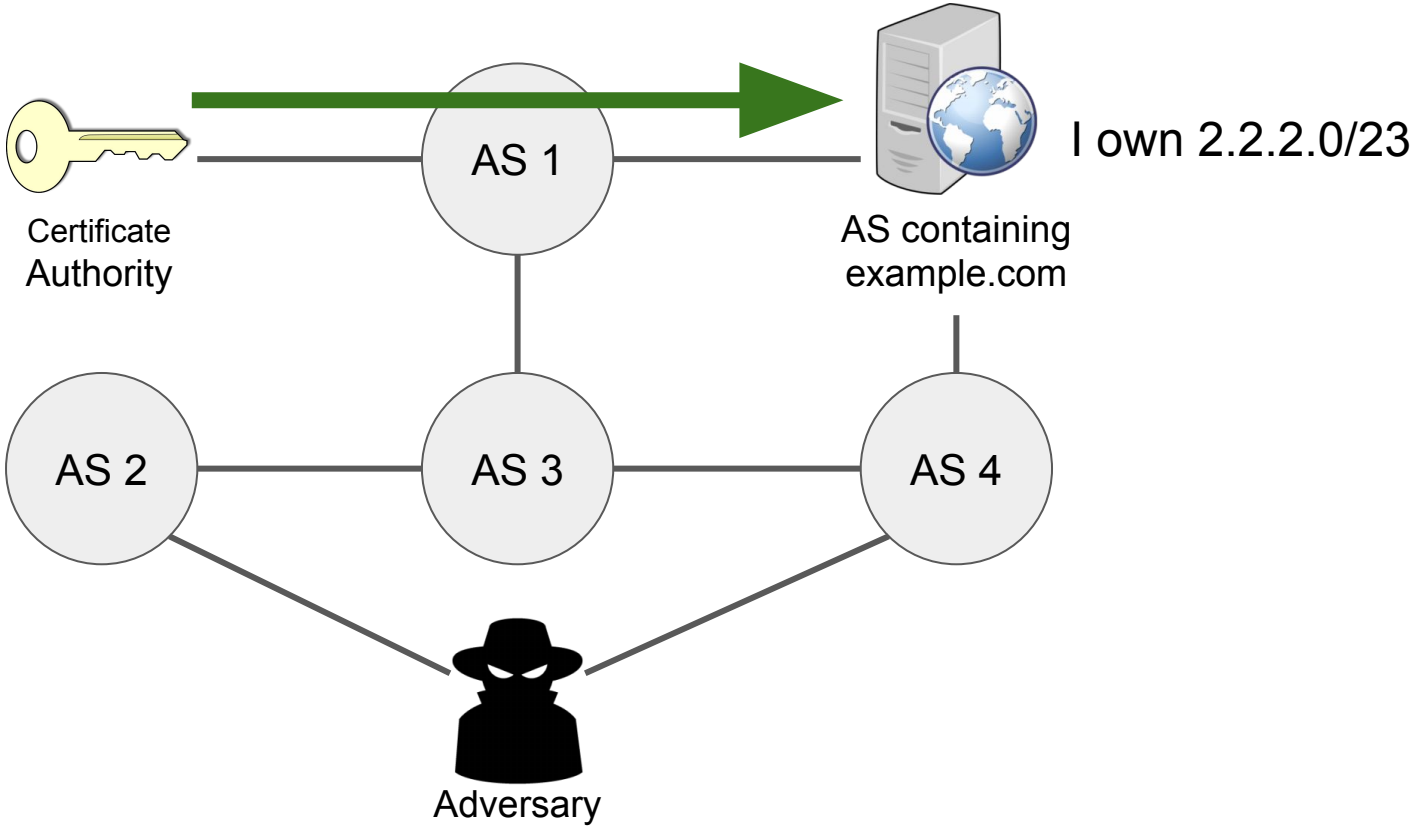
Overview

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

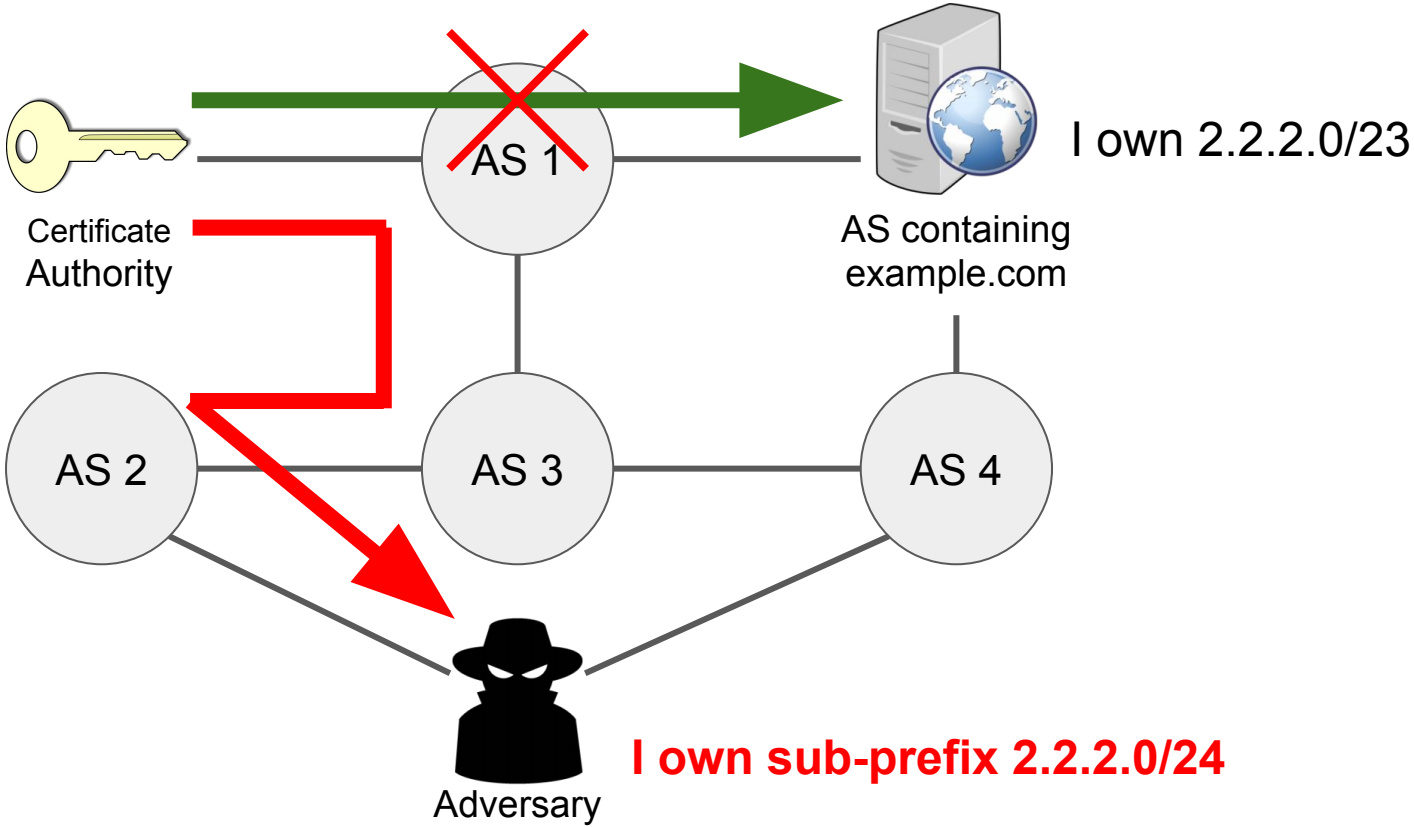
Original BGP route to victim



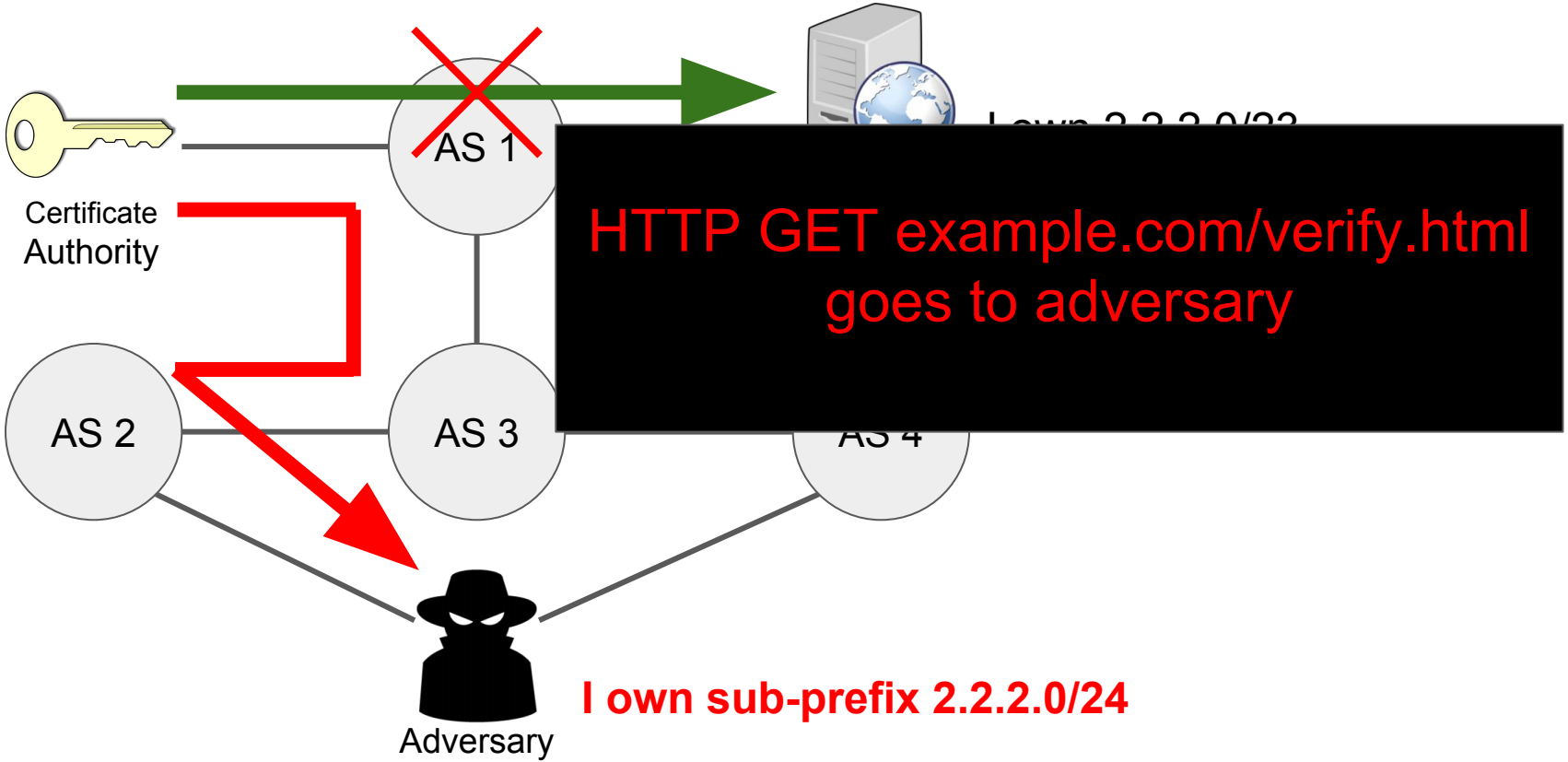
Original BGP route to victim



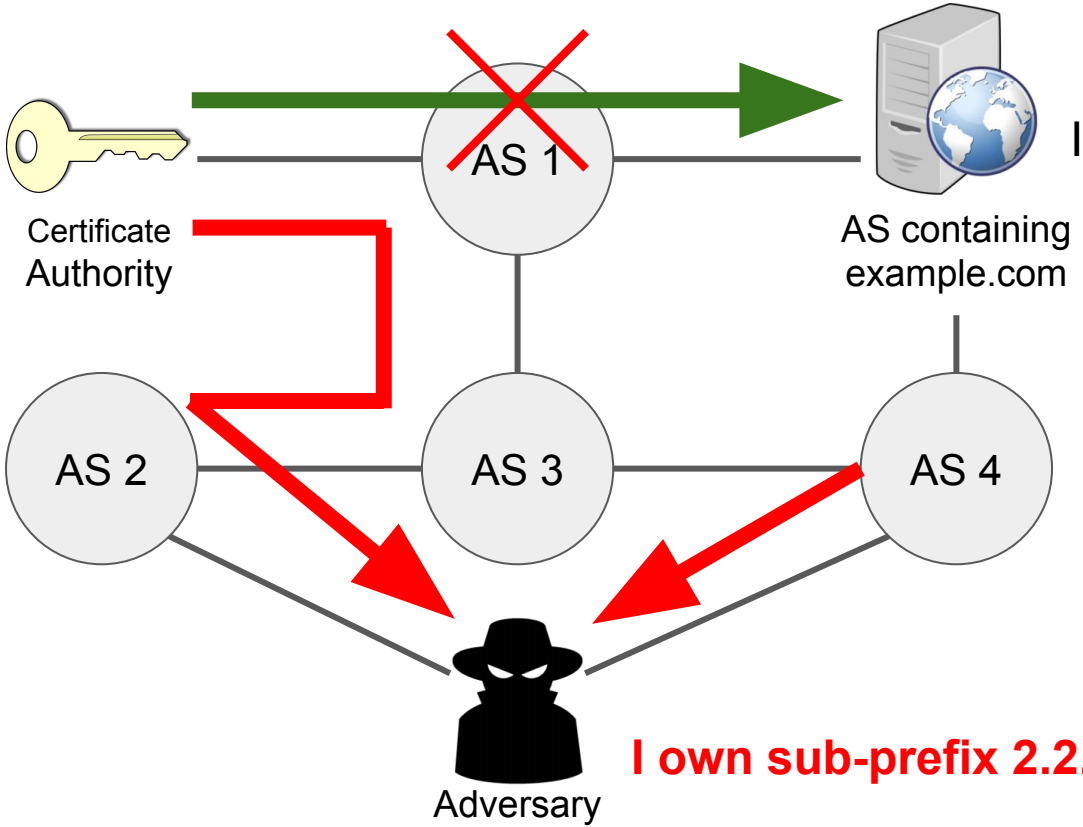
BGP route to victim under sub-prefix attack



BGP route to victim under sub-prefix attack



BGP route to victim under sub-prefix attack

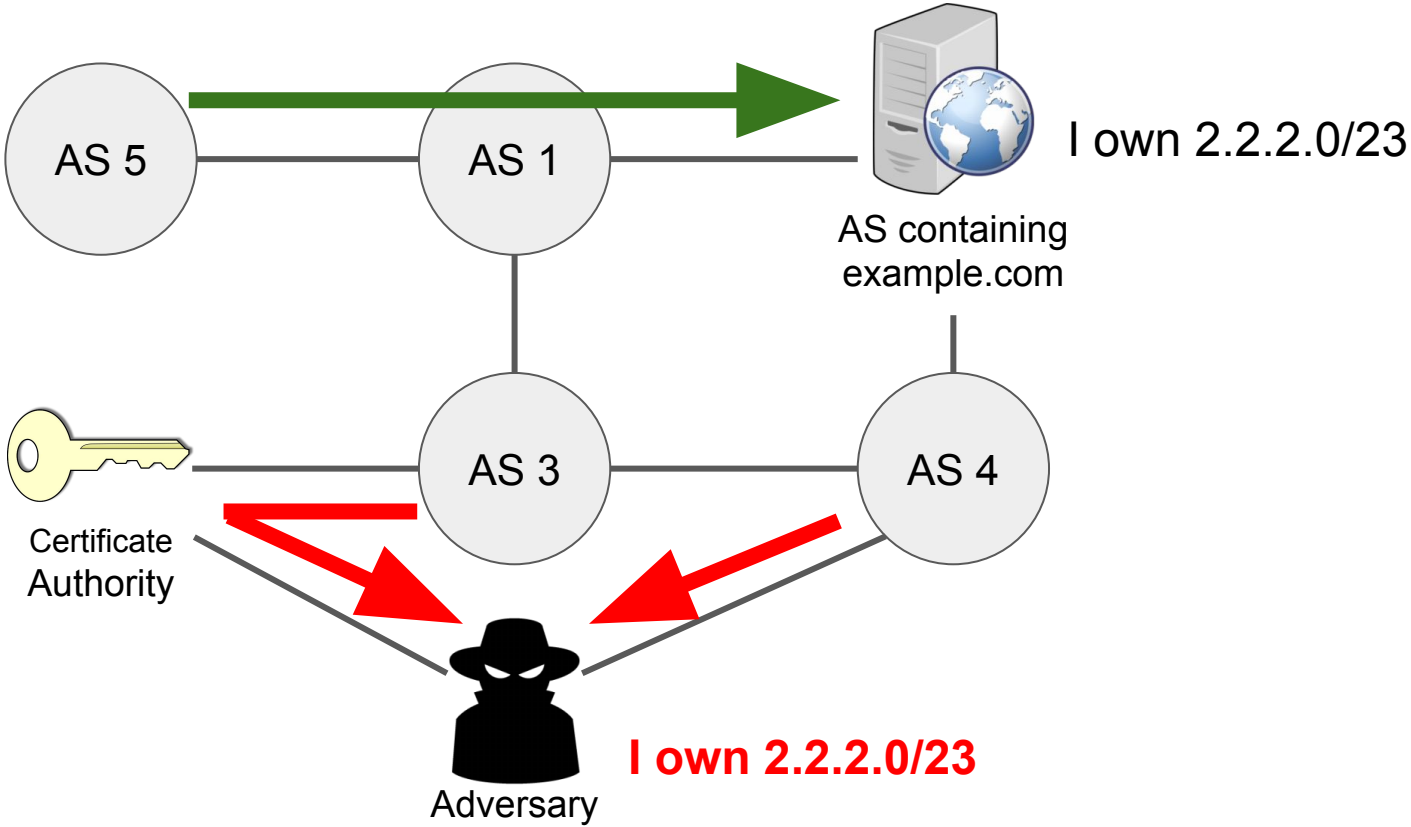


I own 2.2.2.0/23

- Routers prefer more specific announcements
- Global visibility
- Connectivity broken
- Not very stealthy

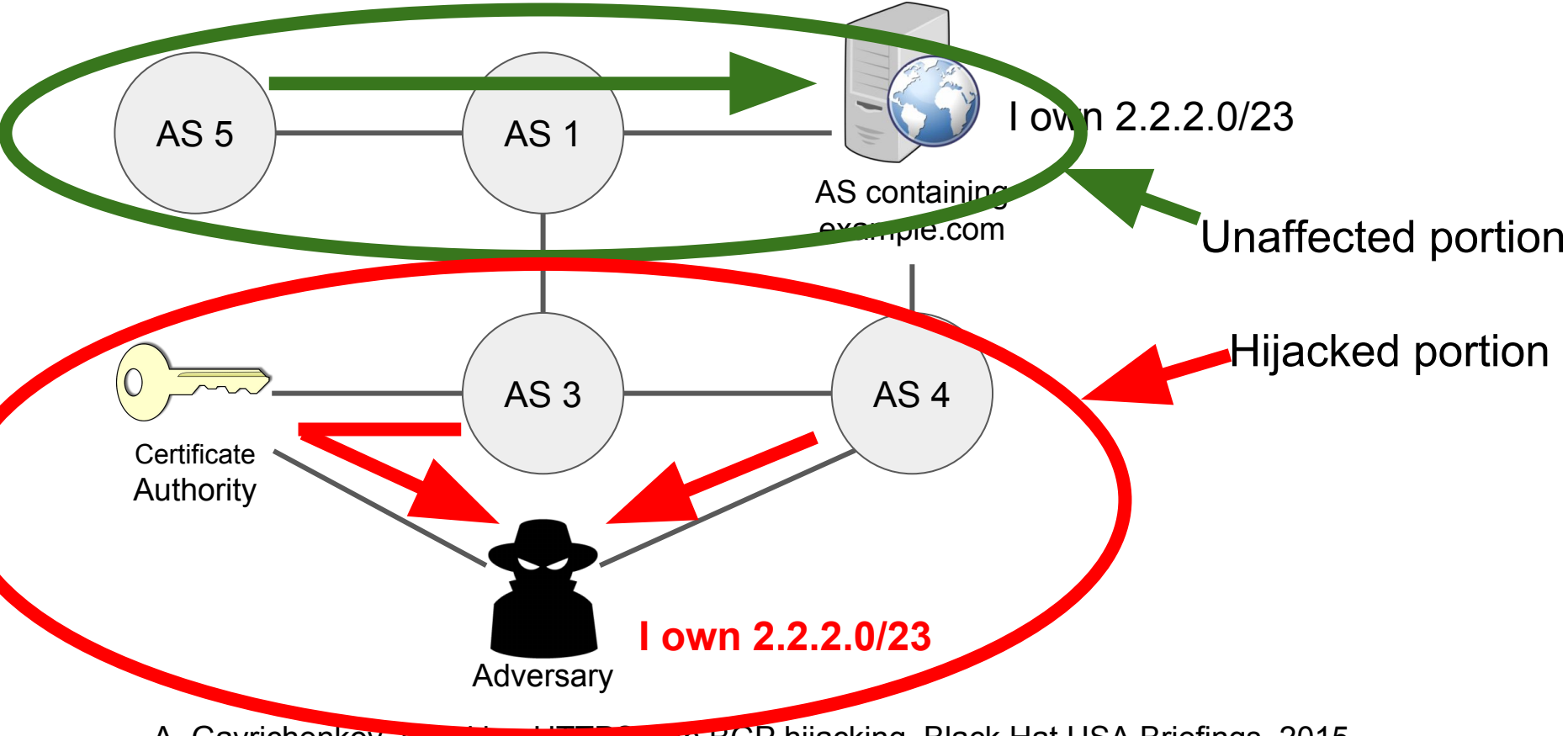
I own sub-prefix 2.2.2.0/24

A local (equally-specific prefix) attack



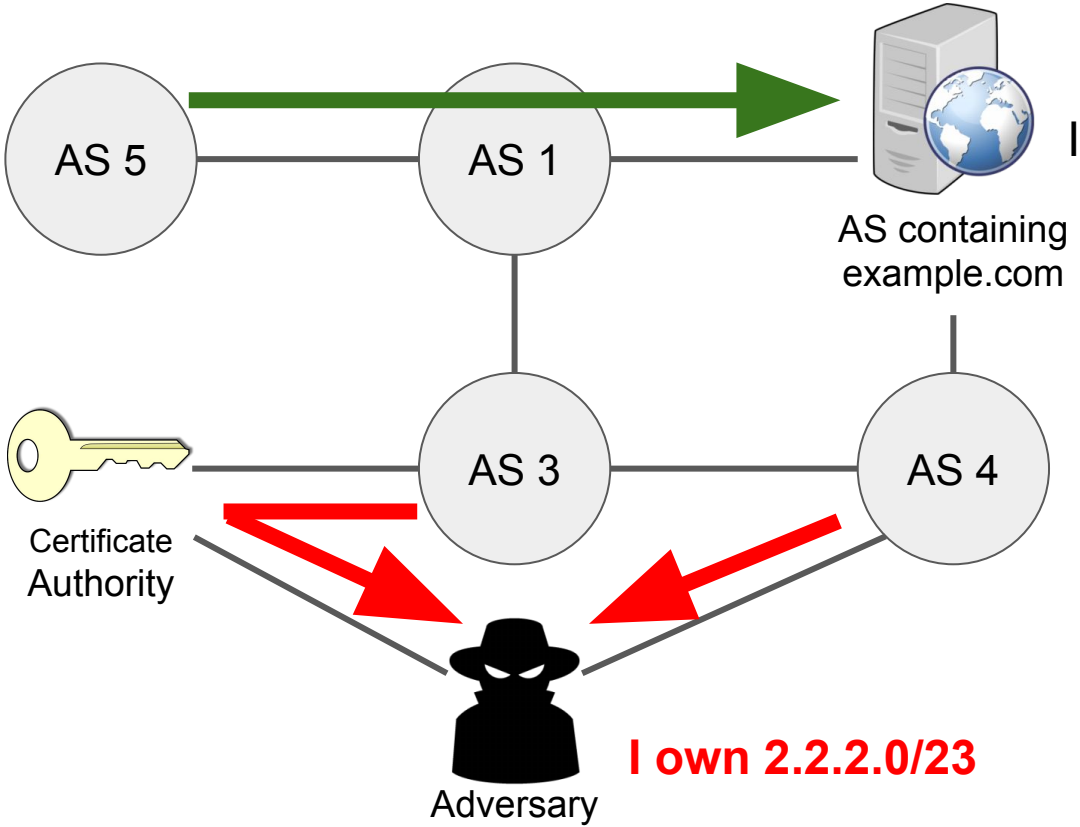
A. Gavrichenkov. Breaking HTTPS with BGP hijacking. Black Hat USA Briefings, 2015

A local (equally-specific prefix) attack



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

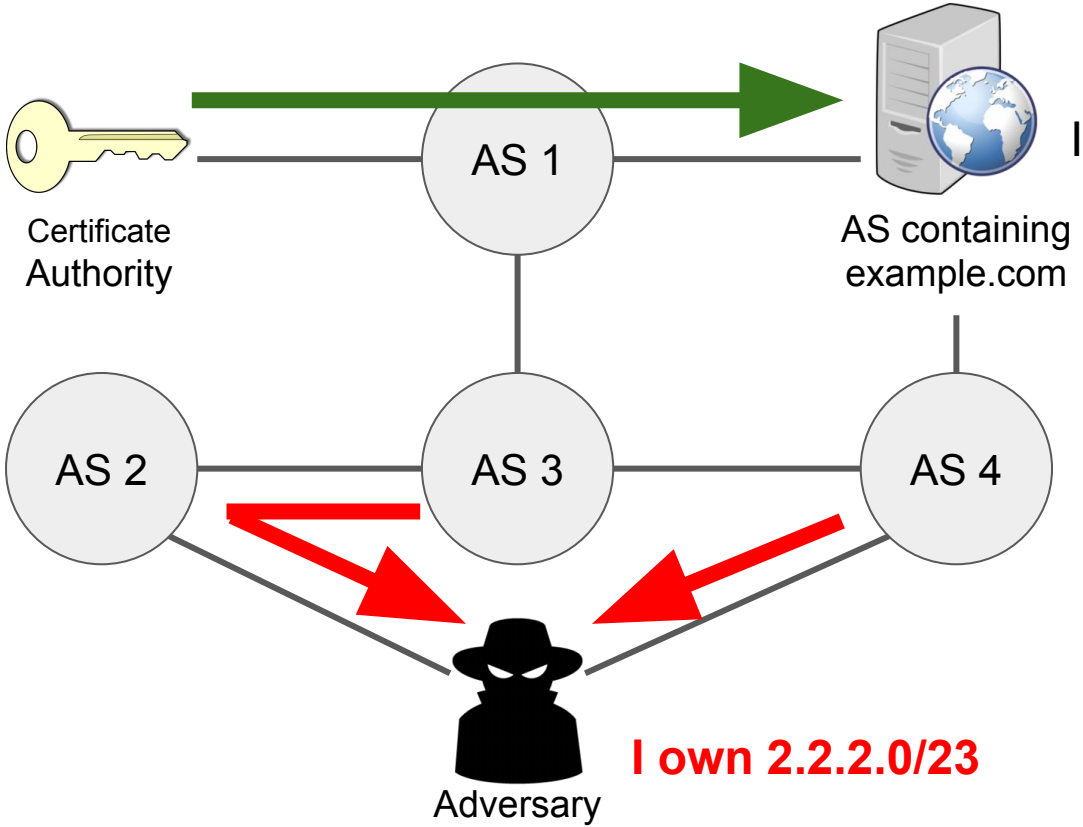
A local (equally-specific prefix) attack



- 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

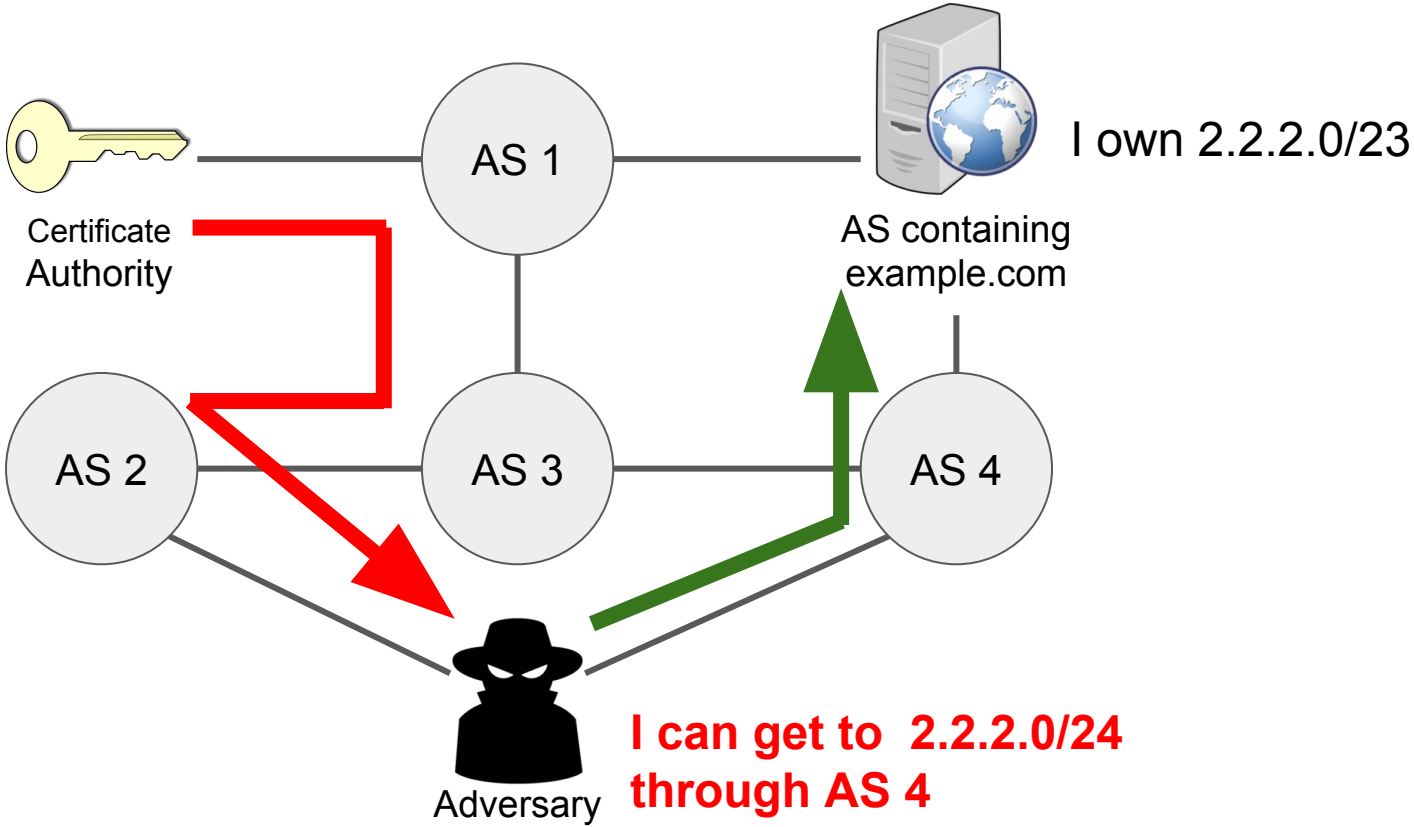
A local (equally-specific prefix) attack



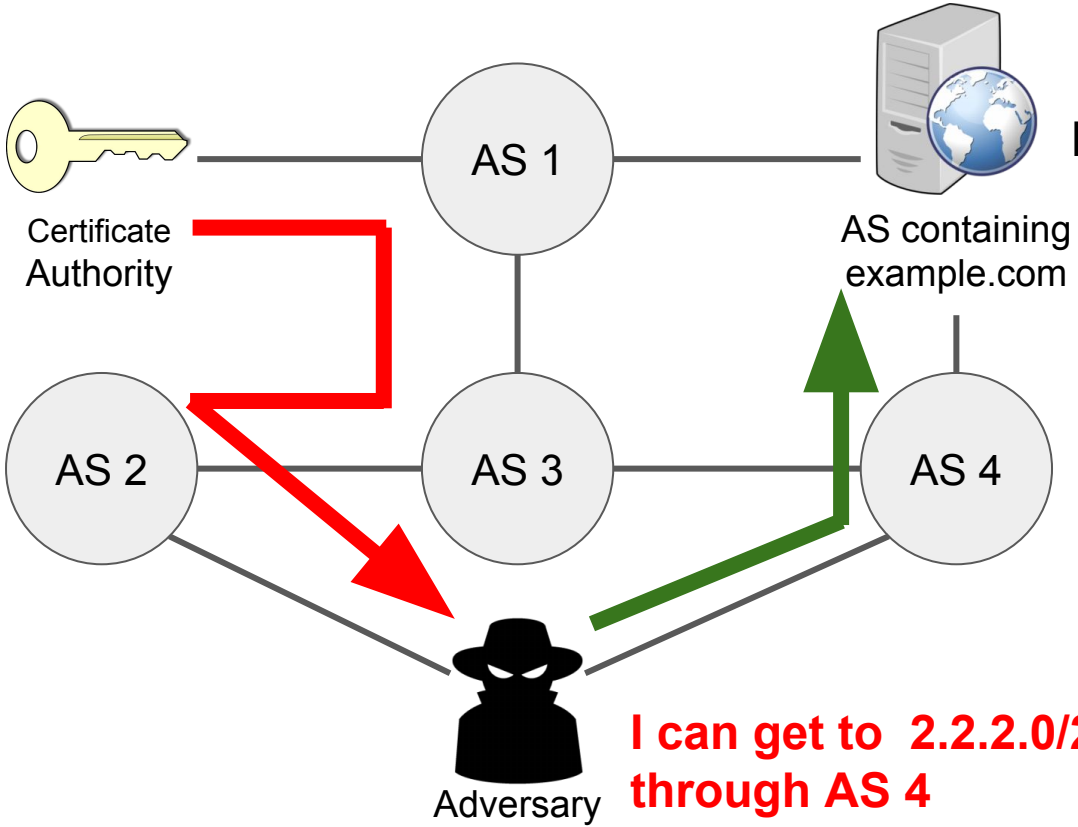
- Equally specific announcements compete for traffic
- Announcement localized
- Local broken connectivity
- Potentially stealthy
- **Not all ASes can perform**

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

AS path poisoning



AS path poisoning



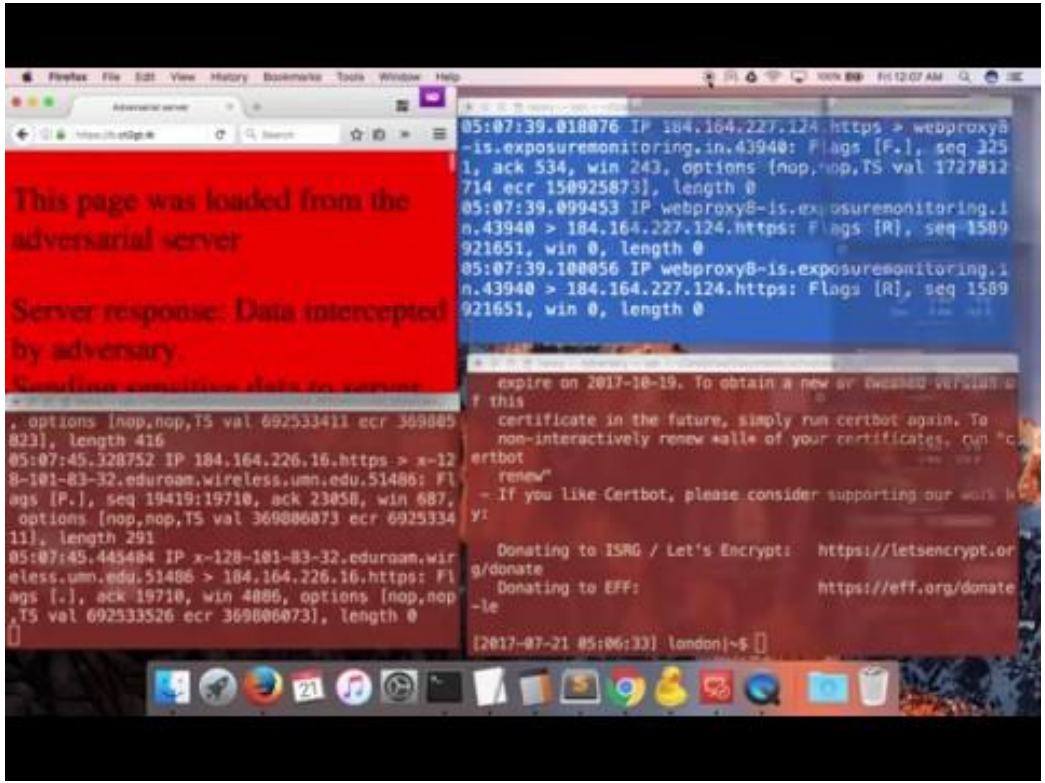
I own 2.2.2.0/23

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

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

	Let’s Encrypt	GoDaddy	Comodo	Symantec*	GlobalSign
Time to issue certificate	35 seconds	< 2 min	< 2 min	< 2 min	< 2 min
Human interaction	No	No	No	No	No
Multiple Vantage Points	Not yet	No	No	No	No
Validation Method Attacked	HTTP	HTTP	Email	Email	Email

*At time of experiments Symantec was still a trusted CA

Results from real world attacks

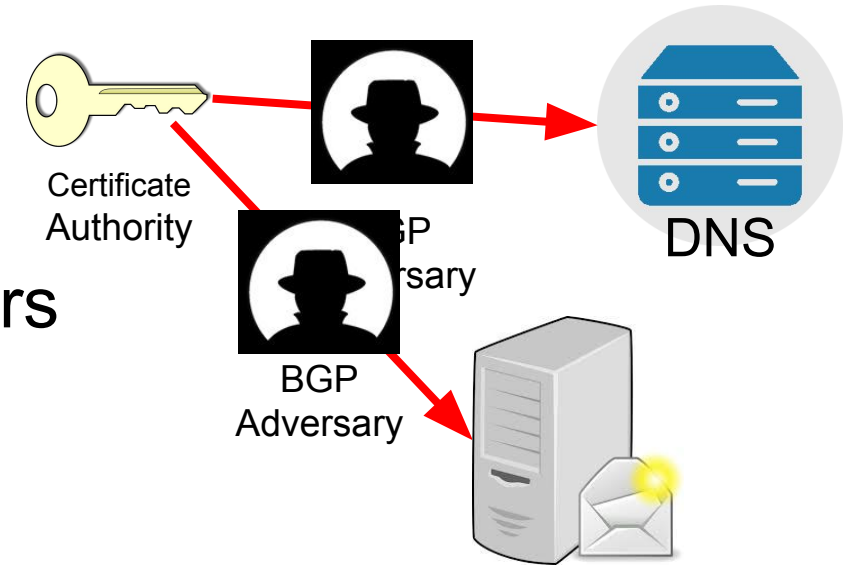
	Let's Encrypt	GoDaddy	Comodo	Symantec	GlobalSign
Time to issue certificate	35 seconds	< 2 min	< 2 min	< 2 min	< 2 min
Human interaction	[redacted]	[redacted]	[redacted]	[redacted]	No
Multiple Vantage Points	[redacted]	[redacted]	[redacted]	[redacted]	No
Validation Method Attacked	HTTP	HTTP	Email	Email	Email

All studied CAs were vulnerable

*At time of experiments Symantec was still a trusted CA

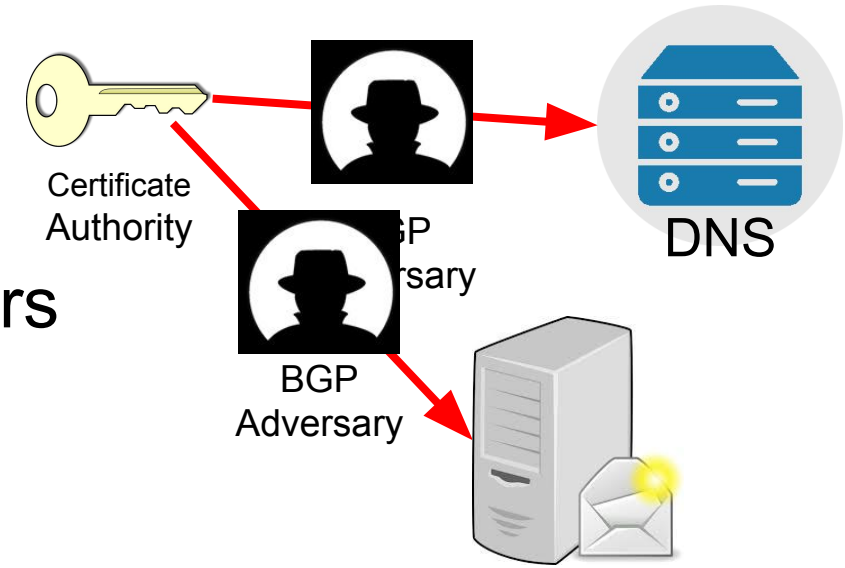
Additional Attacks

- 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

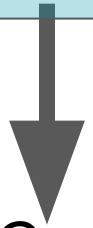
- Domain Control Validation
- BGP Attacks
- Quantifying Vulnerability
- Countermeasures
- Takeaways

Quantifying Vulnerability

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

Quantifying Vulnerability

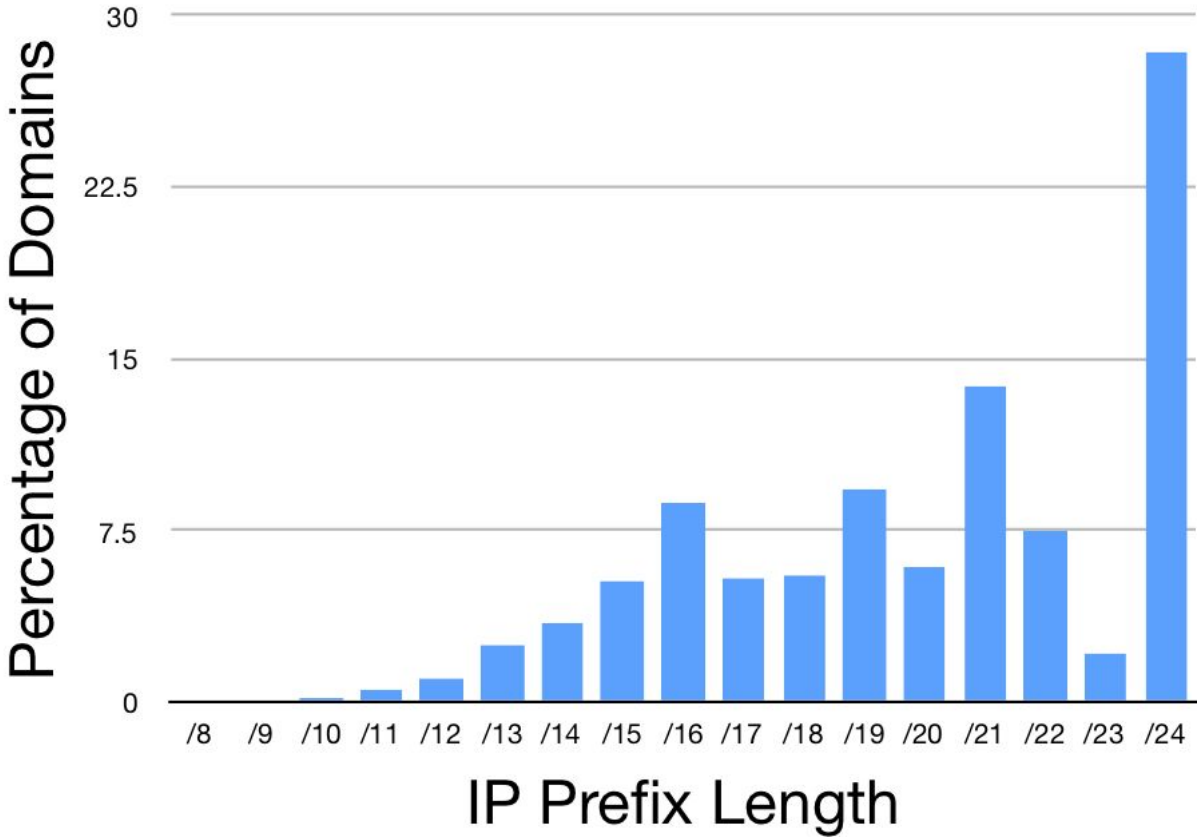
- How many domains are vulnerable?
- How many adversaries can launch attacks?



- 1.8 million certificates via Certificate Transparency
- Common names resolved to IPs
- Recorded the BGP routes used for IPs at time of signing

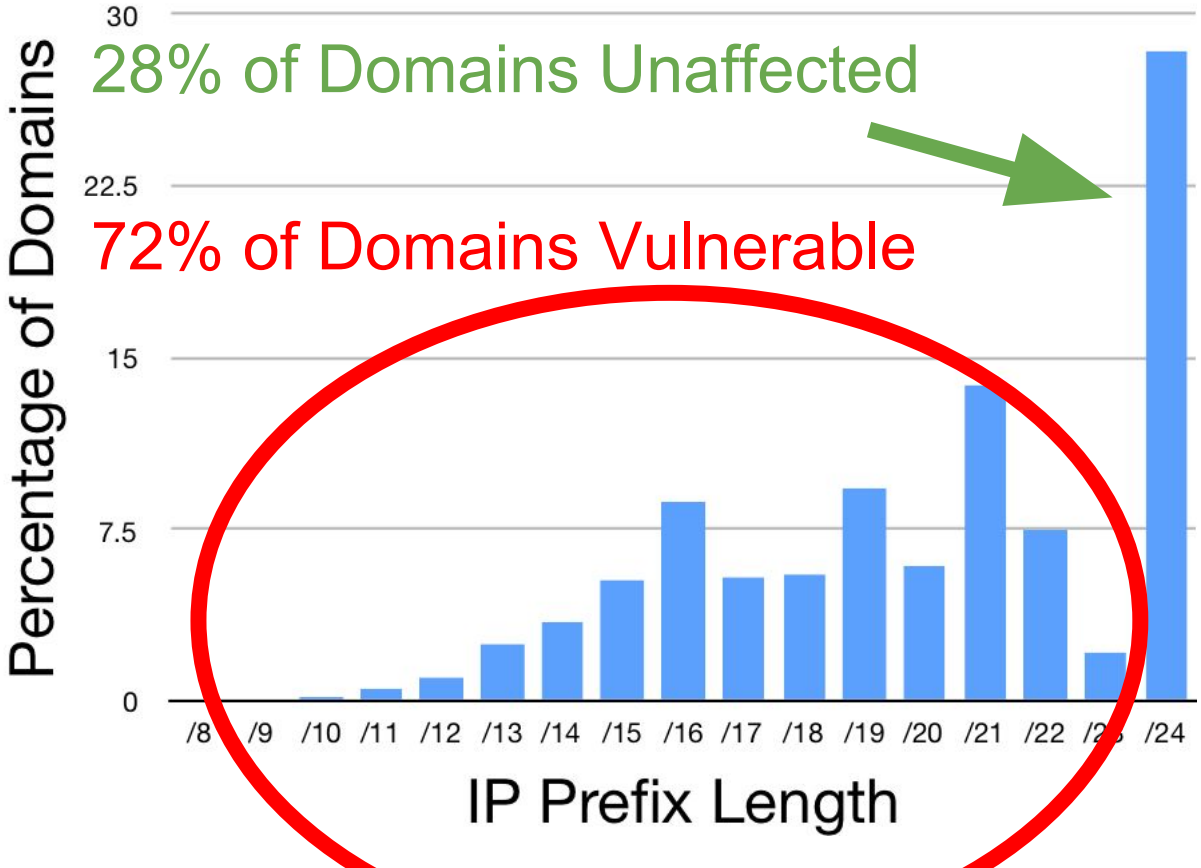
Vulnerability of domains: sub-prefix attacks

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

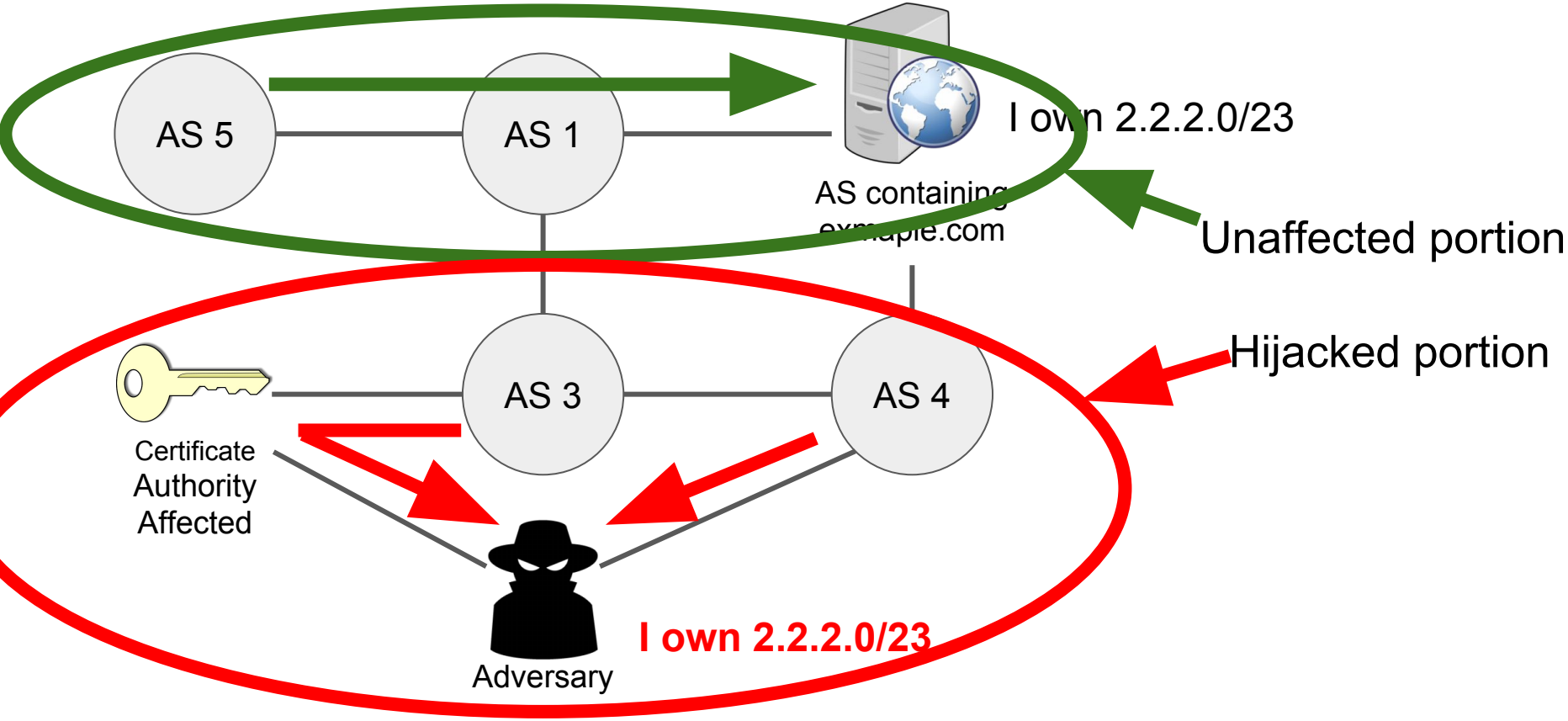


Vulnerability of domains: sub-prefix attacks

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

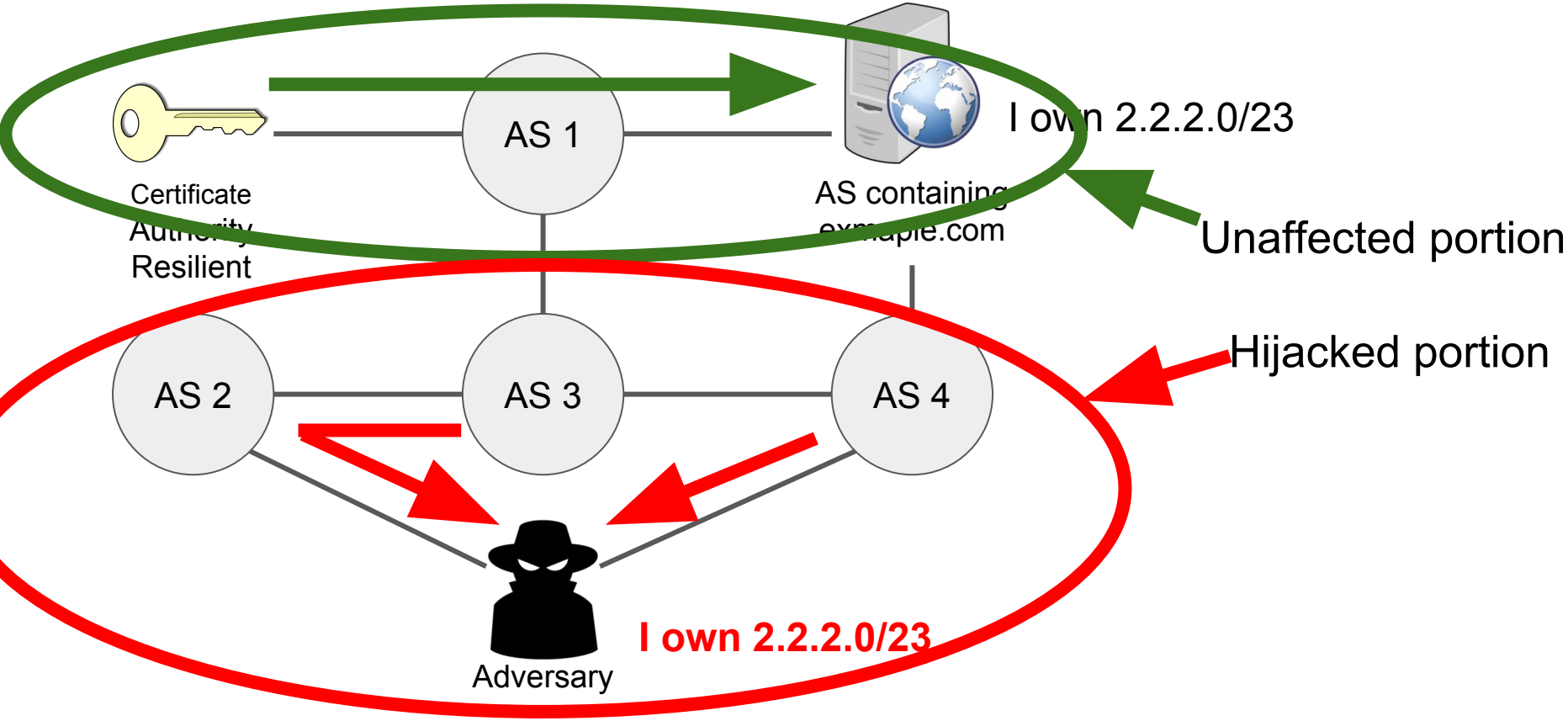


Resilience to equally-specific prefix attacks



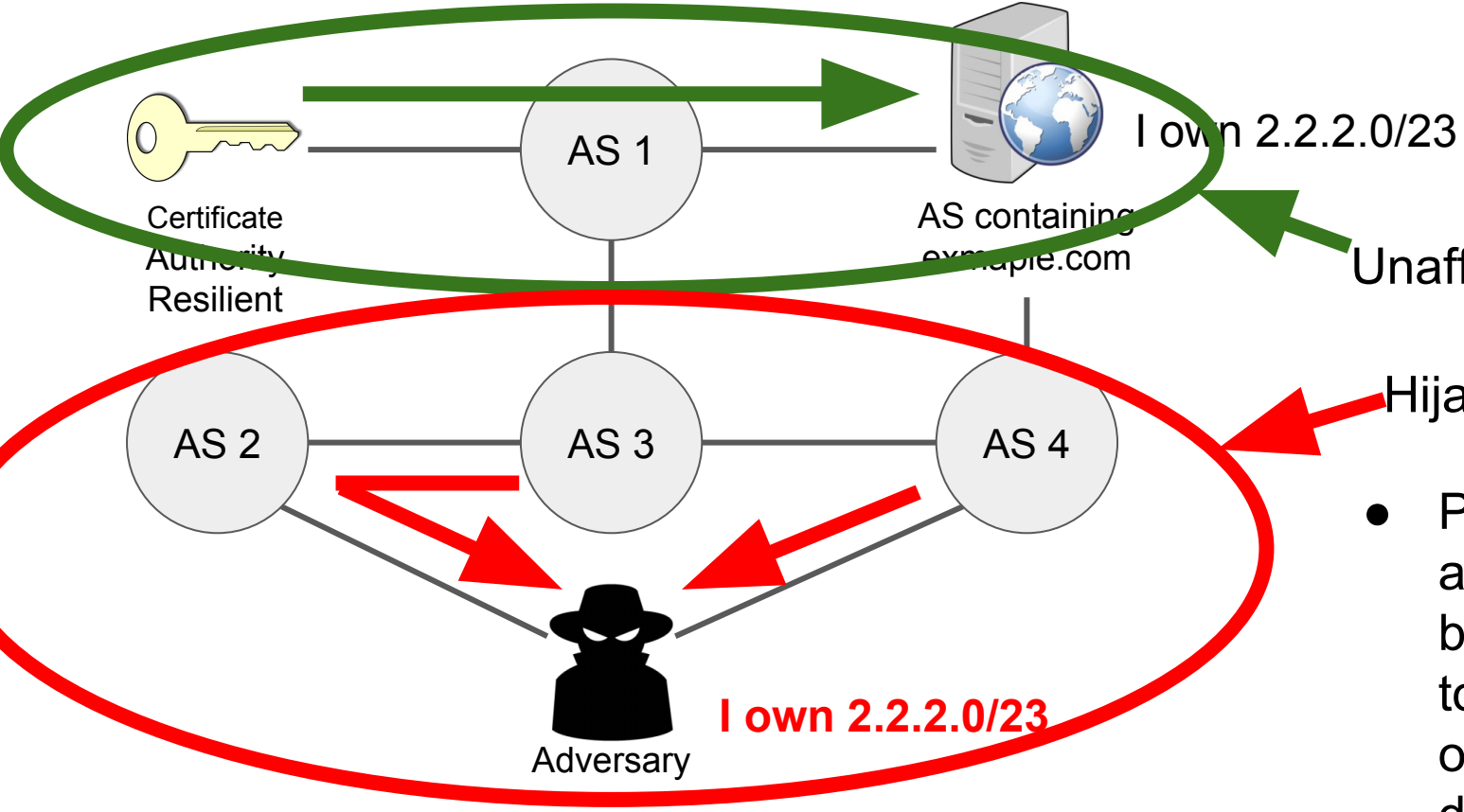
Lad et al., “Understanding resiliency of Internet topology against prefix hijack attacks”, IEEE DSN, 2007

Resilience to equally-specific prefix attacks



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

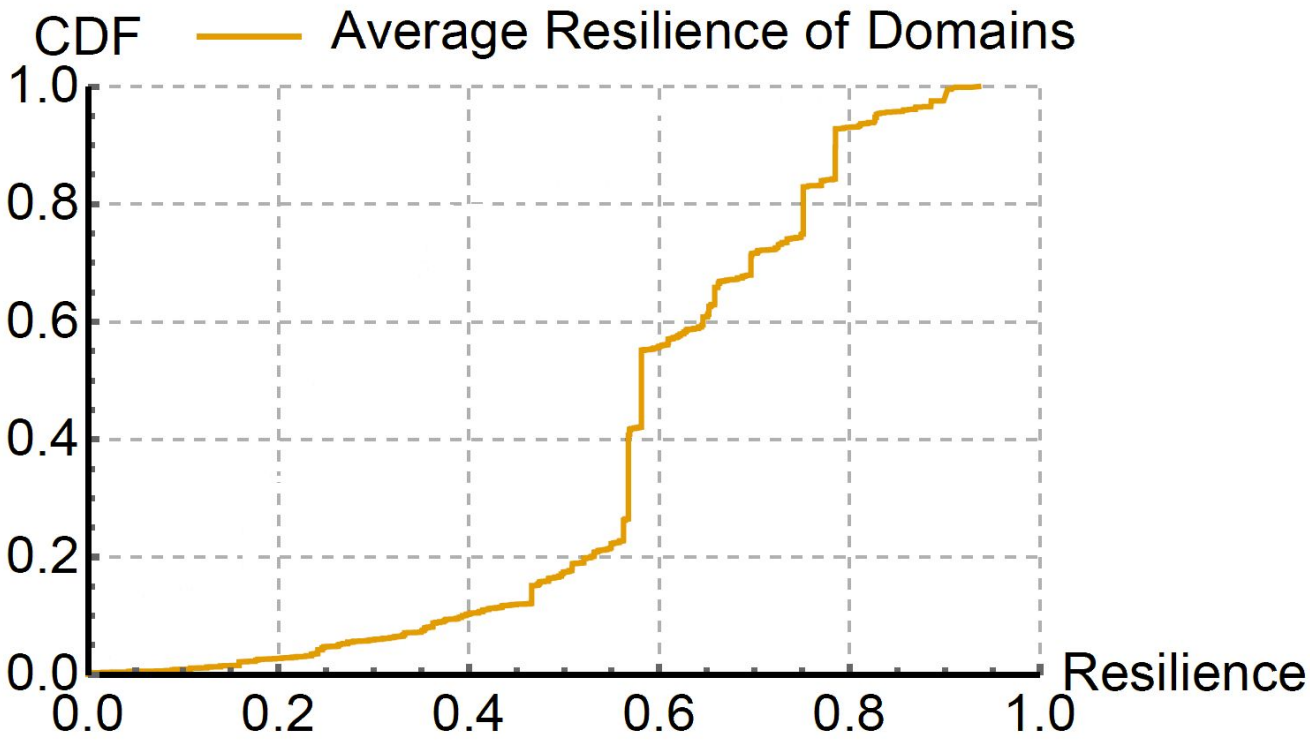
Resilience to equally-specific prefix attacks



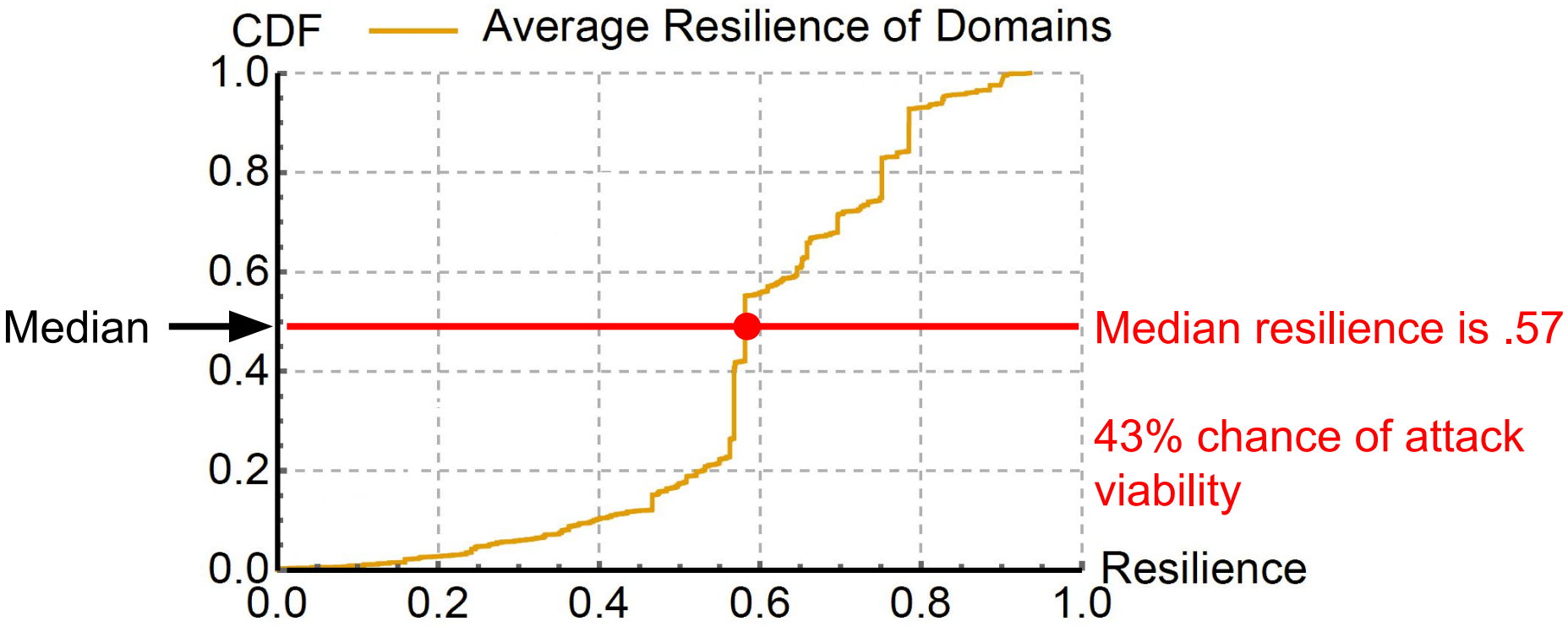
- Probability a CA will be resilient to attacks on a domain

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

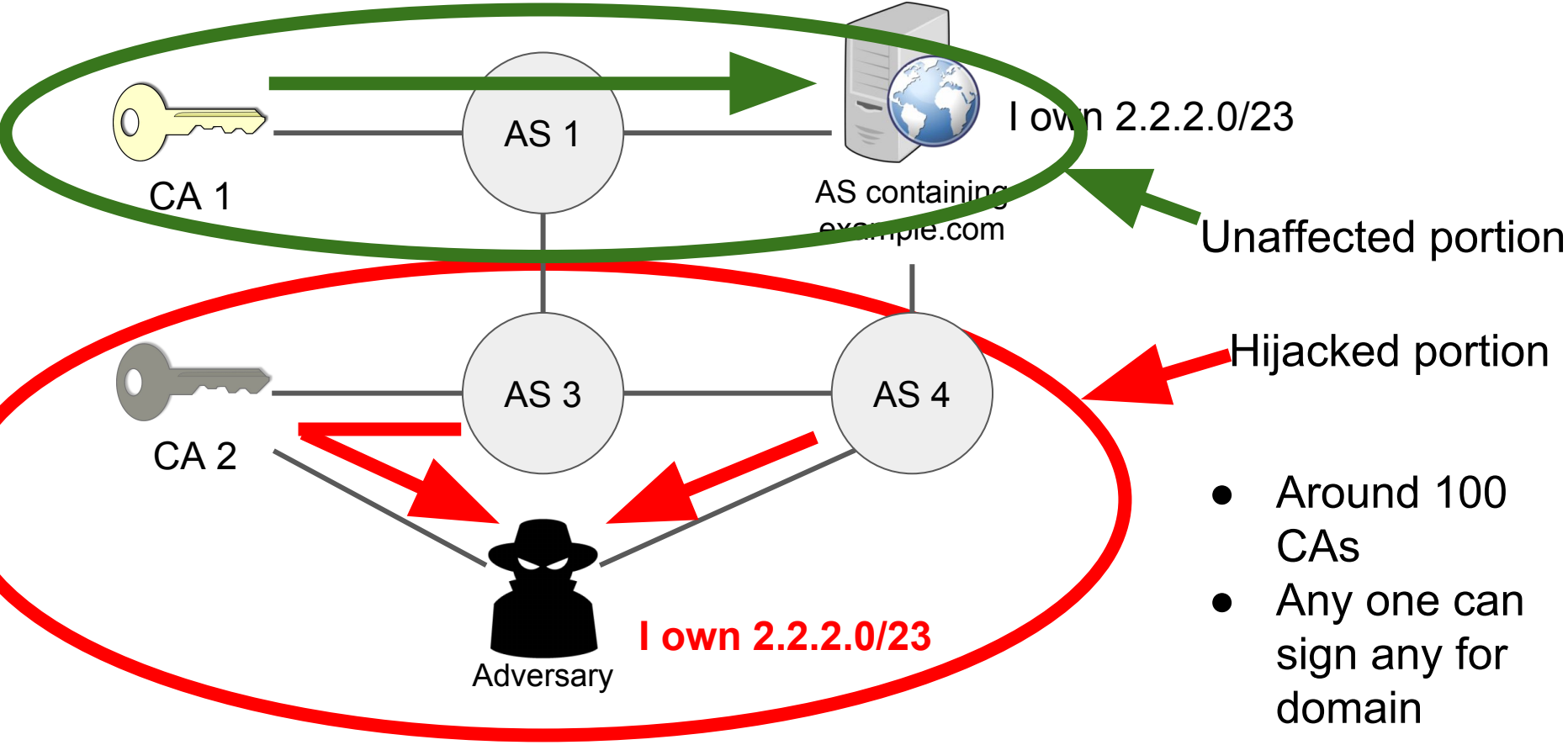
Resilience of domains assuming random CA



Resilience of domains assuming random CA

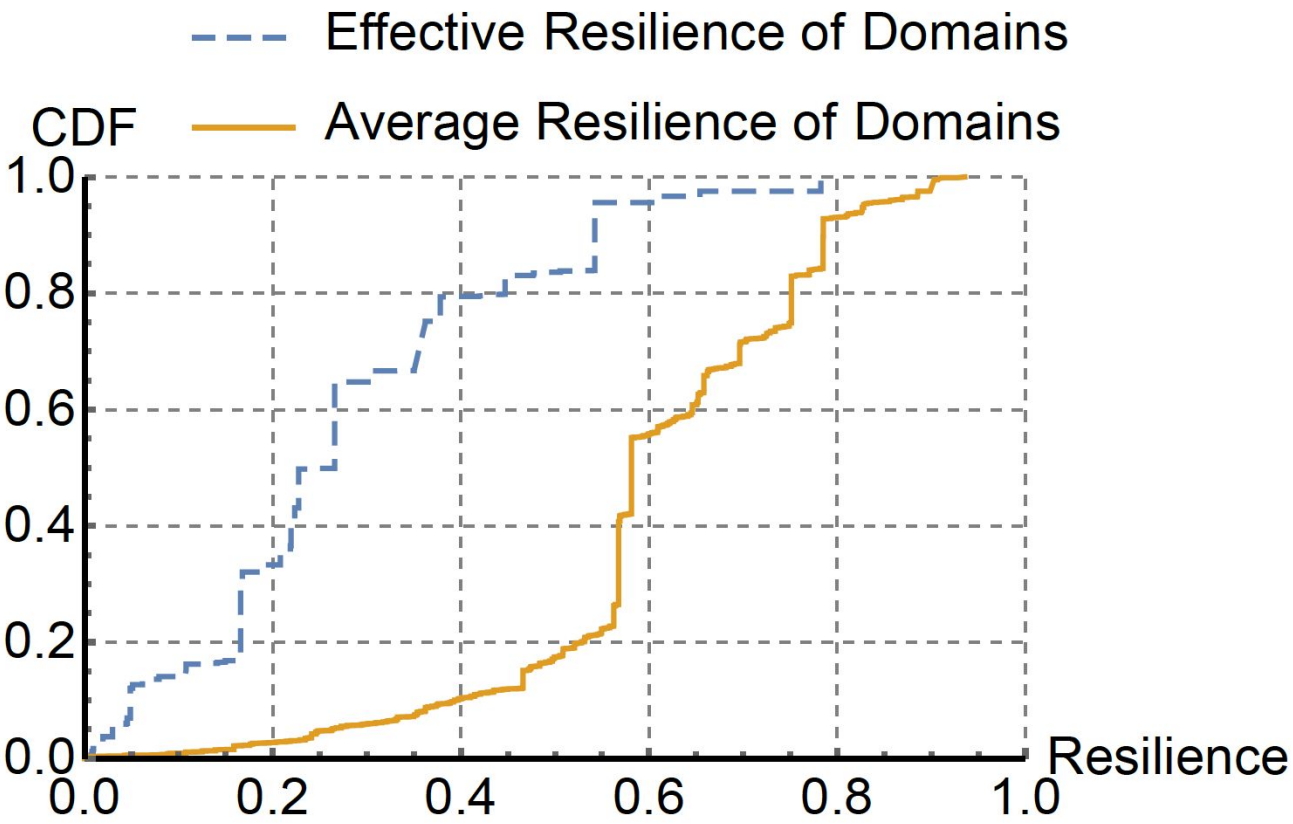


Choosing an affected CA

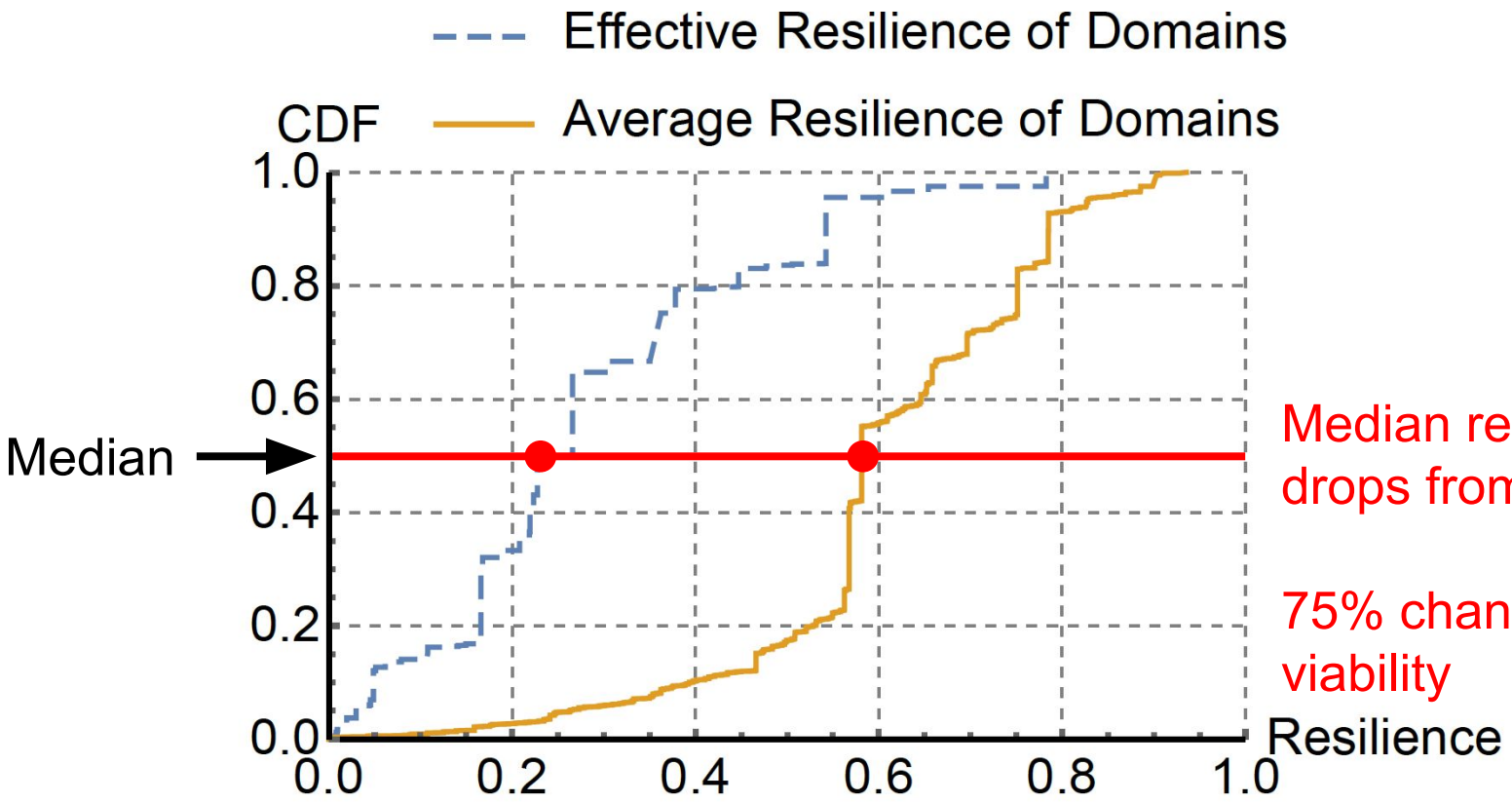


- Around 100 CAs
- Any one can sign any for domain

Vulnerability of Domains: Equally-specific attacks



Vulnerability of Domains: Equally-specific attacks



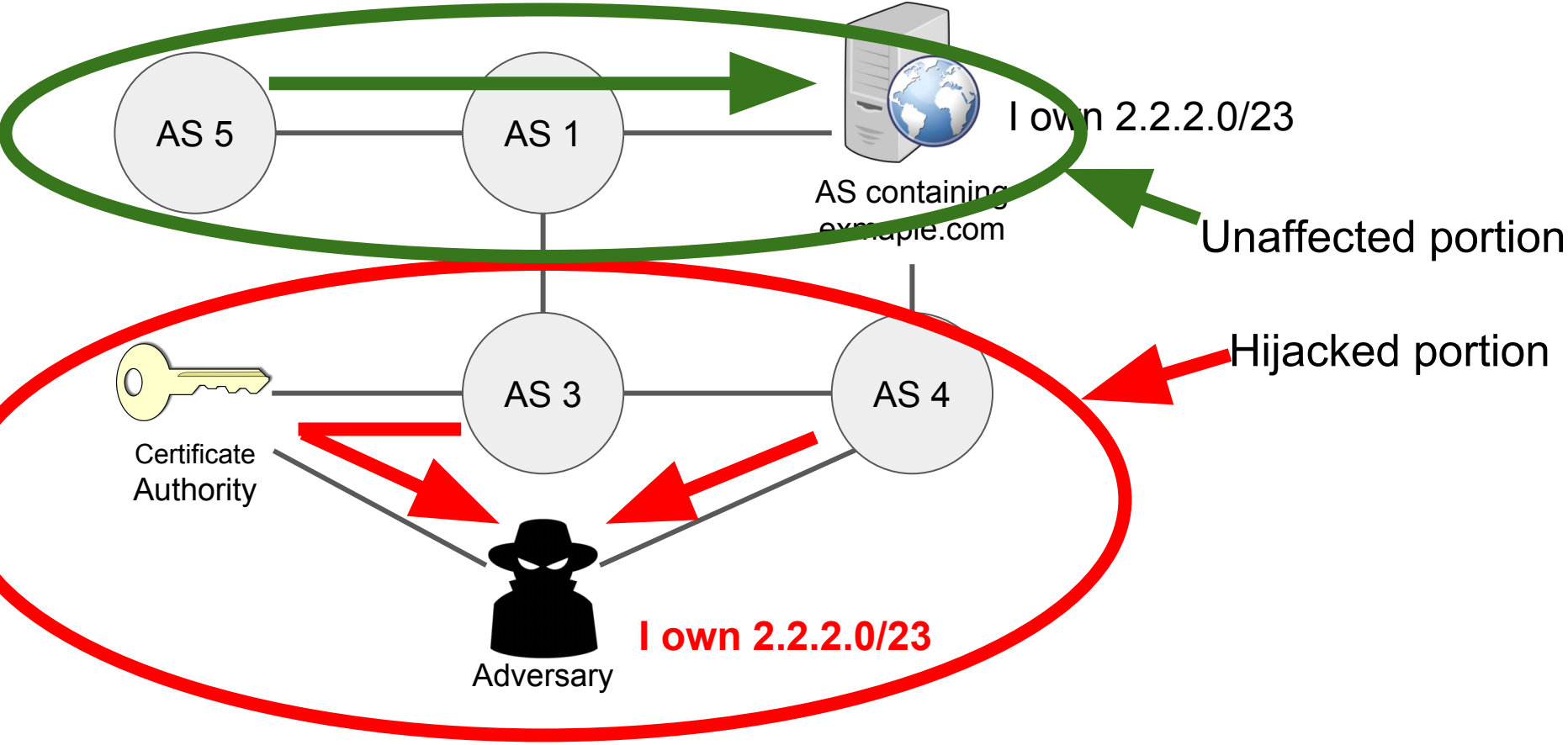
Median resilience drops from .57 to .25

75% chance of attack viability

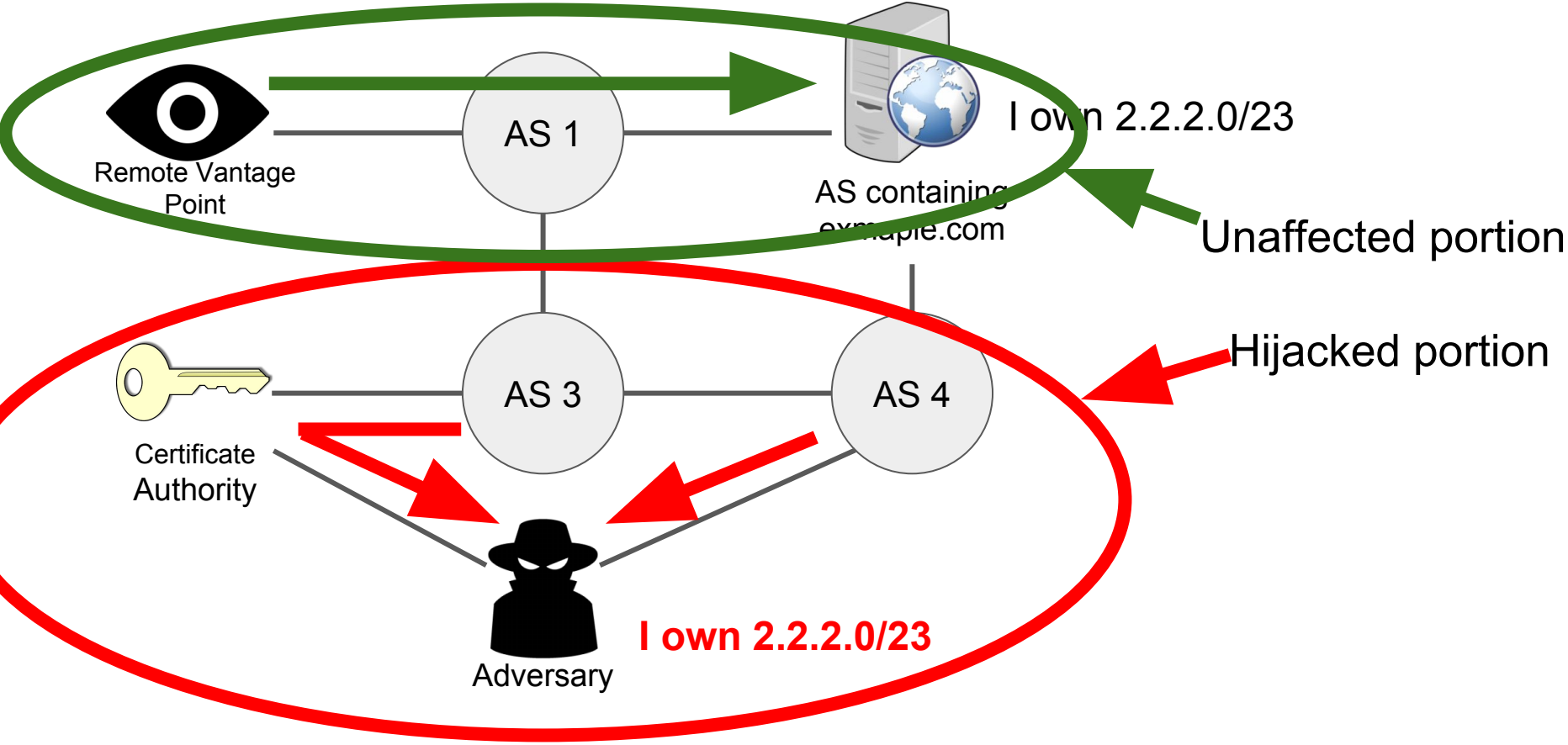
Overview

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

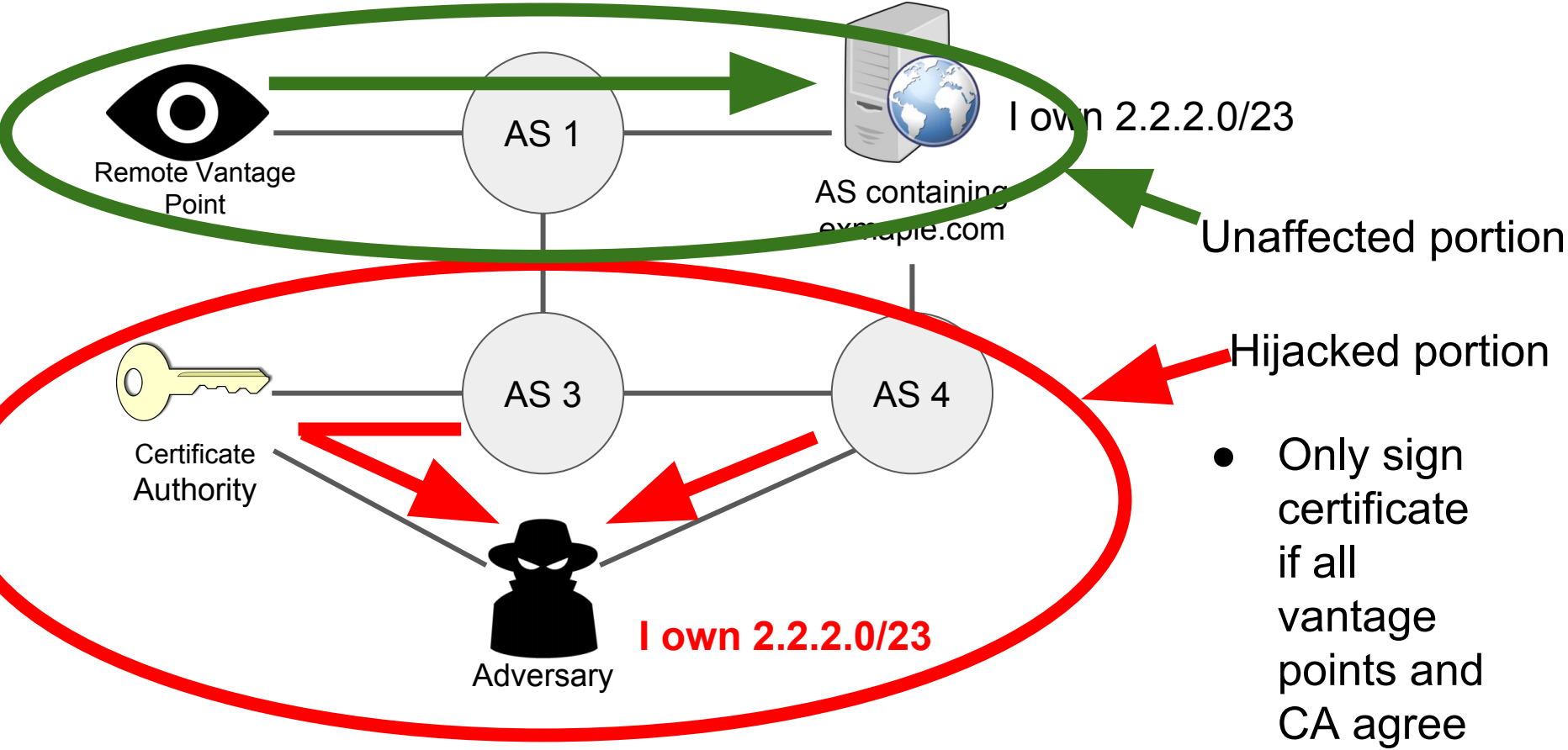
Multiple Vantage Points



Multiple Vantage Points



Multiple Vantage Points



- 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

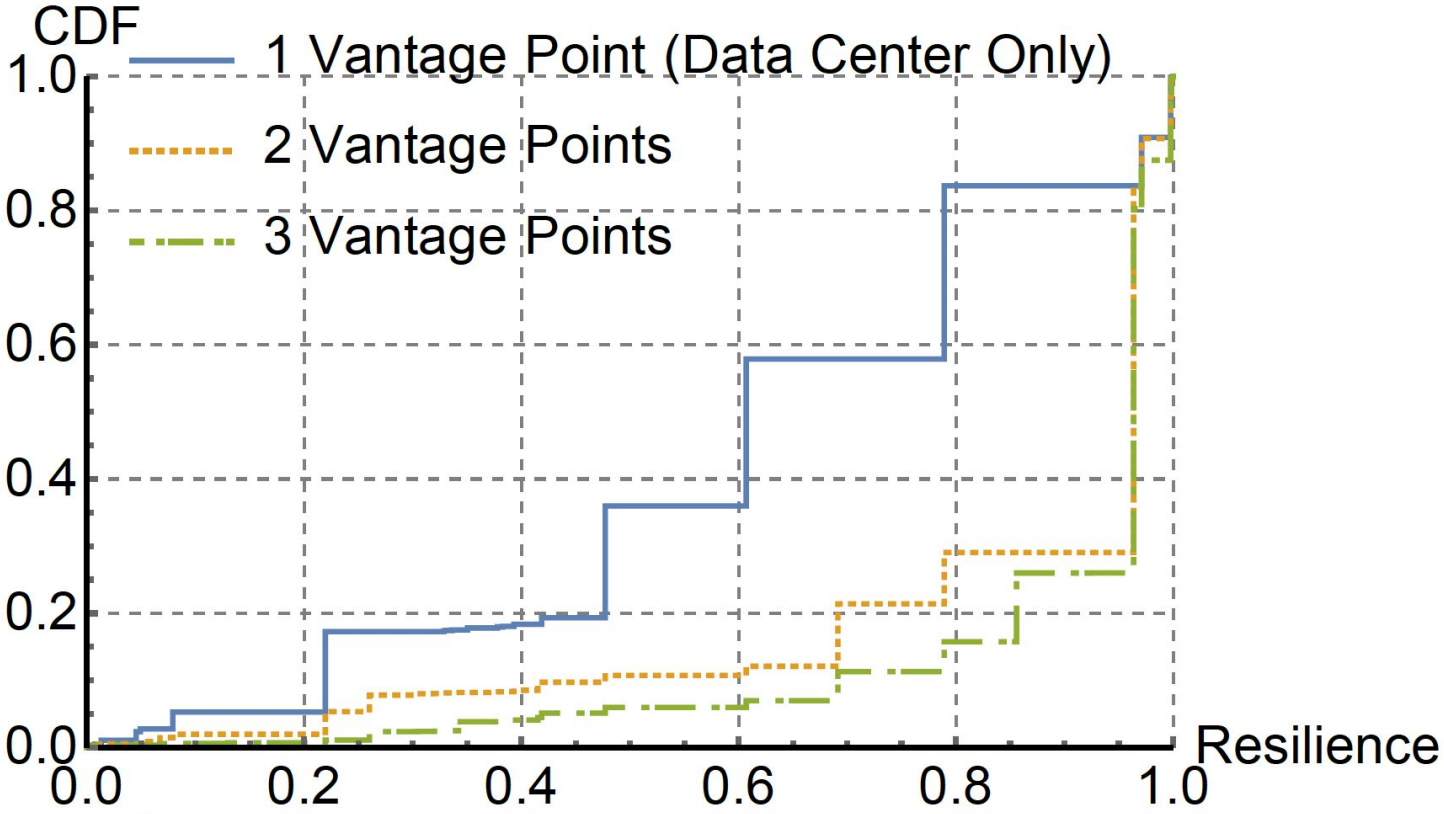
1
2
3

```
52.29.173.72 - - [29/Jul/2018 18:15:09] "GET /.well-
34.213.106.112 - - [29/Jul/2018 18:15:10] "GET /.wel
13.58.30.69 - - [29/Jul/2018 18:15:10] "GET /.well-k
66.133.109.36 - - [29/Jul/2018 18:15:10] "GET /.well
^C
```

Data Center in AS 13649

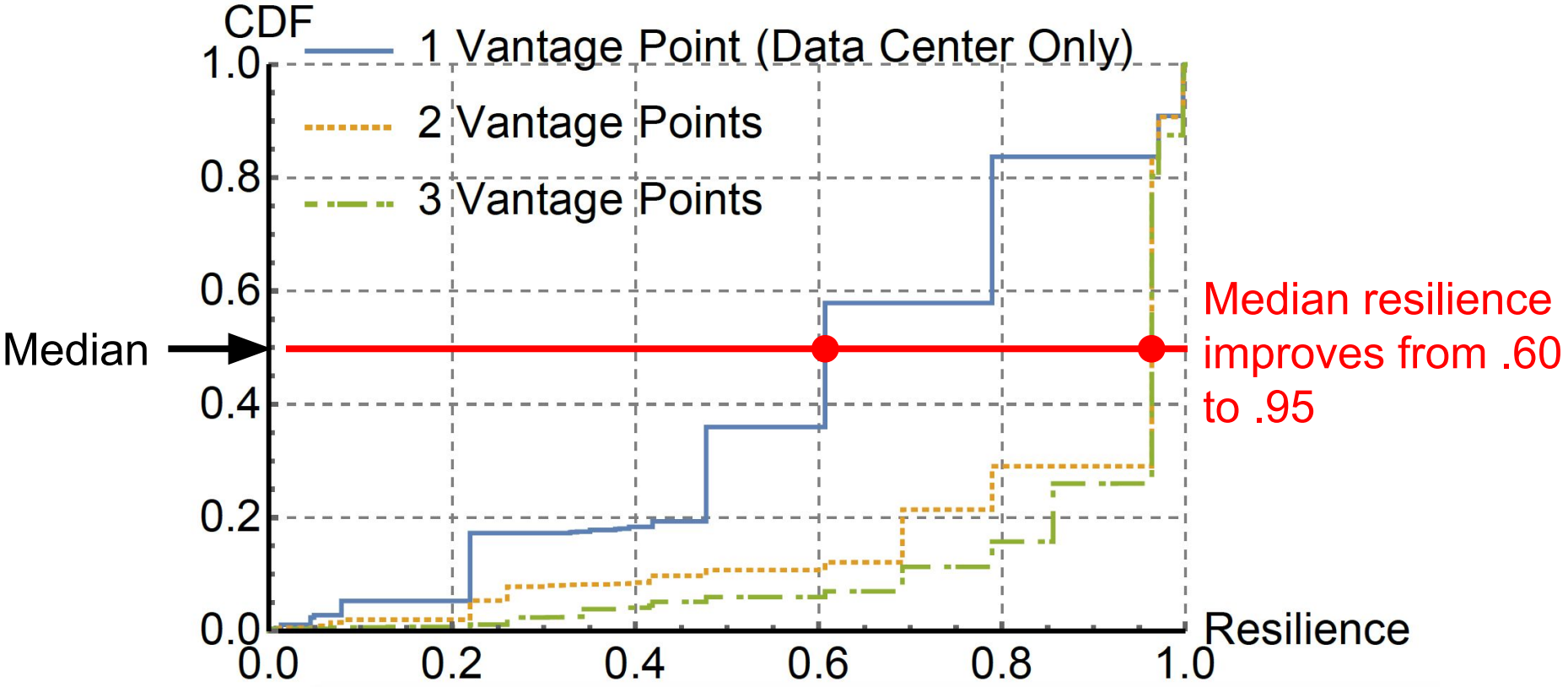
Resilience Improvement of Multiple Vantage Points

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



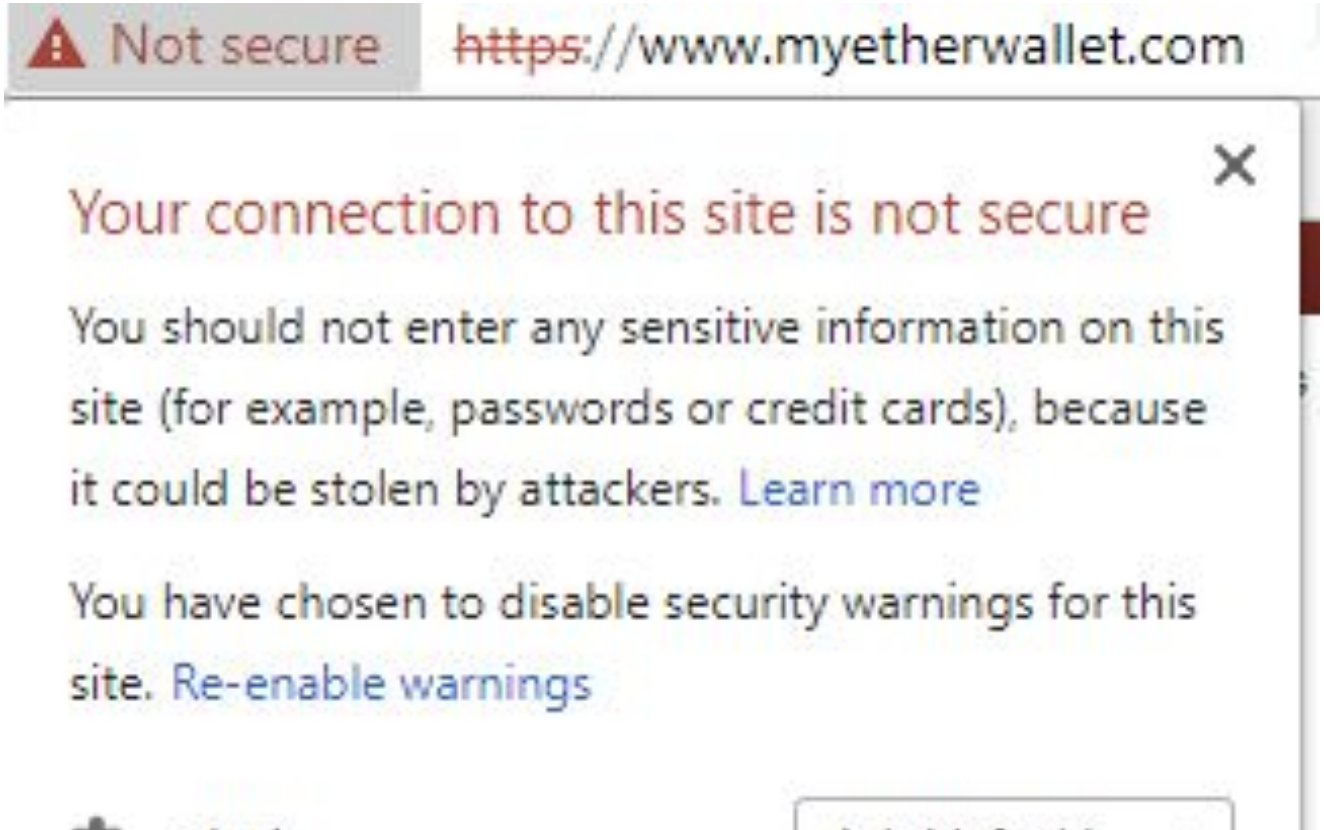
Other Defenses

- CAs:
  - BGP Monitoring
  - CA Prefix Length
  - CA Resilience
- Domains:
  - CAA DNS Records
  - DNSSEC

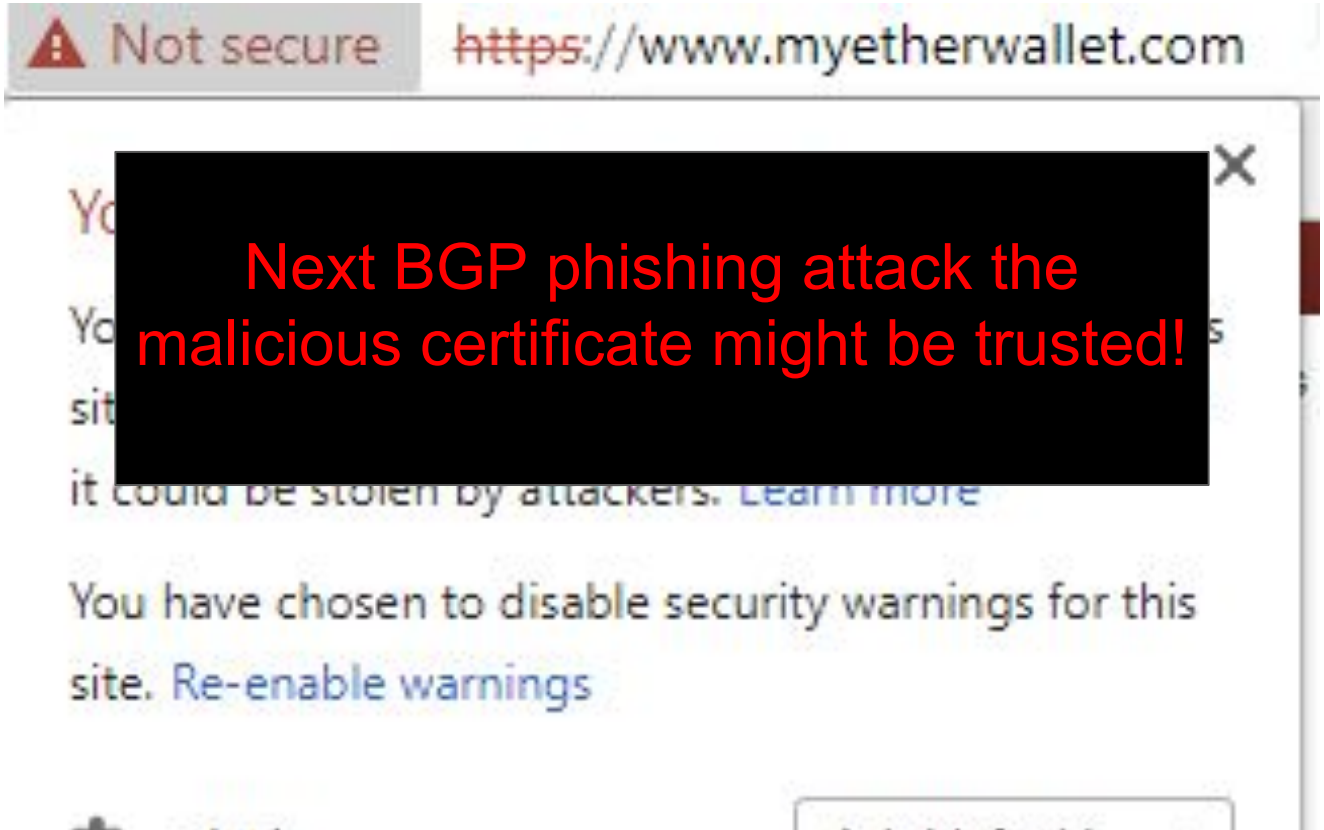
Overview

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

Takeaways


Not secure
https://www.myetherwallet.com
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


Not secure
https://www.myetherwallet.com
Next BGP phishing attack the malicious certificate might be trusted!
You have chosen to disable security warnings for this site. Re-enable warnings

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

OPEN TECHNOLOGY FUND

NSF

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

Takeaways

Questions?

- 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

OPEN TECHNOLOGY FUND

NSF

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