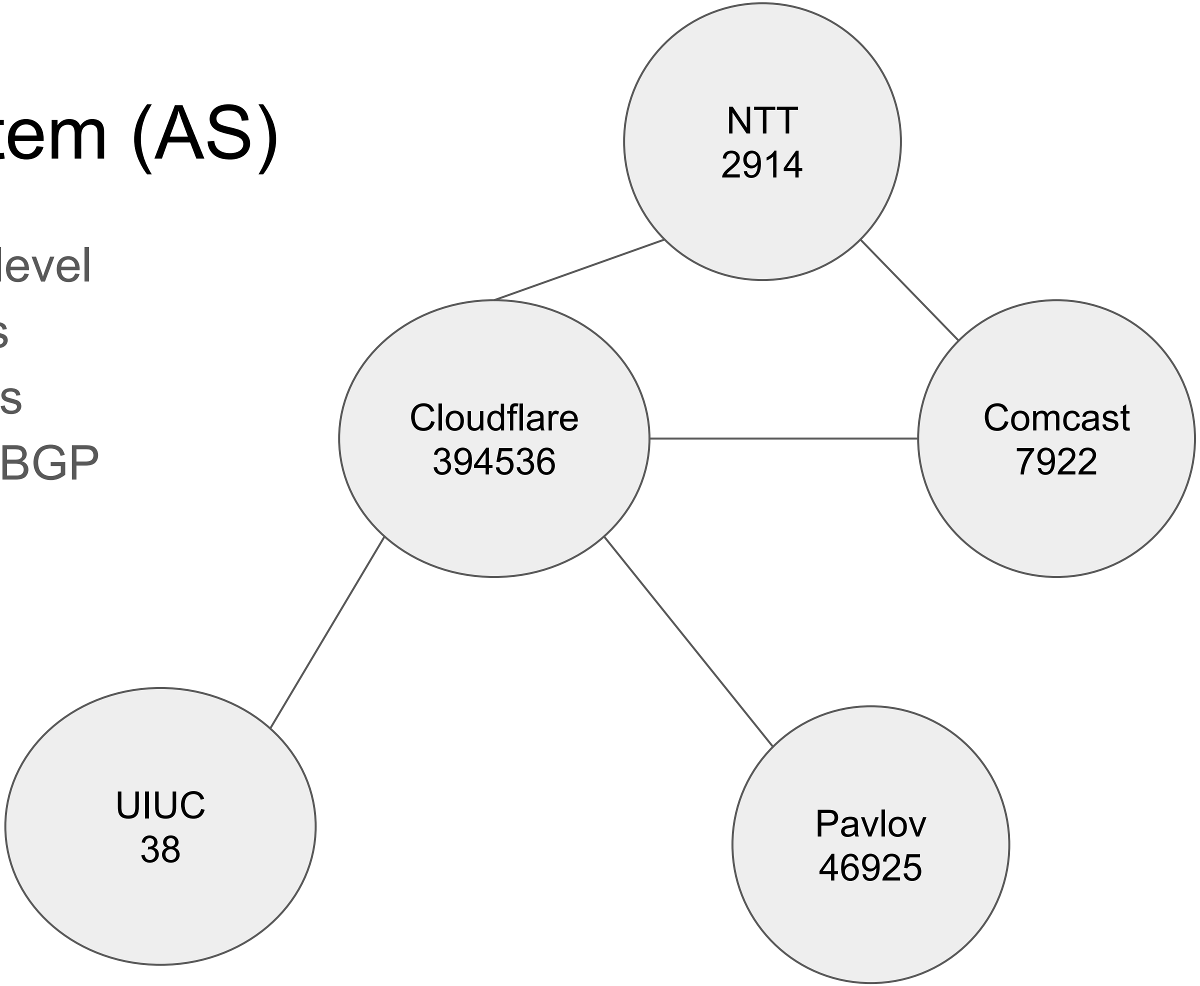
Bamboozling Certificate Authorities with BGP

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

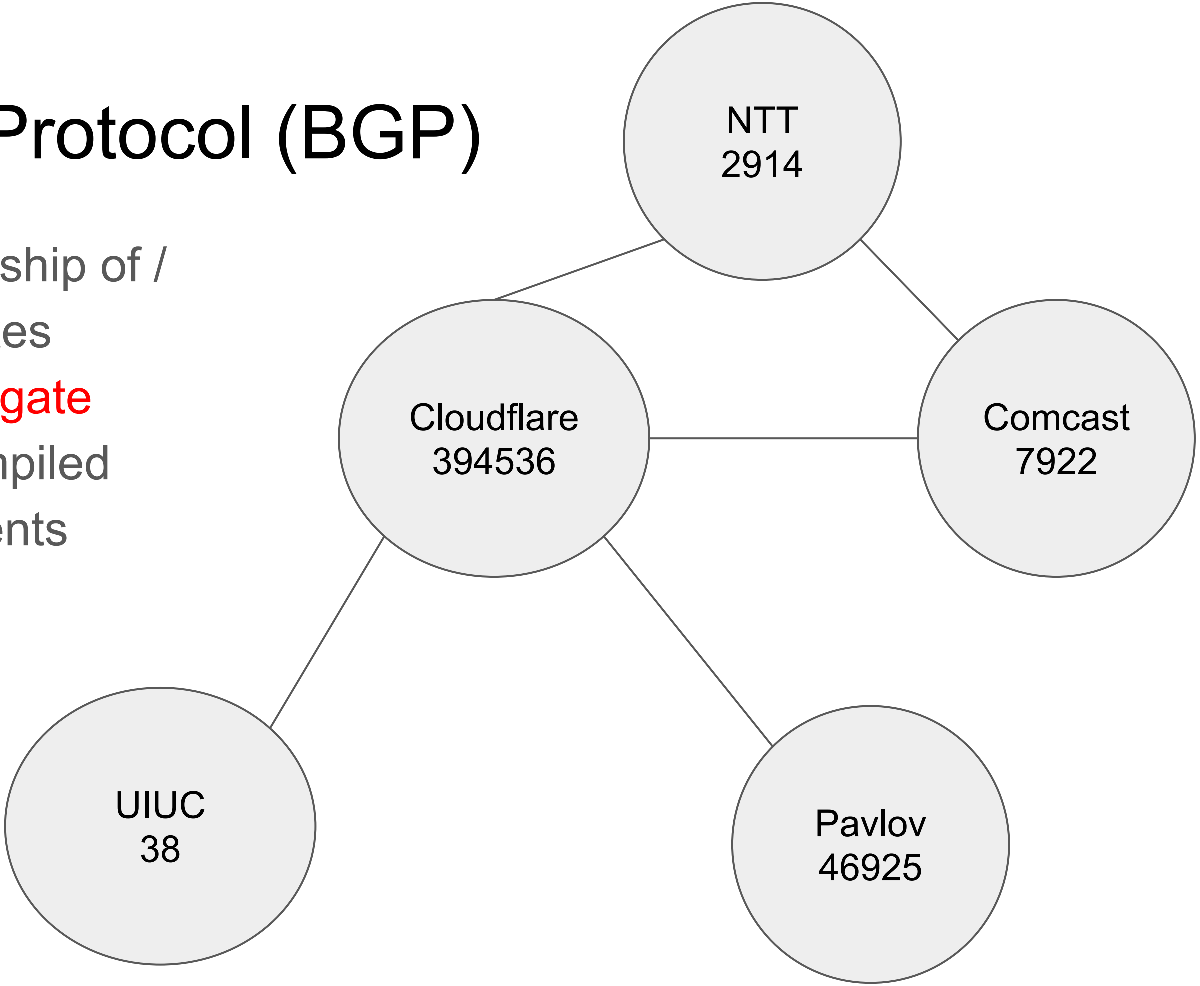
Autonomous System (AS)

- Internet at the highest level
- Routing within an AS is completely autonomous
- Inter-AS Routing uses BGP



Border Gateway Protocol (BGP)

- ASes announce ownership of / reachability to IP prefixes
- Announcements propagate
- Routing tables are compiled based on announcements



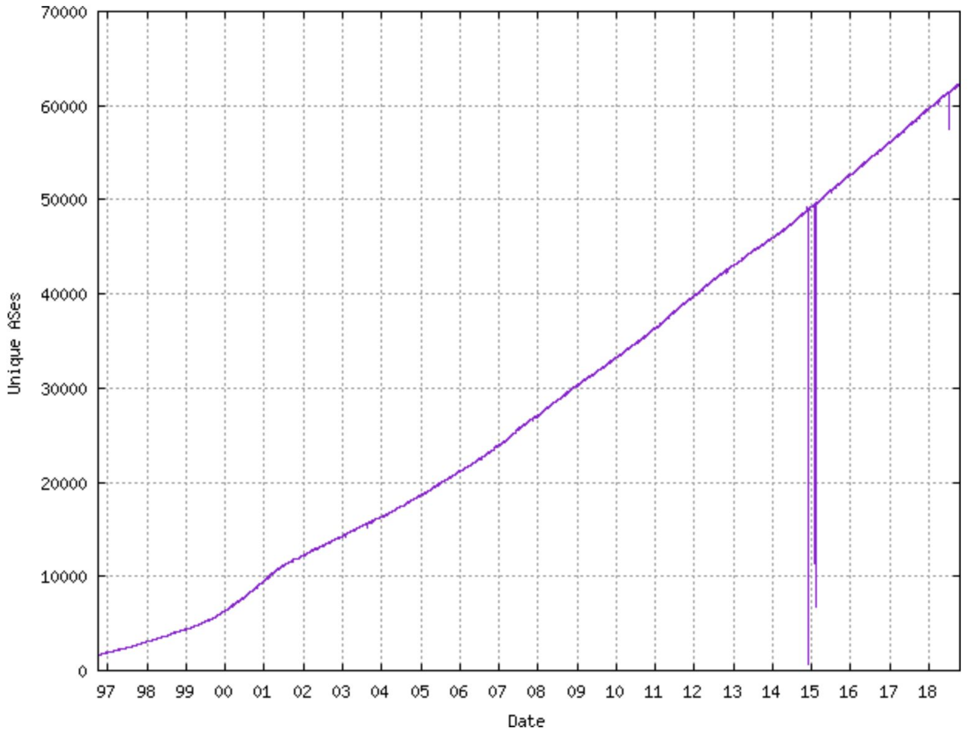
BGP hijack

Using false announcements to corrupt routing tables of others

Threat Model

- Anyone with total control over an AS!
- 60K+ unique ASes as of Oct 2018
- 3000 new ASes per year since 1997

Unique ASes

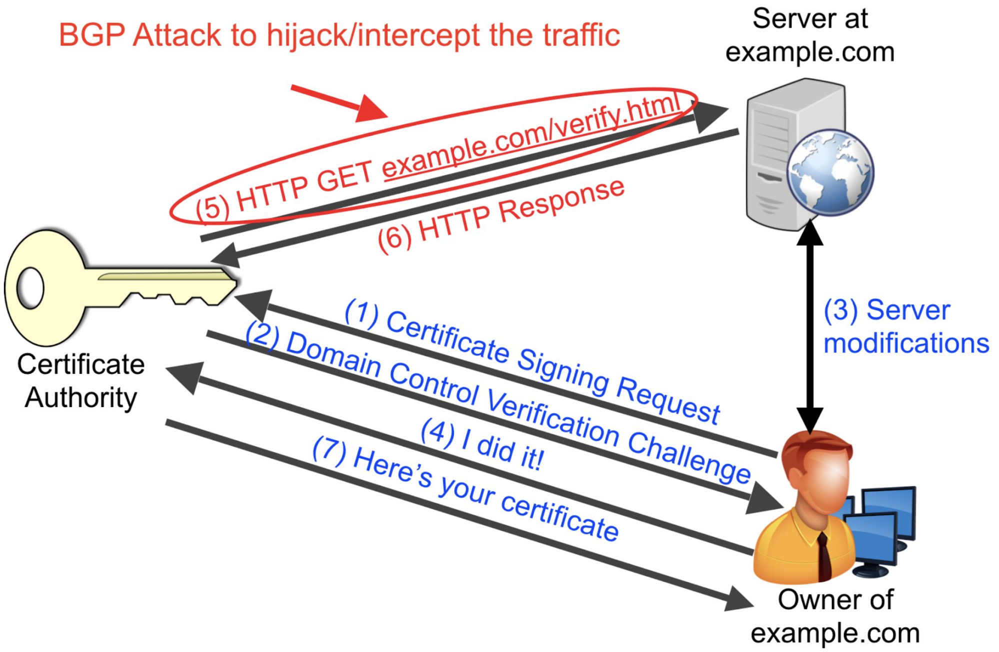


Plot Range: 30-Sep-1996 1430 to 16-Oct-2018 2116

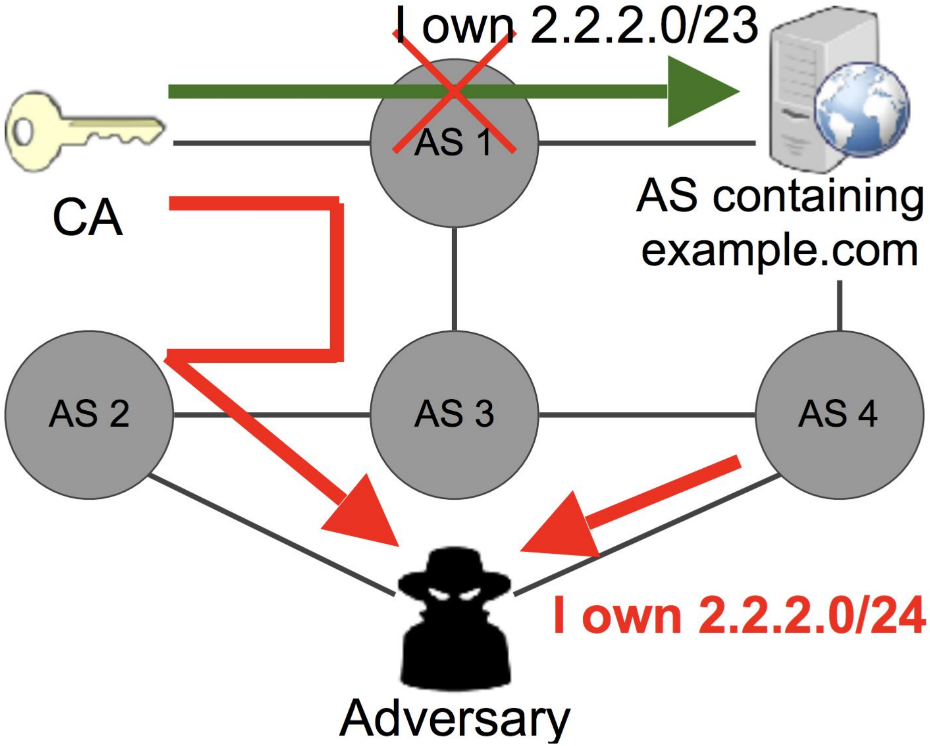
What can an Adversary do with BGP hijacks?

Goal: Fool a CA into authorizing the fake server

MITM between a Certificate Authority and a victim domain


BGP Attack to hijack/intercept the traffic
Server at example.com
(5) HTTP GET example.com/verify.html
(6) HTTP Response
Certificate Authority
(1) Certificate Signing Request
(2) Domain Control Verification Challenge
(3) Server modifications
(4) I did it!
(7) Here's your certificate
Owner of example.com

Sub-Prefix Hijack Attack



- Effective in intercepting traffic
- Easily detectable

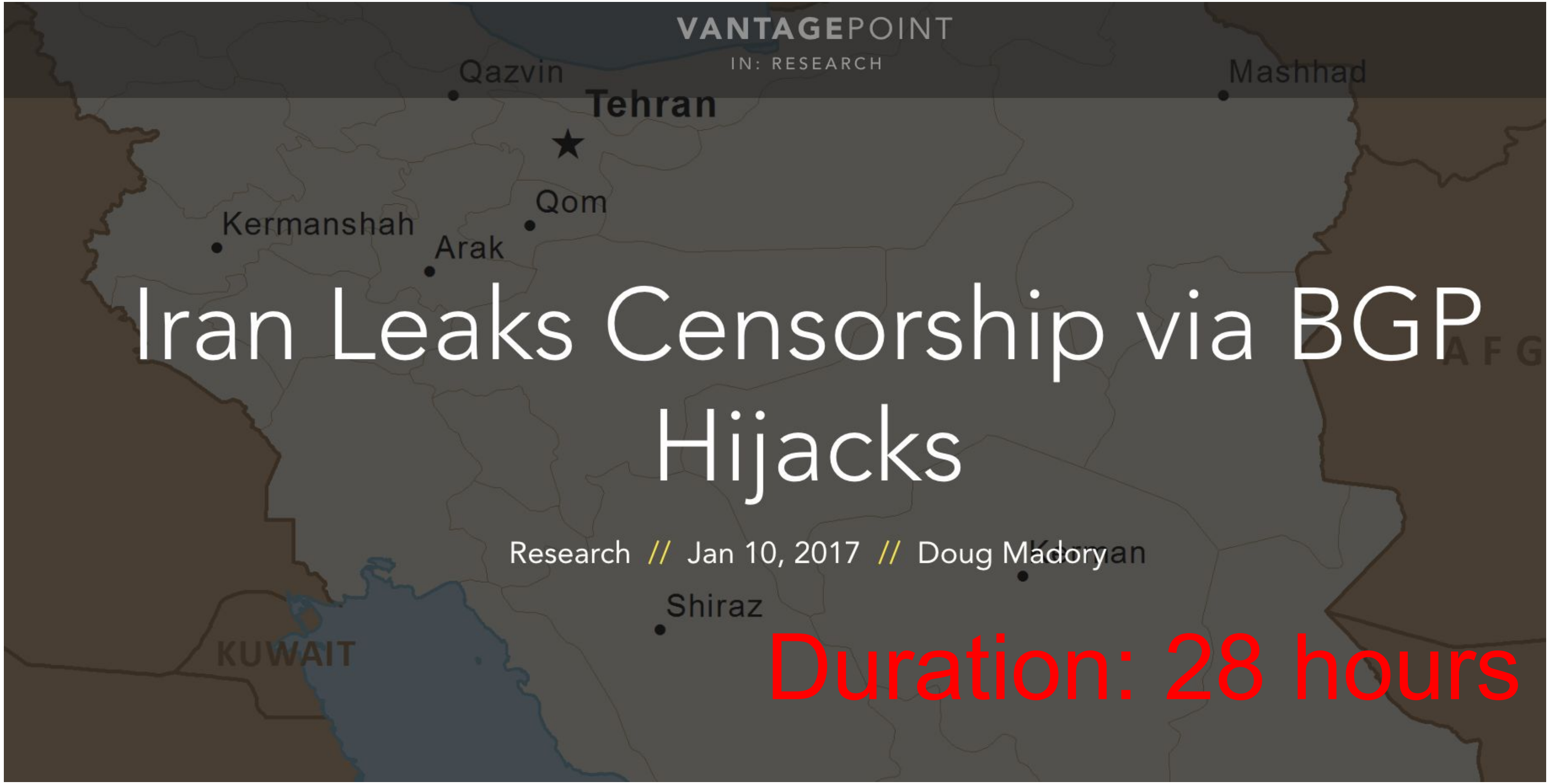
Case: YouTube hijacked by Pakistan! (2008)

RYAN SINGEL SECURITY 02.25.08 10:37 AM

PAKISTAN'S ACCIDENTAL YOUTUBE RE-ROUTING EXPOSES TRUST FLAW IN NET

DT: 2 hours

Case: Iran tried to censor porn (2017)



VANTAGEPOINT

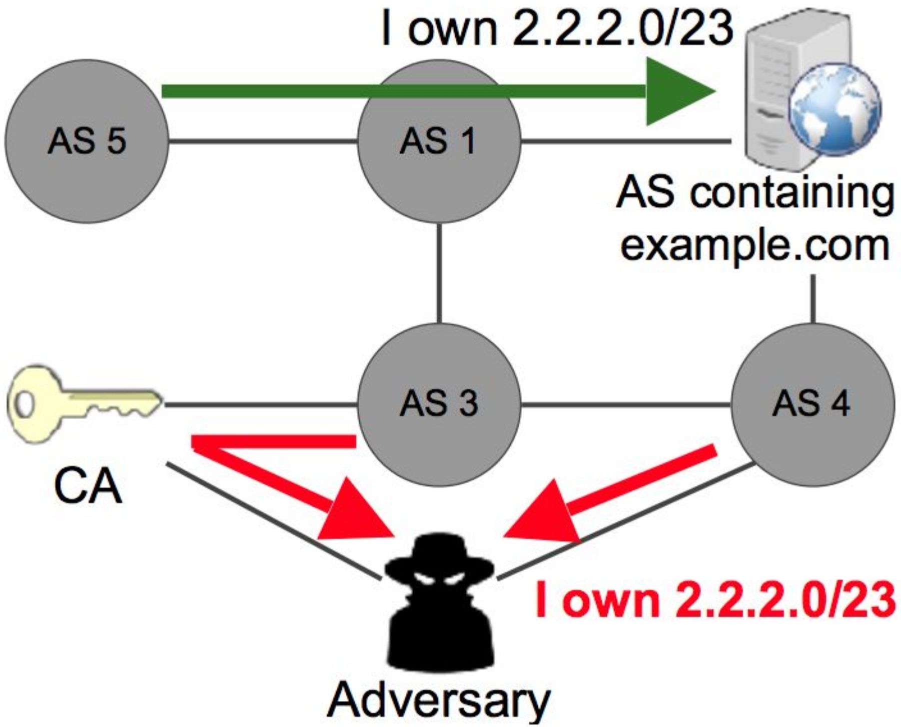
IN: RESEARCH

Iran Leaks Censorship via BGP Hijacks

Research // Jan 10, 2017 // Doug Madory

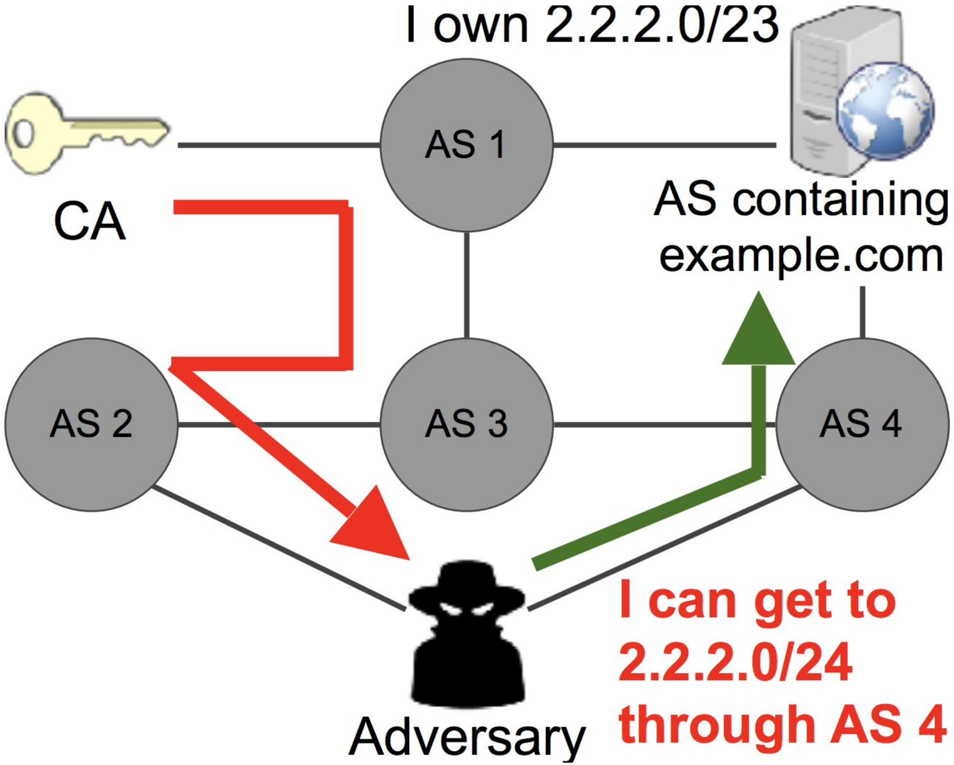
Duration: 28 hours

Same Prefix Hijack



- Less effective in intercepting traffic
- Stealthier compared to Sub-Prefix attacks

Path poisoning attacks (Proposed by the Authors)


I own 2.2.2.0/23
CA
AS 1
AS containing example.com
AS 2
AS 3
AS 4
Adversary
I can get to 2.2.2.0/24 through AS 4

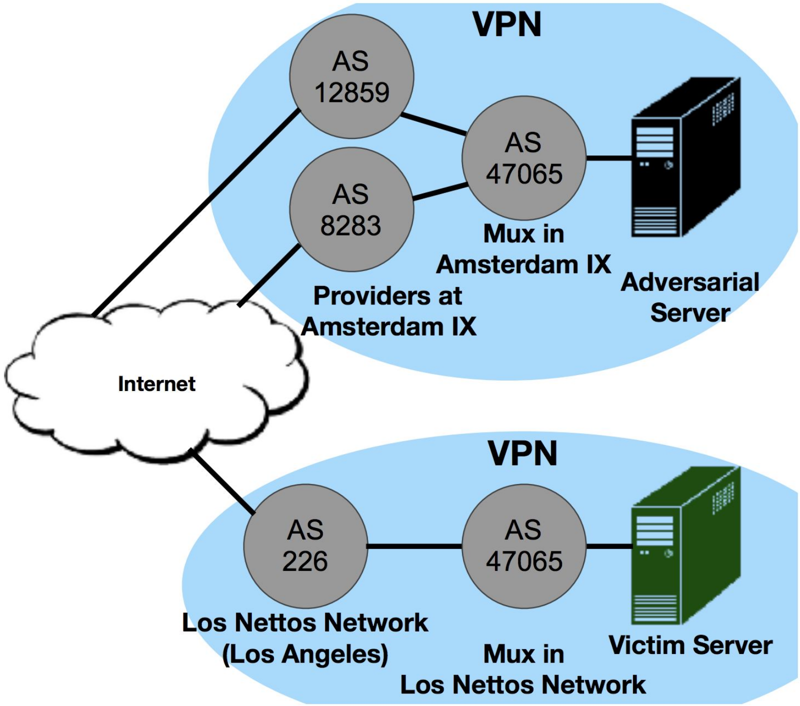
- Effective!
- Stealthy!

Cause of BGP hijacks

- Incompetent network admins?
- Malicious adversaries?

Experiment

- Set up an Adversary server and a victim server under ASes controlled by PEERING
- Approached CAs after BGP hijack

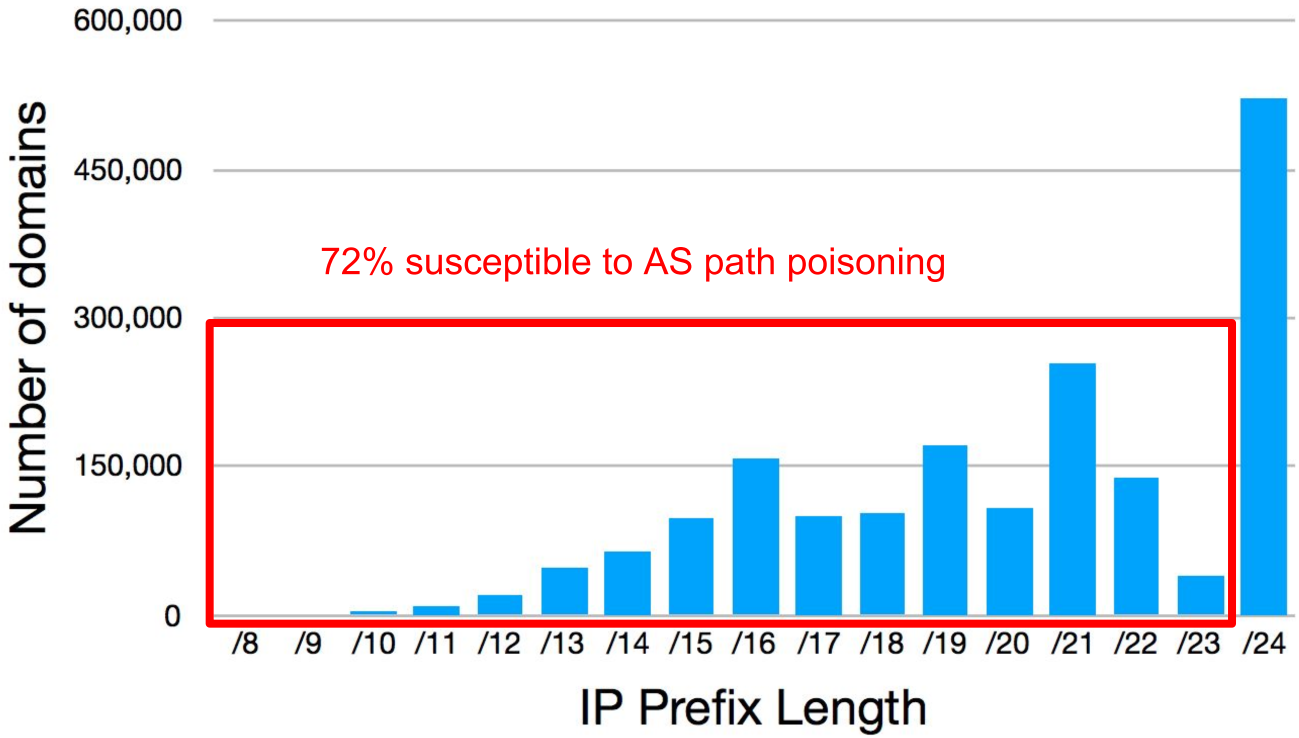


Results from the author’s experiments

	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

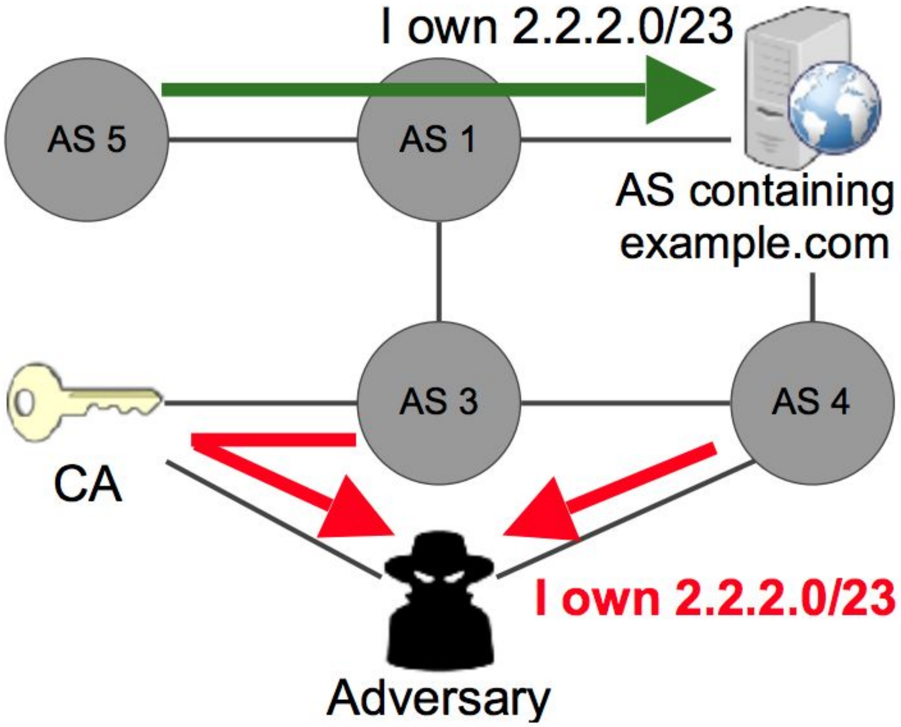
Quantifying vulnerability of domains

Vulnerable Domains running TLS



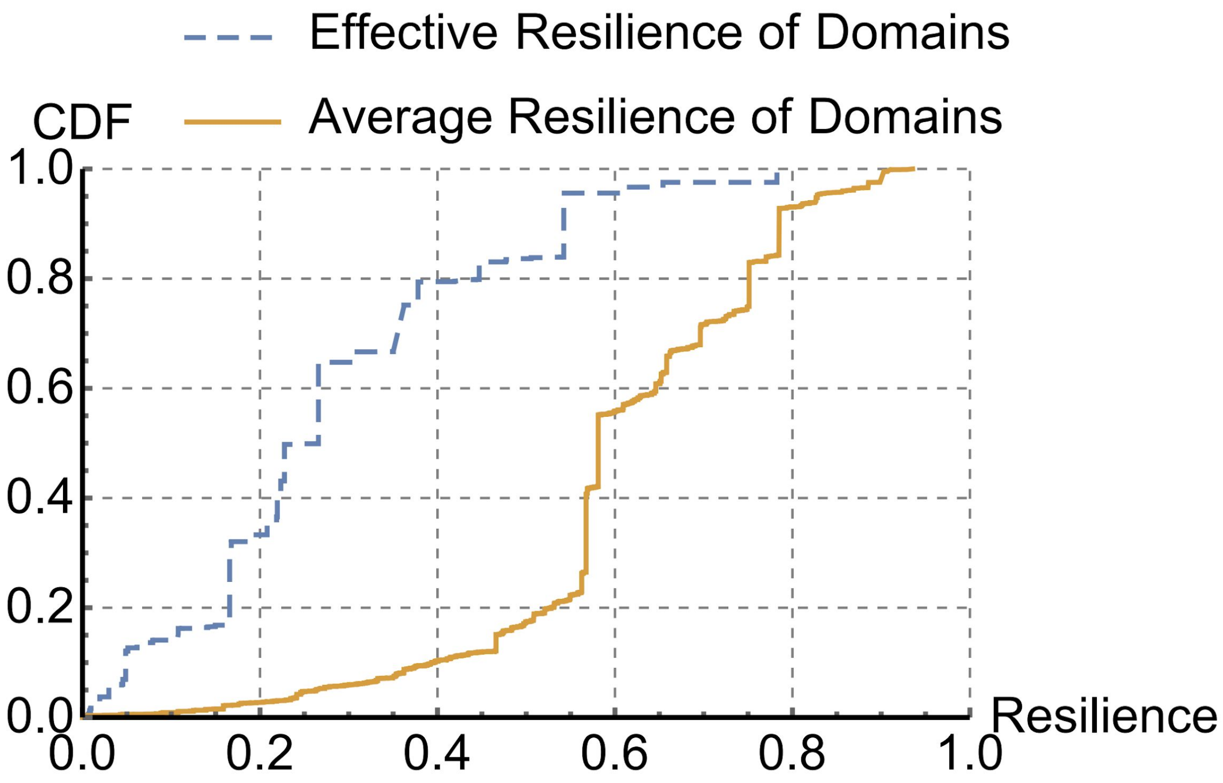
72% susceptible to AS path poisoning

Resilience of TLS domains



Probability of CA routing to the correct AS containing the real server

Domain resilience averaged over CAs

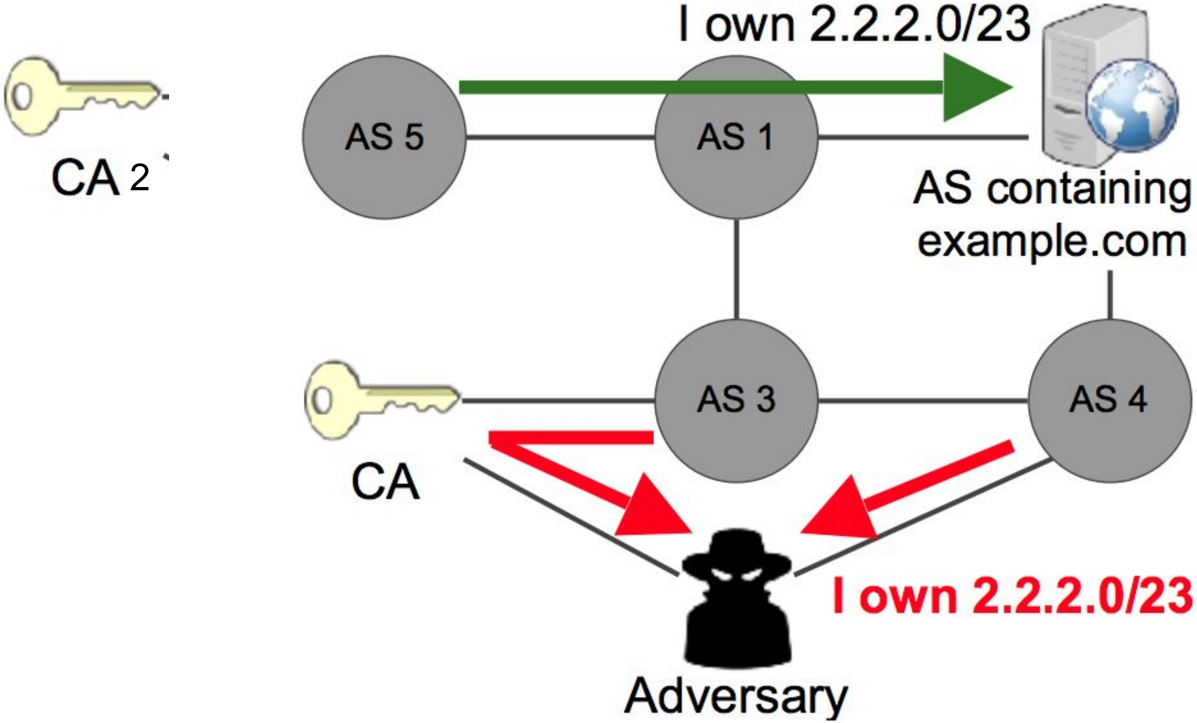


CA’s defense against BGP hijacks

Multiple vantage points

- Protects against same prefix hijacks
- Vantage points need to be thoughtfully chosen
- Improves the “resilience”

Multiple vantage points



Detect malicious/ malformed route announcements

- More flexible against all kinds of attacks
- Uses a timing based analysis
- Needs low false-positive rate
- Harder to deploy

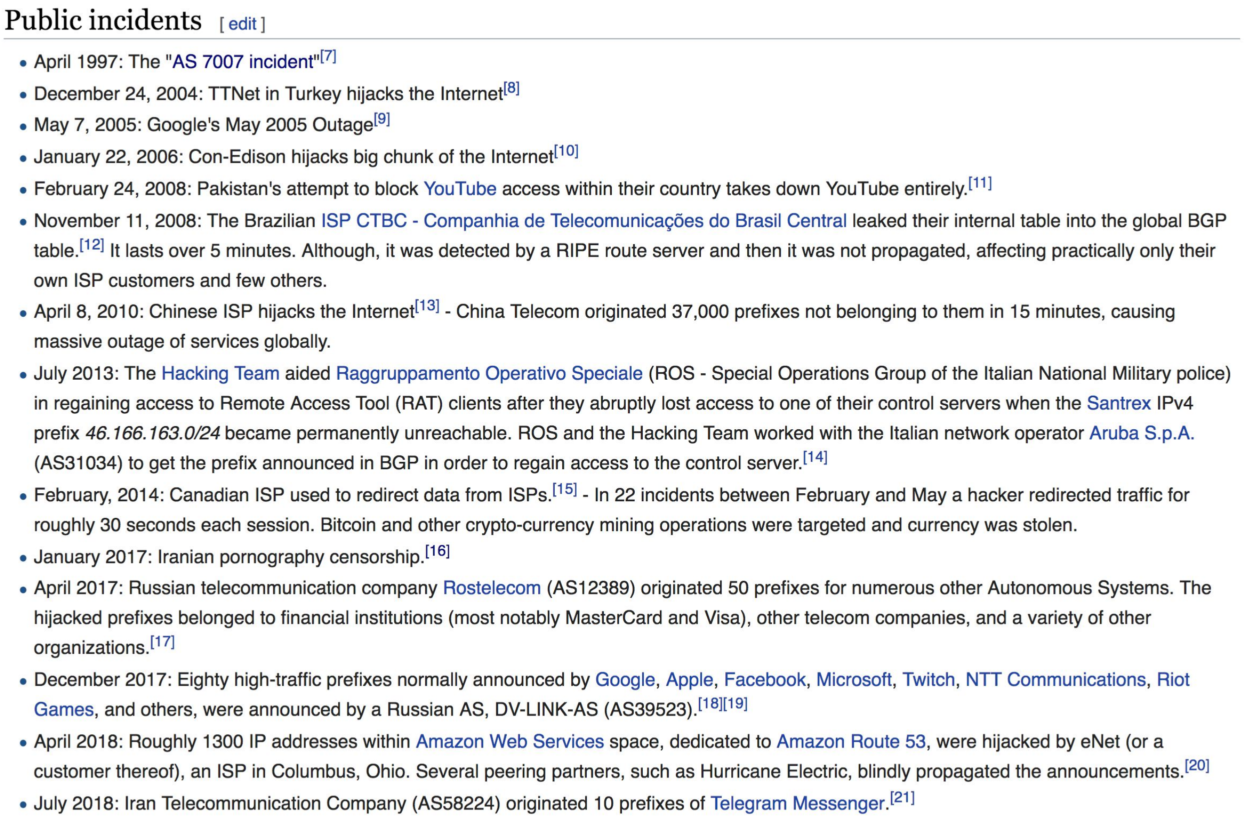
What else can BGP attacks do?

- Deanonymize Tor users
- Attack the Bitcoin protocol
- Bypass US surveillance laws
    - (So the NSA can spy on you)

Inherent Problems with Inter-AS routing / BGP

- Web of trust
- Correcting bad routes requires manual intervention
  - Attacks can potentially last hours
- New, secure protocols are hard to deploy (See secure BGP)

List of BGP hijack incidents on Wikipedia



Public incidents [edit]

- April 1997: The "AS 7007 incident"[7]
- December 24, 2004: TTNet in Turkey hijacks the Internet[8]
- May 7, 2005: Google's May 2005 Outage[9]
- January 22, 2006: Con-Edison hijacks big chunk of the Internet[10]
- February 24, 2008: Pakistan's attempt to block YouTube access within their country takes down YouTube entirely.[11]
- November 11, 2008: The Brazilian ISP CTBC - Companhia de Telecomunicações do Brasil Central leaked their internal table into the global BGP table.[12] It lasts over 5 minutes. Although, it was detected by a RIPE route server and then it was not propagated, affecting practically only their own ISP customers and few others.
- April 8, 2010: Chinese ISP hijacks the Internet[13] - China Telecom originated 37,000 prefixes not belonging to them in 15 minutes, causing massive outage of services globally.
- July 2013: The Hacking Team aided Raggruppamento Operativo Speciale (ROS - Special Operations Group of the Italian National Military police) in regaining access to Remote Access Tool (RAT) clients after they abruptly lost access to one of their control servers when the Santrex IPv4 prefix *46.166.163.0/24* became permanently unreachable. ROS and the Hacking Team worked with the Italian network operator Aruba S.p.A. (AS31034) to get the prefix announced in BGP in order to regain access to the control server.[14]
- February, 2014: Canadian ISP used to redirect data from ISPs.[15] - In 22 incidents between February and May a hacker redirected traffic for roughly 30 seconds each session. Bitcoin and other crypto-currency mining operations were targeted and currency was stolen.
- January 2017: Iranian pornography censorship.[16]
- April 2017: Russian telecommunication company Rostelecom (AS12389) originated 50 prefixes for numerous other Autonomous Systems. The hijacked prefixes belonged to financial institutions (most notably MasterCard and Visa), other telecom companies, and a variety of other organizations.[17]
- December 2017: Eighty high-traffic prefixes normally announced by Google, Apple, Facebook, Microsoft, Twitch, NTT Communications, Riot Games, and others, were announced by a Russian AS, DV-LINK-AS (AS39523).[18][19]
- April 2018: Roughly 1300 IP addresses within Amazon Web Services space, dedicated to Amazon Route 53, were hijacked by eNet (or a customer thereof), an ISP in Columbus, Ohio. Several peering partners, such as Hurricane Electric, blindly propagated the announcements.[20]
- July 2018: Iran Telecommunication Company (AS58224) originated 10 prefixes of Telegram Messenger.[21]

Inherent problems with certificate authorities

- Bar for becoming a CA is low
- Needs more reliable verifying protocols
    - Out of band verification
        - Reliable
        - Inefficient

Takeaway

- BGP hijacks are still happening. How do we make BGP better?
- Certificate authorities make profit-driven decisions that could compromise security. How do we make CAs better?
- Successful BGP hijacks can lead to devastating results

BAMBOOZLED