ATHENE
National Research Center for Applied Cybersecurity

Let‘s Attack Let‘s Encrypt

Dr. Haya Shulman

ATHENE | Fraunhofer SIT
Division Director “Cybersecurity Analytics and Defenses”

Black Hat USA Video Conference, August 2021

Overview

- Ownership validation is vulnerable
- Downgrade attacks
- Experimental issuance of fraudulent certificates
- Countermeasures

Overview

- Ownership validation is vulnerable
- Downgrade attacks
- Experimental issuance of fraudulent certificates
- Countermeasures

Domain Validation

Who owns that domain?

https://www.flickr.com/photos/ben_lawson/155595430

Domain Validation

Who owns that domain?

Domain Validation (DV)	**Automated**	**Fast**	**Free/Cheap**
Organisation Validation (OV)	Manual	Slow	Expensive
Extended Validation (EV)	Manual	Slow	Expensive

Domain Validation

Who owns that domain?

Domain Validation (DV)	**Automated**	**Fast**	**Free/Cheap**
Organisation Validation (OV)	Manual	Slow	Expensive
Extended Validation (EV)	Manual	Slow	Expensive

} > 95% certificates market

Domain Validation

Who owns that domain?

Domain Validation (DV)	**Automated**	**Fast**	**Free/Cheap**
Organisation Validation (OV)	Manual	Slow	Expensive
Extended Validation (EV)	Manual	Slow	Expensive

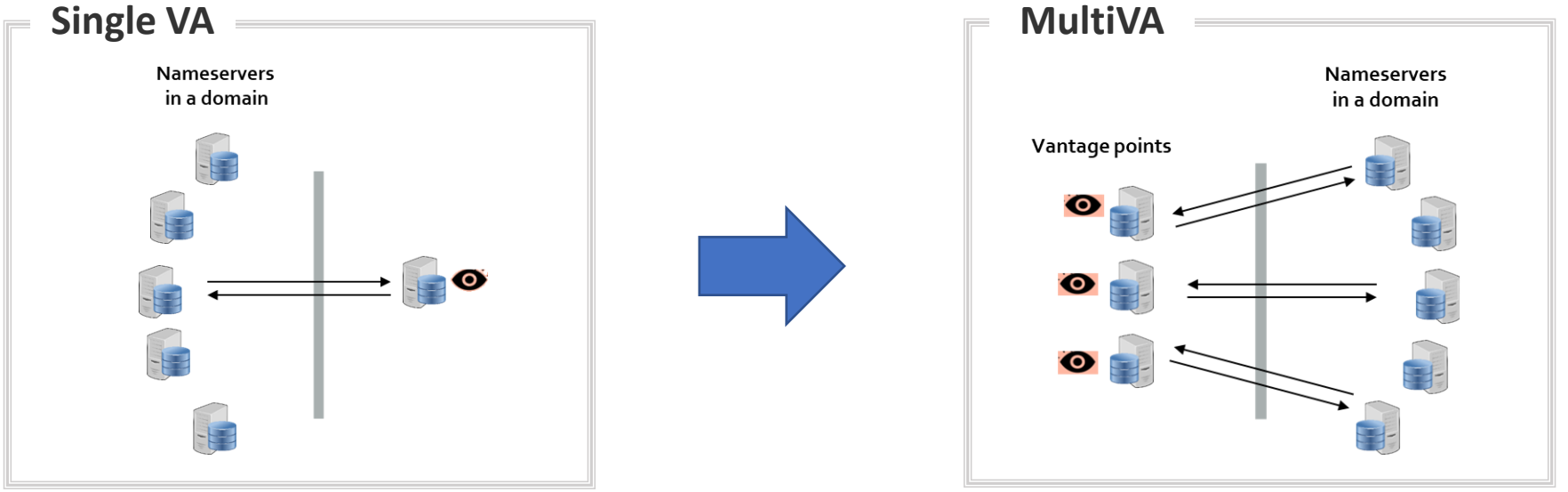
Vulnerable!
Fraudulent certificates via off-path attacks
[USENIX2018,CCS2018]

> 95% certificates market

Let's Encrypt Certificate Authority

- Leads the certificates market
- Among fastest growing CAs
- Over 1 billion certificates, serves over 200M websites

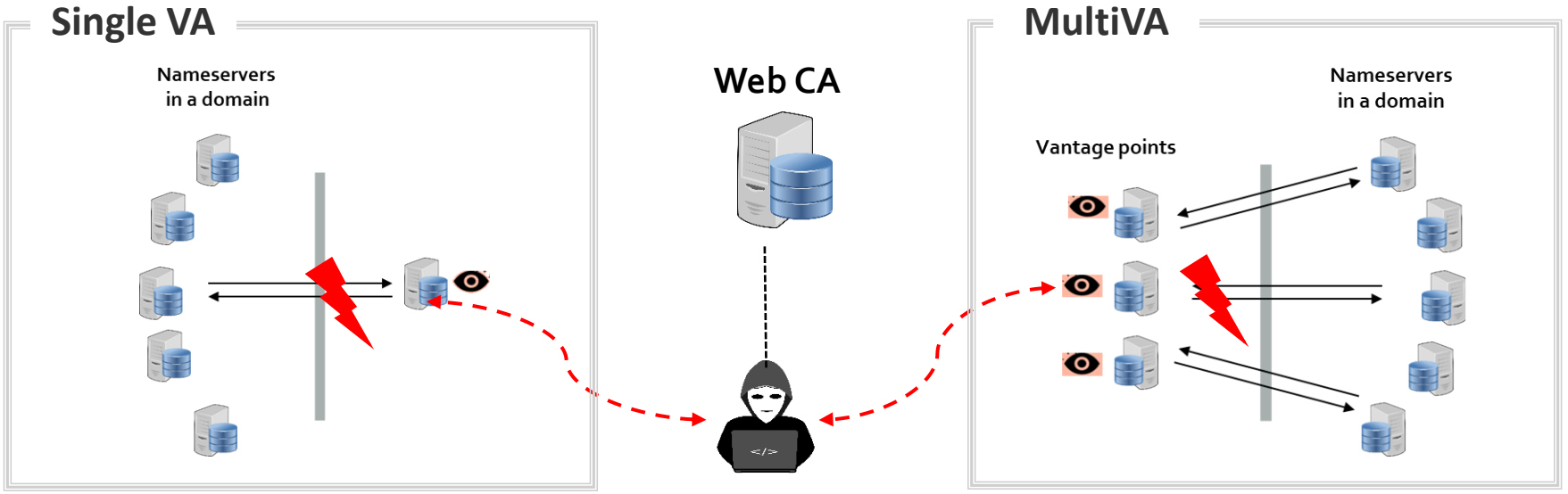
- First to deploy distributed Domain Validation with MultiVA
- In 2020 MultiVA in production environment of Let's Encrypt



Let's Encrypt

Attacker cannot hijack multiple VAs simultaneously

- Assumption: even strong adversaries have limited capabilities
- Simulations in [USENIX2021] showed:
  - MultiVA detects 94% of the BGP prefix hijacks
  - >90% of ASes topologically incapable of launching BGP attacks against most domains
  - Improves resilience of avg domain to attacks from 97% of ASes on the Internet

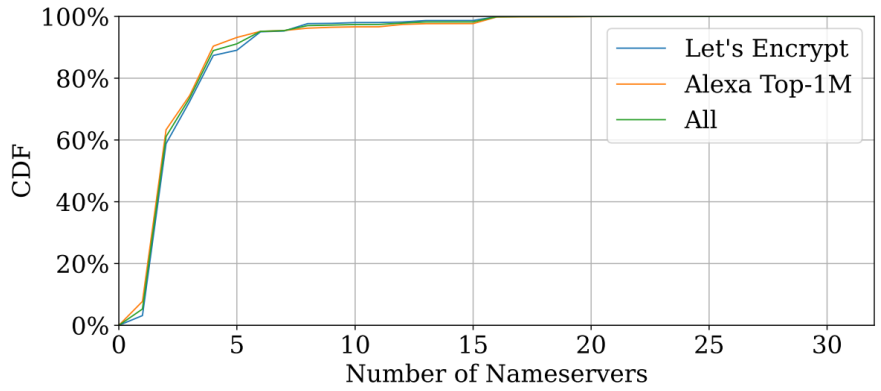


Overview

- Ownership validation is vulnerable
- Downgrade attacks
- Experimental issuance of fraudulent certificates
- Countermeasures

Nameserver Selection
Uniformly at random

- Goal: distribute the load among nameservers
- Unpredictable selection among good performing servers



Number of nameservers per domain

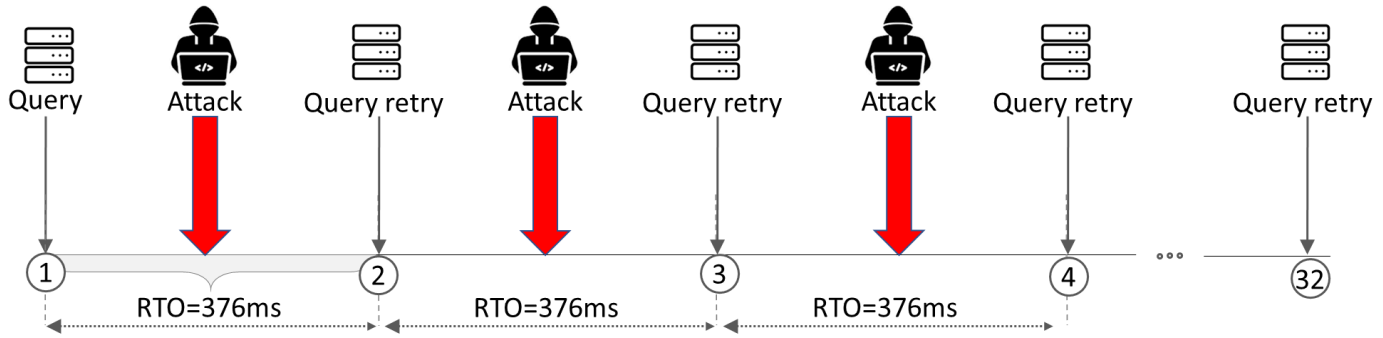
- All SW avoid poorly performing servers
- Packet loss or high latency

DNS Software	Query distribution to servers	Block (min)	% queries to t.o. servers
Unbound	queries all n servers with <400ms with probability $1/n$	15	1%
Knot	>35% queries to fastest server & 10% to others	10	5%
Bind	>95% queries to fastest server & 1% to others	30	1%
PowerDNS	>97% queries to fastest server & 1% to others	3	1%
Windows DNS	uniform query distribution to available servers	<1	1%

Table 1: Server selection in popular DNS implementations.

Nameserver Elimination
Simulate loses

- Cause DNS software at vantage point to avoid a nameserver
- Repeat per nameserver, block all except one (selected) nameserver

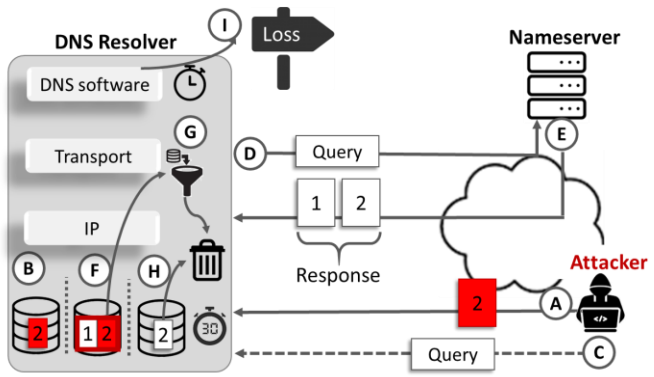


Downgrade Attack via Nameserver Elimination

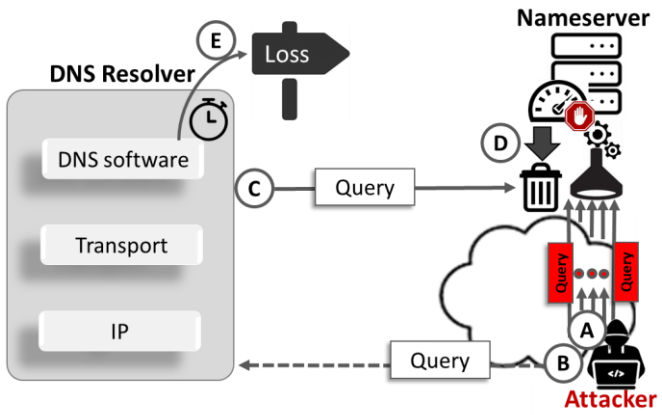
on-path easy… off-path?

- Force the VP to query NS of attacker‘s choice
  - which has vulnerabilities, e.g., can be hijacked

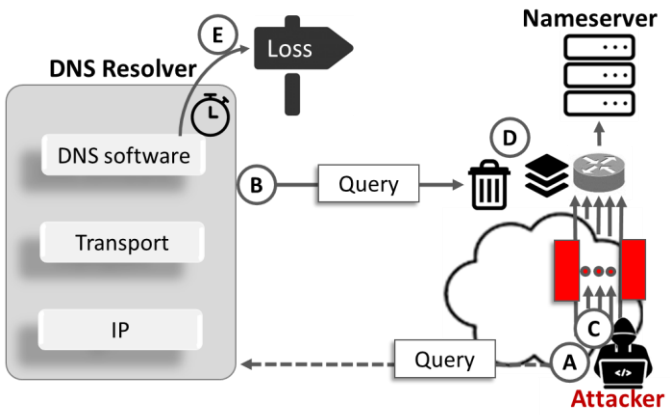
- Loss via fragment mis-association
- Exploit fragmentation



- Loss via excess query rate
- Exploit Rate limiting



- Loss via router buffer overflow
- Low rate bursts



Domains Vulnerable to Off-Path Downgrade Attack

- Apply to 24% of Let's Encrypt-certified domains and 20% of 857K-top Alexa domains

- Loss via fragment mis-association

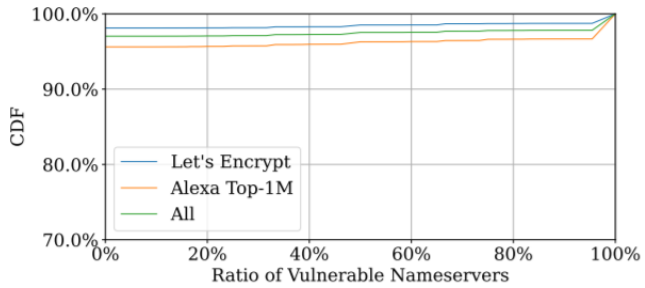


Figure 3: Nameservers per domain vulnerable to frag.

- 1.88% of Let's Encrypt domains and 4.39% of 1M Alexa domains

- Loss via excess query rate

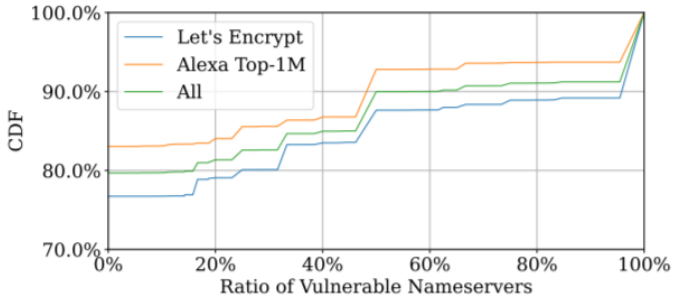


Figure 5: Nameservers per domain vulnerable to rate-limiting.

- 23.27% of Let's Encrypt domains and 16.95% of 1M Alexa domains

- Loss via router buffer overflow

Routers	Buffer sizes	Burst size	Loss rate
Brocade MLXe	1MB	>1550 packets	100%
Cisco Nexus 3064X	9MB	$>10^4$ packets	100%
Juniper EX4600	12MB	$>15 \cdot 10^3$ packets	92%
Cisco 6704	16MB	$18 \cdot 10^3$ packets	89%

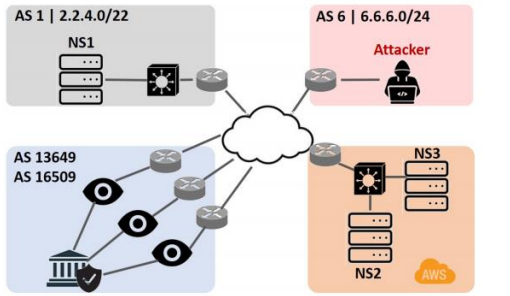
Overview

- Ownership validation is vulnerable
- Downgrade attacks
- Experimental issuance of fraudulent certificates
- Countermeasures

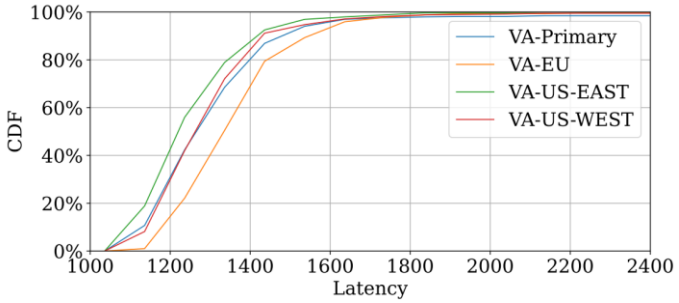
Issue Fraudulent Certificates, *Ethically* …

- Typically: estimate vulnerabilities to prefix hijacks via simulations
  - Good but limited representation of reality
- Idea: two-sided evaluation

- Fraudulent certificates for our own domains with Let‘s Encrypt



Issuing fraudulent Let’s Encrypt certs for our victim domains.



- We pin to servers that can be sub-prefix hijacked

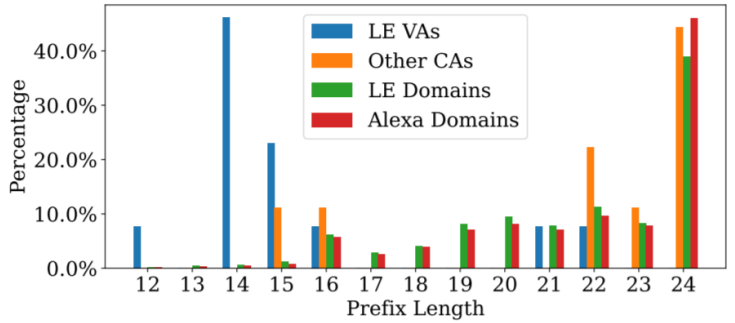


Figure 10: Network prefixes of CAs’ resolvers and of domains’ name-servers vulnerable to sub-prefix hijacks.

- Fraudulent certificates for real domains with our own setup of Let‘s Encrypt

	#Domains	#Nameservers	#ASes	Vuln.
Let’s Encrypt	1,014,056	98,502	8,205	24.53%
Alexa	856,887	171,656	15,899	20.92%
Total	1,858,165	227,734	17,864	22.76%

Table 2: Dataset of domains.

What About Other CAs?

CA	#Vantage Points	Sub-prefix attack	#Time outs	Block (min)	MultiVA
Digicert	1	✗	1	5	✗
Sectigo	1	✗	2	10+	✗
GoDaddy	1	✓	10	10+	✗
GlobalSign	1	✓	4	10+	✗
Certum-Google	20+	✓	2	10+	✗
Certum-Cloudflare	1	✗	16	10+	✗
Let's Encrypt	4	✓	2	15	✓
Actalis	1	✓	2	10+	✗

Table 4: Infrastructure of popular CAs and our evaluations.

Overview

- Ownership validation is vulnerable
- Downgrade attacks
- Experimental issuance of fraudulent certificates
- Countermeasures

Countermeasures
Attacks can be blocked

- Unpredictable VA selection: from a large set of VAs
- Resilient nameserver selection: select randomly out of all nameservers
- Turning off caches: makes the attack more difficult to launch
- Preventing BGP hijacks with RPKI: only prevents the hijack attacks but not other, e.g., [CCS2018]
- Detecting fraudulent certificates with CT

Conclusions

- Verifying ownership over domains is essential for bootstrapping cryptography
- DV is automated, fast, cheap and widely used
  - Single VA is vulnerable [USENIX2018, CCS2018]
- Let‘s Encrypt with MultiVA is vulnerable downgrade attacks
  → reduce validation to attacker selected nameserver
- Ownership verification with DV although simple is yet to be secured

Full paper:
Tianxiang Dai, Haya Shulman, Michael Waidner: *Let's Downgrade Let's Encrypt;* ACM Conf. on Computer and Communications Security (CCS), Nov. 2021.

תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Vielen Dank!

Dank je wel!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

Grazie mille!

شكرا لك