End-Users Get Maneuvered:
Empirical Analysis of Redirection Hijacking in Content Delivery Networks

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

27TH USENIX SECURITY SYMPOSIUM
AUGUST 15–17, 2018 | BALTIMORE, MD, USA

Shuai Hao[*] University of Delaware
Yubao Zhang University of Delaware
Haining Wang University of Delaware
Angelos Starvous George Mason University

[*] **Currently with CAIDA / UC San Diego**

/ Outline

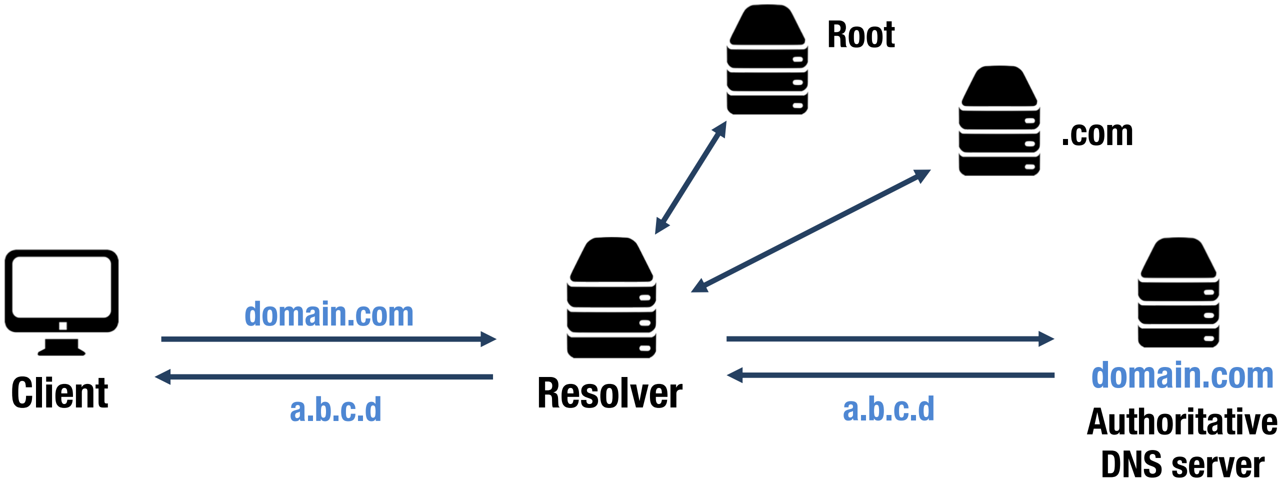
- DNS and DNSSEC
- Redirection Hijacking in CDN
- Threat Analysis
- Countermeasures
- Conclusion

/ Outline

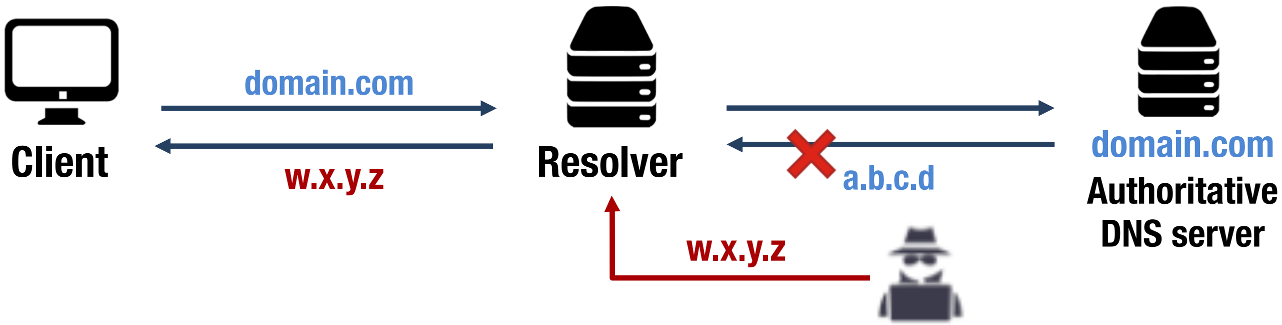
- DNS and DNSSEC
- Redirection Hijacking in CDN
- Threat Analysis
- Countermeasures
- Conclusion

/ Domain Name System (DNS) and DNSSEC

Domain Name System

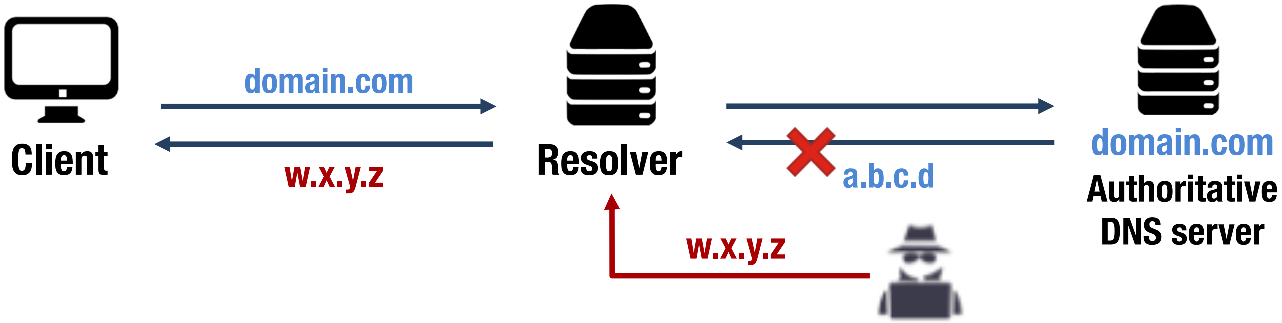


DNS Cache Poisoning / DNS Spoofing



DNS Cache Poisoning / DNS Spoofing

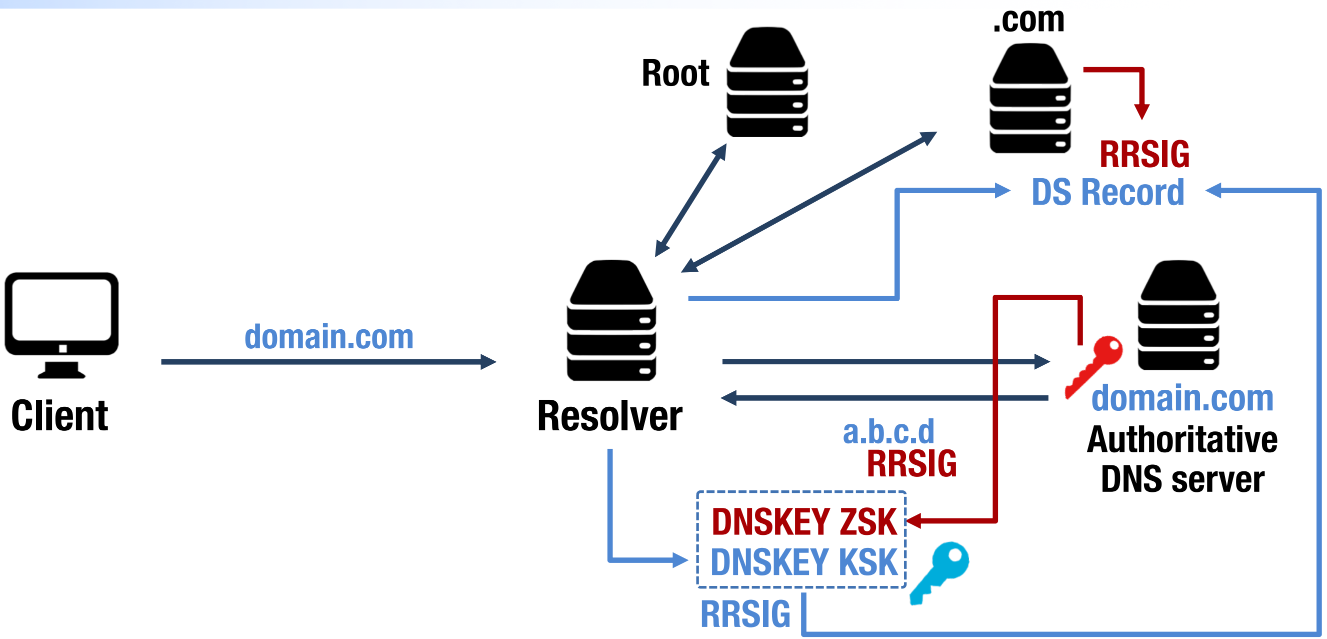
- Challenge-response defense
  - transaction-ID and source port randomization
  - increase the entropy: only effective against the **off-path** attackers



DNSSEC: System-wide solution

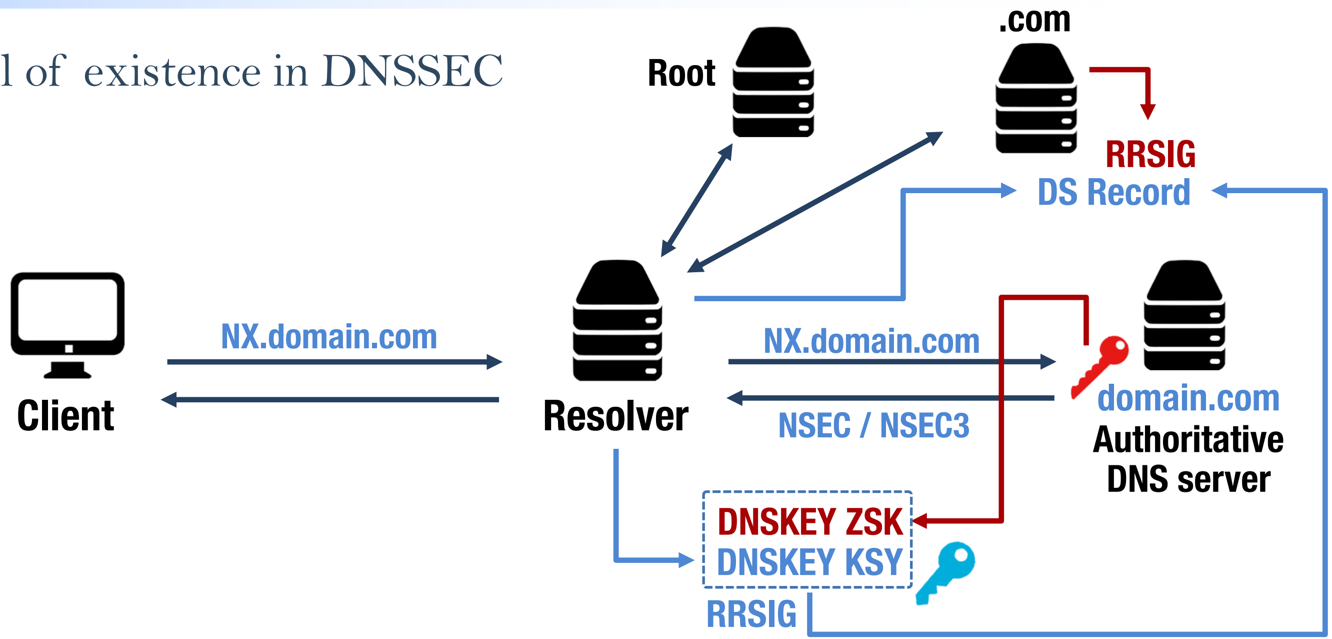
/ Domain Name System (DNS) and DNSSEC

DNSSEC



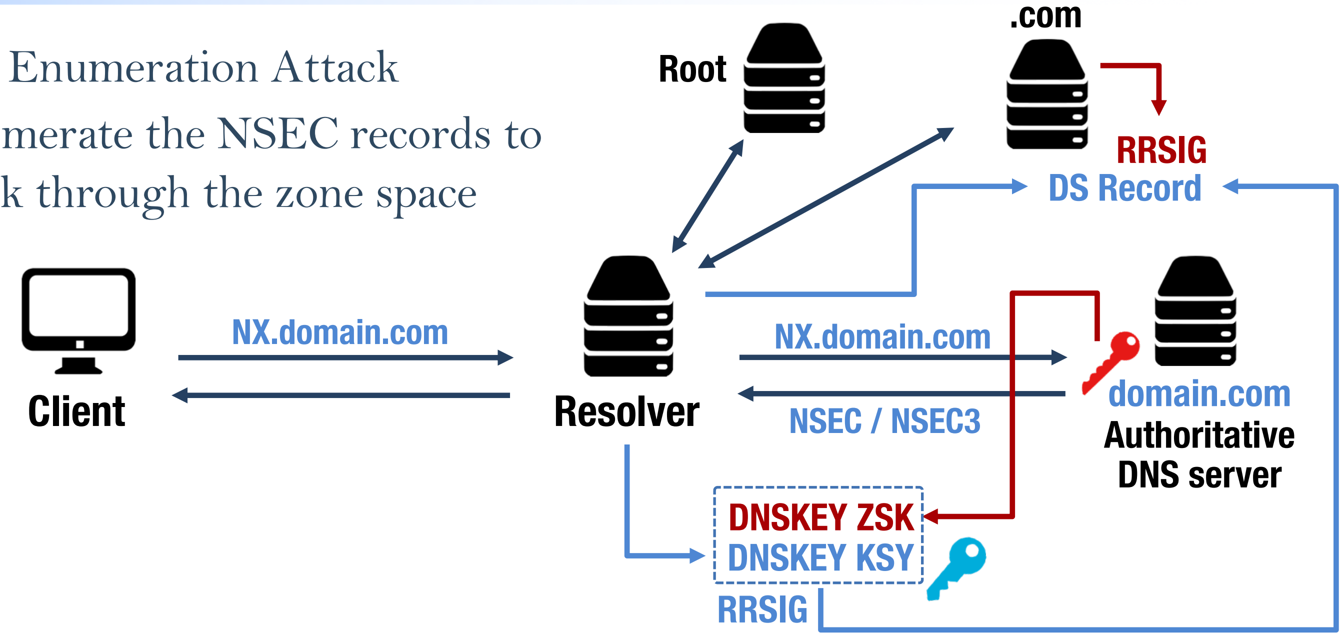
Negative Responses in DNSSEC

- Denial of existence in DNSSEC



Negative Responses in DNSSEC

- Zone Enumeration Attack
  - enumerate the NSEC records to walk through the zone space



Negative Responses in DNSSEC

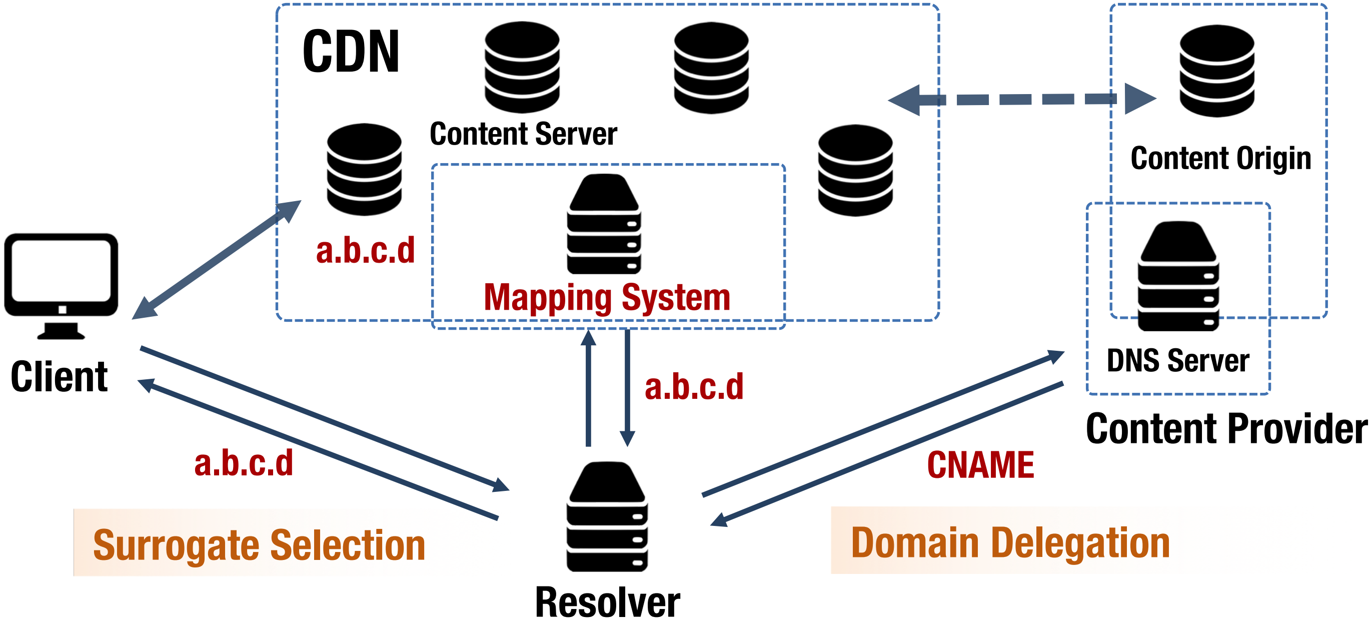
- Zone Enumeration Attack
  - expose private device names; reveal registrant data [RFC 5155]
- ECDSA-based (Live) Signing
  - RSA-based signing is prohibitively expensive to generate real-time, on-demand signature
  - fast key generation
    - live signing - zone enumeration
  - significantly reduced signature size
    - DDoS amplification attack
  - has been adopted by Cloudflare and .nl TLD

/ Outline

- DNS and DNSSEC
- **Redirection Hijacking in CDN**
- Threat Analysis
- Countermeasures
- Conclusion

/ Redirection Hijacking in CDN

Request Routing

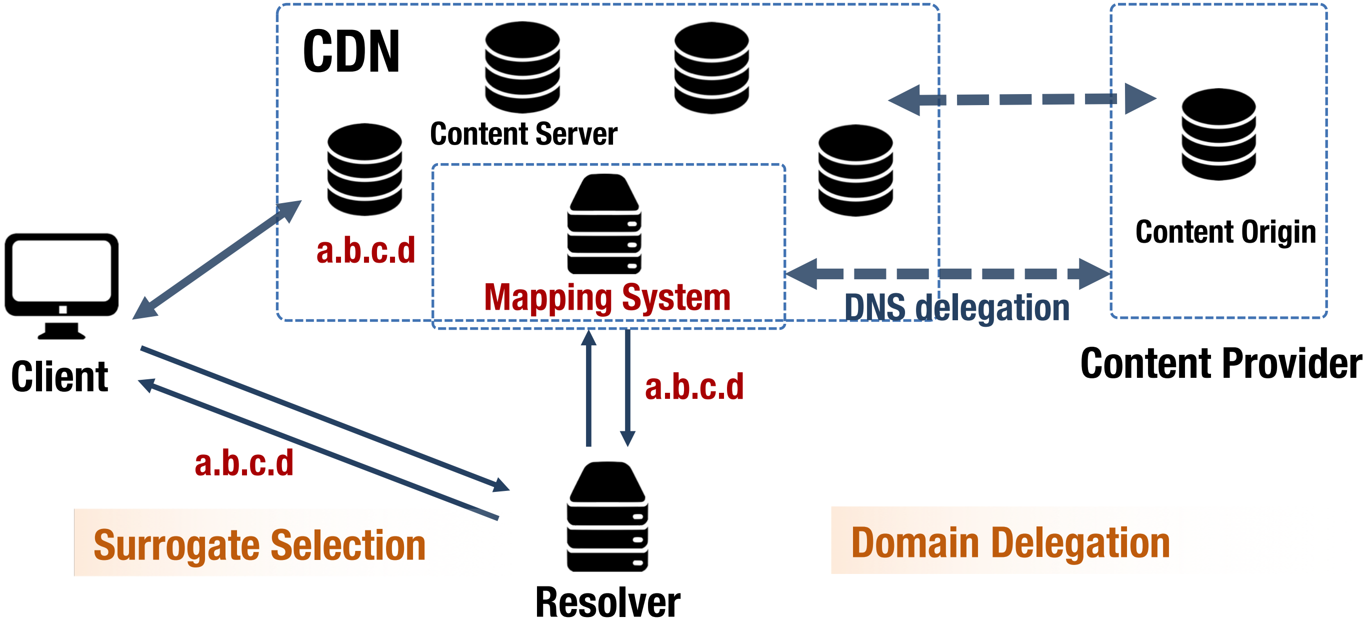


Surrogate Selection

Domain Delegation

/ Redirection Hijacking in CDN

Request Routing

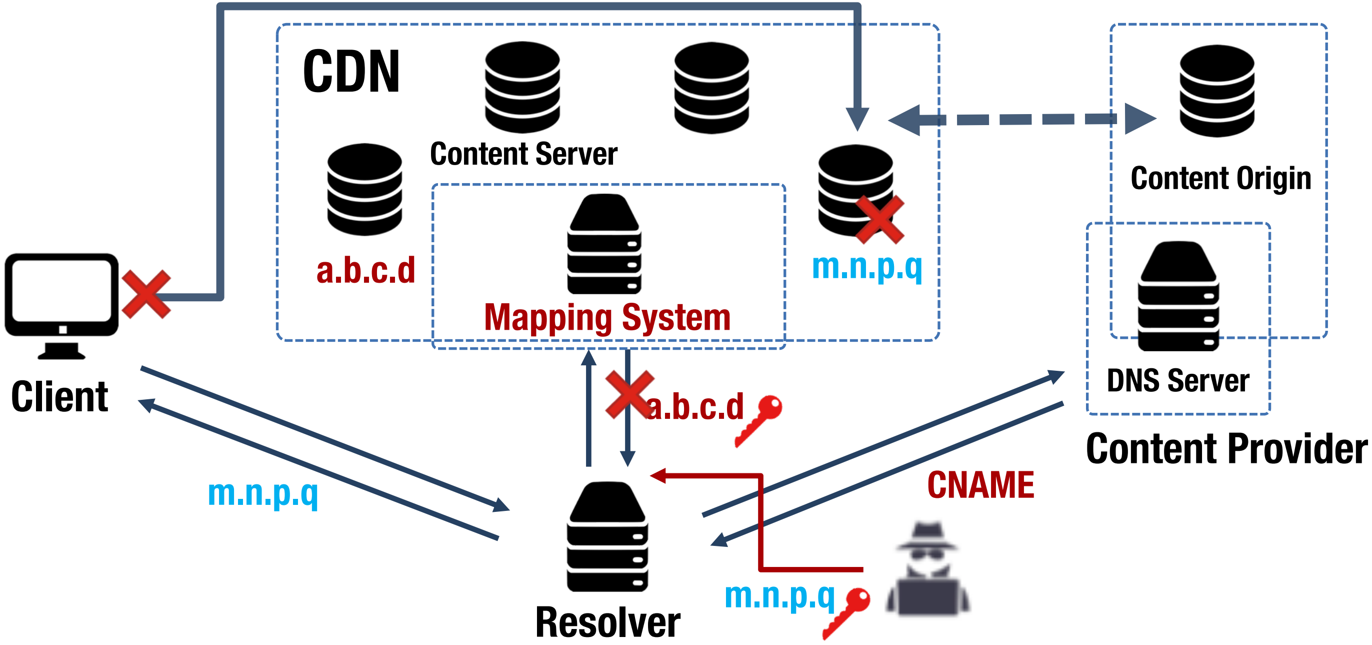


Surrogate Selection

Domain Delegation

/ Redirection Hijacking in CDN

Threat Model: When DNSSEC meets CDN



/ Outline

- DNS and DNSSEC
- Redirection Hijacking in CDN
- Threat Analysis
- Countermeasures
- Conclusion

/ Threat Analysis

Case Studies

- End-User Mapping: Akamai

www.dell.com	CNAME	www1.dell-cidr.akadns.net	
www1.dell-cidr.akadns.net	CNAME	cdn-www.dell.com.edgekey.net	
cdn-www.dell.com.edgekey.net	CNAME	cdn-www.dell.com.edgekey.net.globalredir.akadns.net	
cdn-www.dell.com.edgekey.net.globalredir.akadns.net	CNAME	e28.x.akamaiedge.net	
e28.x.akamaiedge.net	A	104.117.80.33	**dynamic mapping**

/ Threat Analysis

Case Studies

- Dynamic CNAME: KeyCDN

ja.onsen.io	CNAME	jaonsenio-4ecf.kxcdn.com
jaonsenio-4ecf.kxcdn.com	CNAME	p-usse00.kxcdn.com
p-uswd00.kxcdn.com	A	76.164.234.2

ja.onsen.io	CNAME	jaonsenio-4ecf.kxcdn.com
jaonsenio-4ecf.kxcdn.com	CNAME	p-uswd00.kxcdn.com
p-uswd00.kxcdn.com	A	107.182.231.101

CDN	Domain Delegation	Surrogate Selection	DNSSEC	Dynamics	
			A	CNAME	A
Akamai	CNAME Chain	DNS-based Mapping (ECS)	×		●
Cachefly	CNAME/NS Hosting	Anycast Routing	Feasible		
CDN.net	CNAME	DNS-based Mapping	×		●
CDN77	CNAME	DNS-based Mapping (ECS)	×		●
CDNetworks	CNAME	DNS-based Mapping (ECS)	×		●
CDNlion	CNAME	DNS-based Mapping	×		●
CDNsun	CNAME	DNS-based Mapping	×		●
ChinaCache	CNAME/CNAME Chain	DNS-based Mapping (ECS)	×		●
CloudFlare	CNAME/NS Hosting	Anycast Routing	✓		
CloudFront (Amazon)	CNAME/NS Hosting	DNS-based Mapping (ECS)	×		●
EdgeCast (Verizon)	CNAME/CNAME Chain	Hybrid Type I	Feasible		○
Fastly	CNAME	Hybrid Type II	×		●
Highwinds	CNAME	Anycast Routing	Feasible		
Incapsula	CNAME	Hybrid Type I	Feasible		○
KeyCDN	CNAME Chain	DNS-based Mapping (ECS)	×	●	●
LeaseWeb	CNAME	DNS-based Mapping	×		●
Limelight	CNAME	DNS-based Mapping	×		●
MaxCDN/NetDNA	CNAME	Anycast Routing	Feasible		
Rackspace	CNAME Chain	DNS-based Mapping (ECS)	×		●
cedexis (*MultiCDN*)	CNAME Chain	N/A	×	●	

Why DNSSEC adoption is so slow?

- T. Chung et al., Understanding the Role of Registrars in DNSSEC Deployment (IMC'17)

  "Registrars are responsible for the (small) DNSSEC deployment today, and that many leading registrars do not support DNSSEC at all, or require customers to take cumbersome steps to deploy DNSSEC"

- **Why DNSSEC adoption for top domains is also slow?**
  - their registrars are typically DNSSEC-enabled
  - highly reply on CDN to delivery contents: dynamic mapping

Performance Impact

Round-trip time (RTT)

- pure network matric: performance of network path

Time-to-first-byte (TTFB)

- network latency + page construction

Content download speed

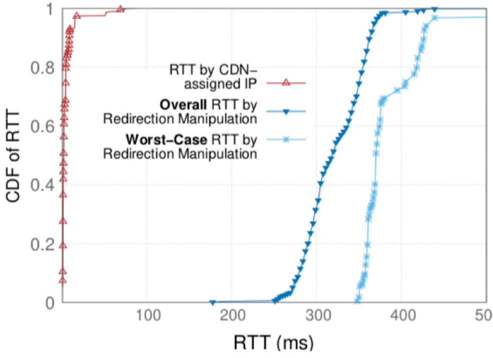
- download a set of medium-sized content files (50k–50M)

```
curl -H Host:i.dell.com –O http://104.78.87.26/sites/imagecontent/products/...jpg
```

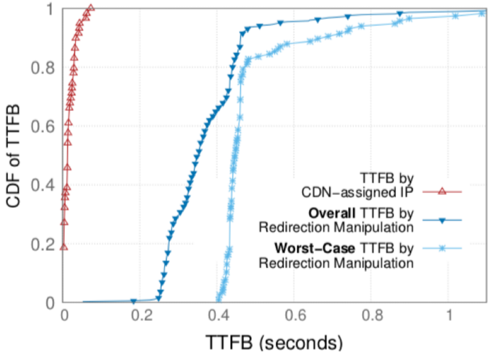
/ Threat Analysis

Performance Impact

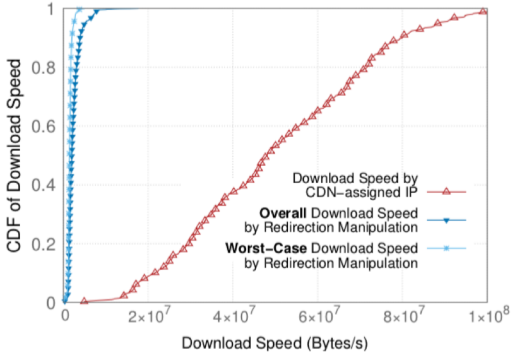
Round-trip time (RTT)



Time-to-first-byte (TTFB)



Content download speed



More Serious Threat

- **Potential DoS attack**
  - directing the requests from a large number of clients to a single victim edge servers (with legitimate traffic)

- **Defeating CDN’s load balancing and DoS protection**
  - easy detection for unresponsive edge servers
  - replaying legitimate mapping records associated with the unresponsive edge servers – still valid for DNSSEC validation
  - interrupting end-user’s access – financial and reputational damage

/ Outline

- DNS and DNSSEC
- Redirection Hijacking in CDNs
- Threat Analysis
- **Countermeasures**
- Conclusion

/ Countermeasures

DNSSEC Consideration

- against record replay: signing with additional information
  - currently practice: long validity period
    - RSA 30 days; ECDSA: 2 days (Cloudflare)
  - use a short validity period
  - sign the signature expiration
    - increase the difficulty of record injection as the validity cannot be altered
    - adversaries will only have a short window to perform the record injection

CNAME Flattening

- the prevalence of CNAME increases the difficulty of securing the mapping in CDNs
  - CNAME Chain
  - dynamic CNAME mapping

- **CNAME Flattening**
  - hide the CNAME chain from resolvers
  - CDN's authoritative nameservers **act as a resolver** by recursively resolving the CNAME chain and finally construct an A record

/ Countermeasures

CNAME Flattening

www.dell.com	CNAME	www1.dell-cidr.akadns.net
www1.dell-cidr.akadns.net	CNAME	cdn-www.dell.com.edgekey.net
cdn-www.dell.com.edgekey.net	CNAME	cdn-www.dell.com. edgekey.net.globalredir.akadns.net
cdn-www.dell.com. edgekey.net.globalredir.akadns.net	CNAME	e28.x.akamaiedge.net
e28.x.akamaiedge.net	A	104.117.80.33

/ Countermeasures

CNAME Flattening

www.dell.com	CNAME	www1.dell-cidr.akadns.net
www1.dell-cidr.akadns.net	~~CNAME~~	~~cdn-www.dell.com.edgekey.net~~
~~cdn-www.dell.com.edgekey.net~~	~~CNAME~~	~~cdn-www.dell.com.edgekey.net.globalredir.akadns.net~~
~~cdn-www.dell.com.edgekey.net.globalredir.akadns.net~~	~~CNAME~~	~~e28.x.akamaiedge.net~~
~~e28.x.akamaiedge.net~~	A	104.117.80.33

/ Outline

- DNS and DNSSEC
- Redirection Hijacking in CDNs
- Threat Analysis
- Countermeasures
- Conclusion

/ Conclusion

- **Problem: When DNSSEC meets CDN**
  - fundamental vulnerability in DNS-based CDNs stemming from the dynamics of DNS mapping records
  - allowing adversaries to manipulate the access of end-users even with DNSSEC signatures (i.e., **replay attack**)
  - Prevalence of redirection by CNAME
- **characterizing the request routing of CDNs**
- **practical impact: performance degradation, nullifying CDN's benefits**
- **countermeasures**

Thank you!

27TH USENIX SECURITY SYMPOSIUM
AUGUST 15–17, 2018 | BALTIMORE, MD, USA

End-Users Get Maneuvered:
Empirical Analysis of Redirection Hijacking in Content Delivery Networks

Shuai Hao

✉ haos@caida.org

⌂ www.caida.org/~haos/