When HTTPS Meets CDN

A Case of Authentication in Delegated Service

Liang, J., Jiang, J., Duan, H., Li, K., Wan, T., & Wu, J

2014 IEEE Symposium on Security and Privacy

Web Traffic Needs Security!

Goals = CIA triad

- Confidentiality
- Integrity
- Availability

Web Traffic Needs Security!

Goals = CIA triad

Confidentiality

Integrity

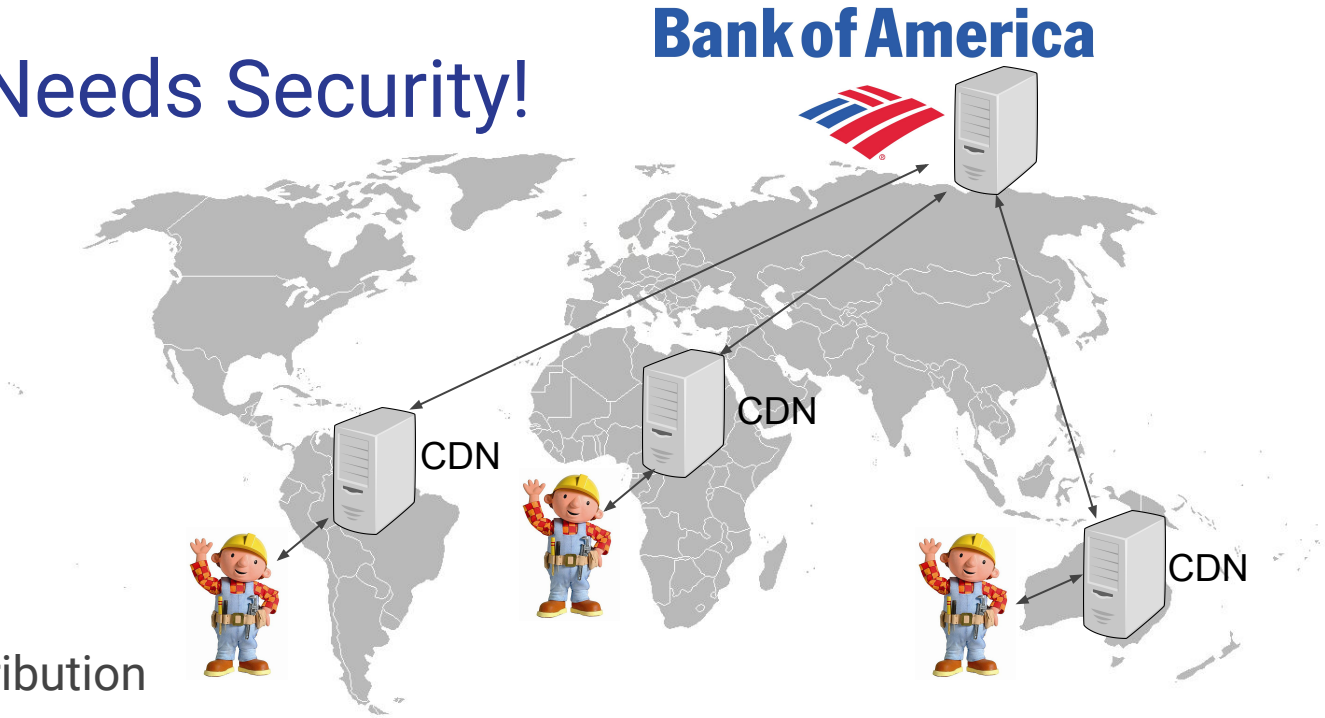
Availability

HTTPS
end-to-end

Web Traffic Needs Security!

Goals = CIA triad

- Confidentiality
- Integrity
- **Availability**
  - Fast → Distribution
  - Reliable → Firewalls, DDoS Protection

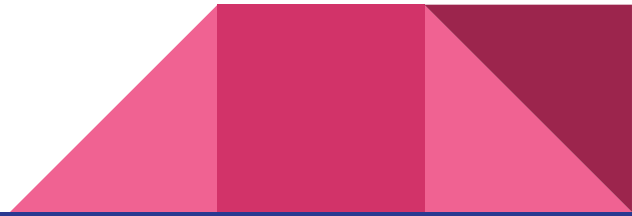


When CDNs meet HTTPS

HTTPS provides end-to-end security

CDN services

1) Fast Availability → Distribution: End-to-many-ends
2) Reliable Availability → Protection: End-to-CDN-to-end

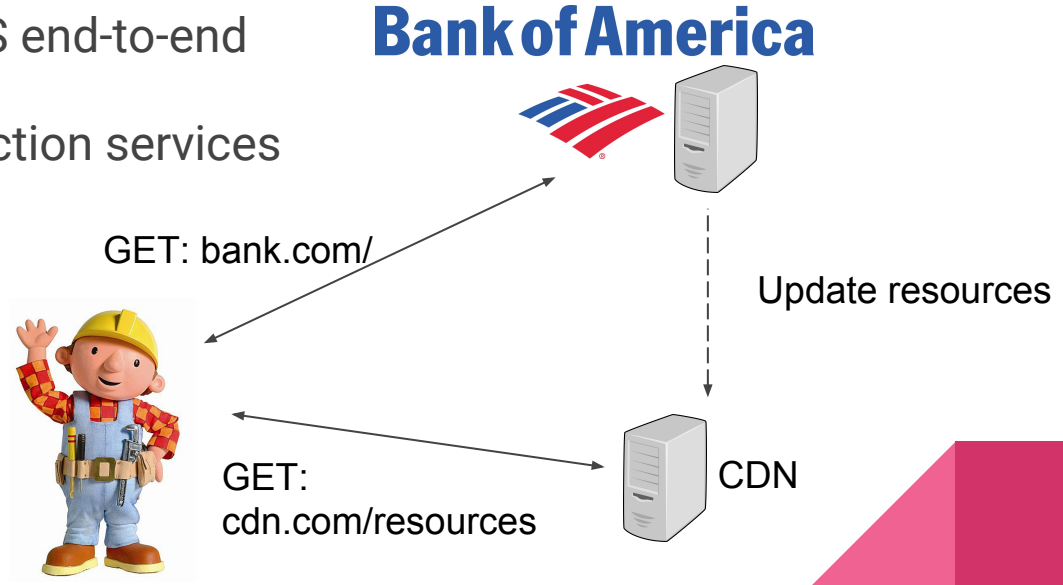


CDN Mechanisms - URL Rewriting

Main HTML on bank.com, bulk static content on cdn.com

Doesn’t violate HTTPS end-to-end

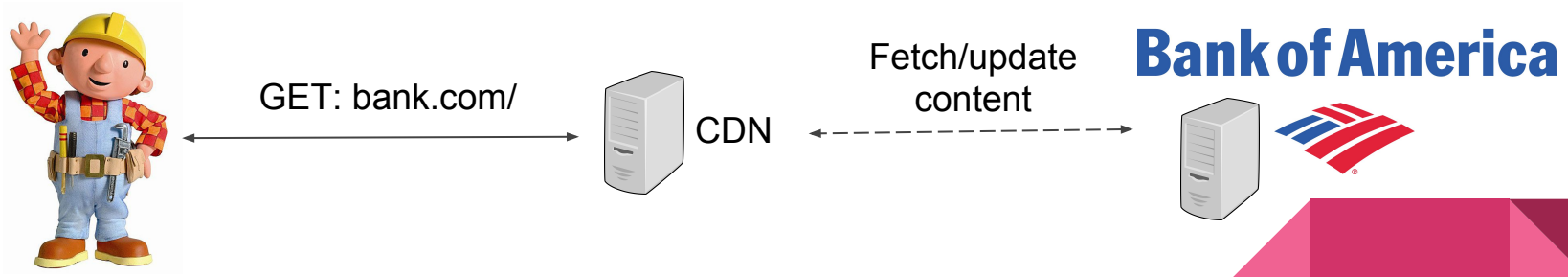
Doesn’t provide protection services



CDN Mechanisms - DNS routing

bank.com resolves to IP address of CDN server

1) CNAME record that maps bank.com → bank.cdn.com
2) CDN is the authoritative Name Server (NS) for bank.com

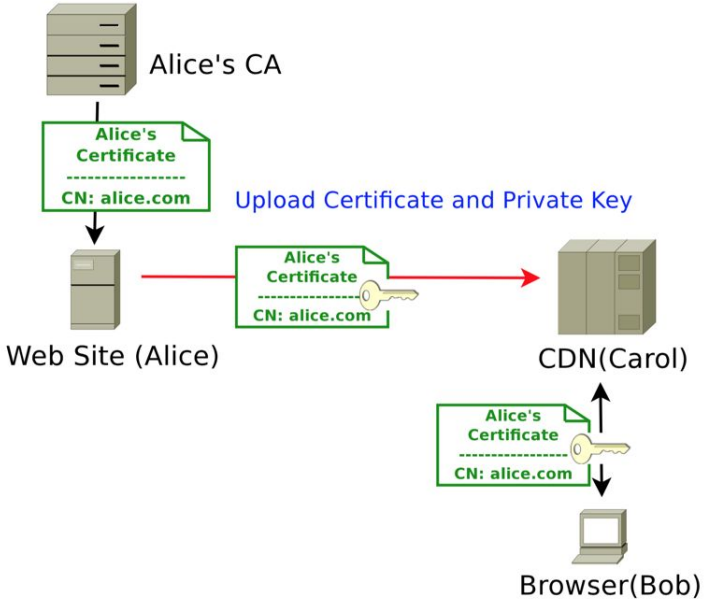


Making HTTPS Work w/ DNS routing

Certificate = public key + common name (CN) + signature chain

Custom certificate

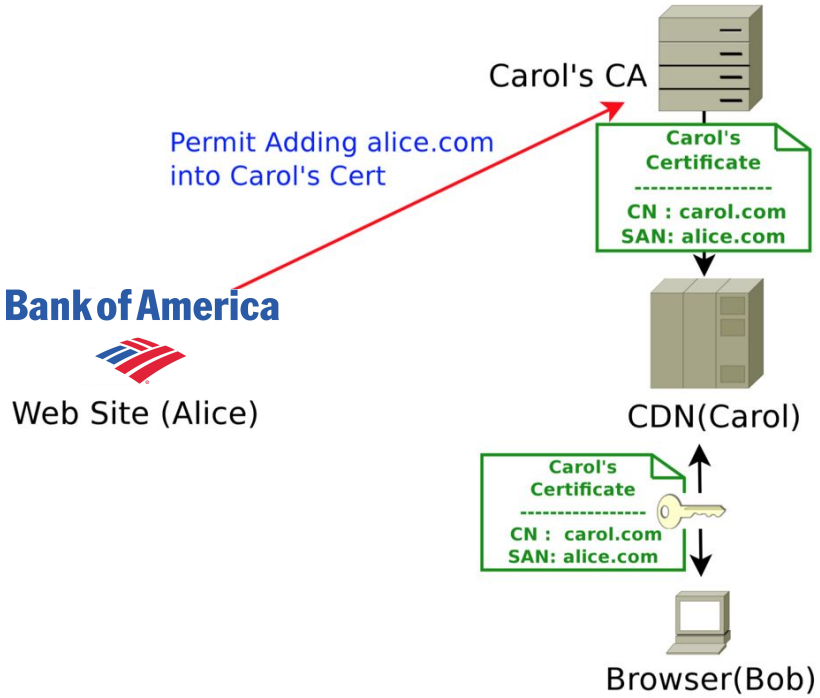
- Give CDN bank.com’s certificate + private key
- Increased attack surface
- Expensive CA revocation



Making HTTPS Work w/ DNS routing

Shared certificate

- cdn.com cert vouches for bank.com
- Subject Alternate Name (SAN) extension
- Loses bank.com cert features - i.e. EV
- Expensive CA revocation



CDN Mechanisms in Practice

Most CDNs use CNAME DNS routing

68% of certs are invalid!

Custom and shared certs are popular

Table II
HTTPS STATUS OF DNS-CDN-ENABLED SITES

HTTPS Status		# of web sites	%
Valid Cert	Custom Cert	2152	20.1%
	Shared Cert	1198	11.1%
Invalid Cert	Status 200	1637	15.3%
	Others	5734	53.5%
Total		10,721	100%

CDN Provider	Request-Routing Mechanism	HTTPS Support
Akamai	CNAME / Domain Hosting	Custom
Azure	CNAME	Not Support
Bitgravity	CNAME	Custom
Cachefly	CNAME	Custom
CDNetworks	CNAME	Custom / Shared
CDN77	CNAME	Custom
CDN.net	CNAME	Custom / Shared
Chinacache	CNAME	Custom
Chinanetcenter	CNAME	Custom / Shared
CloudFlare	CNAME / Domain Hosting	Custom / Shared
CloudFront	CNAME	Custom
Edgecast	CNAME	Custom / Shared
Fastly	CNAME	Custom / Shared
Highwinds	CNAME	Custom
Incapsula	CNAME	Custom / Shared
Internap	CNAME	Custom
KeyCDN	CNAME	Custom / Shared
Limelight	CNAME	Custom / Shared
NetDNA	CNAME	Custom / Shared
Squixa	CNAME	Custom / Shared

Case study: CA Cert Revocation

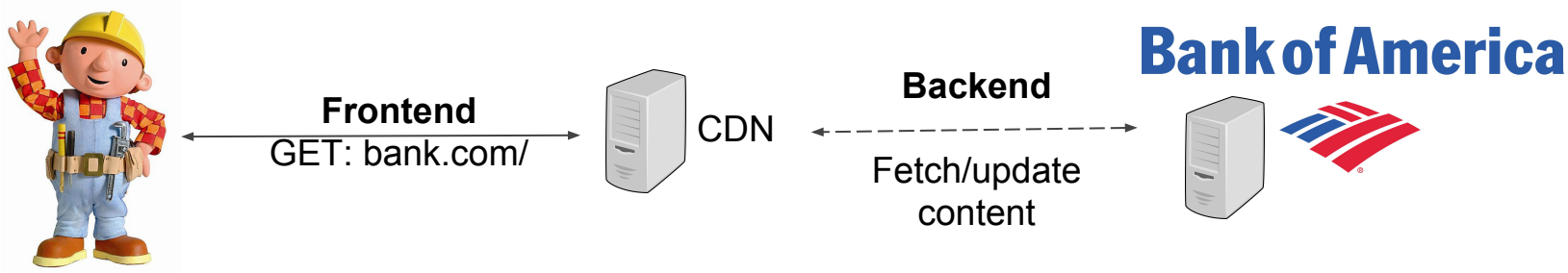
Create, then remove site with Incapsula CDN

- Incapsula quickly updates shared cert to add, then remove SAN
- Globalsign does not revoke old cert with old SAN

Broader study of 1865 shared cert updates across 5 CDNS

- No old certs revoked over the course of 3 months!

Case Study: Backend Connection

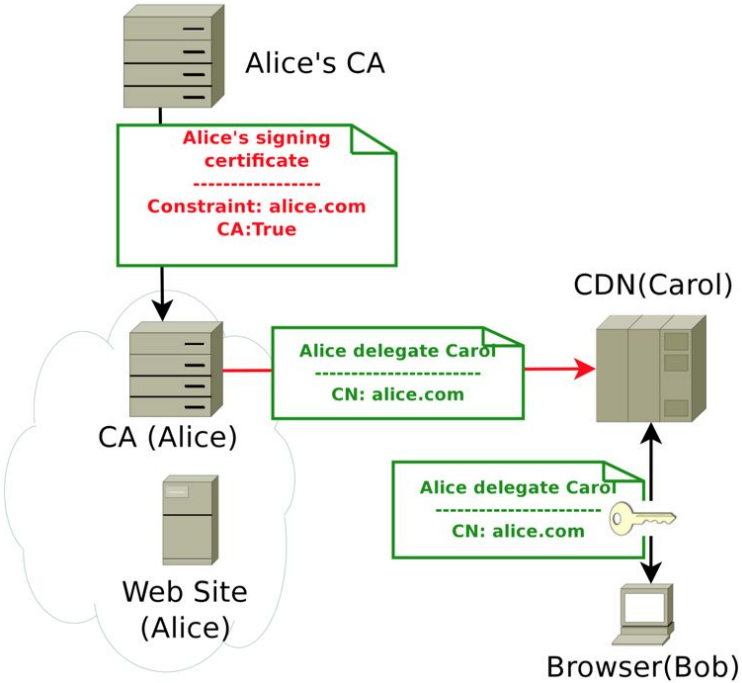


Tested sites behind 5 CDNs - no valid HTTPS!

CDN Provider	Back-end Protocol	Certificate Validation
CDN77	HTTP	–
CDN.net	HTTP	–
CloudFlare	HTTP / HTTPS	No [3]
CloudFront	HTTP / HTTPS	Did not validate CN
Incapsula	HTTP / HTTPS	No

Solution: Name Constraint Certificate

Let bank.com issue its own certificates to CDN!

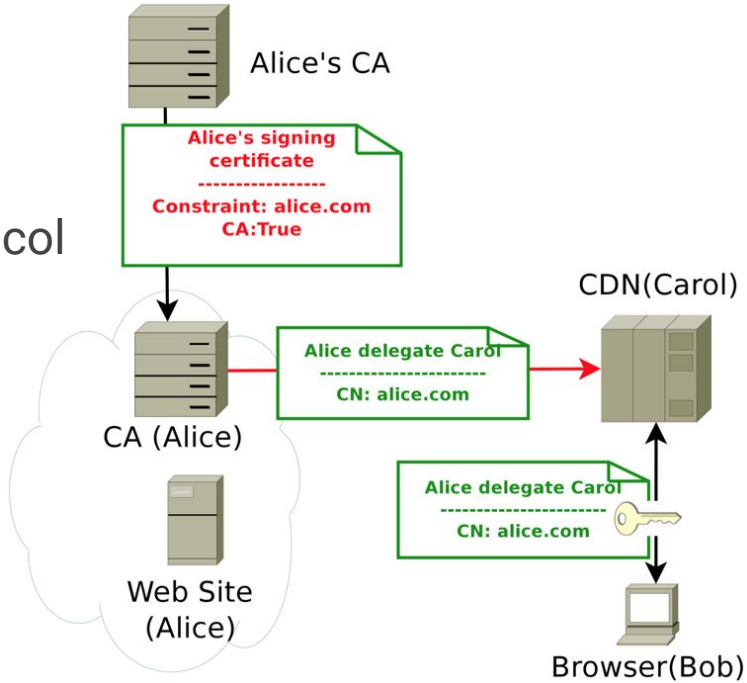


Solution: Name Constraint Certificate

Let bank.com issue its own certificates to CDN!

Issues:

1) Improper enforcement / insecure protocol
2) High operational overhead
3) CA disincentive
4) Rare adoption

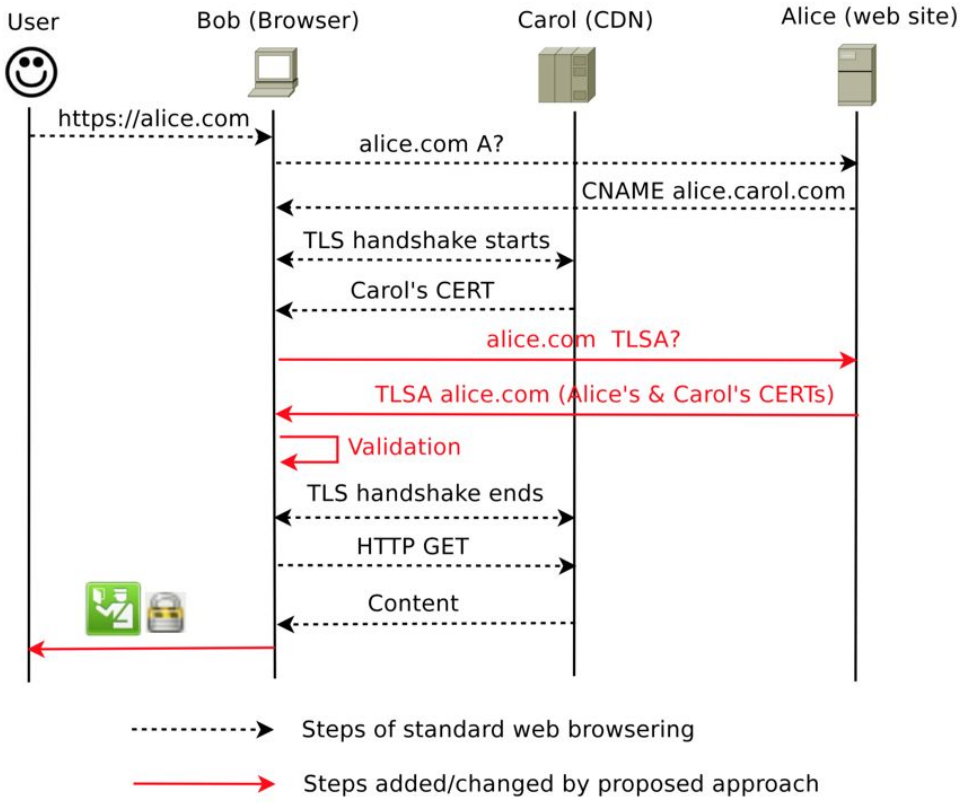


Solution: DANE w/ delegation semantics

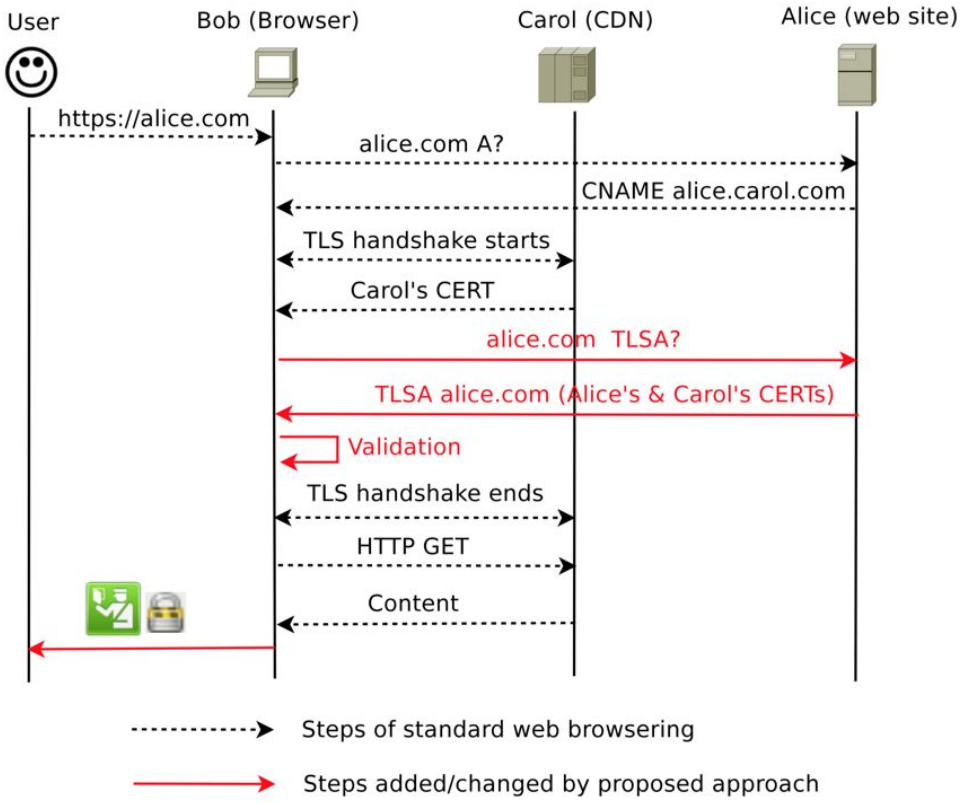
DANE = DNS-based Authentication of Named Entities

- TLSA record that binds domain to a certificate
- Modification: multiple TLSA records for CDNs
- Insight: trust DNS (instead of cert) for domain:public-key mapping
  - Makes revocation trivial - change DNS response (and expire caches)

DANE in Practice



DANE in Practice



Implemented Firefox PoC

Overhead - additional, large DNS request for TLSA record

Potential amplification attack vector

Discussion

Contributions of the paper?

Why were no shared certs revoked within 3 months? Whose fault?

What is a better solution - Name constraint certificates or DANE? Or a third option?