DANE Based Solution for Delegation Problems of HTTPS in CDN

Jinjin Liang, Jian Jiang, Haixin Duan, Jianping Wu
: Tsinghua University, China

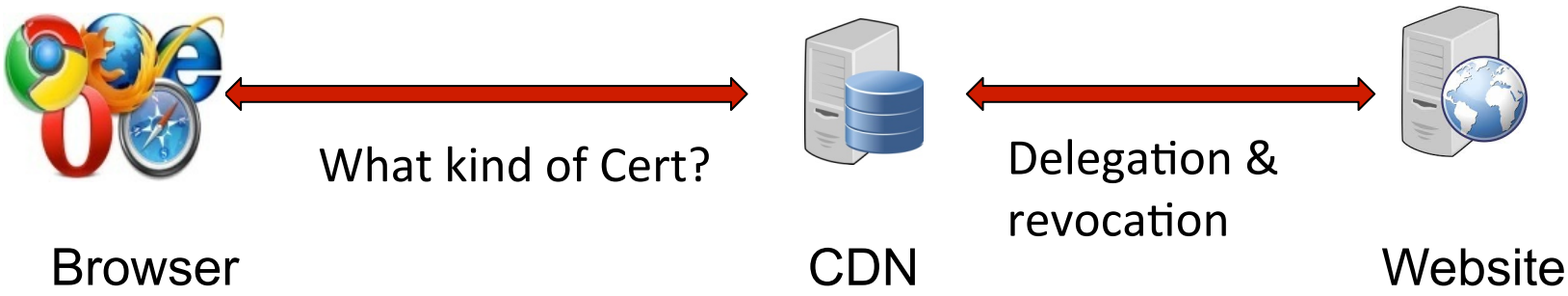
Tao Wan: Huawei, Canada

Kang Li : University of Georgia, USA

This work is part of our published paper in Security & Privacy Symposium, May 18-20, 2014
http://netsec.ccert.edu.cn/duanhx/files/2014/05/httpsincdn.pdf

Overview

- TLS is designed as an E2E protocol, but CDN splits TLS tunnel into 2 segments



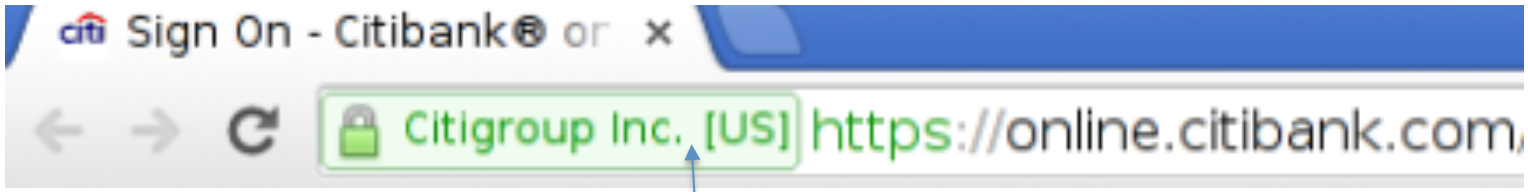
- We study delegation problems in current practices by survey and measurement
- DANE based solution for CDN delegation

Outline

- Delegation Problem of HTTPS in CDN
- DANE Based Solution & Demo

HTTPS in CDN and DNS redirection

- Websites use CDN for performance and security, supporting HTTPS



EV(Extended Validation) cert., other than DV

- DNS CNAME redirection is the most popularly used for request rerouting

```
;; ANSWER SECTION:
online.citibank.com.     285     IN      CNAME   online.citibank.com.edgekey.net.
online.citibank.com.edgekey.net. 15322 IN CNAME e5035.b.akamaiedge.net.
e5035.b.akamaiedge.net. 19       IN      A       23.2.2.106
```

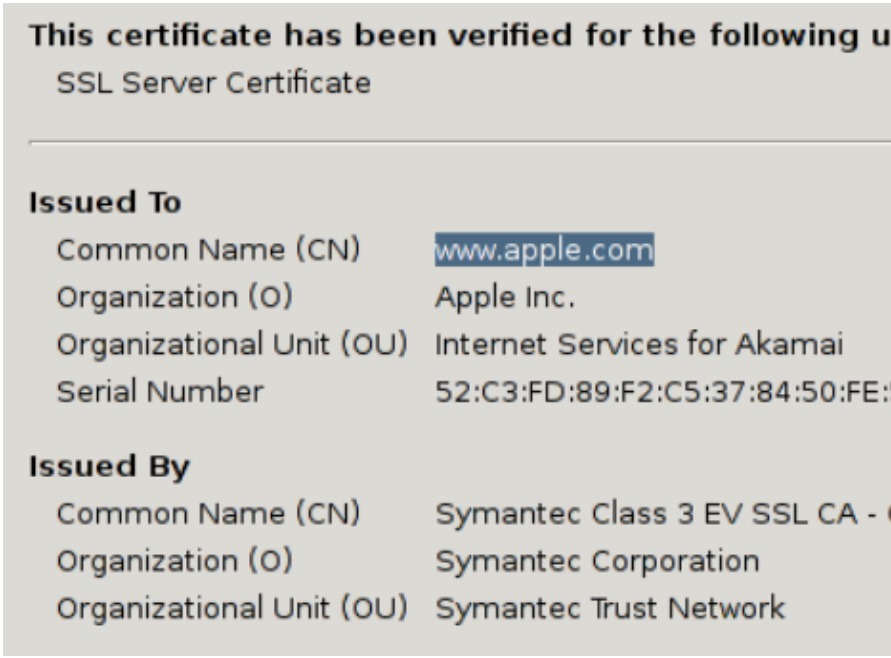
Surveys on top CDNs and websites

- 20 popular CDN providers
  - Akamai, Azure, Bitgravity, Cachefly, CDNetworks, CDN77, CND.net, ChinaCache, CloudFlare, CloudFront, InCapsula….
  - All 20 support DNS CNAME rerouting
  - 19 support HTTPS
- top 1 million websites from Alexia
  - 10,721 support HTTPS and use one of 20 CDNs

Invalid Certificate		Valid Certificate	
Status 200	Other	Custom Cert	Shared Cert
15%	54%	20%	11%
69%		31%	

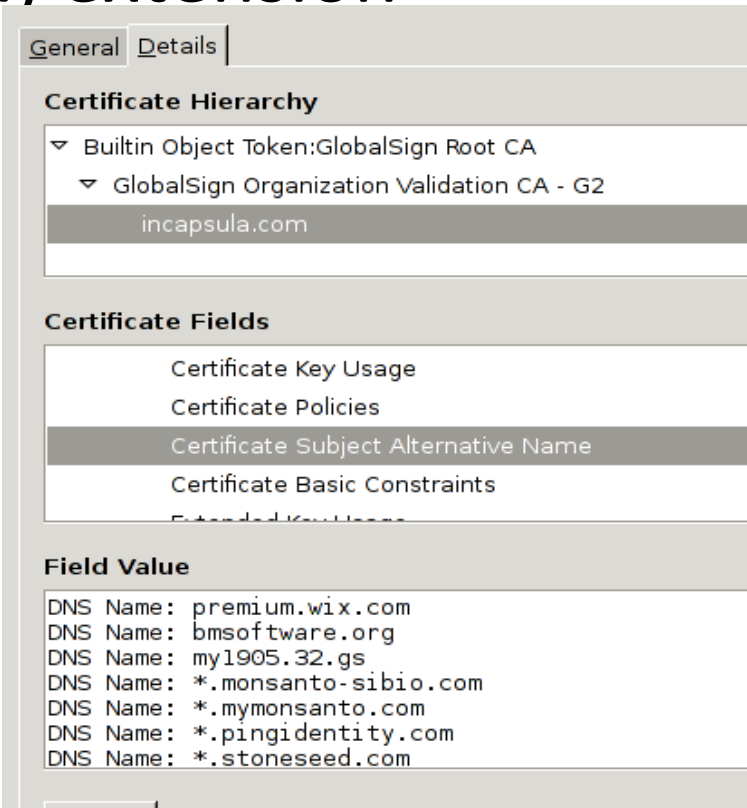
Current practice1 : Custom Certificate

- Type 1: Web owners upload their certificate to CDN, with their private keys(shared private key)
- Type 2: CDN providers apply new certificate on behalf of web owners
- Shortcomings
  - Web owners cannot keep private keys secret
  - Web owners cannot revoke their delegation independently



Current Practice2: Shared Certificate

- CDN providers apply shared certificates, adding web's domain name to the cert's Subject Alternative Name(SAN) extension
- Shortcomings
  - Web sites lose their certified identity(cert.), e.g. website has an EV cert. but CDN has a DV cert.
  - Web owner can not revoke the certificate independently



Requirements/Goals

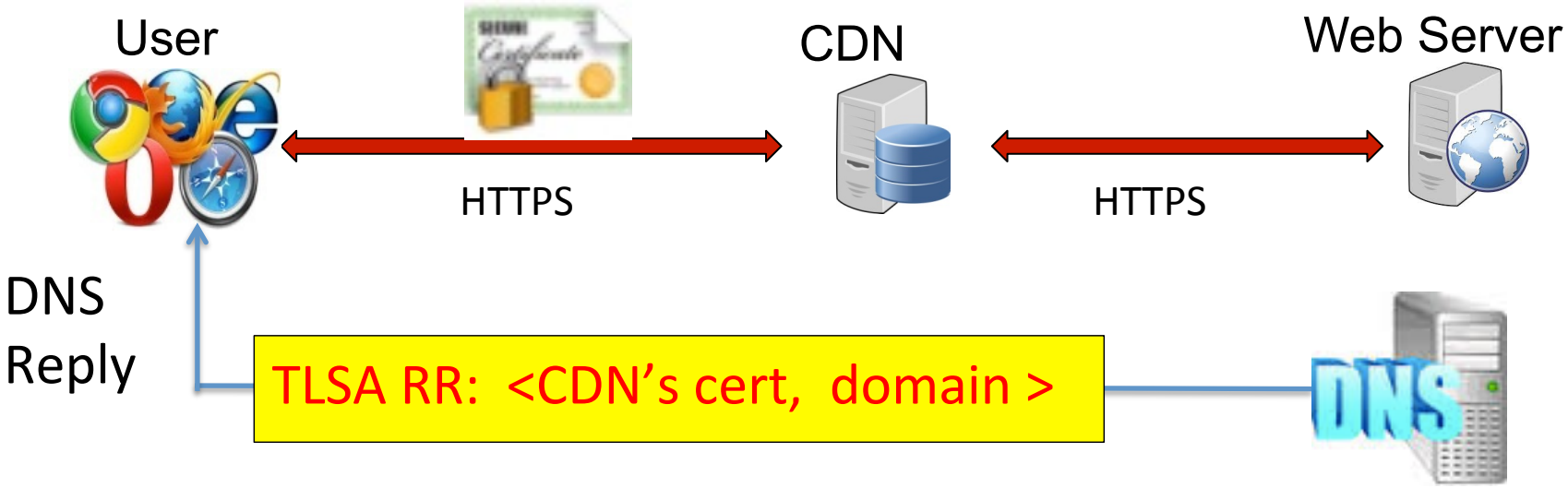
- The browser must be able to obtain the identity (cert.) of the original website and its delegation to the CDN
  - Especially when web site use EV certificate
- Web owners must be able to keep their private key secret
- Web owners must be able to revoke their delegation independently

DNS-based Authentication of Named Entities(DANE) in brief

- DANE binds web site's domain name with its certificate by TLSA RR, secured by DNSSEC
- DANE Usages(RFC 6394,6698):
  - CA constraints (0): <CA, domain>
  - Service Certificate Constraints(1): <cert, domain>
  - Trust Anchor Assertion(2): <self-signed CA, domain>
  - Domain-Issued Certificate(3): <selfsigned cert., domain>

Delegation based on current DANE

- For delegated service (RFC 6394, 3.4) :
  - Web owner uses certificate constraints(usage 1 or 3) to control what cert. CDN should present.



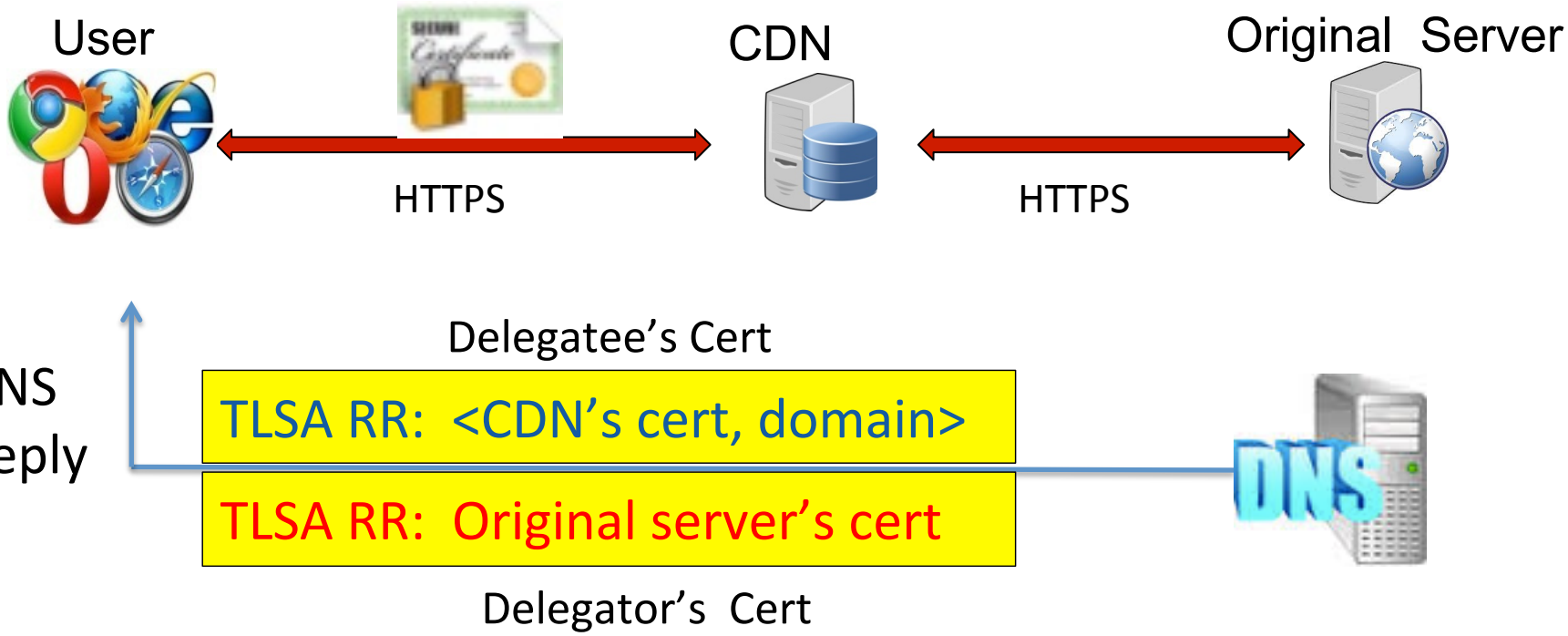
- Web owner can keep their private key
- Revoke delegation by deleting TLSA RR

Problem of current DANE for certificate delegation

- Same as that in shared certificate:
  - Browser cannot know the certified identity of the original website, without it's certificate
  - Especially, if the web owner has an EV certificate, current DANE based solution downgrades the confidence of the user toward the original web server

Extending DANE: Delegation Token

- This problem can be solved by a minor extension : to add the certificate of original web server with a new TLSA RR: original server's cert.



Delegation should be explicitly shown to end users

- Screen capture from our firefox Extension as a POC

Proposed extension to TLSA RRs for delegation

- Reuse current usage to bind CDN's cert.:

_443._tcp.website 1 IN TLSA 1 0 1 ed3c...080

Certificate Constraint (Certificate of delegatee)

Full Certificate

- Extending usage(4) with cert. of delegator (original web site)

_443._tcp.website 1 IN TLSA 4 0 0 3082.... DB39

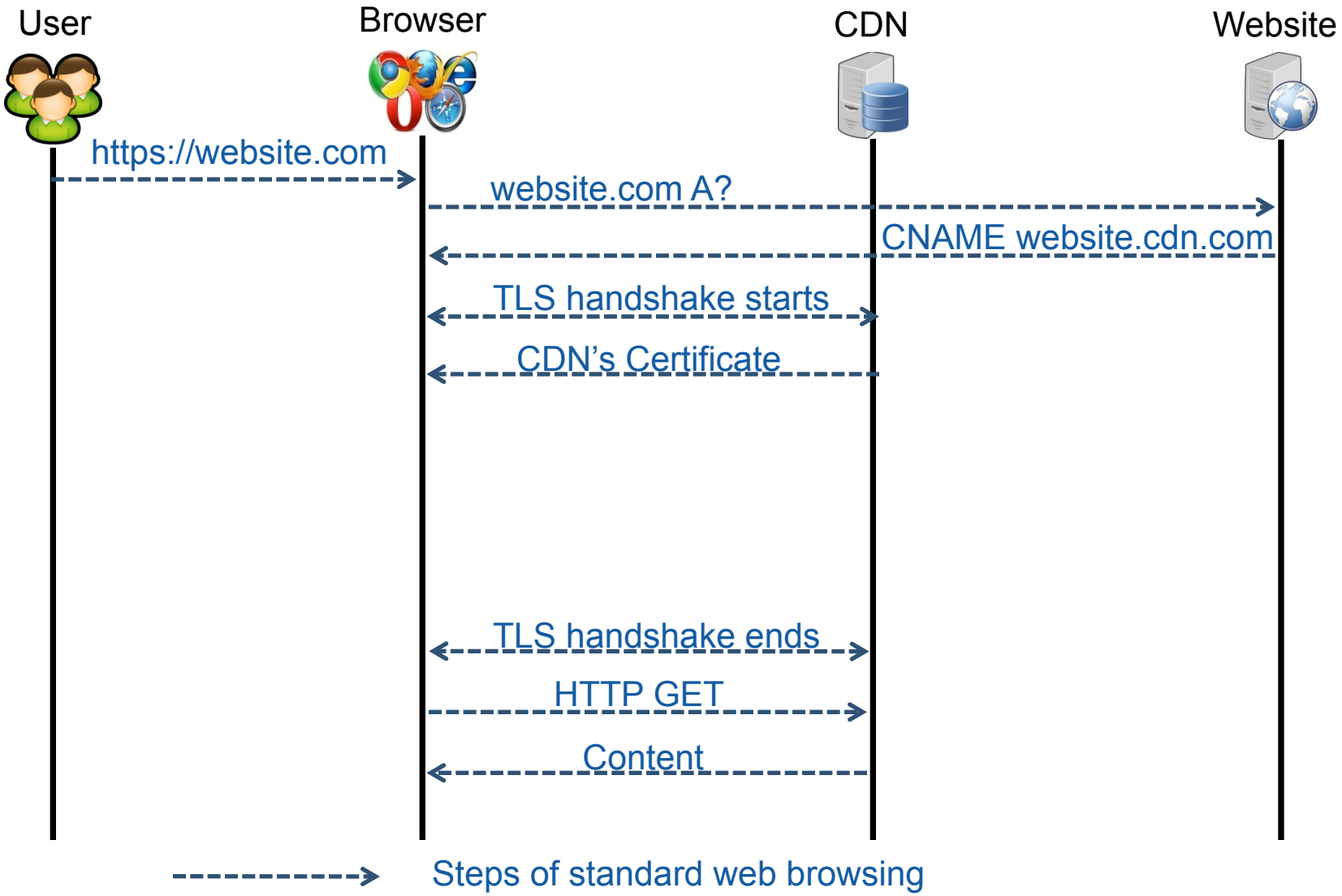
Certificate of delegator

Full Certificate

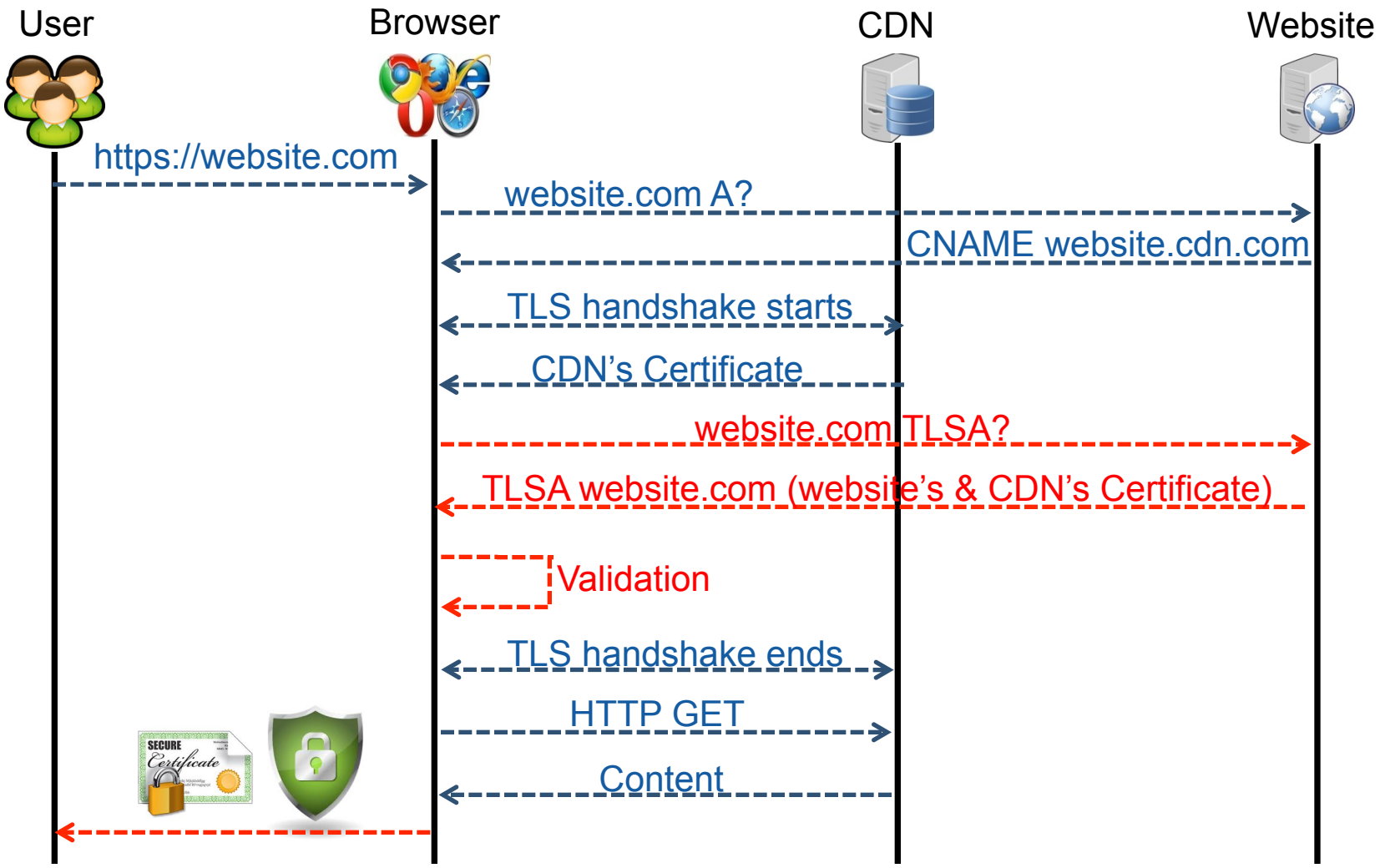
Proposed extension to selector field

- Extending selector field with chain of certificates
  - 0 -- Full certificate: the Certificate binary structure as defined in [RFC5280]
  - 1 -- SubjectPublicKeyInfo: DER-encoded binary structure as defined in [RFC5280]
  - 2 -- Chain of Certificates: to build trust of the delegator, in case that the browser cannot get these certificates by itself.

The Interaction of Authentication



The Interaction of Authentication



Summary

1. Certificate delegation between CDN and website is an emerging requirement.
2. DANE can be used to express such a delegation relationship
3. Current form of delegation in DANE is insufficient: cannot show original certificate, at least could cause cert downgrade.
4. A slight extension could cover such scenario nicely, with a new usage and selector

Demo

& ?

duanhx@tsinghua.edu.cn