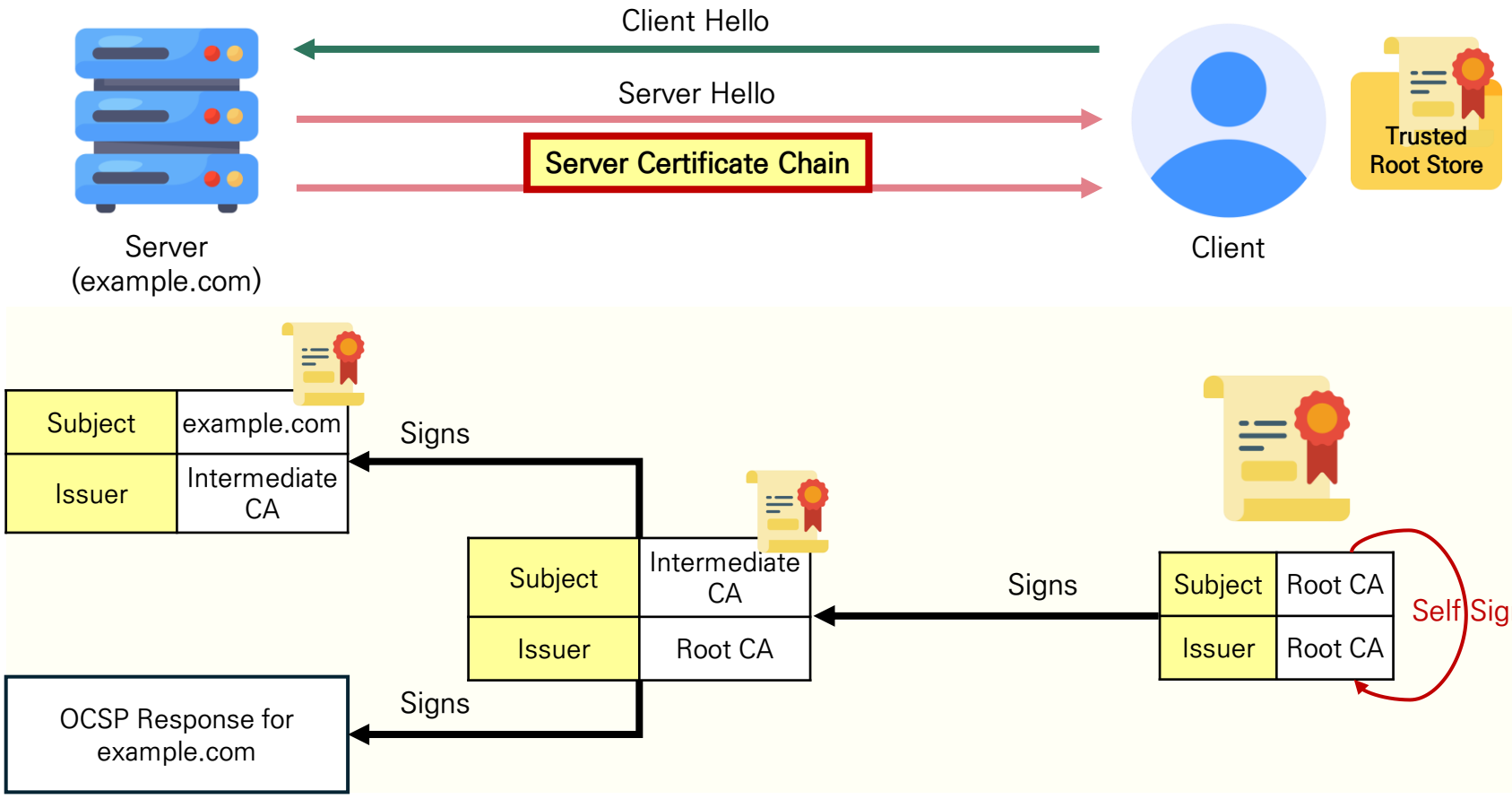
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,
VOL. 19, NO. 1, JANUARY/FEBRUARY 2022

On the Validation of Web X.509 Certificates by TLS Interception Products

황 은 비 | Eunbee Hwang
서울대학교 컴퓨터공학부 석사 과정
인터넷 융합 및 보안 연구실 (MMLAB)

Table of Contents

TLS: Client – Server



Certificate Validation: Certificate Content

- Chain-of-Trust
- Signature Validation
- Validity check
- Subject and Issuer
- (Extended) Key Usage
- And much more…

```
Version: 3 (0x2)
Serial Number:
            f3:c9:29:12:34:18:17:b4:12:8b:8a:31:d4:98:cc:51
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Google Trust Services, CN=WR2
Validity
            Not Before: Oct  7 08:23:38 2024 GMT
            Not After : Dec 30 08:23:37 2024 GMT
Subject: CN=*.google.com
Subject Public Key Info:
...
X509v3 extensions:
            X509v3 Key Usage: critical
               Digital Signature
            X509v3 Extended Key Usage:
               TLS Web Server Authentication
            Authority Information Access:
               OCSP - URI:http://o.pki.goog/wr2
               CA Issuers - URI:http://i.pki.goog/wr2.crt
            X509v3 Subject Alternative Name:
               DNS:*.google.com, DNS:*.appengine.google.com, …
            X509v3 CRL Distribution Points:
               Full Name:
                 URI:http://c.pki.goog/wr2/75r4ZyA3vA0.crl
              ...
Signature Algorithm: sha256WithRSAEncryption
Signature Value:  0e:0d:75:66:4c:68:e9:37:...
```

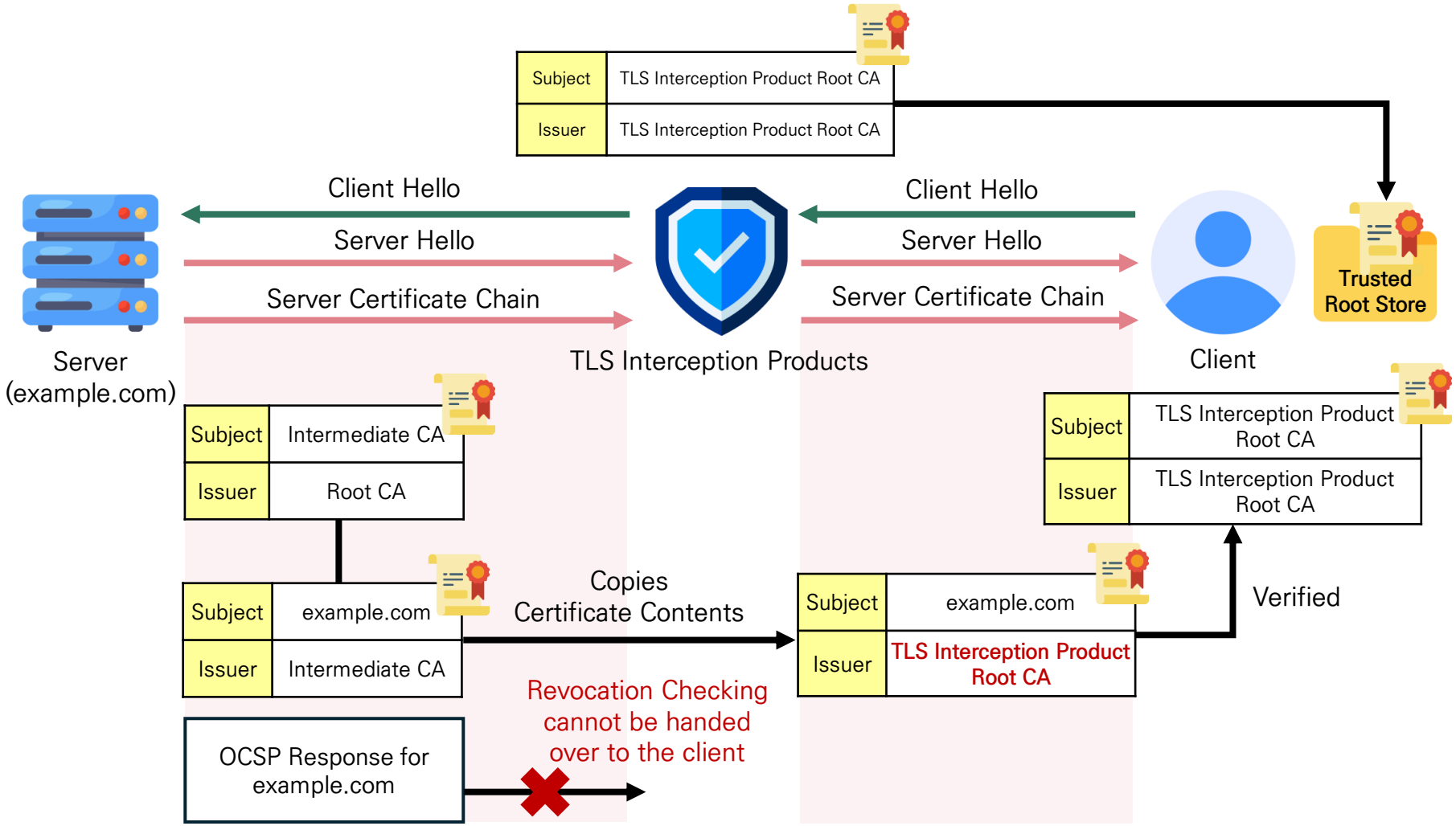
Standards Related to Certificates

- X.509 Standard (ISO/ITU-T)
  - Defines certificate fields (mandatory, optional, extensions)
  - Extensions can be critical or non-critical

- IETF PKIX (RFC 5280 and many more)
  - Developed an X.509 profile specifically for the Internet
  - Reduces complexity by defining mandatory and optional extensions

- CA/Browser Forum
  - Established in 2007 to improve certificate issuance and management
  - Developed guidelines for Extended Validation (EV) certificates
  - Issued “Baseline Requirements”

TLS Interception Products



Types of TLS Interception Products

	Certificate Validation	Revocation Checking
FV (Full Validation)	O	O
DV (Delegated Validation)	X	O
IV (Incorrect Validation)	X	X

FV	DV	IV
mitmproxy kaspersky Squid Proxy Progress Telerik Fiddler	avast ESET AVG	Charles WEB DEBUGGING PROXY

Testing TLS Interception Products

- Subject Common Name (SCN), Subject Alternative Name (SAN)
  - 4 FV products
- Key Usage and Extended Key Usage extensions
  - 4 FV products
- Revocation checking
  - 4 DV products and 3 FV products
- TLS Interception Products exhibit non-standardized behaviour with respect to certificate validation and revocation checking

Subject Fields

```
Version: 3 (0x2)
Serial Number:
            f3:c9:29:12:34:18:17:b4:12:8b:8a:31:d4:98:cc:51
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Google Trust Services, CN=WR2
Validity
            Not Before: Oct  7 08:23:38 2024 GMT
            Not After : Dec 30 08:23:37 2024 GMT
Subject: CN=*.google.com
Subject Public Key Info:
...
X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            Authority Information Access:
                OCSP - URI:http://o.pki.goog/wr2
                CA Issuers - URI:http://i.pki.goog/wr2.crt
            X509v3 Subject Alternative Name:
                DNS:*.google.com, DNS:*.appengine.google.com, …
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://c.pki.goog/wr2/75r4ZyA3vA0.crl
              ...
Signature Algorithm: sha256WithRSAEncryption
Signature Value:  0e:0d:75:66:4c:68:e9:37:...
```

Subject

- Slightly different requirements and guidelines for CN and SAN
  - X.509 Standard: CN is considered as the primary entity
  - RFC 5280: CN and SAN can be used in combination
  - CA/B BR: SAN should be used

- Best Practices for selecting CN and SAN

1. Use SAN to list all domain names and IP addresses associated with the entity.
2. CN can be included for compatibility, but it should mirror one of the values in SAN.
3. Avoid using private IPs (e.g., 192.168.*.*) in both SAN and CN for security and interoperability

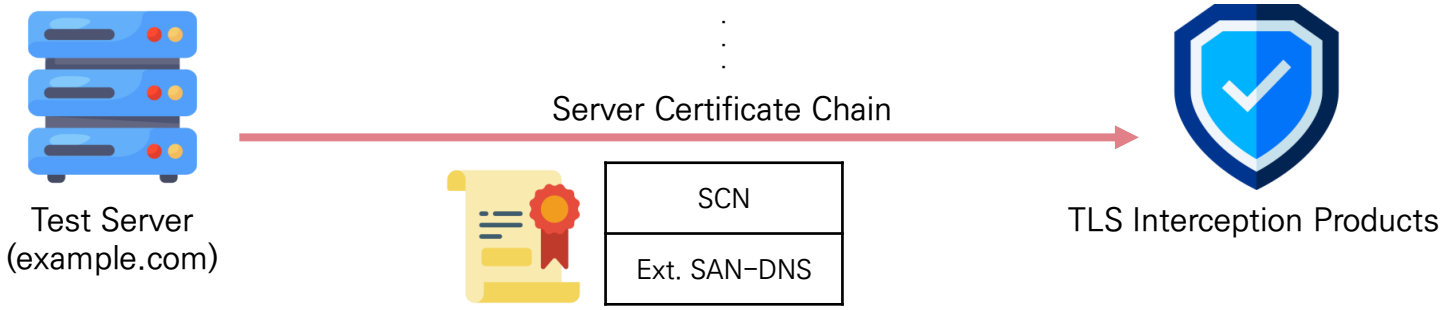
Subject Validation Test

TABLE 3
IP Address Server and/or fqdn Identities

	Antivirus								Proxies									
	Avast		Kaspersky		AVG		ESET		Squid		Charles		Mitm		Fiddler		Standards	
	S1	IP	S1	IP	S1	IP	S1	IP	S1	IP	S1	IP	S1	IP	S1	IP	S1	IP
vi) SCN= null , SAN-IP=192.168.133.149	dV	dV	W	A	dV	dV	dV	dV	R	R	iV	iV	W → R	W → R	W	W → A	I	I
vii) SCN= sana1.fr ,SAN-IP=192.168.133.149	dV	dV	A	A	dV	dV	dV	dV	W	R	iV	iV	A	W → R	A	W → A	V	I
viii) SCN= null, SAN-IP=192.168.133.149 SAN-DNS=sana1.fr	dV	dV	A	A	dV	dV	dV	dV	A	R	iV	iV	W → A	W → R	A	W → A	V	I
ix) SCN= null ,No SAN-IP ,SAN-DNS=sana1.fr	dV	dV	A	W	dV	dV	dV	dV	A	R	iV	iV	A	W → R	A	W	V	I
x) SCN= null ,No SAN-IP ,SAN-DNS=null	dV	dV	W	W	dV	dV	dV	dV	R	R	iV	iV	W → R	W → R	W	W	I	I
xi) SCN= null , SAN-DNS=null , SAN-IP=192.168.133.149	dV	dV	W	A	dV	dV	dV	dV	R	R	iV	iV	W	W	W	W → A	I	I
xii) SCN= null , SAN-IP=141.115.26.43	dV	dV	? → W	? → A	dV	dV	dV	dV	? → R	? → R	iV	iV	? → R	? → R	? → R	? → A	I	V
xiii) SCN= dane.irit.fr ,SAN-IP=141.115.26.43	dV	dV	? → A	? → A	dV	dV	dV	dV	? → W	? → R	iV	iV	? → A	? → R	? → A	? → A	V	V
xiv) SCN= null ,SAN-IP=141.115.26.43 SAN-DNS=dane.irit.fr	dV	dV	? → A	? → A	dV	dV	dV	dV	? → A	? → R	iV	iV	? → A	? → R	? → A	? → A	V	V
xv) SCN= null , SAN-DNS =null, SAN-IP=141.115.26.43	dV	dV	? → W	? → A	dV	dV	dV	dV	? → R	? → R	iV	iV	? → R	? → R	? → W	? → A	I	V

*Where: **S1** = sana1.fr or dane.irit.fr, **IP** = 192.168.133.149 or 141.115.26.43, **Na** = not applicable, **dV** = delegated Validation, **iV** = incorrect Validation, **A** = Accept, **W** = Warn, **R** = Refuse, **I** = Invalid certificate w.r.t standard, **V** = valid certificate w.r.t standard, **?** → = means that we didn't make this specific test in 2017.*

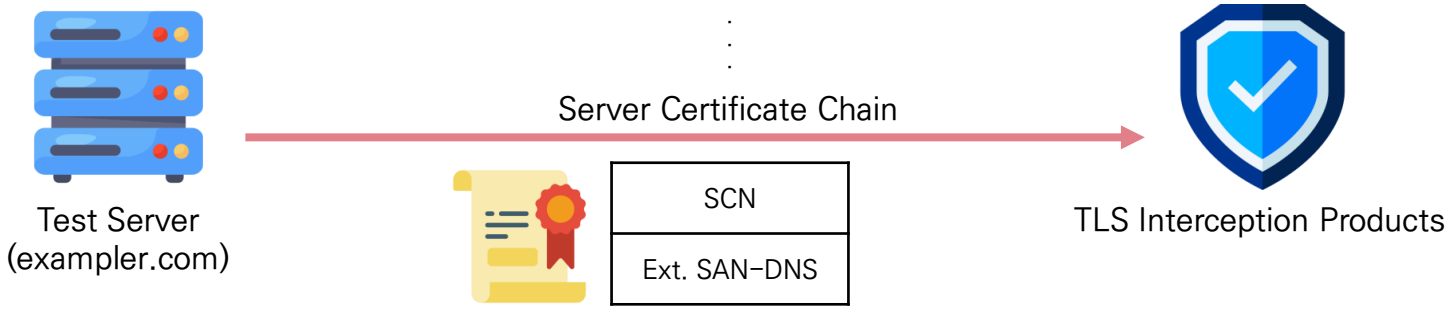
Subject Validation Test: CN, SAN-DNS



3/4 FV Product Passed

Subject Common Name (SCN)	Extension Subject Alt Name (SAN-DNS)	Standards
example.com	exampler.com	X
-	exampler.com	X
example.com	-	?
-	-	X
-	example.com / exampler.com	O

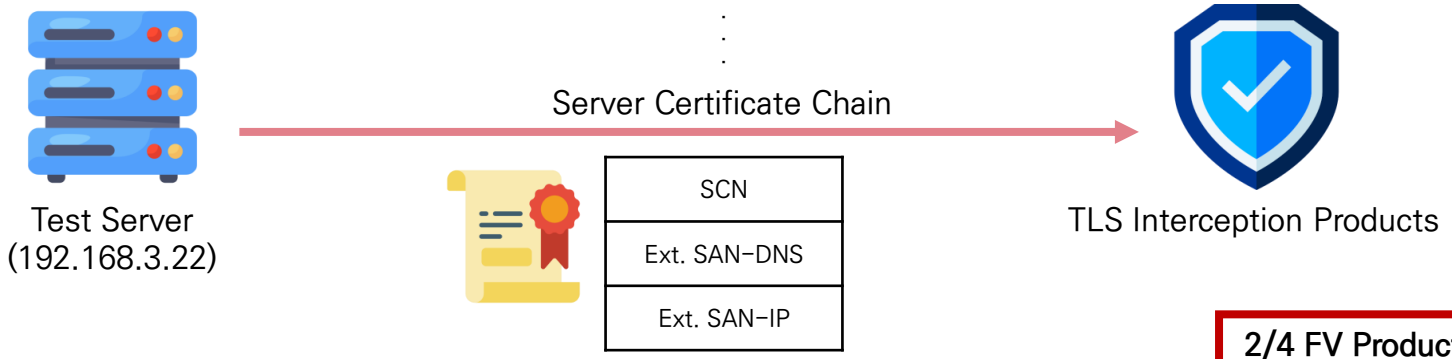
Subject Validation Test: CN, SAN-DNS



4/4 FV Product Passed

Subject Common Name (SCN)	Extension Subject Alt Name (SAN-DNS)	Standards
example.com	exampler.com	O
-	exampler.com	O
example.com	-	X
-	-	X
-	example.com / exampler.com	O

Subject Validation Test: CN, SAN-DNS/IP



2/4 FV Product Passed

Subject Common Name (SCN)	Extension Subject Alt Name (SAN)	Extension SAN IP (SAN-IP)	Standards
-	-	192.168.3.22	X
example.com	-	192.168.3.22	X
-	example.com	192.168.3.22	X
-	example.com	-	X
-	-	-	X
-	-	192.168.3.22	X

Key Usage, Extended Key Usage Fields

```
Version: 3 (0x2)
Serial Number:
            f3:c9:29:12:34:18:17:b4:12:8b:8a:31:d4:98:cc:51
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Google Trust Services, CN=WR2
Validity
            Not Before: Oct  7 08:23:38 2024 GMT
            Not After : Dec 30 08:23:37 2024 GMT
Subject: CN=*.google.com
Subject Public Key Info:
...
X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            Authority Information Access:
                OCSP - URI:http://o.pki.goog/wr2
                CA Issuers - URI:http://i.pki.goog/wr2.crt
            X509v3 Subject Alternative Name:
                DNS:*.google.com, DNS:*.appengine.google.com, …
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://c.pki.goog/wr2/75r4ZyA3vA0.crl
              ...
Signature Algorithm: sha256WithRSAEncryption
Signature Value:  0e:0d:75:66:4c:68:e9:37:...
```

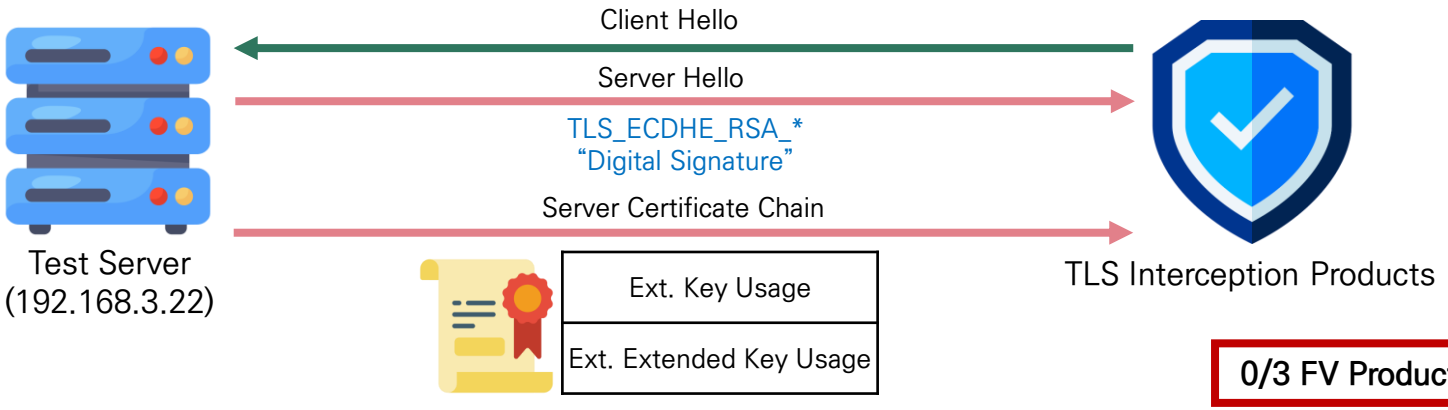
Key Usage, Extended Key Usage

- X.509: Key usage and extended key usage must be consistent; if not, the certificate is invalid
- RFC 5280: Recommends TLS certificates with:
  - Key Usage: "digital signature," "key encipherment," or "key agreement."
  - Extended Key Usage: "Server Authentication."

- Testing Method

1. Certificates generated with RSA algorithm.
2. TLS_ECDHE_RSA_* ciphersuite is selected during TLS handshake which requires ”digitalSignature” key usage
3. Tested TLS Interception Product’s response to mismatched key usage values

Key Usage, Extended Key Usage Tests



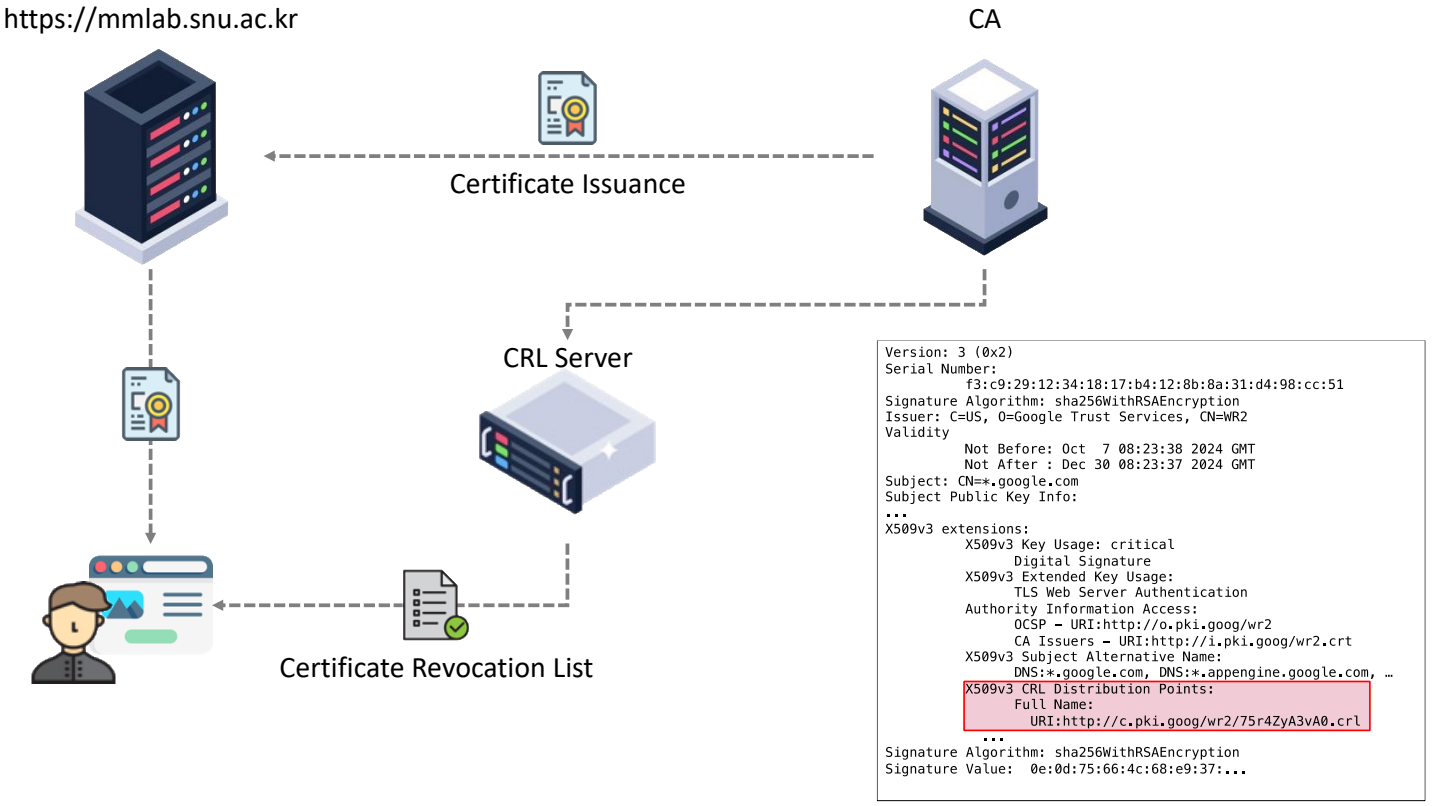
0/3 FV Product Passed

Key Usage	Extended Key Usage		Standards	
Key Agreement	–	SA	X	X
Data Encipherment	–	SA	X	X
Key Encipherment	–	SA	X	X
Digital Signature	–	SA	O	O
–	Client Authentication		X	
Digital Signature	Client Authentication		X	

Revocation Checking Fields

```
Version: 3 (0x2)
Serial Number:
            f3:c9:29:12:34:18:17:b4:12:8b:8a:31:d4:98:cc:51
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Google Trust Services, CN=WR2
Validity
            Not Before: Oct  7 08:23:38 2024 GMT
            Not After : Dec 30 08:23:37 2024 GMT
Subject: CN=*.google.com
Subject Public Key Info:
...
X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            Authority Information Access:
                OCSP - URI:http://o.pki.goog/wr2
                CA Issuers - URI:http://i.pki.goog/wr2.crt
            X509v3 Subject Alternative Name:
                DNS:*.google.com, DNS:*.appengine.google.com, …
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://c.pki.goog/wr2/75r4ZyA3vA0.crl
              ...
Signature Algorithm: sha256WithRSAEncryption
Signature Value:  0e:0d:75:66:4c:68:e9:37:...
```

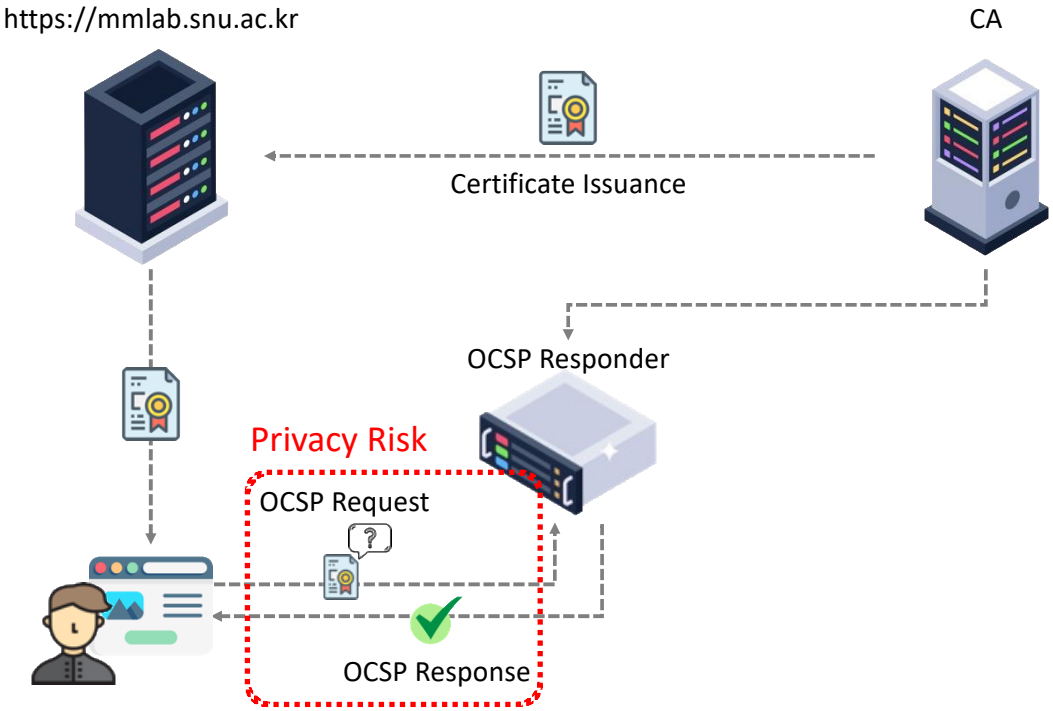
Revocation Checking – CRL



- A list of all certificates that a CA has revoked before their expiration
- Clients are required to update/check before each HTTPS connection

출처: 2023 인터넷 보안 프로그래밍 과제. 김현수, 강상위

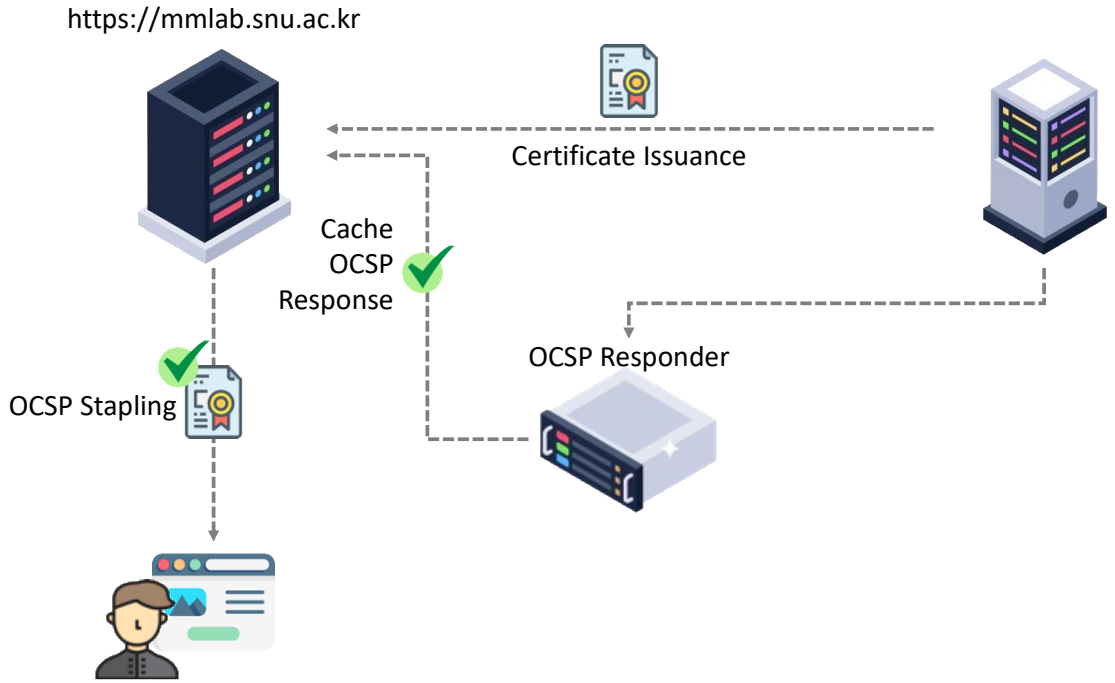
Revocation Checking – OCSP



- CAs maintain simple HTTP servers called OCSP responders
- OCSP responses provide real-time certificate status

출처: 2023 인터넷 보안 프로그래밍 과제. 김현수, 강상위

Revocation Checking – OCSP Stapling



- OCSP queries introduce additional round-trip time (RTT)
- Web servers obtain and cache signed OCSP responses (for up to 7 days), which are sent during the TLS handshake

출처: 2023 인터넷 보안 프로그래밍 과제. 김현수, 강상위

Revocation Checking

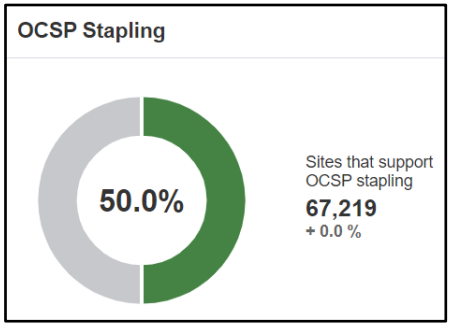
- X.509 Standard
  - CRL Distribution Points (CDP) is recommended as non-critical for interoperability.
  - If critical, the certificate must not be used until revocation check is done

- RFC 5280
  - CDP and AIA Extensions are recommended as non-critical but should be supported by CAs and applications

- CA/Browser Forum and OCSP Stapling
  - OCSP Protocol: Required since January 2013
  - OCSP Stapling: For high-traffic domains, the domain owner must "staple" OCSP responses in the TLS handshake, enforced by contract or technical review

OCSP Stapling Survey

Year	OCSP Stapling	OCSP Must-Staple
2018	19%	0.04%
2019	27%	0%
2022*	31%	0%
2024**	50%	–

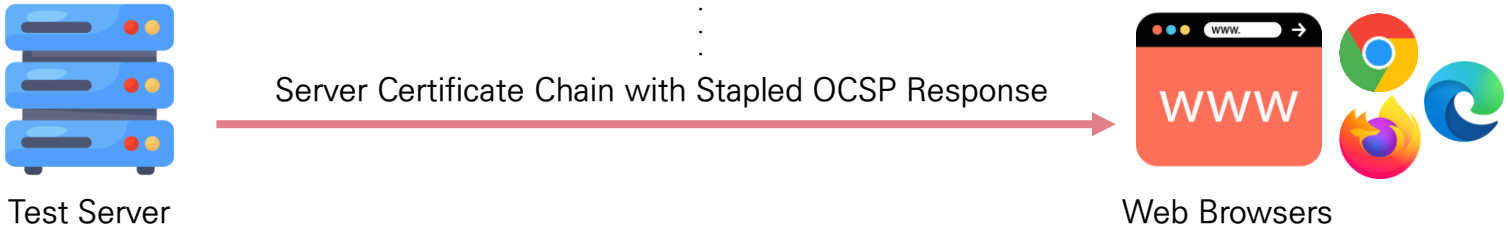


- Alexa Top 1M websites
- Establishes a TLS connection and checks **OCSP Stapling** and **Must-Staple** extension usage
- Decline in OCSP Must-Staple extension may be due to its **implementation challenges**

* Berbecaru, Diana Gratiela, and Antonio Lioy. "An evaluation of X. 509 certificate revocation and related privacy issues in the web PKI ecosystem." *IEEE Access* (2023).

** www.ssllabs.com/ssl-pulse/

Web Browser's Revocation Tests



Stapled OCSP Response	Must-Stapled	Opera	FireFox	Chrome	IE	Edge
Good	TRUE	O	O	O	O	O
Revoked	TRUE	X	X	X	X	X
-	TRUE	O	X	O	O	O

Interception Products Revocation Tests

Revocation Checking Support	Avast	Kaspersky	AVG	ESET	Fiddler
CRL	O	X	O	O	X
Test: CRL Unretrievable	Accept (Soft-Fail)	-	Accept (Soft-Fail)	Accept (Soft-Fail)	-
OCSP	X	O	X	O	O
Test: OCSP Server is down	-	Accept (Soft-Fail)	-	Accept (Soft-Fail)	Accept (Soft-Fail)
OCSP Stapling	O	X	O	X	X
Test: Stapled OCSP response is revoked	Refuse	-	Refuse	-	-
OCSP Must-Stapled	X	X	X	X	X

Conclusion and Critique

- The certificate validation performed by TLS interception products is even worse than that performed by web browsers
  - Compared to their 2017 study on web browsers

- None of the existing revocation checking techniques work consistently or effectively today (as of 2020)
  - This remains true even now in 2024
  - Still, the usage of OCSP stapling has increased to 50%

- The selection of TLS interception products is questionable
  - Why include the Charles proxy, an IV product, in the list of 8 products?
  - Shouldn't other FV or DV products (7 in total) perform revocation checking based on their categorization? Only 5 of them do