PROGRAMMING ASSIGNMENT
VALIDATING CERTIFICATES

Deadline: 2022. 11. 22 (Wed) 23:59

TA: Hyunsoo Kim (hskim@mmlab.snu.ac.kr)
Sangwi Kang (swkang@mmlab.snu.ac.kr)

서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

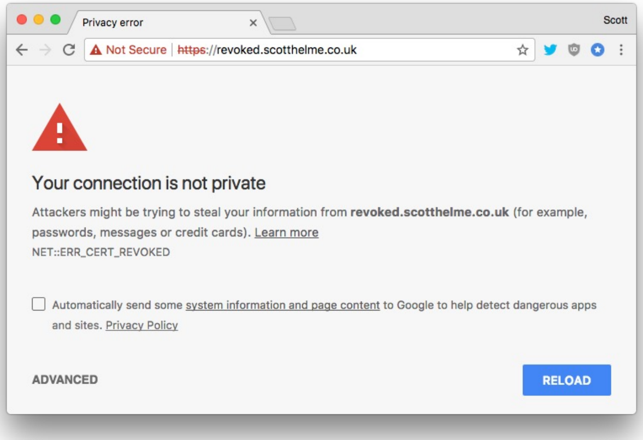
MMLab
Network Convergence & Security Lab

Good Bye, Padlocks

The padlock is shown when **a secure encrypted channel is established** between the server and the browser (TLS/HTTPS)

– This further implies that:

1. **The browser can validate the server's certificate chain using its trusted root certificate**
2. The certificate is logged in the Certificate Transparency log
3. **The certificate is not revoked**



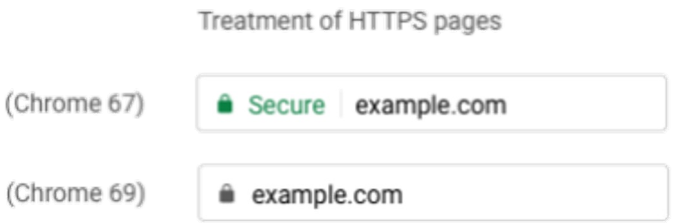
Your connection is not private

Attackers might be trying to steal your information from **revoked.scotthelme.co.uk** (for example, passwords, messages or credit cards). Learn more

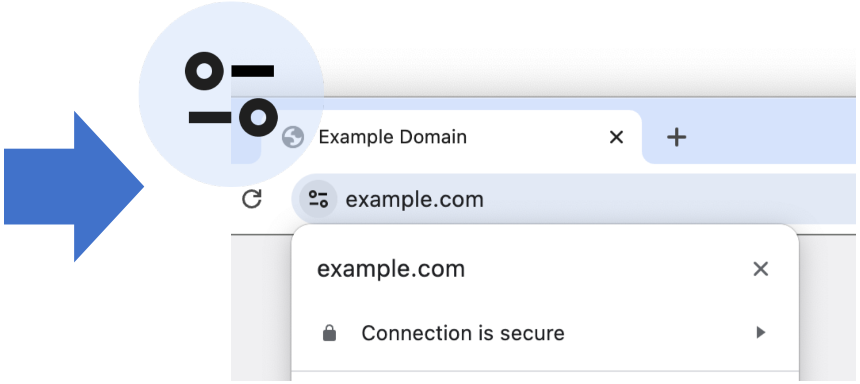
NET::ERR_CERT_REVOKED

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy Policy

ADVANCED RELOAD


Treatment of HTTPS pages

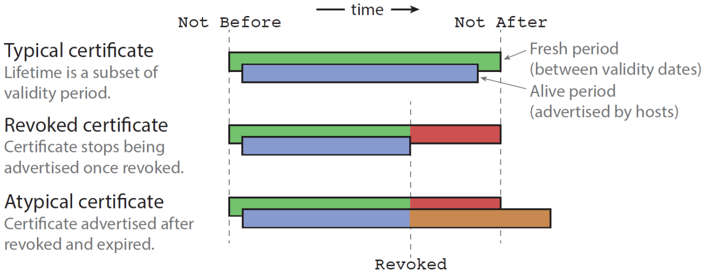
(Chrome 67)	Secure | example.com
(Chrome 69)	example.com



https://blog.chromium.org/2023/05/an-update-on-lock-icon.html

CERTIFICATE REVOCATION

- Invalidating a certificate before it expires
  - Around 1% get revoked in their lifetime
- Massive revocation event occurs when …


Not Before
time
Not After
Typical certificate
Lifetime is a subset of validity period.
Fresh period (between validity dates)
Alive period (advertised by hosts)
Revoked certificate
Certificate stops being advertised once revoked.
Atypical certificate
Certificate advertised after revoked and expired.
Revoked

Security Incidents

E.g., Heartbleed Vulnerability (2014)

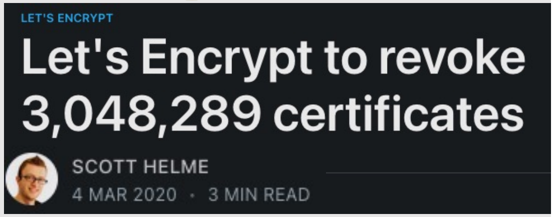
- Compromised many certificates
- Increased revocation percentage from 1% to 11%
- Cost Cloudflare an additional $400,000 per month to publish enlarged CRL

Distrust on CA

DigiNotar
Internet Trust Services

Symantec

沃通
WoSign


LET'S ENCRYPT

Let's Encrypt to revoke 3,048,289 certificates

SCOTT HELME
4 MAR 2020 · 3 MIN READ

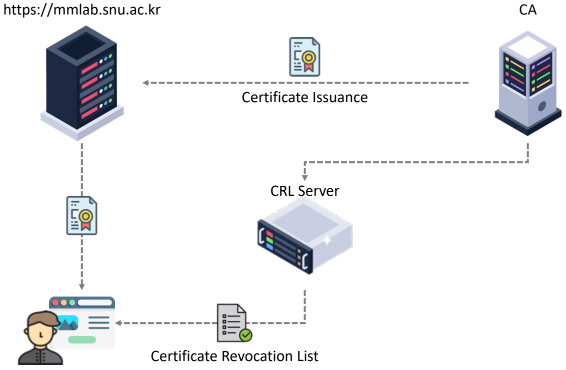
Let's Encrypt

- CA operational issue
- Certificate misissuance
- Implementation bug
- And much more …

REVOCATION CHECKING

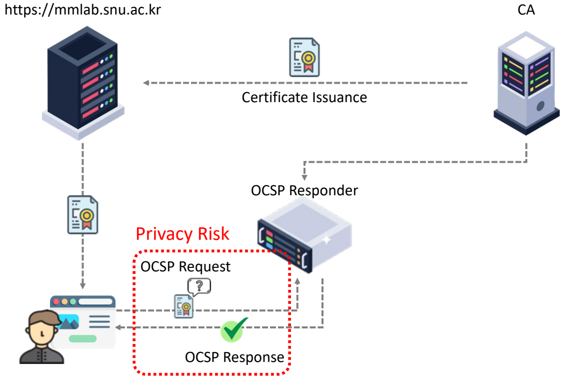
Certificate Revocation List (CRL)

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



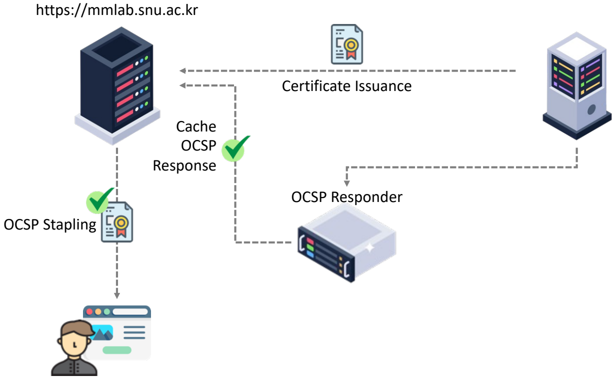
Online Certificate Status Protocol (OCSP)

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



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



ASSIGNMENT

- Write a program that validates the certificate provided by the server
  1. Connects to the server (either URL or IP)
  2. Retrieves the certificate chain during the TLS handshake
  3. Perform a **detailed verification** of the certificate chain
  4. Perform **revocation checking** using **either** CRL or OCSP

  } Sample code provided

- You are free to use any SSL library and programming language of your choice

- However, DO NOT use **shell scripts** or any kind of **automated SSL commands**

SAMPLE CODE

- What it does:

1. OpenSSL initialization, TLS connection, and cleanup
2. OCSP Stapling handling
3. Trusted root store
   - Sets the location of the trusted root store
   - You need to adapt them based on the actual location of the certificates on your system
4. Default Certificate Verification and certificate chain retrieval
   - Checks the result of the SSL certificate verification
   - Retrieves the server's certificate chain and prints out [–v] certificate detail or saves [–o] them to files

Running the Sample Code

- Install OpenSSL (1.1.1v / 1.1.1w)
  - `apt` for Debian-based systems or `yum` for RedHat-based systems
  - On macOS, OpenSSL is usually pre-installed, or you can install it using Homebrew (`brew install openssl`)
- Compile `sampleClient.c`

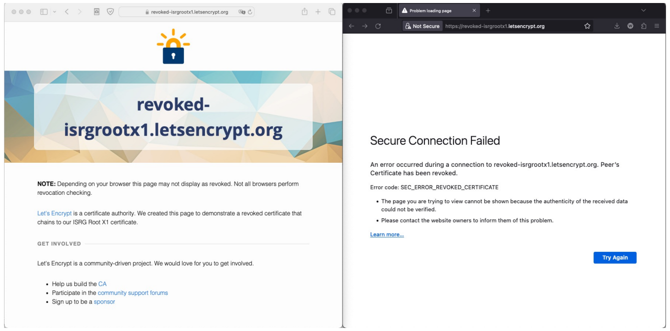
```
gcc sampleClient.c -o sampleClient -lssl -lcrypto
```

  - ✓ Debian Bullseye – gcc/g++ 10.2.1, Bookworm – gcc/g++ 12.0.3
  - ✓ Ubuntu 20.04 LTS: gcc/g++ 9.3.0
  - ✓ Apple clang 15.0.0
- Run `sampleClient`

```
./sampleClient www.google.com
./sampleClient -v 147.46.10.129
./sampleClient -o expired-rsa-dv.ssl.com
```

Some Domains for Retreiving Certificates

- www.google.com
  - OCSP stapling not used, Valid certificate
- www.naver.com
  - OCSP stapling used, Valid certificate
- revoked-isrgrootx1.letsencrypt.org
  - OCSP stapling not used, Revoked certificate (OCSP)


revoked-isrgrootx1.letsencrypt.org
Problem loading page
Not Secure
https://revoked-isrgrootx1.letsencrypt.org
Learn more…
Try Again

revoked-isrgrootx1.letsencrypt.org

NOTE: Depending on your browser this page may not display as revoked. Not all browsers perform revocation checking.

Let's Encrypt is a certificate authority. We created this page to demonstrate a revoked certificate that chains to our ISRG Root X1 certificate.

GET INVOLVED

Let's Encrypt is a community-driven project. We would love for you to get involved.

- Help us build the CA
- Participate in the community support forums
- Sign up to be a sponsor

Secure Connection Failed

An error occurred during a connection to revoked-isrgrootx1.letsencrypt.org. Peer's Certificate has been revoked.

Error code: SEC_ERROR_REVOKED_CERTIFICATE

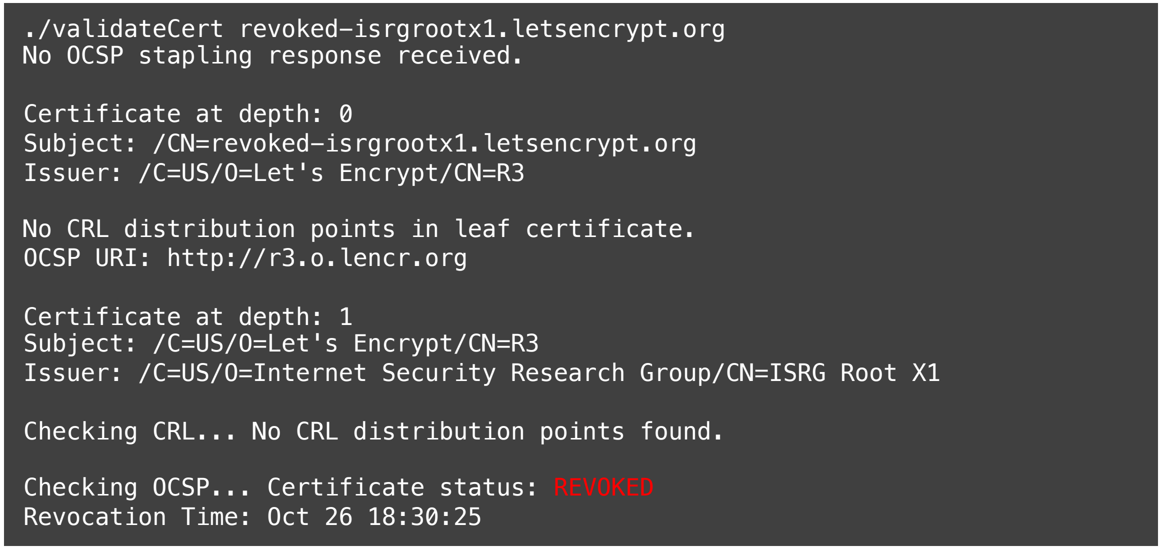
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

- https://www.ssl.com/sample-valid-revoked-and-expired-ssl-tls-certificates/
  - Valid certificates
  - Expired certificates
  - Revoked certificates (provided by both OCSP and CRL)

TEST CASES

1. Invalid certificate
   ➔ 어떤 인증서에서 검증에 실패하였는지, 서명 검증 불가, trusted root 인증서 없음 등 정확한 원인 출력
2. Expired certificate
   ➔ 어떤 인증서가 언제 만료되었는지 출력
3. Valid certificate from OS/Browser trusted root store w/ OCSP stapling
   ➔ 샘플 코드로 이미 PASS
4. Valid certificate w/ both CRL distribution point and OCSP responder
   ➔ CRL distribution point 출력 및 저장 기능 구현, OCSP responder URI 출력 구현
5. Revoked certificate (either through CRL or OCSP)
   ➔ 본인이 구현한 revocation checking 기법으로 revoked 상태 및 관련 정보 출력

- Sample



```
./validateCert revoked-isrgrootx1.letsencrypt.org
No OCSP stapling response received.

Certificate at depth: 0
Subject: /CN=revoked-isrgrootx1.letsencrypt.org
Issuer: /C=US/O=Let's Encrypt/CN=R3

No CRL distribution points in leaf certificate.
OCSP URI: http://r3.o.lencr.org

Certificate at depth: 1
Subject: /C=US/O=Let's Encrypt/CN=R3
Issuer: /C=US/O=Internet Security Research Group/CN=ISRG Root X1

Checking CRL... No CRL distribution points found.

Checking OCSP... Certificate status: REVOKED
Revocation Time: Oct 26 18:30:25
```

Scoring Criteria (Full Score: 10pts)

- For each correct outcome from the test cases, + 2 pts
  - You are already given 2 points!
  - 5 test cases

- Deduction points for:
  - Use of shell scripts
  - Use of hard-coded information
  - Any other direct usage of OpenSSL (or similar SSL libraries) commands

SUBMISSION GUIDELINES

- Upload your compressed archive file (e.g., .zip, tar, gz) to myETL
  - *name_studentIdNumber*.*
  - 멜론머스크_2023-73514.zip
- Include the following items in your submission
  - README
    - ✓ Name, Email, Mobile (we may contact you if we face any issue compiling or running your code)
    - ✓ Development environment, libraries used, compilation commands, and any other necessary details for execution
  - Source code(s) and compiled executable file(s)
- Please write detailed comments in the code!
  For the functions you've written, please provide definitions for their respective functionalities and input/output.

감사합니다

Thank you~!