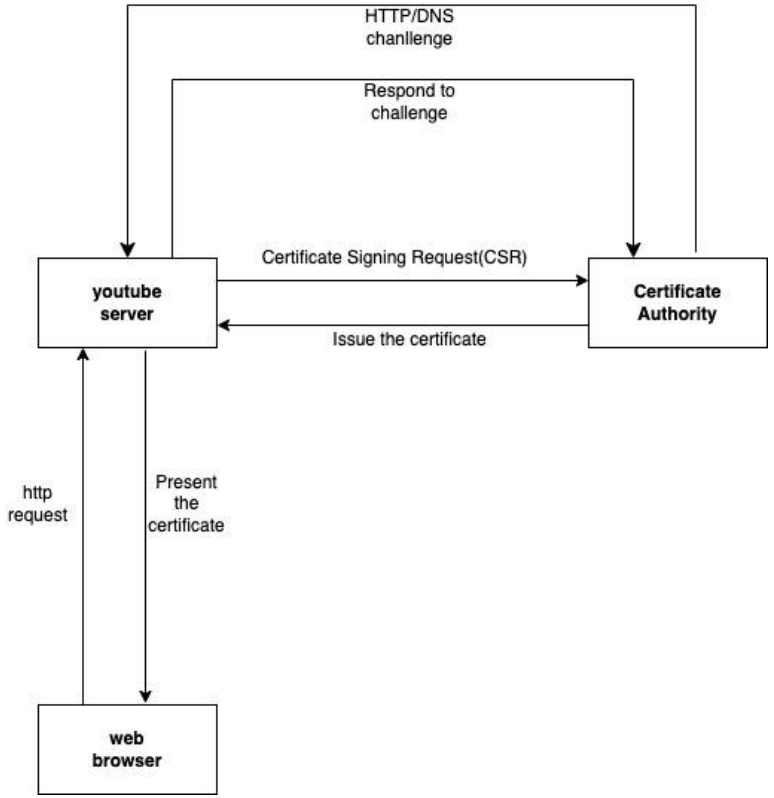
Fuzzing-based Testing of Certificate Authority

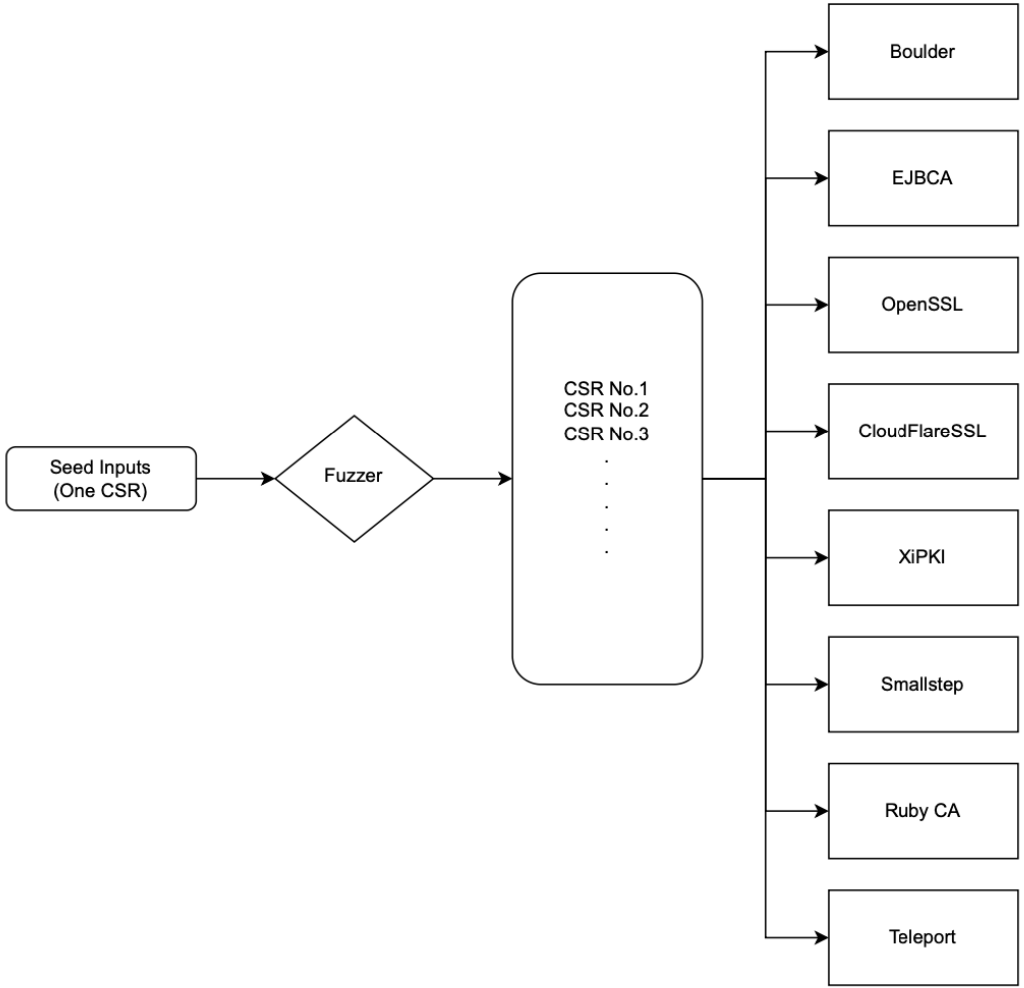
Yunhan Qiao, Yen-Chun Huang, Ming Wei (Group 9)

Motivation

- If someone sends a fake Certificate Signing Request (CSR) and obtains a certificate from a CA, they could intercept users' credentials.
- Users will not be able to access the server if it cannot obtain a certificate, even if the server sends a valid CSR to the CA.
- CAs risk losing their customers if servers are unable to obtain certificates from them.



Approach


Seed Inputs
(One CSR)
Fuzzer
CSR No.1
CSR No.2
CSR No.3
Boulder
EJBCA
OpenSSL
CloudFlareSSL
XiPKI
Smallstep
Ruby CA
Teleport

Research Question

RQ1: How effective is CATest in detecting CA bugs?

Approach:

Fuzzing-based approach, custom mutator

Metrics:

1. Code coverage
2. Number of fields that are mutated in Certificate Signing Request
3. Number of True positives (Actual bugs)

Research Question

RQ2: How can a custom mutator improve the performance of a fuzzer? (ablation study)

Approach:

Fuzzer default mutation strategy

Metrics:

1. Code coverage
2. Number of fields of Certificate Signing Request that are mutated
3. Number of True positives (Actual bugs)

Research Question

RQ3: How does CATest compare with the other state-of-the-art tools?

Approach:

Searching other tools of testing CA

Metrics:

1. True positives

Dataset

CA libraries	Programming Language it used	What it is used for
Boulder	Go	The software powering Let's Encrypt, designed to automate the issuance, renewal, and revocation of SSL/TLS certificates for secure web communications.
EJBCA	Java	Is a robust, scalable open source PKI solution for managing digital certificates for secure communication and identity authentication across various applications and systems.
OpenSSL	C	It provides a comprehensive toolkit for SSL/TLS certificate management, including generation, signing, and encryption, to secure communications over the internet.

Dataset

CA libraries	Programming Language it used	What it is used for
Cloudflare SSL	Rust	It offers integrated, automated SSL/TLS certificate issuance and management, enhancing website security and performance across Cloudflare's global network.
XiPKI	Java	Is a high-performance, scalable open source solution for PKI management, offering certificate issuance, revocation, and OCSP services for secure digital communications.
Smallstep	Go	It simplifies secure and automated certificate management for TLS, enabling easy issuance, renewal, and revocation of certificates for secure web services.

Dataset

CA libraries	Programming Language it used	What it is used for
r509	Ruby	It is a Ruby library for simplified management of X.509 certificates, facilitating certificate generation, signing, and revocation within applications.
Teleport	Go	It provides secure identity-based access and authentication for SSH, Kubernetes, web applications, and databases through certificate management and role-based access control.

Benchmark

Approach:

Finding bugs that can affect CA produce certificate from the above dataset.

Thank you for your attention!