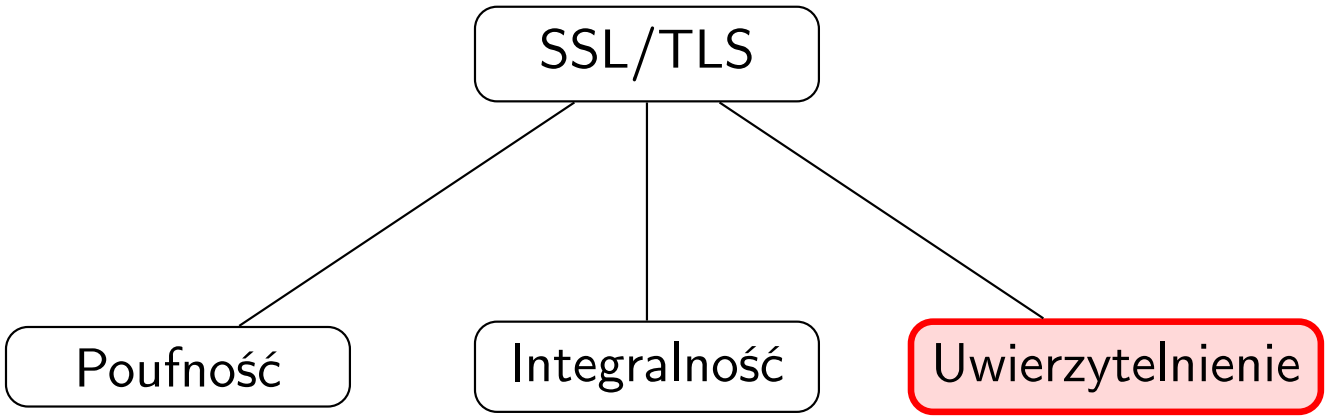
Kryptoanaliza stosowana

Frankencerts - Jak testować certyfikaty SSL/TLS

Rafał Leja (UWr)

26 listopada 2025

SSL/TLS



Rysunek: SSL/TLS gwarantuje poufność, integralność i uwierzytelnienie.

SSL/TLS - uwierzytelnienie

- SSL/TLS używa certyfikatów X.509
- Certyfikaty są wydawane przez zaufane podmioty zwane Urzędami Certyfikacji (CA).
- Przeglądarka posiada listę zaufanych CA
- Certyfikat jest zweryfikowany jeśli:
  - jest ważny
  - został wydany przez zaufanego CA

SSL/TLS - certyfikaty X.509

- Certyfikat X.509 zawiera (między innymi):
  - Nazwę podmiotu (np. nazwę domeny).
  - Klucz publiczny podmiotu.
  - Dane o wydającym CA.
  - Data wystawienia certyfikatu.
  - Okres ważności certyfikatu.
  - Podpis cyfrowy wydającego CA.

SSL/TLS - weryfikacja certyfikatu

- Przeglądarka musi zweryfikować certyfikat domeny, sprawdzając:
  - Czy certyfikat jest podpisany przez zaufanego CA.
  - Czy nazwa domeny w certyfikacie pasuje do odwiedzanej strony.
  - Czy certyfikat nie wygasł.
  - Czy certyfikat nie został unieważniony (CRL, OCSP).
- Trzeba również sprawdzić certyfikaty pośrednie w łańcuchu zaufania.

SSL/TLS - Podatności

- Podatności weryfikacji w SSL/TLS mogą wynikać z:
  - Błędów implementacji weryfikacji SSL/TLS.
  - Słabych algorytmów kryptograficznych (np. RC4, MD5).
- Przy błędniej weryfikacji, atak MitM staje się możliwy, nawet przy użyciu SSL/TLS.

Jak testować poprawność implementacji

- Skąd brać różne certyfikaty do testów?

Jak testować poprawność implementacji

- Skąd brać różne certyfikaty do testów?
  - Prawdziwe certyfikaty z Internetu $\Rightarrow$ Tylko poprwane certyfikaty.
  - Fuzzing $\Rightarrow$ Większość certyfikatów będzie odrzucona na poziomie parsowania.
  - Manualne tworzenie certyfikatów $\Rightarrow$ Czasochłonne.
- Potrzebne jest automatyczne generowanie certyfikatów z kontrolowanymi błędami.

Jak testować poprawność implementacji

- Jak interpretować wyniki testów?

Jak testować poprawność implementacji

- Jak interpretować wyniki testów?
  - Manualna analiza wyników $\Rightarrow$ Czasochłonna i podatna na błędy.
  - Automatyczna analiza wyników $\Rightarrow$ Wymaga bezbłędnego zaimplementowania SSL/TLS.
- Potrzebujemy "Wyroczni" weryfikującej certyfikaty.

Frankencerts

- Frankencerts to podejście do automatycznego testowania implementacji SSL/TLS.
- Składa się z dwóch głównych komponentów:
  - Generatora certyfikatów z kontrolowanymi błędami.
  - Wyroczni do weryfikacji certyfikatów.

Źródła

- C. Brubaker, S. Jana, B. Ray, S. Khurshid, and V. Shmatikov. Using Frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations. In 35th IEEE Symposium on Security and Privacy, pages 114–129. IEEE Computer Society, 2014.
- Wikipedia: Transport Layer Security
- Wikipedia: X.509
- Cloudflare: What is a TLS handshake?
- Cloudflare: What is an SSL certificate?