Kryptoanaliza stosowana

Frankencerts - Jak testować certyfikaty SSL/TLS

Rafał Leja

26 listopada 2025

Scenariusz: odwiedzanie strony www w 1994 r.

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.

Scenariusz: odwiedzanie strony www w 1994 r.

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.

Scenariusz: odwiedzanie strony www w 1994 r.

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Otrzymuje odpowiedź z adresem IP i łączy się z serwerem na porcie 80.

Scenariusz: odwiedzanie strony www w 1994 r.

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Otrzymuje odpowiedź z adresem IP i łączy się z serwerem na porcie 80.
- Wysyła żądanie HTTP o stronę www.example.com.

Scenariusz: odwiedzanie strony www w 1994 r.

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Otrzymuje odpowiedź z adresem IP i łączy się z serwerem na porcie 80.
- Wysyła żądanie HTTP o stronę www.example.com.
- Serwer odpowiada stroną HTML, którą przeglądarka renderuje i wyświetla użytkownikowi.

Scenariusz: Ewa przekieruje ruch do swojego serwera

Przed atakem Ewa musi się przygotować.

- Ewa rejestruje domenę www.eve.com i ustawia jej rekord A na swój serwer.

Scenariusz: Ewa przekieruje ruch do swojego serwera

Przed atakem Ewa musi się przygotować.

- Ewa rejestruje domenę www.eve.com i ustawia jej rekord A na swój serwer.
- Ewa modyfikuje rekordy DNS dla www.example.com, aby wskazywały na jej serwer (np. poprzez atak DNS spoofing).

Scenariusz: odwiedzanie strony www po ataku Ewy

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.

Scenariusz: odwiedzanie strony www po ataku Ewy

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.

Scenariusz: odwiedzanie strony www po ataku Ewy

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Ewa odpowiada, podając adres IP swojego serwera.

Scenariusz: odwiedzanie strony www po ataku Ewy

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Ewa odpowiada, podając adres IP swojego serwera.
- Wysyła żądanie HTTP o stronę www.example.com.

Scenariusz: odwiedzanie strony www po ataku Ewy

Chcemy wejść na strone www.example.com.

- Wpisujemy w przeglądarce adres URL i naciskamy Enter.
- Przeglądarka musi znaleźć adres IP serwera, na którym znajduje się strona. Wysyła zapytanie do DNS.
- Ewa odpowiada, podając adres IP swojego serwera.
- Wysyła żądanie HTTP o stronę www.example.com.
- Serwer Ewy odpowiada stroną HTML, która może wyglądać jak oryginalna strona, ale jest fałszywa.

Słabe punkty scenariusza

- Brak uwierzytelniania serwera DNS: przeglądarka ufa odpowiedzi DNS bez weryfikacji.

Słabe punkty scenariusza

- Brak uwierzytelniania serwera DNS: przeglądarka ufa odpowiedzi DNS bez weryfikacji.
  - Współczesne rozwiązanie: DNSSEC.

Słabe punkty scenariusza

- Brak uwierzytelniania serwera DNS: przeglądarka ufa odpowiedzi DNS bez weryfikacji.
  - Współczesne rozwiązanie: DNSSEC.
  - Problem: DNSSEC nie jest powszechnie wdrożony.

Słabe punkty scenariusza

- Brak uwierzytelniania serwera DNS: przeglądarka ufa odpowiedzi DNS bez weryfikacji.
  - Współczesne rozwiązanie: DNSSEC.
  - Problem: DNSSEC nie jest powszechnie wdrożony.
- Brak uwierzytelniania serwera WWW: przeglądarka nie sprawdza, czy serwer WWW jest tym, za kogo się podaje.

Słabe punkty scenariusza

- Brak uwierzytelniania serwera DNS: przeglądarka ufa odpowiedzi DNS bez weryfikacji.
  - Współczesne rozwiązanie: DNSSEC.
  - Problem: DNSSEC nie jest powszechnie wdrożony.
- Brak uwierzytelniania serwera WWW: przeglądarka nie sprawdza, czy serwer WWW jest tym, za kogo się podaje.
  - Współczesne rozwiązanie: SSL/TLS z certyfikatami X.509.

SSL/TLS - Podstawy

- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.

SSL/TLS - Podstawy

- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.
- Główne cele SSL/TLS:

SSL/TLS - Podstawy

- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.
- Główne cele SSL/TLS:
  - Poufność: szyfrowanie danych przesyłanych między klientem a serwerem.

SSL/TLS - Podstawy

- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.
- Główne cele SSL/TLS:
  - Poufność: szyfrowanie danych przesyłanych między klientem a serwerem.
  - Integralność: zapewnienie, że dane nie zostały zmienione podczas transmisji.

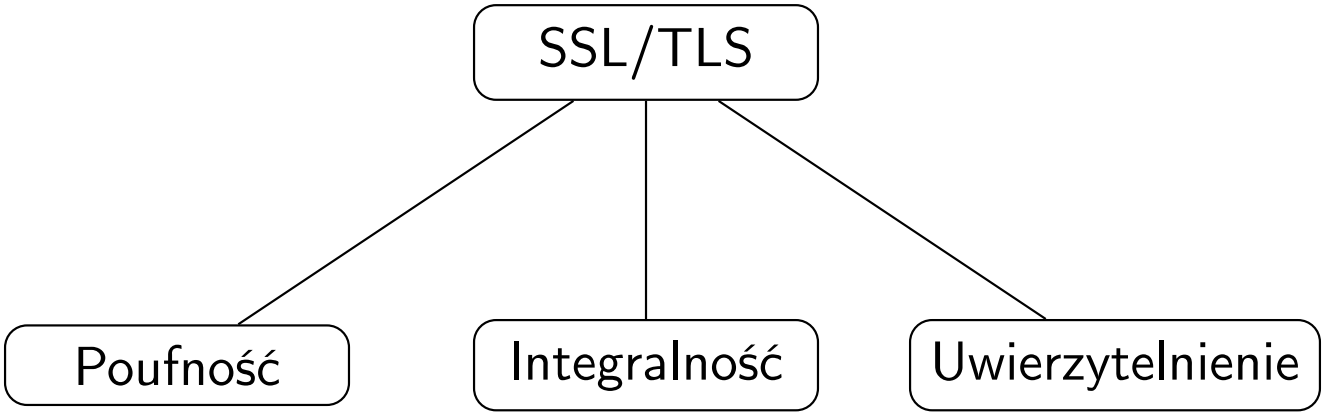
SSL/TLS - Podstawy

- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.
- Główne cele SSL/TLS:
  - Poufność: szyfrowanie danych przesyłanych między klientem a serwerem.
  - Integralność: zapewnienie, że dane nie zostały zmienione podczas transmisji.
  - Uwierzytelnianie: weryfikacja tożsamości serwera (i opcjonalnie klienta) za pomocą certyfikatów cyfrowych.

SSL/TLS - Podstawy

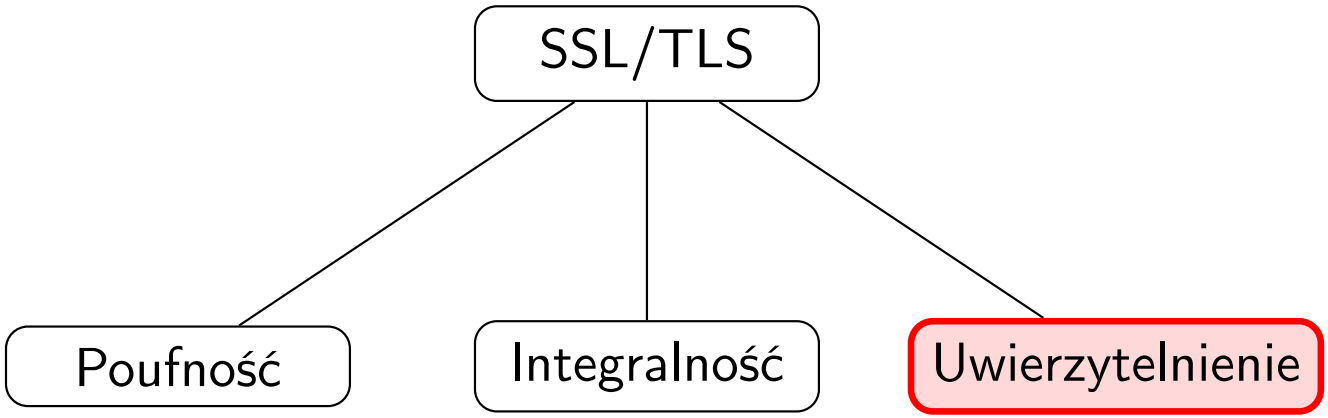
- SSL (Secure Sockets Layer) i jego następca TLS (Transport Layer Security) to protokoły kryptograficzne zapewniające bezpieczną komunikację w sieci.
- Główne cele SSL/TLS:
  - Poufność: szyfrowanie danych przesyłanych między klientem a serwerem.
  - Integralność: zapewnienie, że dane nie zostały zmienione podczas transmisji.
  - Uwierzytelnianie: weryfikacja tożsamości serwera (i opcjonalnie klienta) za pomocą certyfikatów cyfrowych.
- SSL/TLS jest szeroko stosowany w protokołach takich jak HTTPS, SMTP, FTP itp.

SSL/TLS - Struktura



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

SSL/TLS - Struktura



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