AGH

Akademia Górniczo-Hutnicza
Wydział Elektroniki, Automatyki i Inżynierii Biomedycznej

Sposoby ochrony informacji przesyłanych siecią Internet

Jakub Rakoczy, Michał Rus

Spis treści

Bezpieczeństwo przesyłu danych

Bezpieczeństwo przesyłu danych

Własność tę definiuje się jako możliwość przesyłu informacji pomiędzy systemami komputerowymi w taki sposób, by tylko wyznaczony odbiorca otrzymał wiadomość, której treść nie uległa żadnym modyfikacjom.

Sposoby ochrony danych

1. Kontrola dostępu.
2. Zapewnienie spójności danych.
3. Szyfrowanie.
4. Certyfikacja.

Kontrola dostępu

Kontrola dostępu

Kontrola dostępu jest terminem obejmującym **ogół metod ograniczających dostęp do zasobów**. Pomaga to zapobiec nieautoryzowanemu przeglądaniu, modyfikowaniu oraz kopiowaniu zasobów, czyli gwarantuje szeroko pojętą ochronę danych.

Uwierzytelnianie

Uwierzytelnianie

Sposób potwierdzenia zadeklarowanej (w procesie *identyfikacji*) przez podmiot tożsamości, np. za pomocą zgodności hasła lub poprawności podpisu pod zaprezentowanym certyfikatem.

- Celem jest uzyskanie określonego poziomu pewności, że podmiot jest rzeczywiście tym z *identyfikacji*.
- Niepoprawne tłumaczenia: *autentykacja*, *autentyfikacja*.

2FA

2-Factor Authentication

Użytkownik oprócz loginu i hasła musi podać jednorazowy kod z fizycznej karty kodów, otrzymany SMS-em albo odczytany z tokena.

- Przy przechwyceniu loginu i hasła, atakujący nie ma i tak dostępu do źródła kodów.
- Tokeny — zarówno software'owe (np. aplikacja mobilna Google Authenticator), jak i sprzętowe — mają w pamięci pewien klucz. Na podstawie klucza i aktualnego czasu obliczają tę samą liczbę, co serwer.
- Problem: synchronizacja czasu serwera i tokena (rzadko).
- Problem: czynnik ludzki.

ACL

Access Control List

Lista uprawnień dołączona do danego zasobu. Każdy element składa się z przypisania konkretnych uprawnień do uwierzytelnionej grupy/użytkownika.

Dwa użycia w kontekście bezpieczeństwa komunikacji:

1. dostęp do konkretnych zasobów serwera po uwierzytelnieniu (por. Mumble Server),
2. w routerach i in. urządzeniach sieciowych do definicji widoczności usług (por. Cisco).

OAuth2, tokeny

OAuth 2.0

Otwartym standardem autoryzującym umożliwiający użytkownikowi udzielenie zewnętrznej aplikacji (Z) uprawnień dostępu do części zasobów innej aplikacji (A), w której ma on konto.

Przebieg:

1. (Z) wysyła (A) prośbę o token (z listą żądanych uprawnień),
2. (A) pokazuje użytkownikowi ekran akceptacji,
3. użytkownik akceptuje,
4. (Z) dostaje *tylko* token,
5. (Z) używa tokenu zwracając się do (A).

Token pozwala na dostęp tylko do wybranych zasobów i najczęściej wygasa po ustalonym czasie.

Niezaprzeczalność

Niezaprzeczalność

Brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

Autoryzacja

Autoryzacja

Nadanie uwierzytelnionym podmiotom konkretnych uprawnień dostępu do danych zasobów.

Cele:

- kontrola dostępu;
- potwierdzenie, że dany podmiot ma uprawnienia do korzytania z danych zasobów.

Spójność danych

Spójność/integralność danych

Możliwość stwierdzenia, że dane nie zostały nieautoryzowanie zmienione, dodane, usunięte.

- Szalenie ważne jest, abyśmy mogli stwierdzić z *dużą dozą pewności*, iż dane po stronie odbiorcy i nadawcy są dokładnie takie same.
- Chcielibyśmy móc to sprawdzić, przesyłając znacząco mniej danych niż same dane.
- Do tego celu fenomenalnie nadają się kryptograficzne funkcje hashujące.

Kryptograficzne funkcje haszujące

Kryptograficzna funkcja haszująca

Funkcja haszująca (f. skrótu) bezpieczna do zastosowań kryptograficzych; dla stosunkowo dużych danych wejściowych zwraca stosunkowo małą liczbę, typowo 128–512 bitów.

Własności:

- najdrobniejsza zmiana danych wejściowych — np. flipnięcie 1 bitu wśród 100 GiB — całkowicie zmienia wyjście tej funkcji,
- danej wartości funkcji jest niesłychanie trudno spreparować generujące ją wejście,
- jeśli odbiorca i nadawca porównają kryptograficzny skrót ze swych kopii danych, i jeśli skróty te będą takie same, z dość *dużym prawdopodobieństwem* dane są identyczne.

Prawdopodobieństwo kolizji dla 128-bitowej funkcji

W poprzednim slajdzie mówimy o *dużym prawdopodobieństwie*:

- Prawdopodobieństwo kolizji dla dwóch hashy przy 128-bitowej zwracanej liczbie to $\frac{1}{2^{128}} = \frac{1}{340282366920938463463374607431768211456}$.
- Jeśli jednak weźmiemy pod uwagę paradoks urodzin, możemy uzyskać prawdopodobieństwo kolizji $\frac{1}{2}$ wśród 2^{64} takich haszy.
- Haszując 6 *miliardów* plików na sekundę przez następne 100 lat, hasze którychś dwu będą kolidować ze sobą prawdopodobieństwem $\frac{1}{2}$.

MD5

- Wynaleziona w 1991 przez Rona Rivesta z MIT.
- Popularna kryptograficzna funkcja haszująca.
- Zwraca 128-bitową liczbę.
- W 2004 znaleziono sposób na generowanie kolizji...
- ... dlatego odradza się używanie jej.

SHA-1

- Opublikowana w 1995 przez NSA.
- Popularna kryptograficzna funkcja haszująca.
- Zwraca 160-bitową liczbę.
- W 2005–2008 opublikowano m.in. atak, który wymaga 2^{63} operacji funkcji kompresującej, żeby znaleźć kolizję (w porównaniu do 2^{80} przy brute-force)...
- ... dlatego SHA-1 nie powinna być używana w nowych aplikacjach.

SHA-2

- 4 funkcje zaprojektowane w 2001 przez NSA.
- Bitowości: SHA-224, SHA-256 oraz SHA-384, SHA-512.
- Do tej pory nie znaleziono kolizji.

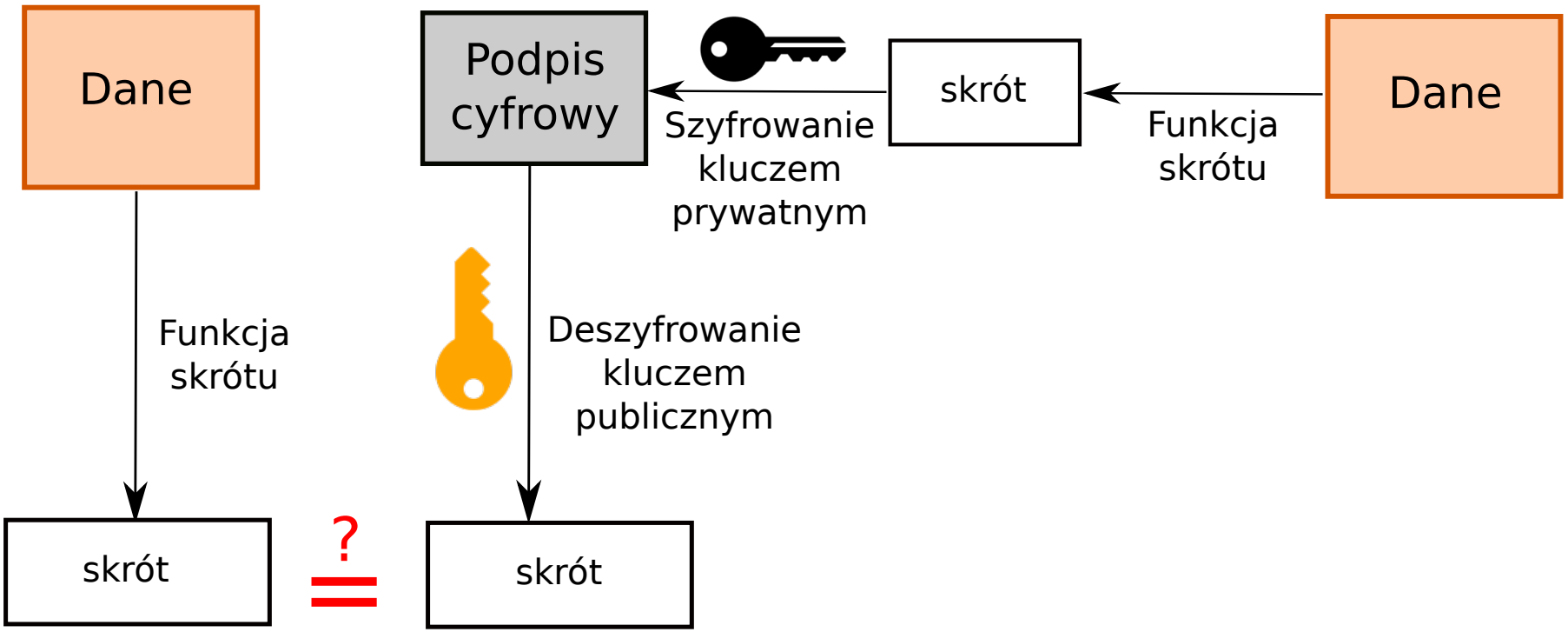
Podpis cyfrowy

Podpis cyfrowy

Schemat pozwalający na zweryfikowanie, czy wiadomość została stworzona przez wiarygodnego nadawcę. Gwarantuje, że jej treść nie była modyfikowana podczas transmisji danych.

Algorytmy wykorzystujące podpis cyfrowy są powrzechnie wykorzystywane do uwierzytelniania i zapewniania spójności danych podczas transakcji finansowych oraz dystrybucji oprogramowania.

Podpis cyfrowy



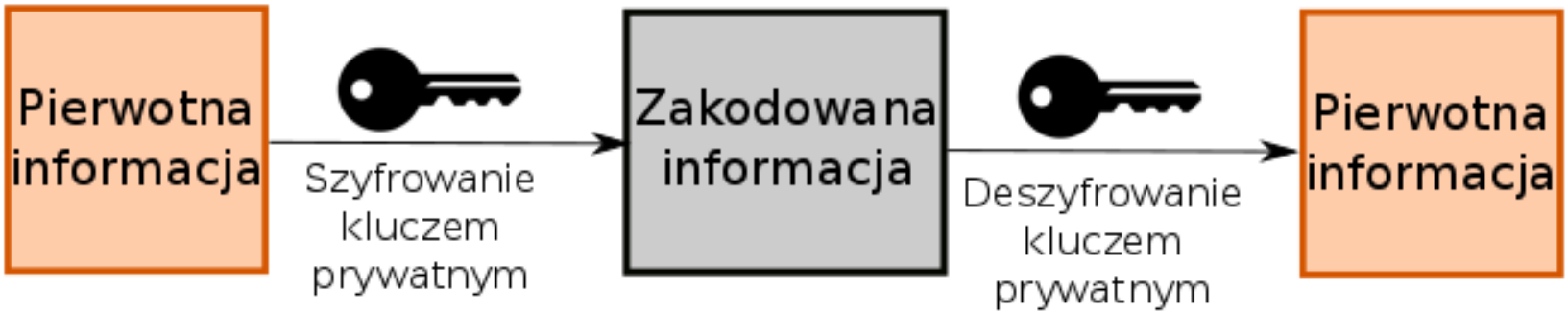
Szyfrowanie

Szyfrowanie

Jest to proces przetwarzania przesyłanej informacji w taki sposób, by była czytelna tylko dla uprawnionych stron komunikacji. Wiadomość zostaje przesłana w zakodowanej postaci, co znacznie utrudnia lub uniemożliwia zrozumienie jej treści w przypadku przechwycenia.

Szyfrowanie symetryczne

Zarówno odbiorca, jak i nadawca dysponują takim samym kluczem.

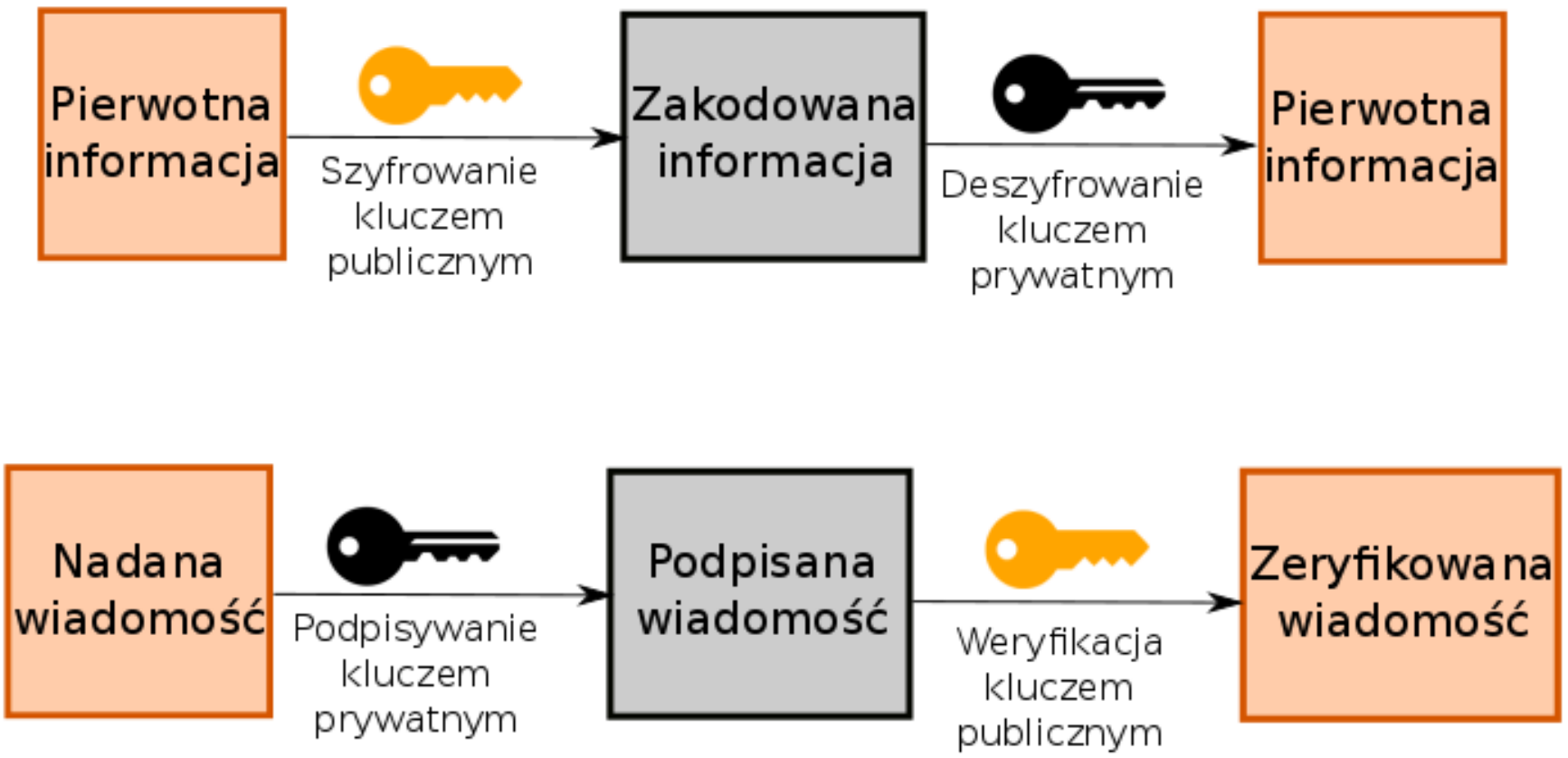


Obie strony muszą znać klucz przed rozpoczęciem komunikacji.
Zwiększa to prawdopodobieństwo jego przechwycenia.

Szyfrowanie asymetryczne

- Generowane są dwa klucze, prywatny i publiczny.
- Klucz publiczny jest ogólnie dostępny.
- Utworzenie dwóch takich par eliminuje konieczność wymiany kluczów prywatnych.

Szyfrowanie asymetryczne



Algorytmy szyfrujące asymetrycznie

- Digital Signature Algorithm (DSA).
- ElGamal.
- NTRUEncrypt.
- Algorytmy bazujące na kryptografii krzywych eliptycznych.
- RSA.

Algorytmy szyfrujące symetrycznie

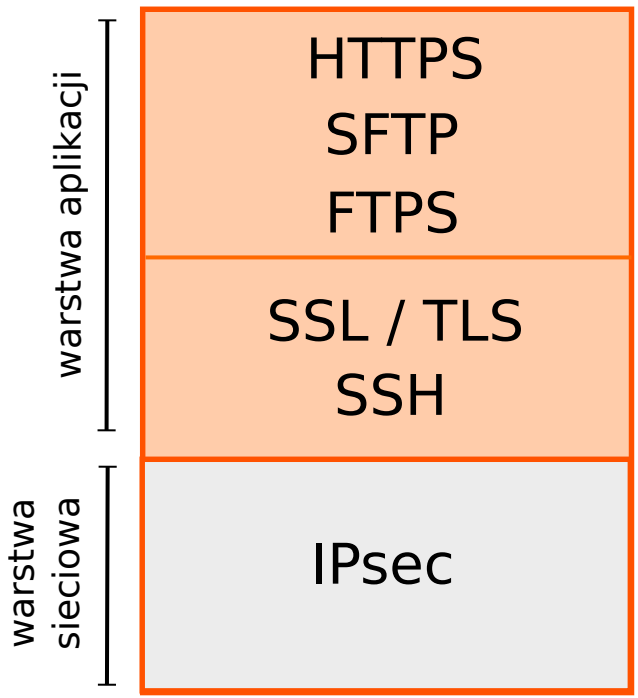
- Advanced Encryption Standard (AES).
- Data Encryption Standard (DES).
- Blowfish.
- IDEA.
- RC4.
- Tiny Encryption Algorithm.

Symetryczne — po co?

- Algorytmy symetryczne są dużo tańsze i prostsze obliczeniowo (mniejsze obciążenie CPU, tańsze koszty utrzymania serwerów, znacząco szybsze prędkości zapisu na szyfrowane nośniki itd.).
- AES ma nawet swoje natywne instrukcje w niektórych CPU.
- Pozostaje problem bezpiecznej wymiany klucza prywatnego.
- Rozwiązaniem jest wymiana klucza w *asymetrycznie* szyfrowanym kanale i dopiero późniejsze przejście na komunikację *symetryczną*.

Protokoły

W celu zagwarantowania bezpieczeństwa transmisji danych w sieci, w ustandaryzowanym pakiecie protokołów internetowych wykorzystane szereg metod kryptograficznych.



IPsec

Internet Protocol Security

Zestaw protokołów wykorzystujących szyfrowanie pakietów i uwierzytelnianie na poziomie warsty sieciowej.

Może zostać zaimplementowany w dwóch trybach:

1. **transportowym** — szyfrowane są tylko dane;
2. **tunelowym** — szyfrowany jest cały pakiet.

SSH

Secure Shell

Protokół wykorzystujący kryptografię asymetryczną do bezpiecznego zdalnego dostępu do komputera.

Połączenie jest realizowane w architekturze klient–serwer. Uwierzytelnienie może zostać przeprowadzone w dwóch wariantach:

1. z automatycznym generowaniem par kluczy oraz wykorzystaniem hasła (tzw. wariant BZP — bardzo złego pomysłu);
2. z ręcznym generowaniem kluczy.

SSH

Protokół SSH charakteryzuje się szerokim spektrum zastosowań:

- zdalne wykonywanie komend (które mogą być organiczone na serwerze, a nawet dowolnie przez niego interpretowane, por. chat over SSH, Gitolite itd.);
- tunelowanie/przekierowywanie portów TCP;
- przekazywanie sesji graficznej X11 (system okien);
- przesył plików.

TLS

Transport Layer Security

Protokół zapewniający bezpieczną wymianę informacji pomiędzy aplikacjami w obrębie Internetu. W celu uwierzytelnienia stron wykorzystuje certyfikację.

TLS

TLS również bazuje na architekturze klient-serwer. Można wyróżnić dwie warstwy komunikacji:

1. **„uścisk dłoni”** — komunikacja szyfrowana asymetrycznie — w tej fazie dochodzi do uwierzytelnienia stron oraz negocjacji formatowania i porządku wymiany wiadomości oraz klucza prywatnego używanego w 2 etapie;

2. **wymiana danych** — szyfrowanie symetryczne — wiadomości przechodzą proces kapsułkowania, tworząc zaszyfrowane rekordy, których spójność jest weryfikowana.

SSL vs TLS

Protokół SSL jest obecnie uznawany jako przestarzały poprzednik TLS. Względem SSL dodano następujące usprawnienia:

- bezpieczniejsze funkcje haszujące;
- wyrugowano błędy logiczne;
- standaryzacja w RFC 2246;
- rozluźniono restrykcje przy pozyskiwaniu certyfikatów z urzędów uwierzytelniających;
- dodatkowe wiadomości z ostrzeżeniami.

Warstwy protokołów

Protokół kryptograficzny	Protokół bez szyfrowania	Warstwa wynikowa
TLS	HTTP FTP	HTTPS FTPS
SSH	FTP RCP	SFTP SCP

Certyfikacja

Certyfikat klucza publicznego

Elektroniczny dokument używany w kryptografii asymetrycznej, będący dowodem własności danego klucza publicznego przez dany rzeczywisty podmiot.

- Wydawany przez urząd certyfikacji (CA — Certification Authority) po weryfikacji podmiotu.
- Użytkownicy korzystający z klucza publicznego opatrzonego certyfikatem mają dużą pewność, że podmiot po drugiej stronie jest rzeczywiście tym, za który się podaje.

Zawartość certyfikatu

Certyfikat zawiera m.in.:

- *podpis urzędu certyfikacji*,
- informacje o podmiocie (np. domena, dla której certyfikat obowiązuje),
- przedział czasu ważności,
- numer seryjny, użyte algorytmy kryptograficzne, zakres użycia certyfikatu,
- certyfikowany klucz publiczny.

Klasyfikacja

Klasa certyfikatu

Verisign wprowadza pojęcie klasy dla różnych typów (zastosowań) certyfikatów.

Klasy:

1. Indywidualne — przeznaczone do obsługi e-maili.
2. Dla organizacji — gdzie potrzebny jest dowód tożsamości.
3. Serwerowe i do podpisywania oprogramowania — przeprowadzana niezależna weryfikacja tożsamości i upoważnień.
4. Dla transakcji B2B.
5. Dla prywatnych organizacji i bezpieczeństwa rządowego.