Technologie informacyjne i komunikacyjne

Wykład 7, dn. 20.04.2026

Źródło obrazka: pngtree

Bezpieczeństwo w sieci

Internet został zaprojektowany jako sieć odporną na awarie. Jego struktura ma zapewniać ciągłość działania nawet w przypadku uszkodzenia części węzłów czy połączeń. Nie oznacza to jednak, że jest odporny na **oszustwa**.

Pomimo swoich wojskowych korzeni, architektura Internetu nie zawiera wbudowanych mechanizmów chroniących przed oszustwami, inwigilacją czy kradzieżą danych. Oznacza to, że dane przesyłane w sieci mogą być potencjalnie przechwycone lub zmodyfikowane przez osoby trzecie.

Jedynym skutecznym sposobem zapewnienia poufności informacji jest **szyfrowanie**. Dzięki niemu dane stają się nieczytelne dla nieuprawnionych odbiorców.

Dodatkowo kryptografia klucza publicznego umożliwia wprowadzenie podpisu cyfrowego, który pozwala potwierdzić autentyczność nadawcy oraz integralność przesyłanych danych.

Kryptografia klasyczna

Jest to dziedzina szyfrowania informacji stosowana przed erą komputerów, oparta głównie na prostych operacjach na znakach tekstu.

Najważniejsze cechy:

używała metod manualnych lub mechanicznych

opierała się na przekształceniach litery i symboli

klucz był zazwyczaj prosty i symetryczny

bezpieczeństwo zależało od tajności algorytmu lub klucza

Przykłady szyfrów:

Szyfr Cezara – przesunięcie liter o stałą liczbę pozycji

Szyfr Vigenère'a – wieloalfabetyczne podstawienie z użyciem hasła

Szyfry podstawieniowe – zamiana liter na inne znaki

Szyfry przestawieniowe – zmiana kolejności liter w tekście

Ograniczenia:

łatwe do złamania metodami analizy częstotliwości

brak odporności na nowoczesne metody kryptoanalizy

mała liczba możliwych kluczy

Kryptografia klasyczna

Skytale (ok. 400 p.n.e.)

- jedno z najstarszych znanych urządzeń szyfrujących
- stosowane w starożytnej Sparcie

Zasada działania:

- tekst zapisywano na pasku pergaminu owiniętym wokół cylindra
- po rozwinięciu litery tworzyły nieczytelny ciąg
- odczyt możliwy był tylko przy użyciu cylindra o tej samej średnicy

Znaczenie:

- przykład szyfru przestawieniowego
- wczesna forma szyfrowania wojskowego

Źródło zdjęcia: Wikipedia

Skytale (współczesna replika)

Kryptografia klasyczna

Enigma (1918 / 1923)

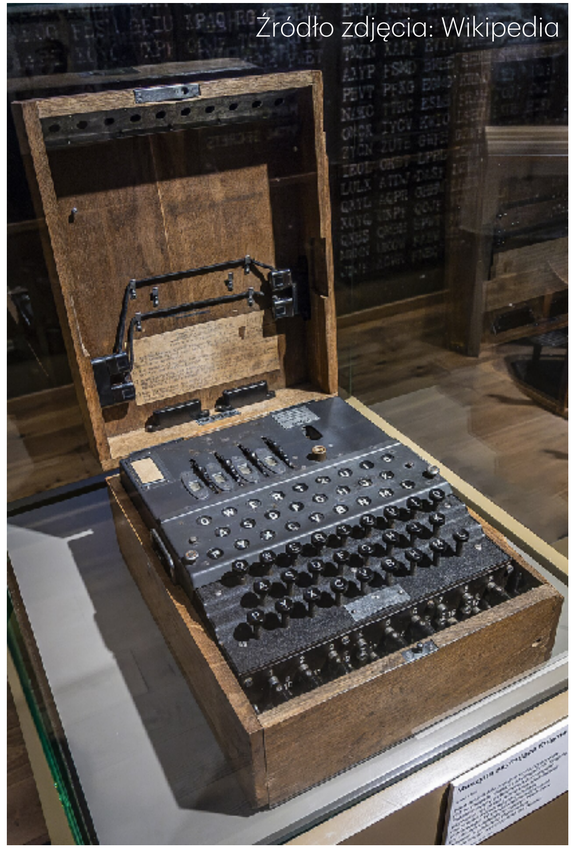
- niemiecka maszyna szyfrująca używana głównie w II wojnie światowej
- rozwinięta komercyjnie od 1918, używana wojskowo od lat 20. XX w.

Zasada działania:

- wykorzystuje wirniki do wieloetapowego szyfrowania liter
- każda litera była szyfrowana inaczej (szyfr polialfabetyczny)
- ustawienia maszyny stanowiły klucz szyfru

Znaczenie:

- uznawana za bardzo silny szyfr jak na swoje czasy
- złamanie Enigmy przez aliantów miało kluczowe znaczenie w II wojnie światowej
- przyczyniła się do rozwoju nowoczesnej kryptografii i informatyki



Enigma, model M10148 w Muzeum II Wojny Światowej w Gdańsku

Polscy kryptolodzy - złamanie Enigmy

Marian Rejewski – matematyk, główny twórca metody złamania Enigmy

Jerzy Różycki – specjalista od analizy kryptologicznej i logiki szyfrów

Henryk Zygalski – opracował metodę „arkuszy Zygalskiego”

- w latach 1932–1939 złamali szyfr niemieckiej maszyny Enigma
- stworzyli pierwsze skuteczne metody jej deszyfracji
- przekazali wiedzę aliantom przed II wojną światową

Źródło zdjęcia: portal British Poles

<u>Znaczenie historyczne:</u>

- ich praca umożliwiła aliantom odczytywanie niemieckich depesz
- miała ogromny wpływ na przebieg II wojny światowej
- uznawani za pionierów nowoczesnej kryptologii matematycznej

Szyfr Vernama

Jest to metoda szyfrowania oparta na operacji XOR, uznawana za jedyny teoretycznie doskonale bezpieczny szyfr (przy spełnieniu określonych warunków).

Zasada działania:

- tekst jawny łączony jest z kluczem za pomocą operacji XOR
- klucz musi być:
  - całkowicie losowy
  - tak długi jak wiadomość
  - użyty tylko jeden raz (one-time pad)

Właściwości:

- jeśli klucz jest prawdziwie losowy → szyfr jest nie do złamania
- brak wzorca w szyfrogramie
- bezpieczeństwo nie zależy od mocy obliczeniowej

Ograniczenia:

- trudność w bezpiecznym przekazaniu klucza
- konieczność generowania bardzo długich kluczy
- klucz może być użyty tylko raz

Szyfr z Kluczem Jednorazowym

szyfrowanie

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E	4	K
N	13	E
I	8	Y
G	6	W
M	12	O
A	0	R

tekst jawny: ENIGMA

słowo klucz: KEYWORD

Źródło: https://www.youtube.com/watch?v=xPhruL4yCgM

Szyfr z Kluczem Jednorazowym

szyfrowanie

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E	4	K	10
N	13	E	4
I	8	Y	24
G	6	W	22
M	12	O	14
A	0	R	17

tekst jawny: ENIGMA

słowo klucz: KEYWORD

Źródło: https://www.youtube.com/watch?v=xPhruL4yCgM

Szyfr z Kluczem Jednorazowym

szyfrowanie

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E 4 + K 10 = 14

N 13 + E 4 = 17

I 8 + Y 24 = 6

G 6 + W 22 = 2

M 12 + O 14 = 0

A 0 + R 17 = 17

tekst jawny: ENIGMA

słowo klucz: KEYWORD

Źródło: https://www.youtube.com/watch?v=xPhruL4yCgM

Szyfr z Kluczem Jednorazowym

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E 4 + K 10 = 14
N 13 + E 4 = 17
I 8 + Y 24 = 6
G 6 + W 22 = 2
M 12 + O 14 = 0
A 0 + R 17 = 17

tekst jawny: ENIGMA

słowo klucz: KEYWORD

szyfrogram: ORGCAR

Źródło: https://www.youtube.com/watch?v=xPhruL4yCgM

Kryptografia klucza publicznego

Jest to niezwykła właściwość informacji, wynikająca z głębokiej struktury matematycznej świata, która umożliwia tworzenie bezpiecznych kanałów komunikacji we współczesnym świecie. Jej „magia” polega na wykorzystaniu trudnych problemów matematycznych, dzięki którym możliwe jest rozdzielenie klucza na dwie części: publiczną, dostępną dla wszystkich, oraz prywatną, znaną wyłącznie właścicielowi.

Takie podejście pozwala na bezpieczne przesyłanie informacji bez konieczności wcześniejszego uzgadniania tajnego klucza. W efekcie kryptografia klucza publicznego zapewnia poufność komunikacji, umożliwia uwierzytelnianie użytkowników oraz tworzenie podpisów cyfrowych.

Stanowi ona fundament współczesnego Internetu i jest szeroko wykorzystywana w protokołach takich jak **HTTPS**, umożliwiając bezpieczne korzystanie z usług online, takich jak bankowość, zakupy czy komunikacja.

Algorytm RSA

Jest to jeden z najważniejszych algorytmów kryptografii klucza publicznego, opracowany w 1977 roku przez **Rona Rivesta**, **Adiego Shamira** oraz **Leonarda Adlemana**. Jego działanie opiera się na matematycznej trudności faktoryzacji dużych liczb, czyli rozkładu ich na czynniki pierwsze.

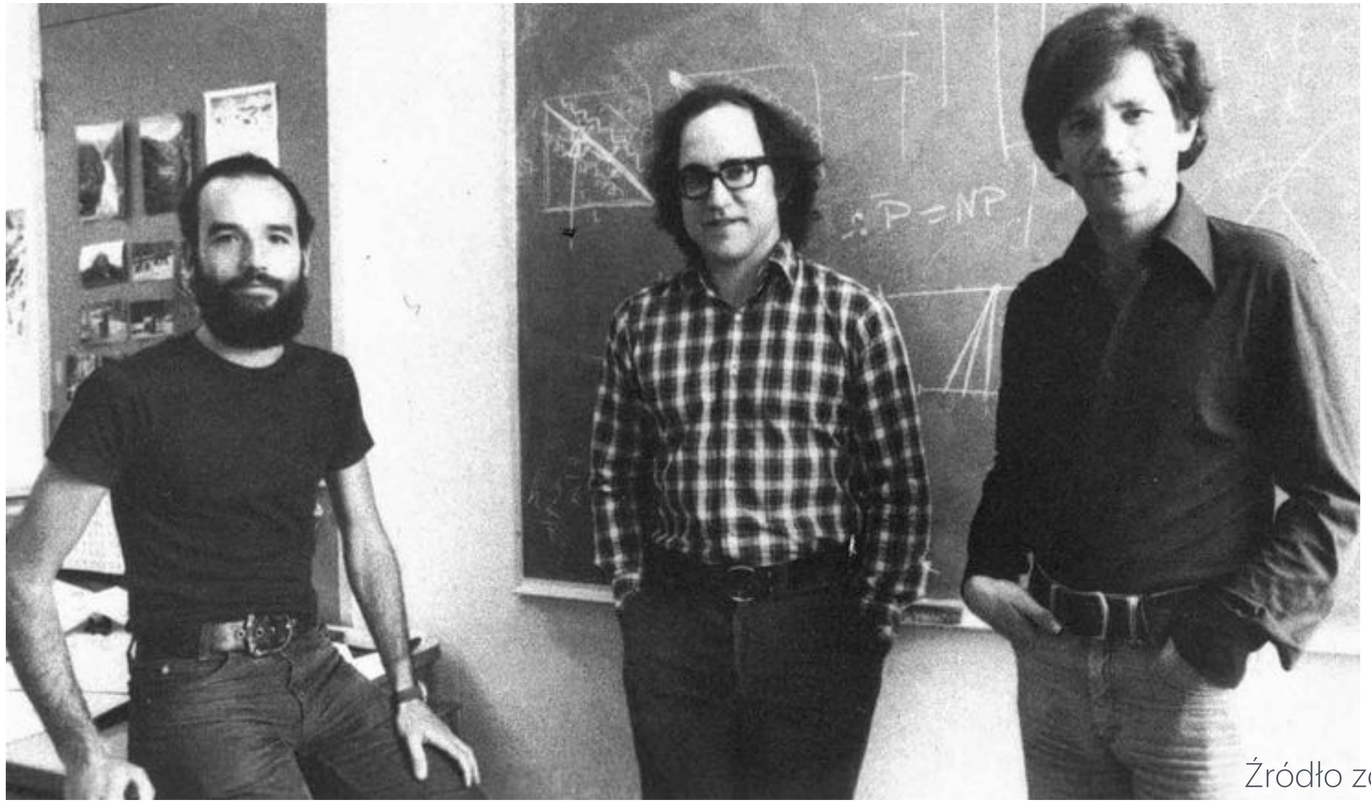
Zasada działania:

- opiera się na trudności faktoryzacji dużych liczb pierwszych
- generowane są dwa klucze:
- publiczny – do szyfrowania
- prywatny – do odszyfrowania

Proces:

- wybór dwóch dużych liczb pierwszych
- obliczenie ich iloczynu (modułu n)
- wyznaczenie kluczy publicznego i prywatnego
- szyfrowanie i deszyfrowanie z użyciem działań modulo

Algorytm RSA

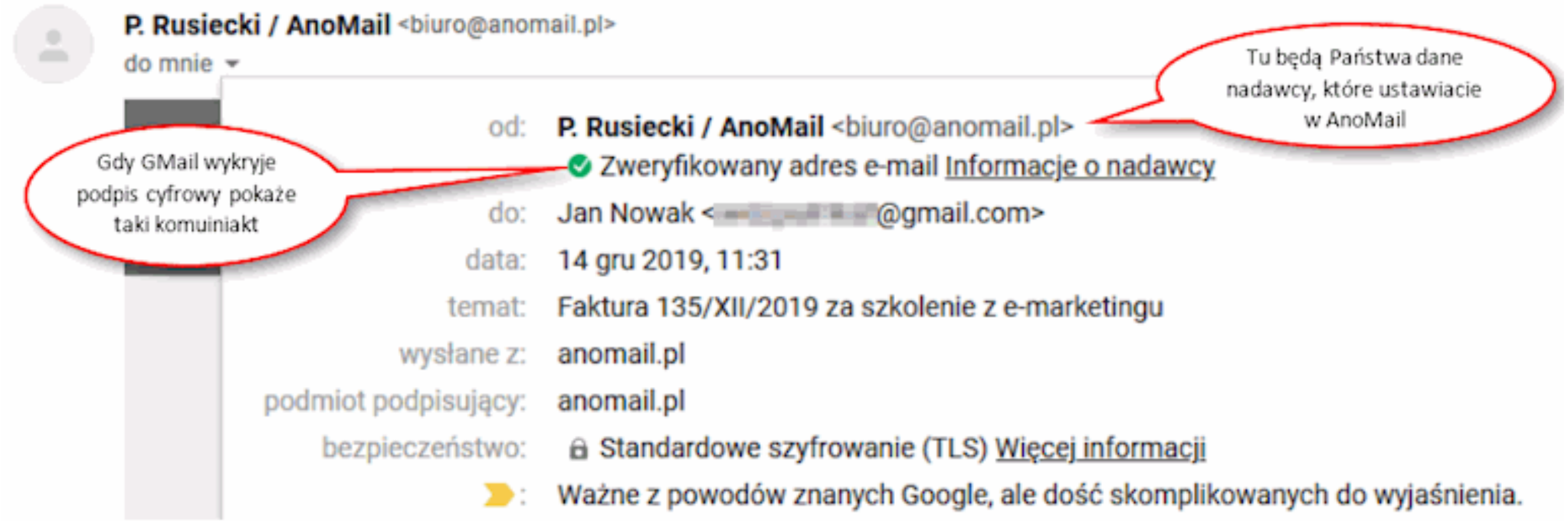


Źródło zdjęcia: Pinterest

Nagroda Turinga: W 2002 roku cała trójka otrzymała prestiżową nagrodę ACM Turing Award za swój wkład w rozwój kryptografii

Podpis cyfrowy w poczcie elektronicznej

Jest to metoda zapewniająca autentyczność nadawcy oraz integralność wiadomości. Oznacza to, że odbiorca ma pewność, kto wysłał e-mail, oraz że jego treść nie została zmieniona w trakcie przesyłania.



Źródło zdjęcia: https://anomail.pl/elektroniczne-podpisy-wiadomosci-email/

Hasła

Hasła w systemach komputerowych nie są przechowywane w postaci jawnej, lecz jako wynik działania funkcji haszującej (funkcji skrótu). Oznacza to, że nawet administrator systemu nie zna rzeczywistego hasła użytkownika – może je jedynie zmienić, ale nie odczytać.

Funkcje skrótu są jednokierunkowe, co oznacza brak możliwości odtworzenia hasła na podstawie jego skrótu. Podczas logowania wpisane hasło jest ponownie przetwarzane tą samą funkcją i porównywane z wartością zapisaną w systemie.

W praktyce jedyną skuteczną metodą łamania haseł jest ich odgadywanie, np. poprzez ataki słownikowe lub brute-force.

Jak wybierać hasło?

Siła hasła zależy przede wszystkim od liczby możliwych kombinacji, które musi sprawdzić atakujący. Dla przykładu:

- hasło złożone z 8 cyfr to około 100 000 000 kombinacji
- 8 liter to już około 200 000 000 000 możliwości
- 8 znaków (małe i duże litery oraz znaki specjalne) to około 7 000 000 000 000 000 kombinacji
- 16 znaków z pełnego zestawu to aż około 400 000 000 000 000 000 000 000 000 000 000 możliwości

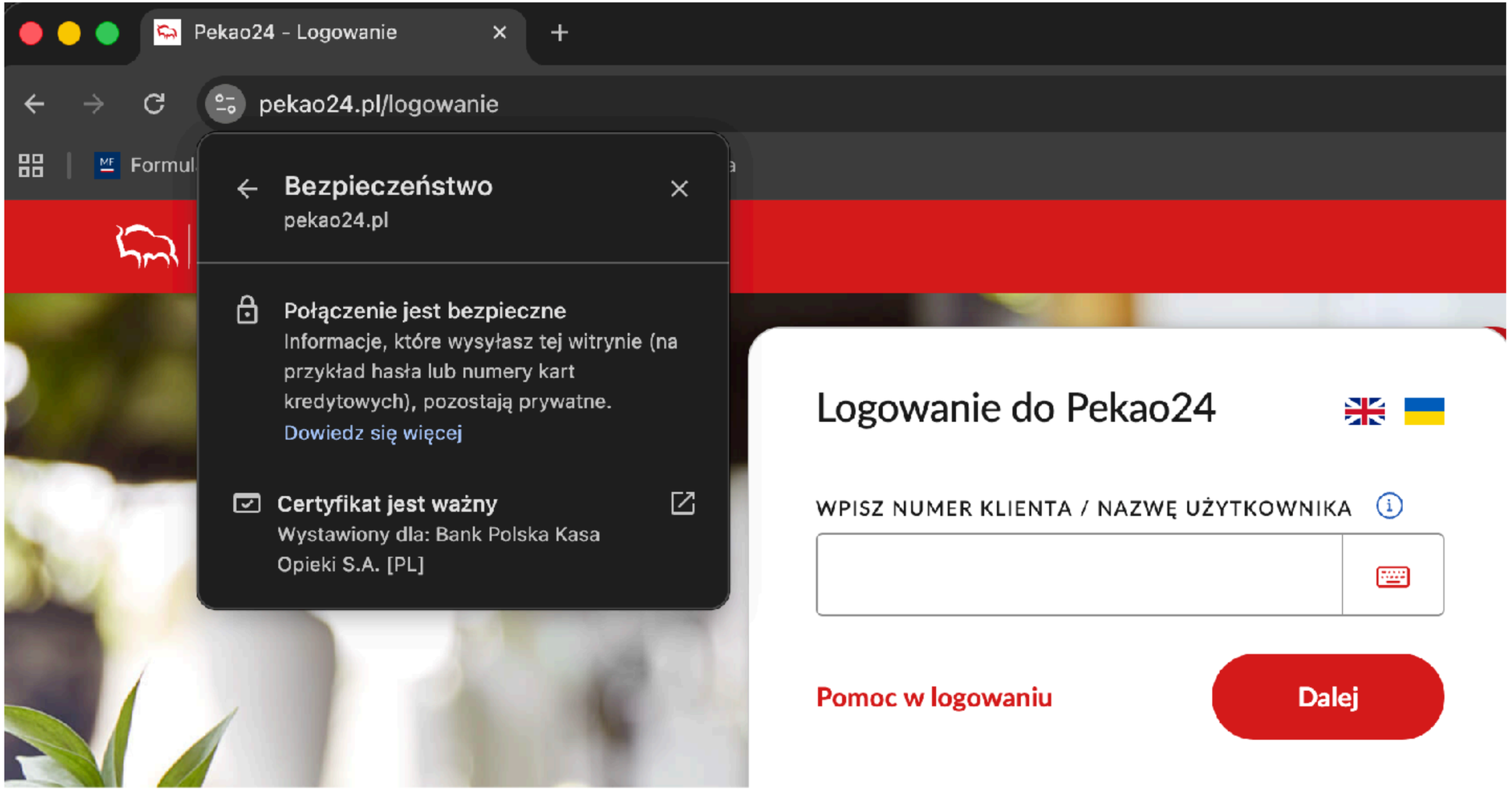
Dla porównania, wiek wszechświata to mniej niż 1 000 000 000 000 000 000 sekund, co pokazuje, jak ogromne znaczenie ma długość i złożoność hasła.

W praktyce oznacza to, że:

- warto używać **długich haseł** (minimum kilkanaście znaków)
- należy łączyć **małe i wielkie litery, cyfry oraz znaki specjalne**
- unikać prostych i popularnych słów

Szczególnie niebezpieczne są tzw. **ataki słownikowe**, w których sprawdzane są najczęściej używane hasła i ich warianty. Dlatego dobre hasło powinno być trudne do odgadnięcia i nieoparte na oczywistych słowach lub schematach.

Szyfrowanie stron



Aktualizacje systemu operacyjnego

Jest to jeden z **najważniejszych elementów bezpieczeństwa komputera**. Obejmują one poprawki błędów, ulepszenia funkcji oraz, co najważniejsze, **łatki bezpieczeństwa**.

Są bardzo ważne, ponieważ cyberprzestępcy stale odkrywają nowe luki w systemach. Brak aktualizacji oznacza pozostawienie tych luk otwartych, co może prowadzić do kradzieży danych, infekcji złośliwym oprogramowaniem lub przejęcia kontroli nad urządzeniem.

Szczególnie niebezpieczne są tzw. **zero-day exploits**, czyli ataki wykorzystujące nieznane jeszcze lub niezałatane podatności. Aktualizacje często zawierają poprawki właśnie dla takich krytycznych błędów.

Nie zaleca się używania systemów, które nie są już wspierane, takich jak Windows 7, ponieważ nie otrzymują one już aktualizacji bezpieczeństwa. Oznacza to, że wszelkie nowe luki pozostają nieusunięte, co znacząco zwiększa ryzyko ataku.

Regularne aktualizowanie systemu to podstawowy krok w ochronie danych i zapewnieniu bezpieczeństwa w sieci.

Twój komputer to broń, której może używać ktoś inny

Komputer podłączony do Internetu może zostać przejęty przez cyberprzestępców i wykorzystany bez wiedzy właściciela do działań nielegalnych. Zainfekowane urządzenia tworzą tzw. **botnety**, czyli „armie komputerów zombie".

Botnety są wykorzystywane m.in. do:

- rozsyłania spamu
- kradzieży danych
- przeprowadzania ataków DDoS (blokowania stron internetowych przez przeciążenie ich ruchem)

Aby zmniejszyć ryzyko przejęcia komputera, należy stosować podstawowe zasady bezpieczeństwa:

- regularnie instalować aktualizacje systemu i oprogramowania
- używać programu antywirusowego i dbać o jego aktualność
- stosować silne, unikalne hasła

Dbanie o bezpieczeństwo własnego urządzenia oznacza również ochronę innych użytkowników Internetu przed skutkami ataków.

Eugene Kaspersky

Rosyjski informatyk i przedsiębiorca, specjalizujący się w dziedzinie cyberbezpieczeństwa. Jest współzałożycielem firmy **Kaspersky Lab**, która zajmuje się tworzeniem oprogramowania antywirusowego oraz systemów ochrony przed zagrożeniami w Internecie.

- absolwent kryptografii i informatyki
- współtwórca jednego z najbardziej znanych programów antywirusowych na świecie

Działalność:

- rozwój technologii wykrywania i analizy malware
- badania nad zaawansowanymi zagrożeniami cybernetycznymi (APT)
- promowanie edukacji w zakresie bezpieczeństwa IT

Znaczenie:

Eugene Kaspersky odegrał ważną rolę w rozwoju nowoczesnego cyberbezpieczeństwa, a jego firma stała się jednym z globalnych liderów w ochronie przed wirusami i atakami sieciowymi.

Źródło zdjęcia: Wikipedia

Kaspersky Security Network (KSN)

Jeżeli użytkownik wyrazi zgodę na udział w usłudze Kaspersky Security Network, program automatycznie przesyła do serwerów Kaspersky Lab określone informacje w celu poprawy ochrony przed zagrożeniami.

Jakie dane są wysyłane:

- sumy kontrolne (hashes) analizowanych plików
- informacje o adresach URL w celu oceny ich wiarygodności (bez danych osobowych, np. danych rejestracyjnych)
- statystyki pomagające w ochronie przed spamem (np. adresy IP wiadomości, sumy kontrolne załączników i obrazów)
- informacje o sprzęcie i oprogramowaniu komputera
- czas analizy obiektów przez komponenty programu

Bezpieczeństwo danych:

Otrzymane informacje są chronione przez Kaspersky Lab zgodnie z obowiązującymi przepisami prawa oraz standardami ochrony danych.

Cel: Zbierane dane służą wyłącznie do

- wykrywania nowych zagrożeń
- poprawy skuteczności ochrony antywirusowej
- zwiększania bezpieczeństwa użytkowników na całym świecie

Stuxnet

Jest to robak komputerowy dla systemu Windows, wykryty w 2010 roku. Był pierwszym znanym malware, który służył do szpiegowania i modyfikowania systemów przemysłowych.

Działanie:

- wykorzystywał wiele luk typu zero-day
- infekował systemy Windows i szukał sterowników PLC
- atakował głównie systemy Siemens SIMATIC S7-300 i S7-400
- zmieniał działanie urządzeń przemysłowych przez oprogramowanie WinCC / Step 7

Efekt:

- ingerował w kontrolę procesów przemysłowych (np. wirówki gazowe)
- działał tylko w określonych, docelowych systemach

Znaczenie:

Stuxnet pokazał, że cyberataki mogą wpływać na realne obiekty fizyczne, nie tylko dane komputerowe.

Aviel D. Rubin

Amerykański ekspert ds. cyberbezpieczeństwa, który zajmuje się analizą bezpieczeństwa systemów komputerowych i urządzeń sieciowych.

Główna idea:

Stwierdzenie „All your devices can be hacked” oznacza, że każde urządzenie podłączone do sieci może zostać potencjalnie zhakowane, niezależnie od producenta czy poziomu zabezpieczeń.

Co to oznacza w praktyce:

- komputery, telefony i tablety mogą być podatne na ataki
- także urządzenia „inteligentne” (IoT), np. kamery, telewizory, samochody
- bezpieczeństwo zależy od oprogramowania i aktualizacji, nie tylko sprzętu

Wniosek:

Nie istnieją urządzenia w 100% odporne na ataki. Każdy system może zawierać błędy, które mogą zostać wykorzystane przez cyberprzestępców.

Czy ktoś nas śledzi?

Współczesny Internet i technologie mobilne sprawiają, że wiele podmiotów może gromadzić informacje o użytkownikach – zarówno w celach usługowych, jak i analitycznych czy nadzorczych.

Korporacje:

Duże firmy technologiczne zbierają dane o aktywności użytkowników, m.in.:

- Facebook – analiza aktywności, treści i kontaktów
- Google – wyszukiwania, lokalizacja, historia przeglądania
- LinkedIn – dane zawodowe i sieć kontaktów

Rządy i służby:

- np. program PRISM (USA)
- systemy masowej analizy danych i komunikacji
- monitoring ruchu sieciowego w celach bezpieczeństwa państwa

Czy ktoś nas śledzi?

Inne źródła śledzenia:

- operatorzy sieci komórkowych – zawsze znają przybliżoną lokalizację użytkownika
- aplikacje mobilne z dostępem do GPS i danych urządzenia
- geotagging zdjęć i postów (automatyczne dodawanie lokalizacji)

Ciekawostki:

- system SORM w Rosji umożliwia monitorowanie ruchu internetowego
- wiele darmowych aplikacji „płaci” za usługę danymi użytkownika
- nawet proste zdjęcie może ujawnić miejsce i czas jego wykonania

Wnioski:

W dzisiejszym świecie prywatność online zależy w dużej mierze od świadomych decyzji użytkownika dotyczących udostępniania danych i korzystania z usług.

Smartfon szuka Wi-Fi

Podczas wyszukiwania sieci Wi-Fi smartfon często wysyła tzw. „listę znanych sieci”, czyli nazwy punktów dostępowych, z którymi wcześniej się łączył.

Może to prowadzić do dwóch istotnych zagrożeń:

1. **Ułatwienie ataku typu „man-in-the-middle”** – urządzenie może połączyć się z fałszywą siecią podszywającą się pod znaną, co umożliwia przechwytywanie danych.
2. **Ujawnienie informacji o użytkowniku** – lista sieci może zdradzać miejsca, w których przebywaliśmy, np. firmy, lotniska, hotele, a nawet domowe sieci Wi-Fi. Takie dane mogą być następnie wykorzystane do lokalizacji użytkownika za pomocą dostępnych baz i serwisów internetowych.

Geotagowanie (Geotagging)

Proces automatycznego dołączania informacji o lokalizacji geograficznej do zdjęć wykonywanych smartfonem lub aparatem z modułem GPS. W praktyce oznacza to, że każde zdjęcie może zawierać dane o współrzędnych miejsca, w którym zostało zrobione.

Dlaczego to ważne:

- zdjęcia często mają domyślnie włączoną funkcję zapisywania lokalizacji
- użytkownik może nieświadomie ujawniać swoje miejsce pobytu
- dane mogą wskazywać dokładny adres domu, pracy lub innych odwiedzanych miejsc

Ryzyko:

- możliwość śledzenia codziennych tras i nawyków
- ujawnienie lokalizacji w mediach społecznościowych
- potencjalne wykorzystanie przez osoby trzecie

Geotagowanie zwiększa wygodę organizacji zdjęć, ale jednocześnie może stanowić zagrożenie dla prywatności, jeśli nie kontrolujemy udostępnianych danych.

Wnioski

Świat cyfrowy niesie ze sobą zarówno ogromne możliwości, jak i realne zagrożenia. Internet, kryptografia i nowoczesne technologie stały się podstawą współczesnej komunikacji, bankowości i życia codziennego.

Bezpieczeństwo w sieci zależy nie tylko od technologii, ale również od świadomości użytkownika.

Dlatego kluczowe znaczenie mają proste zasady:

- dbanie o silne hasła i aktualizacje
- korzystanie z szyfrowania i bezpiecznych połączeń
- świadome udostępnianie danych i treści

Technologia sama w sobie nie jest ani dobra, ani zła – to sposób jej użycia decyduje o skutkach. Świadomy użytkownik potrafi korzystać z jej możliwości, jednocześnie minimalizując ryzyko.

Bibliografia

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.

Comer, D. E. (2018). *Internetworking with TCP/IP* (6th ed.). Pearson.

ENISA. (2023). *Threat Landscape Report*.

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.

Kaspersky. (2023). *Cyberthreat Report*.

NIST. (2022). *Digital Identity Guidelines* (SP 800-63).

Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

Stallings, W. (2017). *Cryptography and Network Security* (7th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage.

Verizon. (2023). *Data Breach Investigations Report*.

ISO/IEC 27001. (2022). *Information Security Management Systems*.

General Data Protection Regulation. (2016).