



PK 1



Metody uwierzytelniania użytkowników
w systemach komputerowych

Garść konkretów



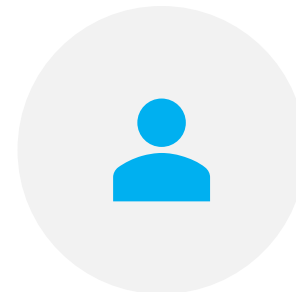
Temat prezentacji

Metody uwierzytelniania
użytkowników w systemach
komputerowych
(sposoby, wady, zalety)



Pytanie

Kierunkowe nr 1

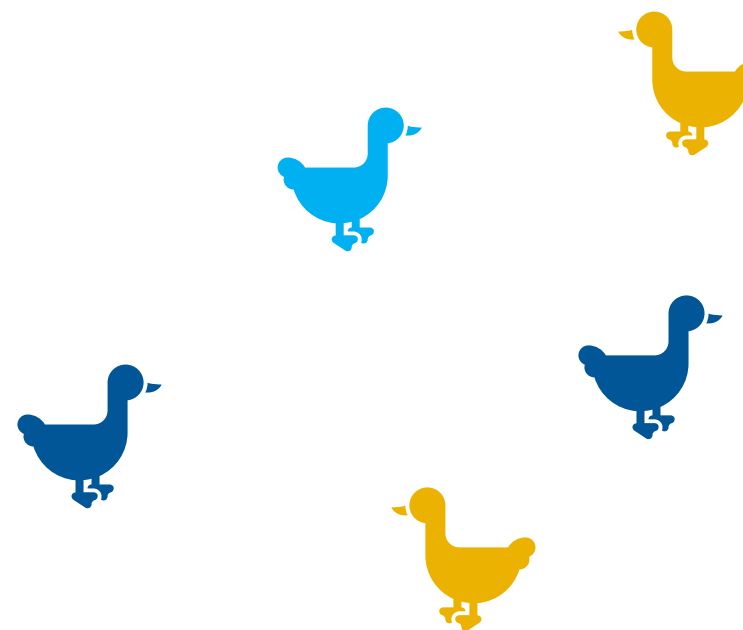


Autor prezentacji

inż. Jakub Batogowski

Co nas czeka?

- **Wstęp**
 - *Pojęcia*
 - *Uzyskiwanie dostępu do chronionych zasobów*
 - *Podział metod uwierzytelniania*
- *Hasła tradycyjne*
- *Listy haseł*
- *Hasła S/Key*
- *Systemy challenge-response*
- *Hasła zmienne w czasie*
- **Techniki kryptograficzne**
 - *Podpis cyfrowy*
 - *Certyfikaty*
- *Zabezpieczenia biometryczne*
- *Podsumowanie*

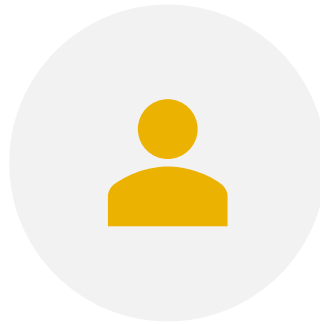


Metody **u**wierzytelniania **u**żytkowników w **s**ystemach **k**omputerowych



System komputerowy

- sprzęt komputerowy
- oprogramowanie



Użytkownik systemu

- ludzie
- maszyny
- inne komputery



Uwierzytelnianie

- proces
- potwierdzenie tożsamości

Uzyskiwanie dostępu do chronionego zasobu



Identyfikacja

Deklaracja tożsamości
przez podmiot



Uwierzytelnienie

Weryfikacja tożsamości
podmiotu przez stronę
ufającą



Autoryzacja

Sprawdzenie uprawnień
podmiotu przez stronę
ufającą

Podział metod uwierzytelniania



Coś, co wiesz

- Hasło tradycyjne
- PIN



Coś, co masz

- Token
- Karta
- Hasło jednorazowe
- Certyfikat



Coś, czym jesteś

- Linie papilarne
- Obraz tęczy
- Naczynia krwionośne
- Punkty charakterystyczne twarzy

Hasła tradycyjne



Aspekt techniczny

- Przechowywane po stronie serwera
- Często szyfrowane funkcją skrótu
- Możliwość „zasolenia”



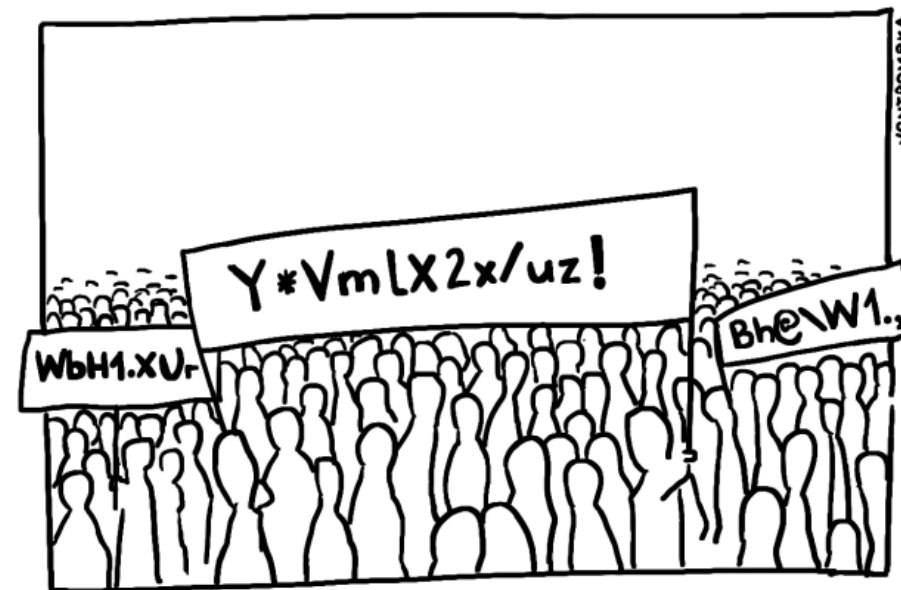
Zalety

- Proste w użyciu



Wady

- Łatwe do zgadnięcia
- Łatwe po podejrzeniu
- Można przechwycić / podsłuchać / ukraść
- Kosztowne w zarządzaniu
- Łatwe do zapomnienia
- Wiele kont – jedno hasło ?!



DEMONSTRANCI PRZYNIEŚLI MOCNE HASŁA

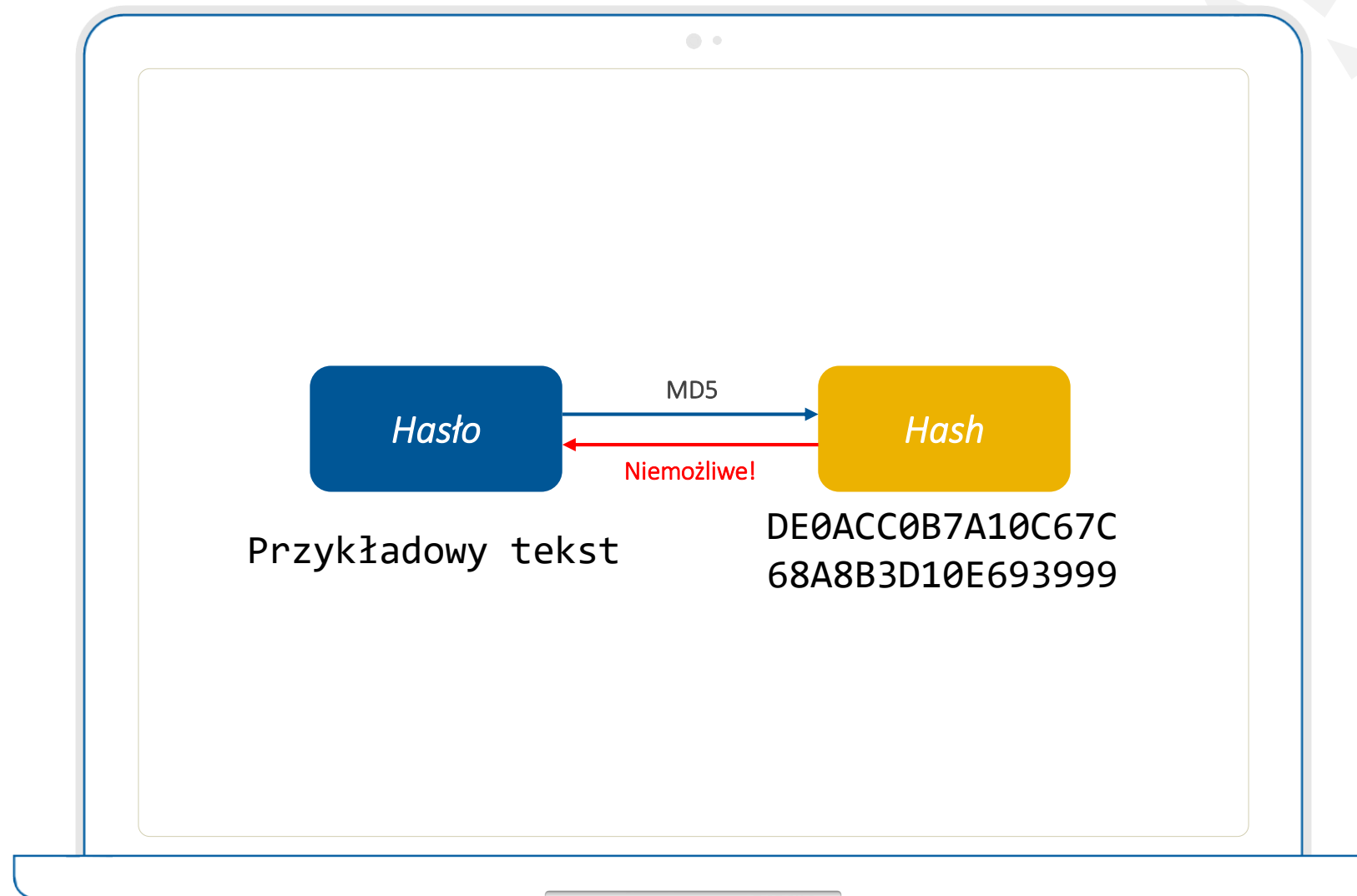
Funkcja skrótu

Funkcja mieszająca

Funkcja haszująca

Cechy funkcji skrótu

- Nieodwracalność operacji
- Stała długość hash'a
- Niejednoznaczność
- Szybka



Hasła tradycyjne



Aspekt techniczny

- Przechowywane po stronie serwera
- Często szyfrowane funkcją skrótu
- Możliwość „zasolenia”



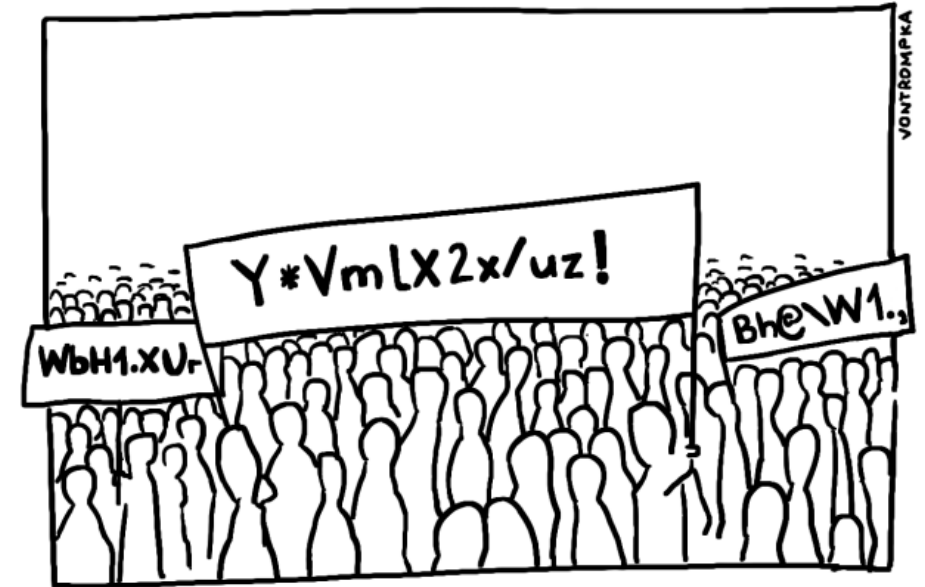
Zalety

- Proste w użyciu



Wady

- Łatwe do zgadnięcia
- Łatwe po podejrzeniu
- Można przechwycić / podsłuchać / ukraść
- Kosztowne w zarządzaniu
- Łatwe do zapomnienia
- Wiele kont – jedno hasło ?!



DEMONSTRANCI PRZYNIEŚLI MOCNE HASŁA

Listy haseł



Aspekt techniczny

- Przy każdorazowym logowaniu należy podać wybrane przez serwer, nieużywane dotąd hasło



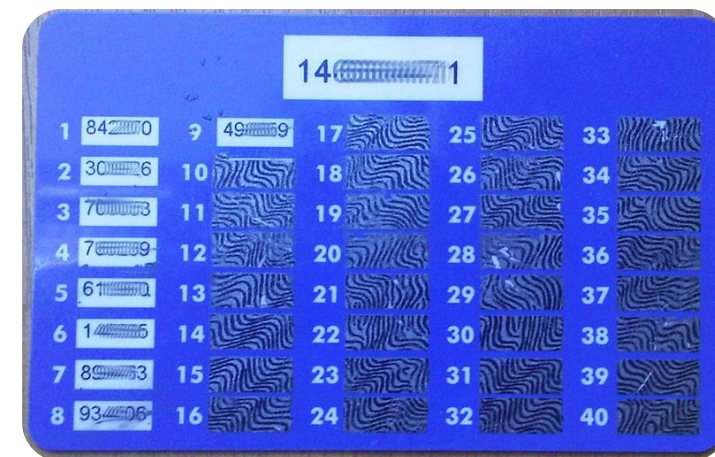
Zalety

- Najtańsza implementacja haseł jednorazowych
- Wiemy, czy ktoś skorzystał z kodu



Wady

- Wysyłane pocztą
- Lepszą alternatywą są jednorazowe hasła SMS
- Kartę trzeba mieć przy sobie



Hasła jednorazowe S/Key



Aspekt techniczny

- Hasła są kodowane funkcją skrótu
- Hasło n to *hash* hasła $n-1$
- Tajne hasło to hasło zerowe
- Podczas logowania podajemy hasła od końca



Zalety

- Zwiększony poziom bezpieczeństwa
- Przechwycenie ostatnio użytego hasła nie prowadzi do tragedii



Wady

- Trzeba w jakiś sposób pamiętać hasło zerowe aby móc obliczyć obecne hasło

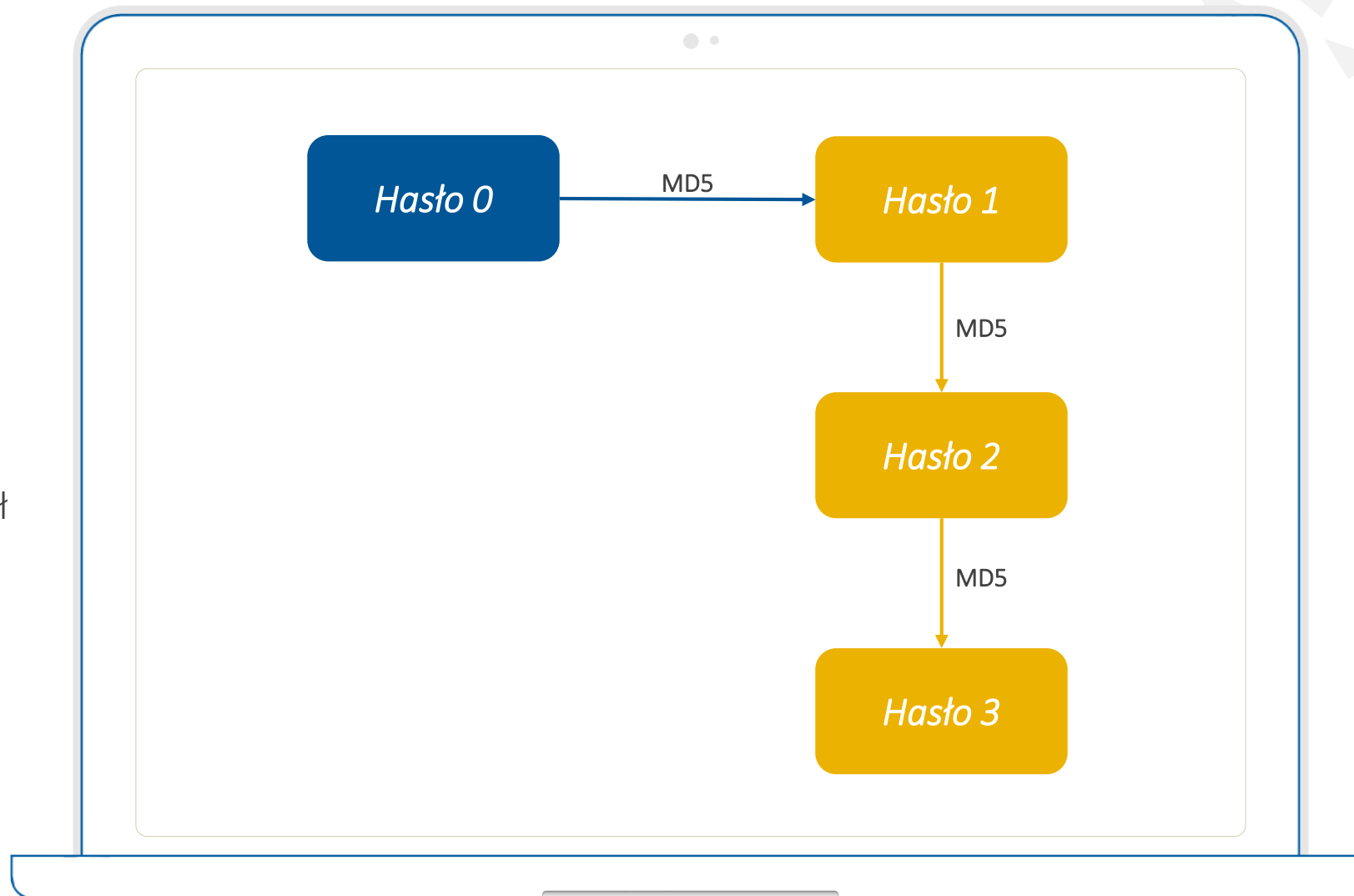


single use

Hasła jednorazowe S/Key

Generowanie haseł jednorazowych

- Podając hasło 0 generujemy np. 100 jednorazowych haseł
- Przy pierwszej próbie logowania system prosi o hasło 100
- Przy następnej próbie logowania o hasło 99, itd..



Hasła jednorazowe S/Key



Aspekt techniczny

- Hasła są kodowane funkcją skrótu
- Hasło n to *hash* hasła $n-1$
- Tajne hasło to hasło zerowe
- Podczas logowania podajemy hasła od końca



Zalety

- Zwiększony poziom bezpieczeństwa
- Przechwycenie ostatnio użytego hasła nie prowadzi do tragedii



Wady

- Trzeba w jakiś sposób pamiętać hasło zerowe aby móc obliczyć obecne hasło



single use

Systemy challenge-response



Aspekt techniczny

- Identyfikacja na podstawie znajomości pewnego algorytmu
- Najczęściej algorytm ten „zaszyty” jest w urządzeniu zewnętrznym



Zalety

- Przy nietrywialnym algorytmie poziom bezpieczeństwa jest wyższy
- Podśluchanie hasła nie prowadzi do tragedii...



Wady

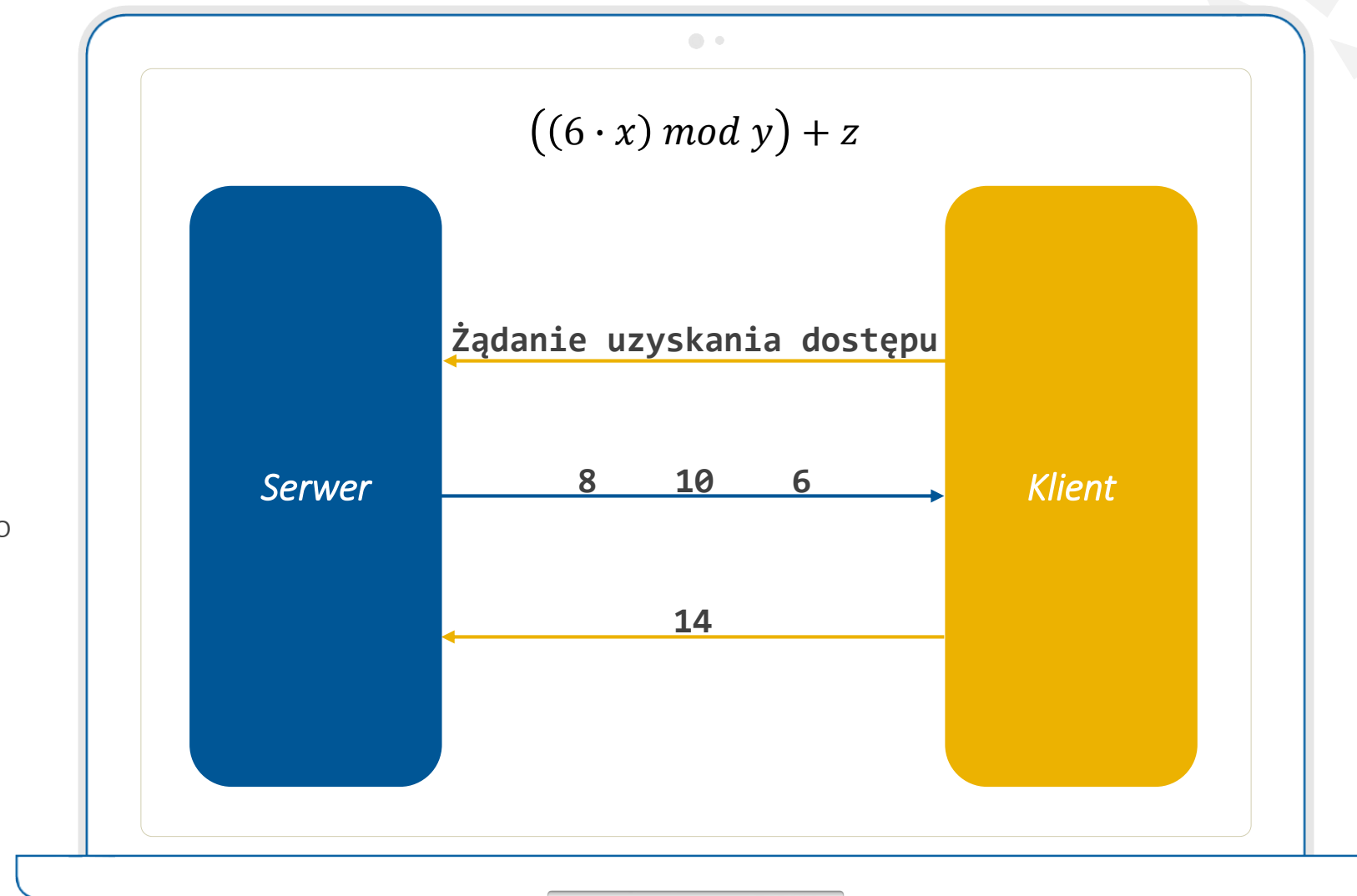
- ...ale złamanie algorytmu już tak
- Konieczność posiadania przy sobie zewnętrznego urządzenia
- Uciążliwość procesu logowania



Systemy challenge-response

Sposób działania

1. Klient żąda dostępu do pewnego zasobu
2. Serwer „zadaje pytanie”
3. Klient znając algorytm wylicza odpowiedź
4. Serwer weryfikuje poprawność odpowiedzi



Systemy challenge-response



Aspekt techniczny

- Identyfikacja na podstawie znajomości pewnego algorytmu
- Najczęściej algorytm ten „zaszyty” jest w urządzeniu zewnętrznym



Zalety

- Przy nietrywialnym algorytmie poziom bezpieczeństwa jest wyższy
- Podśluchanie hasła nie prowadzi do tragedii...



Wady

- ...ale złamanie algorytmu już tak
- Konieczność posiadania przy sobie zewnętrznego urządzenia
- Uciążliwość procesu logowania



Hasła zmienne w czasie



Aspekt techniczny

- Hasło zmienia się co minutę
- Hasło jest jednorazowe



Zalety

- Zwiększony poziom bezpieczeństwa
- Gwarancja tokena na 2-3 lata
- Możliwość zabezpieczenia tokena PINem



Wady

- Do zalogowania się potrzebne jest specjalne urządzenie
- Problem synchronizacji tokena z serwerem

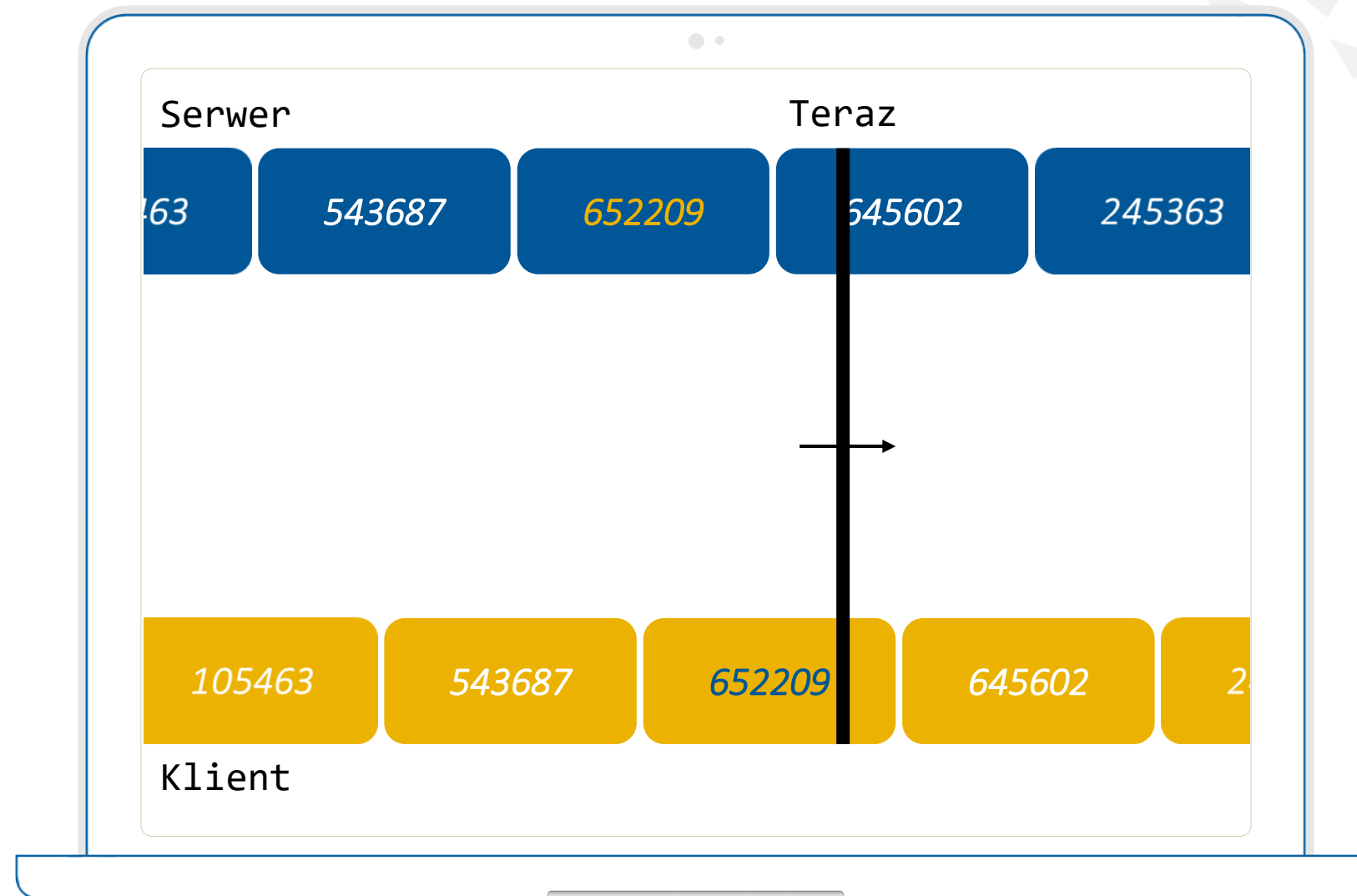


Hasła zmienne w czasie

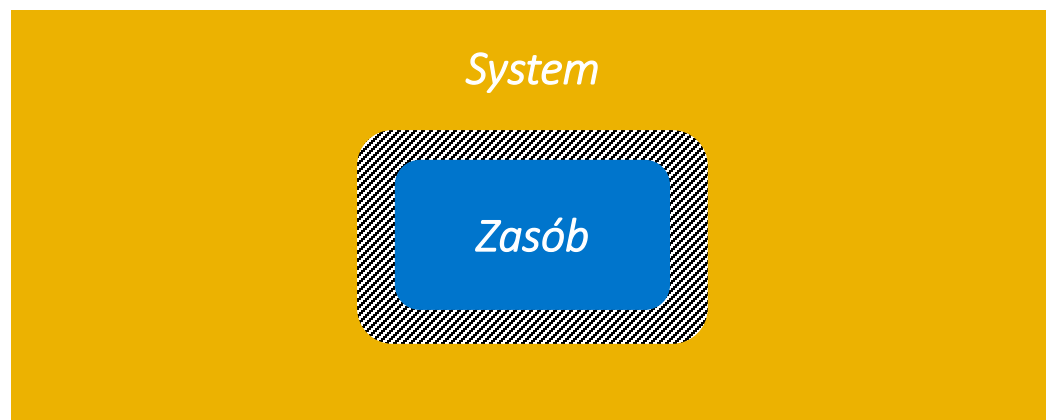
*Problem synchronizacji
tokena z serwerem*

Cechy

- Modyfikacja czasu tokena nie jest możliwa
- Serwer może wyliczyć poprzednie i następne hasło
- W przypadku rozbieżności serwer może oszacować różnicę i zapamiętać poprawkę



Techniki kryptograficzne



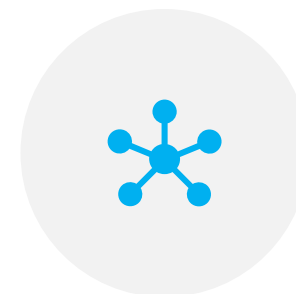
Zabezpieczają zasoby

Nawet jeżeli te są dostępne i widoczne publicznie



Wykorzystują szyfry

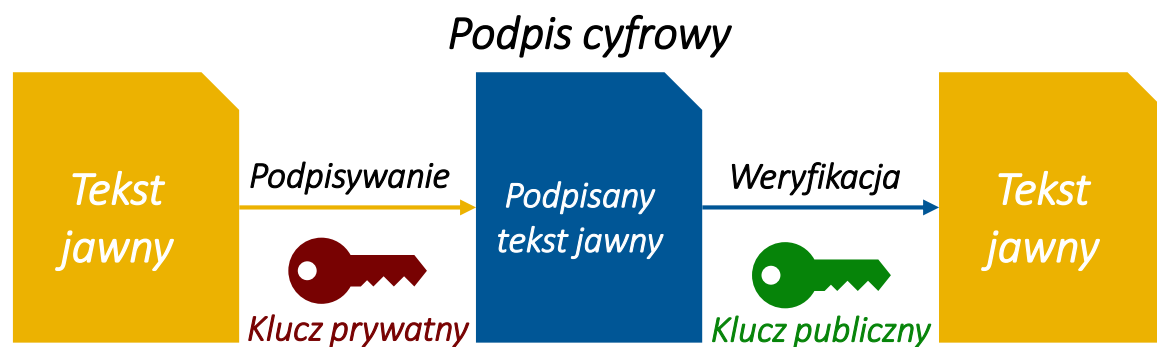
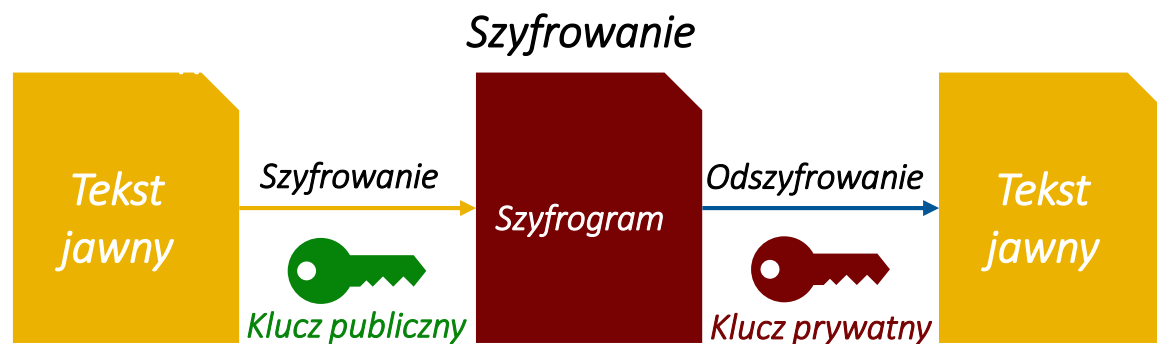
Szyfry z kluczem publicznym i prywatnym, podpis cyfrowy, certyfikaty



Możliwość wykorzystania z poprzednimi metodami

Zabezpieczają zasoby, jak również weryfikują tożsamość

Podpis elektroniczny



Aspekt techniczny

- Wykorzystuje algorytmy szyfrujące z kluczem publicznym



Zalety

- Skutecznie zabezpieczają przez spoofingiem
- Możliwość zaszyfrowania danych



Wady

- Kosztowne obliczeniowo... chyba że podpisujemy tylko hash

Certyfikaty cyfrowe



Aspekt techniczny

- Wykorzystują podpis cyfrowy
- Używane w usługach korzystających z protokołu TCP



Zalety

- Skutecznie zabezpieczają przez spoofingiem
- Wbudowane w przeglądarki internetowe



Wady

- Scentralizowane instytucje certyfikujące dla standardu X.509

Zabezpieczenia biometryczne



Czytnik linii papilarnych

- Sprawdza cechy charakterystyczne
- Musi działać szybko i dokładnie
- Można oszukać



Skaner twarzy

- Robi zdjęcia twarzy
- Sprawdza cechy charakterystyczne
- Łatwe do oszukania w przypadku użycia kamer 2D



Skaner tęczówki oka

- Lokalizuje oczy
- Wykonuje zdjęcia tęczówki
- Odporne na mruganie, przymykanie oczu
- Niezadowalająca skuteczność



Wykrywacz układu naczyń krwionośnych

- Skanowanie dłoni przy pomocy promieni podczerwonych



Skaner geometrii dłoni

- Robi zdjęcia 3D
- Oblicza grubość, długość i szerokość czterech palców

Podsumowanie

Czyli co warto zapamiętać



**Nie ma idealnej metody.
Każdy sposób
uwierzytelniania ma
swoje mocne i słabe
strony – poznaj je!**



**Dowiedz się jak
działają poszczególne
metody, aby uniknąć
późniejszych
niespodzianek!**



**Stosuj co najmniej dwie
metody uwierzytelniania,
a jak nie chce Ci się to
przynajmniej zmieniaj
hasło raz na jakiś czas!**





Źródła


Dostęp – kwiecień 2019

- Własna wiedza ☺
- *Systemy Ochrony Informacji*
dr Tomasz Surmacz [19 czerwca 2017]
- *Definicja systemu komputerowego*
https://pl.wikipedia.org/wiki/System_komputerowy
- *Zabezpieczenia biometryczne*
https://pl.wikipedia.org/wiki/Zabezpieczenie_biometryczne
- *O czytnikach linii papilarnych*
<http://www.egospodarka.pl/141042,Czytnik-linii-papilarnych-Nie-taki-bezpieczny-jakby-sie-wydawalo,1,12,1.html>

Dziękuję!

inż. Jakub Batogowski 

Metody uwierzytelniania użytkowników w systemach komputerowych 

kwiecień 2019 





Grafiki

Dostęp – kwiecień 2019

- *Mocne hasła*
<http://www.vontrompka.com/blog/2017/01/znaki-specjalne-na-niebie-i-ziemi/>
- *Token typu challenge-response*
https://www.vasco.com/images/de-de/DIGIPASS-260_tcm45-47199.pdf
- *Karta z kodami jednorazowymi*
<https://www.pcworld.pl/g1/news/2/0/203786>
- *Token SecureID*
http://www.cs.cornell.edu/courses/cs5430/2017sp/l/1/5-tokens/rsa_token.gif



Grafiki

Dostęp – kwiecień 2019

- *Single use icon*
https://cdn.shopify.com/s/files/1/0833/0289/files/9a99a679-e76b-4fe4-830c-3f11a175b620_large.png?1380188065745677036
- *Grafika po lewej stronie, na którą właśnie patrzysz*
<https://www.pexels.com/photo/blur-book-stack-books-bookshelves-590493/>



