Plan całości wykładu

- Wprowadzenie (2 wykłady)
- Warstwa aplikacji (2 wykłady)
- Warstwa transportu (2 wykłady)
- Warstwa sieci (3 wykłady)
- Warstwa łącza i sieci lokalne (3 wykłady)
- Podstawy ochrony informacji (3 wykłady)

1

Literatura do ochrony informacji w sieciach komputerowych

Rozdział 8, J. Kurose, K. Ross *Sieci komputerowe. Od ogółu do szczegółu z Internetem w tle.* Wydanie 3 wydawnictwo: Helion, Czerwiec 2006

2

Ochrona informacji w sieciach komputerowych

Cele wykładu:

- zrozumienie zasad ochrony informacji:
  - kryptografia i jej *wiele* zastosowań poza "poufnością"
  - uwierzytelnienie
  - integralność
  - dystrybucja kluczy
- ochrona informacji w praktyce:
  - ściany ogniowe i systemy wykrywania włamań
  - ochrona informacji w warstwach aplikacji, transportu, sieci, łącza, i fizycznej

3

Mapa wykładu

7.1 Co to jest ochrona informacji?
7.2 Zasady działania kryptografii
7.3 Uwierzytelnienie
7.4 Integralność
7.5 Dystrybucja kluczy i certyfikacja
7.6 Kontrola dostępu: ściany ogniowe
7.7 Ataki i środki zaradcze
7.8 Wykrywanie włamań i cyfrowa kryminalistyka
7.9 Ochrona informacji w wielu warstwach

4

Co to jest ochrona informacji?

Poufność: tylko nadawca, zamierzony odbiorca powinien "rozumieć" zawartość wiadomości
- nadawca *szyfruje* wiadomość
- odbiorca *odszyfrowuje* wiadomość

Uwierzytelnienie: nadawca, odbiorca chcą wzajemnie potwierdzić swoją tożsamość

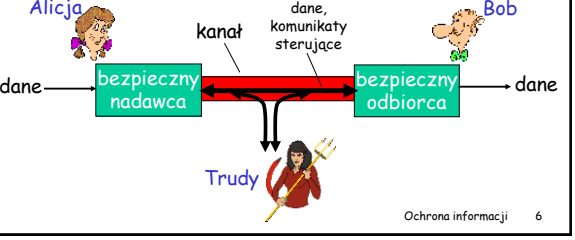
Integralność: nadawca, odbiorca chcą zapewnić, że wiadomość nie zostanie zmodyfikowana (podczas komunikacji, lub później) niepostrzeżenie

Dostępność: usługi muszą być dostępne dla użytkowników

5

Przyjaciele i wrogowie: Alicja, Bob, Trudy

- dobrze znani w środowisku ochrony informacji
- Bob, Alicja (dobrzy znajomi) chcą porozumiewać się "bezpiecznie"
- Trudy (intruz) może przechwytywać, usuwać, dodawać komunikaty



6

Kim mogą być Bob i Alicja?

- … najprościej, *prawdziwymi* ludźmi!
- Przeglądarka/serwer WWW dla elektronicznych transakcji (n.p., zakupy on-line)
- klient/serwer banku on-line
- serwery DNS
- rutery wymieniające aktualizacje tablic rutingu
- inne przykłady?

Na świecie są źli ludzie…

Co może zrobić "zły człowiek"?

Odpowiedź: bardzo dużo!

- *podsłuchiwać:* przechwytując wiadomości
- aktywnie *dodawać* wiadomości do komunikacji
- *podszywać się:* może fałszować (spoof) adres nadawcy w pakiecie (lub dowolne pole w pakiecie)
- *przechwytywać:* "przejmować" istniejące połączenie przez usunięcie nadawcy lub odbiorcy, zastępując go sobą, przejmować kontrolę nad hostem nadawcy/odbiorcy
- *zablokować usługę*: uniemożliwić dostęp do usługi innym (ang. *denial of service*)

Na świecie są źli ludzie…

Czy można się zabezpieczyć technologicznie?

Odpowiedź: nie można!

- ataki technologiczne i środki zaradcze to przedmiot tego wykładu, lecz…
- …najprostszy atak, to wykorzystanie słabości człowieka!
  - karteczki z hasłami
  - "pożyczanie" konta
  - logowanie się na obcym komputerze
- …a najskuteczniejszy atak, to połączenie socjotechniki z atakiem technologicznym…
  - np., nakłonienie ofiary do zainstalowania konia trojańskiego..

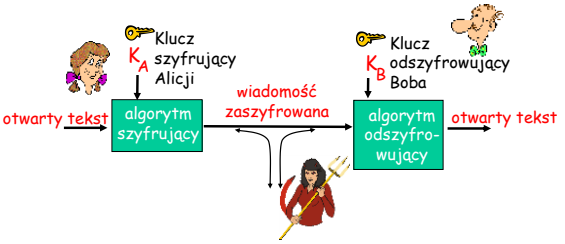
Bądźcie ciągle czujni!!
(Mad-Eyed Moody)

Mapa wykładu

Krypto… -grafia, -analiza i NSA

- Od początku, konkurują ze sobą dwie dziedziny wiedzy:
  - kryptografia
  - kryptoanaliza
  - nowe dziedziny: steganografia, steganaliza
- NSA: globalna tajna służba?
- Palladium (& TCPA): globalne tylne drzwi?
  - zapewne będzie częścią MS Longhorn
  - obecna oficjalna nazwa: Next-Generation Secure Computing Base for Windows, „Trusted Computing"
  - tak naprawdę chodzi o … DRM (*Digital Rights Management*)

Język kryptografii



kryptografia z kluczem symetrycznym:
klucze nadawcy, odbiorcy są *identyczne*

kryptografia z kluczem publicznym:
jeden klucz *publiczny*, drugi klucz *tajny* (prywatny)

Kryptografia z kluczem symetrycznym

szyfr zastępujący: zastępuje niektóre części przez inne
- szyfr monoalfabetyczny: zastępuje jeden znak przez inny

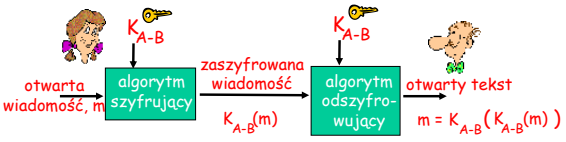
```
otwarty tekst:   abcdefghijklmnopqrstuvwxyz
zaszyfrowany tekst:  mnbvcxzasdfghjklpoiuytrewq
```

N.p.: `otwarty t.: Kocham cię, Bob. Alicja`
`zaszyfrowany t.: nkn. s gktc wky. mgsbc`

Pytanie: Jak trudno jest złamać ten prosty szyfr?:
- brutalnie (jak trudno?)
- w inny sposób?

13

Kryptografia z kluczem symetrycznym



kryptografia z kluczem symetrycznym: Bob i Alicja znają ten sam (symetryczny) klucz: K_{A-B}
- n.p., kluczem może być wzorzec zastępowania w monoalfabetycznym szyfrze zastępującym
- Pytanie: jak Bob i Alicja mają uzgodnić wartość klucza?

14

Idealnie bezpieczny szyfr

- Czy istnieje szyfr nie do złamania?
- Odpowiedź: tak!
  - wystarczy zaszyfrować wiadomość za pomocą klucza, który jest losowym ciągiem bitów tak samo długim jak wiadomość
  - algorytm szyfrujący: m XOR k
  - niestety: to nie jest praktyczne rozwiązanie...
  - Kryptografia: sztuka znajdowania szyfrów, które wykorzystują *krótkie* klucze i nie dają się łatwo złamać

15

Kryptografia symetryczna: DES

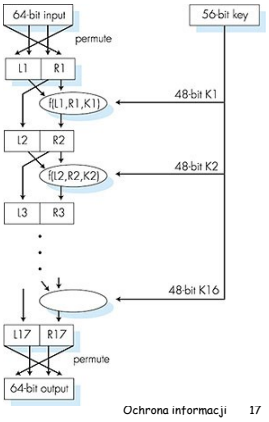
DES: Data Encryption Standard
- Amerykański standard szyfrowania [NIST 1993]
- 56-bitowy klucz symetryczny, otwarty tekst w blokach 64-bitowych
- Jak bezpieczny jest DES?
  - DES Challenge: wiadomość zaszyfrowana 56-bitowym kluczem ("Strong cryptography makes the world a safer place") została odszyfrowana (za pomocą brutalnej siły) w 4 miesiące
  - nie są znane "tylne drzwi" do odszyfrowywania
- zwiększanie bezpieczeństwa DES:
  - używanie 3 kluczy po kolei (3-DES)
  - łączenie bloków szyfru

16

Kryptografia symetryczna: DES

Działanie DES

początkowa permutacja
16 identycznych "rund", każda używa innych 48 bitów klucza
końcowa permutacja



17

AES: Advanced Encryption Standard

- nowy (Listopad 2001) standard NIST kryptografii symetrycznej, zastępujący DES
- przetwarza dane w 128-bitowych blokach
- 128, 192, lub 256 bitowe klucze
- brutalne odszyfrowanie (wypróbowanie każdego klucza) dla wiadomości i długości klucza, które trwa 1 sekundę dla DES, trwa 149 bilionów lat dla AES

18

Kryptografia z kluczem publicznym

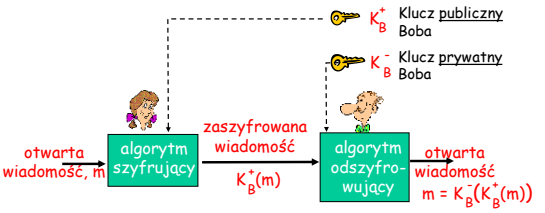
kryptografia symetryczna

- nadawca i odbiorca muszą znać wspólny, tajny klucz symetryczny
- Pytanie: jak uzgodnić wartość klucza (szczególnie, jeśli nadawca i odbiorca nigdy się nie "spotkali")?

kryptografia klucza publicznego

- radykalnie inne podejście [Diffie-Hellman 1976, RSA 1978]
- nadawca, odbiorca *nie* mają wspólnego klucza
- *publiczny* klucz nadawcy/odbiorcy jest znany *wszystkim*
- *prywatny* klucz jest znany tylko właścicielowi

Kryptografia klucza publicznego



Algorytmy szyfrujące z kluczem publicznym

Wymagania:

1. potrzeba $K_B^+(\cdot)$ i $K_B^-(\cdot)$ takich, że
$$K_B^-(K_B^+(m)) = m$$
2. znając klucz publiczny K_B^+, obliczenie klucza prywatnego K_B^- powinno być niemożliwe

RSA: algorytm Rivest, Shamir, Adleman

RSA: Wybór kluczy

1. Wybierz dwie duże liczby pierwsze *p*, *q*. (n.p., po 1024 bity każda)
2. Oblicz $n = pq$, $z = (p-1)(q-1)$
3. Wybierz *e* (przy tym $e<n$) które nie ma takich samych podzielników (>1) co z. (*e*, *z* są "względnie pierwsze").
4. Wybierz *d* takie, że *ed-1* jest podzielne przez *z*. (innymi słowy: *ed* mod *z* = *1*).
5. Klucz *publiczny* to $\underbrace{(n,e)}_{K_B^+}$. Klucz *prywatny* to $\underbrace{(n,d)}_{K_B^-}$.

RSA: Szyfrowanie, odszyfrowywanie

0. Mając (*n*,*e*) oraz (*n*,*d*) obliczone jak powyżej
1. Żeby zaszyfrować ciąg bitów, *m*, oblicz
$c = m^e \bmod n$ (resztę z dzielenie m^e przez *n*)
2. Żeby odszyfrować ciąg bitów, *c*, oblicz
$m = c^d \bmod n$ (resztę z dzielenia c^d przez *n*)

Czary z mleka! $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

Przykład RSA:

Bob wybiera *p=5*, *q=7*. Then *n=35*, *z=24*.
e=5 (tak że *e*, *z* względnie pierwsze).
d=29 (tak że *ed-1* podzielne przez *z*.

	litera	m	m^e	$c = m^e \bmod n$
szyfrowanie:	l	12	1524832	17

	c	c^d	$m = c^d \bmod n$	litera
odszyfro-wywanie:	17	48196857210675091509141182522307169 7	12	l

Praktyczne problemy przy implementacji RSA

- Szukanie dużych liczb pierwszych
  - testy na liczby pierwsze
- Jak sprawdzić, że e jest względnie pierwsze z z?
  - algorytm Euklidesa
- Jak obliczyć d z e?
  - zmodyfikowany algorytm Euklidesa
- Jak podnieść liczbę do bardzo dużej potęgi?
  - arytmetyka dowolnej precyzji

25

RSA: Dlaczego $m = (m^e \bmod n)^d \bmod n$

Pożyteczny wynik z teorii liczb: Jeśli p,q są liczbami pierwszymi i $n = pq$, to:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(używając wyniku opisanego powyżej)

$$= m^1 \bmod n$$

(ponieważ wybraliśmy ed podzielne przez $(p-1)(q-1)$ z resztą 1)

$$= m$$

26

Dlaczego RSA trudno odszyfrować?

- Przecież w kluczu publicznym znane jest n=pq? Czy nie da się z niego poznać p,q?
- Odpowiedź: nie tak łatwo...
  - problem poznania wszystkich liczb pierwszych, których iloczyn równy jest danej liczbie, to *faktoryzacja*
  - Faktoryzacja jest problemem NP-trudnym (bardzo złożonym obliczeniowo)
  - Odpowiedź: da się złamać RSA, ale trwa to bardzo długo...
    - jeśli P=NP, to może kryptografia klucza publicznego przestanie być skuteczna

27

RSA: inna ważna własność

Następująca własność będzie *bardzo* ważna później:

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

użyj najpierw klucza publicznego, potem prywatnego

użyj najpierw klucza prywatnego, potem publicznego

Wynik jest ten sam!

28

Mapa wykładu

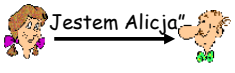
- 7.1 Co to jest ochrona informacji?
- 7.2 Zasady działania kryptografii
- 7.3 Uwierzytelnienie
- 7.4 Integralność
- 7.5 Dystrybucja kluczy i certyfikacja
- 7.6 Kontrola dostępu: ściany ogniowe
- 7.7 Ataki i środki zaradcze
- 7.8 Wykrywanie włamań i cyfrowa kryminalistyka
- 7.9 Ochrona informacji w wielu warstwach

29

Uwierzytelnienie

Cel: Bob chce, żeby Alicja "udowodniła" jemu swoją tożsamość

Protokół uwierz1.0: Alicja mówi: "Jestem Alicja".



Scenariusz błędny??

30

Uwierzytelnienie

Cel: Bob chce, żeby Alicja "udowodniła" jemu swoją tożsamość

Protokół uwierz1.0: Alicja mówi: "Jestem Alicja".

w sieci, Bob nie "widzi" Alicji, zatem Trudy po prostu oświadcza, że jest Alicją

31

Uwierzytelnienie: druga próba

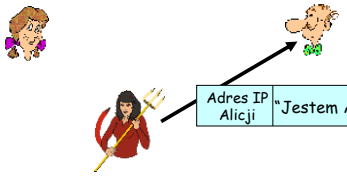
Protokół uwierz2.0: Alicja mówi "Jestem Alicja" w pakiecie IP, który zawiera jej adres IP

Scenariusz błędny??

32

Uwierzytelnienie: druga próba

Protokół uwierz2.0: Alicja mówi "Jestem Alicja" w pakiecie IP, który zawiera jej adres IP

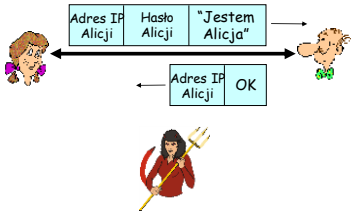


Trudy może stworzyć pakiet, w którym podaje adres IP Alicji jako adres źródła (IP spoofing")

33

Uwierzytelnienie: kolejna próba

Protokół uwierz3.0: Alicja mówi "Jestem Alicja" i wysyła swoje tajne hasło, żeby "udowodnić" tożsamość.

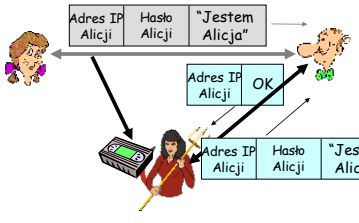


Scenariusz błędny??

34

Uwierzytelnienie: kolejna próba

Protokół uwierz3.0: Alicja mówi "Jestem Alicja" i wysyła swoje tajne hasło, żeby "udowodnić" tożsamość.

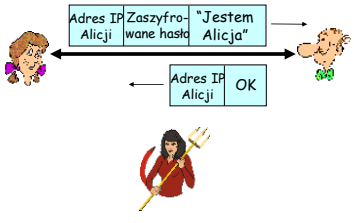


Atak odtwarzający: Trudy nagrywa pakiet Alicji i później odtwarza go dla Boba

35

Uwierzytelnienie: jeszcze jedna próba

Protokół uwierz3.1: Alicja mówi "Jestem Alicja" i wysyła swoje *zaszyfrowane* tajne hasło, żeby "udowodnić" tożsamość.

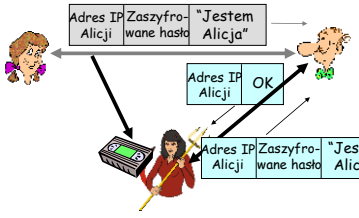


Scenariusz błędny??

36

Uwierzytelnienie: jeszcze jedna próba

Protokół uwierz3.1: Alicja mówi "Jestem Alicja" i wysyła swoje *zaszyfrowane* tajne hasło, żeby "udowodnić" tożsamość.



nagrywanie i odtwarzanie ciągle działa!

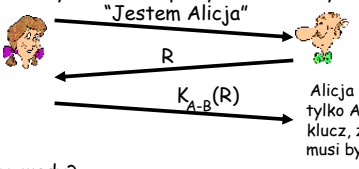
37

Uwierzytelnienie: ponowna próba

Cel: uniknąć ataku odtwarzającego

Identyfikator jednorazowy: liczba (R) używana *raz w życiu*

uwierz4.0: żeby sprawdzić, czy Alicja "żyje", Bob wysyła jej id. jednorazowy, R. Alicja musi odesłać R, zaszyfrowane wspólnym kluczem symetrycznym



Alicja "żyje", i tylko Alicja zna klucz, zatem to musi być Alicja!

Błędy, wady?

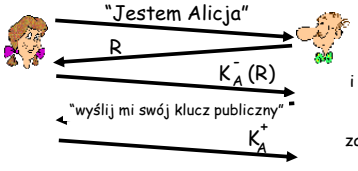
38

Uwierzytelnienie: uwierz5.0

uwierz4.0 wymaga wspólnego klucza symetrycznego

- czy możemy uwierzytelniać za pomocą kryptografii klucza publicznego?

uwierz5.0: używa id. jednorazowego, kryptografii klucza publicznego

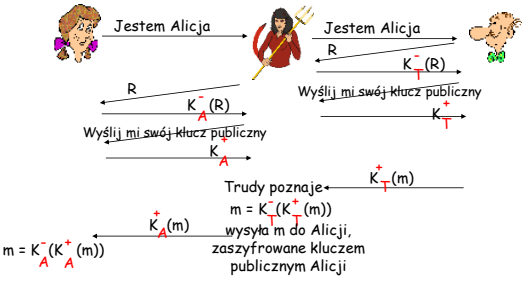


Bob oblicza $K_A^+(K_A^-(R)) = R$ i wie, że tylko Alicja może znać klucz prywatny, który zaszyfrował R tak, że $K_A^+(K_A^-(R)) = R$

39

uwierz5.0: luka w bezpieczeństwie

Atak pośrednika (ang. *man in the middle*): Trudy udaje Alicję (dla Boba) i Boba (dla Alicji)



40

"Atak na RSA"

Atak pośrednika (ang. *man in the middle*): Trudy udaje Alicję (dla Boba) i Boba (dla Alicji)

Trudny do rozpoznania:

- Bob otrzymuje wszystko, co Alicja wysłała, i na odwrót. (dzięki temu Bob, Alicja mogą się spotkać później i wiedzą, o czym rozmawiali)
- rzecz w tym, że Trudy też zna wszystkie wiadomości!
- Problem polega na tym, że Bob "poznał" klucz publiczny Alicji w niebezpieczny sposób
- Problem dotyczy wszystkich zastosowań kryptografii z kluczem publicznym

41

Mapa wykładu

42