

Kryptografia

Protokoły kryptograficzne

dr Robert Borowiec

Politechnika Wrocławska

Instytut Telekomunikacji i Akustyki

pokój 908, C-5

tel. 3203083

e-mail: robert.borowiec@ita.pwr.wroc.pl

www: lstwww.ita.pwr.wroc.pl/~RB/

Wykład XI

2-godziny

Protokół

- **Protokół** jest szeregiem kroków podejmowanych przez co najmniej dwie strony w celu realizacji zadania.
- **Protokół kryptograficzny** jest protokołem wykorzystującym kryptografię. Umożliwiają one realizację zadań nawet przez strony nie dążące się zaufaniem.
- Własności protokołu:
 - ⇒ Każdy użytkownik protokołu musi go znać i kolejno wykonywać wszystkie kroki
 - ⇒ Każdy użytkownik musi zgodzić się na jego stosowanie.
 - ⇒ Protokół musi być nie mylący, tj. każdy krok musi być dobrze zdefiniowany i nie może wystąpić szansa na nieporozumienie
 - ⇒ Protokół musi być kompletny, tj. dla każdej możliwej sytuacji musi być podany odpowiedni sposób postępowania.

Typy protokołów

- Arbitrażowe
- Rozjemcze
- Samowymuszające

x



Protokół arbitrażowy

x



Protokół arbitrażowy

➤ Problemy związane z implementacją protokołu arbitrażowego w sieci komputerowej:

- ⇒ dużo łatwiej można znaleźć i obdarzyć zaufaniem trzecią neutralną stronę, jeżeli znamy tę osobę, możemy ujrzeć jej twarz lub jesteśmy przekonani, że jest to postać rzeczywista, niż zaufać komuś bezosobowemu gdzieś w sieci komputerowej;
- ⇒ sieć komputerowa musi ponosić koszty utrzymania arbitra;
- ⇒ z każdym protokołem arbitrażowym jest związane pewne opóźnieniem;
- ⇒ arbitrzy są potencjalnym wąskim gardłem każdego protokołu zaimplementowanego na wielką skalę;
- ⇒ każdy użytkownik sieci komputerowej jest zmuszony ufać arbitrowi. Arbitr jest więc narażony na oddziaływanie każdego intruza podejmującego próby oszustwa w sieci.



Protokół rozjemczy

➤ *Protokół arbitrażowy dzieli się na protokoły niższego rzędu:*

- ⇒ *protokół niearbitrażowy-sytuacja standardowa;*
- ⇒ *protokół rozjemczy-sytuacja wyjątkowa.*



Protokół samowymuszający

- Budowa protokołu gwarantuje uczciwość stron. Jeżeli bowiem jedna ze stron zaczyna oszukiwać, druga natychmiast to może wykryć
- Nie ma protokołów samowymuszających^x odpowiednich na każdą sytuację.



Łamanie protokołów

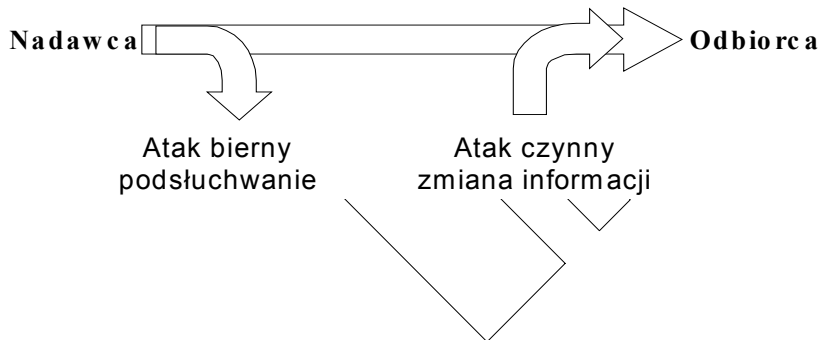
- Łamanie protokołu może być skierowane na:
 - ⇒ na sam protokół;
 - ⇒ algorytmy kryptograficzne;
 - ⇒ techniki kryptograficzne^x służące do implementacji algorytmu (generowanie klucza);



Atak na protokół

➤ Łamanie protokołów

- ⇒ *biernie*
- ⇒ *aktywne*



Protokół wymiany informacji za pomocą kryptografii symetrycznej

➤ Przebieg protokołu:

- ⇒ *Uzgodnienie algorytmu kryptograficznego jaki będzie wykorzystywany do szyfrowania*
- ⇒ *uzgodnienie klucza szyfrującego*
- ⇒ *zaszyfrowanie wiadomości przez jedną ze stron*
- ⇒ *przesłanie szyfrogramu na drugą stronę*
- ⇒ *deszyfrowanie wiadomości przez drugą stronę*



Protokół wymiany informacji za pomocą kryptografii z kluczem publicznym

➤ Przebieg protokołu:

- ⇒ Uzgodnienie algorytmu kryptograficznego z kluczem jawnym jaki będzie wykorzystywany do szyfrowania
- ⇒ Strony wymieniają się swoimi kluczami jawnymi lub pobierają je z serwera kluczy publicznych.
- ⇒ Strony szyfrują wiadomości kluczami jawnymi strony przeciwnej i wysyłają do siebie informacje.
- ⇒ Strony odszyfrowują otrzymane wiadomości swoimi kluczami prywatnymi.



Systemy z kluczem sesyjnym

- Używanie jednego klucza do szyfrowania całej wymiany informacji jest niekorzystne, gdyż dostarcza stronie atakującej coraz więcej materiału do kryptoanalizy;
- Wskazane jest więc stosowanie kluczy sesyjnych wykorzystywanych tylko na czas pojedynczej transmisji.
- Strony przed rozpoczęciem transmisji informacji muszą ustalić klucz sesyjny
- Klucz zasadniczy służy tylko i wyłącznie do szyfrowania i bezpiecznego przesyłania kluczy sesyjnych.



Protokół wymiany klucza w systemach z kluczem tajnym

- *Alicja chce nawiązać łączność z Robertem w tym celu:*
 - ⇒ *kieruje do centrali zajmującej się dystrybucją kluczy zamówienie na klucz sesyjny;*
 - ⇒ *centrala generuje odpowiedni klucz losowy. Następnie jedną kopię szyfruje kluczem tajnym Alicji, a drugą Roberta. Następnie centrum szyfruje dane o tożsamości Alicji kluczem Roberta i wysyła te informacje do Alicji;*
 - ⇒ *Alicja deszyfruje swój klucz sesyjny;*
 - ⇒ *Alicja wysyła Robertowi jego kopię klucza wraz ze swoją tożsamością;*
 - ⇒ *Robert teraz wie, kto chce z nim nawiązać połączenie*
 - ⇒ *zestawiany jest bezpieczny kanał komunikacyjny w oparciu o klucz sesyjny;*



Protokół wymiany klucza w systemach z kluczem publicznym

- *Alicja chce nawiązać łączność z Robertem w tym celu:*
 - ⇒ *Alicja pobiera klucz jawny Roberta z centrum dystrybucji kluczy lub zwraca się o niego wprost do Roberta;*
 - ⇒ *Alicja generuje losowy klucz sesyjny, szyfruje go kluczem jawnym Roberta i wysyła mu go*
 - ⇒ *Robert deszyfruje klucz sesyjny za pomocą swojego klucza prywatnego.*
 - ⇒ *Wymieniony klucz sesyjny może posłużyć do zestawienia szyfrowanego kanału komunikacyjnego.*



Bezpieczeństwo algorytmu wymiany klucza

- Żaden z przedstawionych systemów nie jest bezpieczny jeżeli atakujący wniknie do centrum dystrybucji kluczy.
- System wymiany klucza bezpośrednio pomiędzy Alicją i Robertem jest narażony na atak typu man in the middle.
- Rozwiązaniem zapewniającym bezpieczeństwo wymiany klucza sesyjnego jest:
 - ⇒ protokół blokujący
 - ⇒ trójpzbiegowy algorytm Shamira



Protokół blokujący

- Protokół umożliwia wykluczenie ataku man in the middle.
 - ⇒ Alicja przesyła Robertowi swój klucz jawny
 - ⇒ Robert Przesyła Alicji swój klucz jawny
 - ⇒ Alicja szyfruje swoją wiadomość kluczem jawnym Roberta i przesyła mu połowę zaszyfrowanej wiadomości.
 - ⇒ Robert robi to samo ze swoją wiadomością
 - ⇒ Alicja wysyła Robertowi drugą połowę zaszyfrowanej wiadomości
 - ⇒ Robert składa obie połówki i deszyfruje je swoim kluczem prywatnym
 - ⇒ Robert wysyła drugą połówkę wiadomości do Alicji
 - ⇒ Alicja składa obie połówki i deszyfruje używając swojego klucza prywatnego.



Protokół blokujący

➤ *Dzielenie szyfrogramu.*

- ⇒ *Możemy wysłać co drugi bit szyfrogramu*
- ⇒ *Możemy wprowadzić transmisję CBC i najpierw wysłać wektor inicjujący, a potem dopiero informację*
- ⇒ *Pierwszą połową może być funkcja skrótu^x, a drugą sama wiadomość, której funkcja skrótu dotyczy.*



Tróiprzebiegowy algorytm Shamira

➤ *Korzysta z zasady, że $E_A(E_B(M))=E_B(E_A(M))$.*

- ⇒ *Alicja szyfruje tekst jawny M swoim kluczem i przesyła do Roberta $C_1=E_A(M)$*
- ⇒ *Robert szyfruje otrzymaną wiadomość swoim kluczem i z powrotem przesyła ją do Alicji. Wysyła $C_2=E_B(E_A(M))$*
- ⇒ *Alicja deszyfruje tekst jawny C_2 za pomocą swojego klucza i z powrotem przesyła do Roberta. Wysyła więc $C_3=D_A(E_B(E_A(M)))=D_A(E_A(E_B(M)))=(E_B(M))$*
- ⇒ *Robert deszyfruje wiadomość C_3 swoim kluczem i otrzymuje tekst jawny M*
- ⇒ *Jako system szyfrujący nie może być wykorzystane sumowanie modulo 2.*



A series of parallel diagonal lines crossing the slide from the top-left to the bottom-right.

KONIEC

Dziękuję za uwagę