Wrocław 01.10.2020

C Y B E R B E Z P I E C Z E Ń S T W O

L A B O R A T O R I U M N R 6
J E D N O K I E R U N K O W E F U N K C J E S K R Ó T U
A L G O R Y T M Y W Y M I A N Y K L U C Z A
P O D P I S E L E K T R O N I C Z N Y

Plan zajęć

1. Podstawowe wiadomości na temat: funkcji skrótu, podpisu elektronicznego oraz wymiany kluczy kryptograficznych.
2. Zapoznanie się ze środowiskiem pracy - program CrypTool.
3. Podpis elektroniczny.
4. Jednokierunkowe funkcje skrótu.
5. Wymiana klucza kryptograficznego.
6. Raport z przeprowadzonych eksperymentów.

1. Podstawowe wiadomości na temat: funkcji skrótu, podpisu elektronicznego oraz wymiany kluczy kryptograficznych.

- Proszę zapoznać się z charakterystyką blokowych algorytmów szyfrowania. (Dokument w załączeniu oraz materiały do wykładów)
- Dodatkowe informacje mogą państwo znaleźć na stronach:
  - http://cacr.uwaterloo.ca/hac/about/chap9.pdf
  - http://cacr.uwaterloo.ca/hac/about/chap11.pdf
  - http://pl.wikipedia.org/wiki/Funkcja_haszująca
  - http://pl.wikipedia.org/wiki/Atak_urodzinowy
  - http://pl.wikipedia.org/wiki/PKI
  - http://www.signet.pl/pomoc/pki.html
  - http://pl.wikipedia.org/wiki/Diffie-Hellman

2. Zapoznanie się ze środowiskiem pracy - program CrypTool.

- Na tych zajęciach laboratoryjnych będą wykorzystywane głównie narzędzia dostępne z zakładki z programu CrypTool:
  - *Podpis cyfrowy/PKI*
  - *Algorytmy/Hasz*
  - *Kryptoanaliza/Hasz*
  - *Algorytmy/Demosntracja protokołu Diffie-Hellman*

3. Podpis elektroniczny.

Zadania:

1. Proszę sprawdzić listę posiadanych kluczy.
   Zakładka: *Podpis cyfrowy/PKI/Generowanie klucza*
2. Proszę wygenerować własny klucz (algorytm RSA lub DSS) i w raporcie umieścić jego certyfikat.
   Zakładka: *Podpis cyfrowy/PKI/Generowanie klucza*
3. Proszę spróbować eksportować własny certyfikat, a następnie go importować do przeglądarki WWW.
4. Proszę sprawdzić podstawowe dane o certyfikacie serwera:
   - poczty studenckiej: https://smail.pwr.wroc.pl/
   - systemu JSOS: https://jsos.pwr.edu.pl/
   - systemu edukacja: https://edukacja.pwr.wroc.pl/
   - dowolnego wybranego serwisu https
5. Proszę obejrzeć demonstrację ilustrującą proces podpisywania dokumentu.
6. Proszę podpisać dowolny dokument własnym kluczem.
7. Proszę porównać czas podpisywania dokumentów o różnym rozmiarze posługując się różnymi kluczami.
8. Proszę sprawdzić w jaki sposób możliwe jest wykrycie zmian w dokumentach uprzednio podpisanych elektronicznie.

Pytania/Wnioski:

1. Z jakich elementów składają się certyfikaty klucza publicznego?
2. Co to jest podpis elektroniczny? W jaki sposób jest generowany?
3. Jak zmienia się i od czego zależy czas realizacji podpisu elektronicznego dokumentu
4. Jakie certyfikaty (klasy,grupy) znajdują się w przeglądarce? (kilka przykładowych)
5. Co zmieni dodanie nowego certyfikatu do listy zaufanych certyfikatów przeglądarki?

4. Jednokierunkowe funkcje skrótu.

Zadania:

1. Proszę spróbować dokonać ataku na funkcję skrótu dla utworzonych przez siebie plików.
   Zakładka:*Kryptoanaliza/Hasz/*
2. Proszę sprawdzić różnice w realizacji tego typu ataku dla różnej konfiguracji parametrów (inna funkcja skrótu, inna liczba wspólnego ciągu bitów, ...)

Pytania/Wnioski:

1. Jak rośnie czas realizacji ataku wraz ze wzrostem wartości parametru opisującego długość ustalonego ciągu bitów?
2. Czy wybór funkcji skrótu ma wpływ na czas realizacji zadania poszukiwania kolizji?
3. Na czym polega przewaga modyfikowania dwóch dokumentów nad poszukiwaniem kolizji przy modyfikacji tylko jednego dokumentu?
4. Czy w świetle uzyskanych wyników możemy ufać funkcjom skrótu?
5. Jakiego typu problemy zostały zidentyfikowane dla popularnych funkcji skrótu (MD5,SHA)?

6. Wymiana klucza kryptograficznego.

Zapoznaj się z demonstracją algorytmu Diffiego-Hellmana dostępną w Cryptool. W celach demonstracyjnych użyj wartości wygenerowanych w Cryptool. Następnie do praktycznego zastosowania protokołu DH posłużymy się biblioteką OpenSSL. Użyj dwóch maszyn wirtualnych jako klientów (Kali linux, Ubuntu) do wymiany kluczy.

Krótki opis kolejnych kroków:

- Wygeneruj wspólne publiczne elementy dla schematu DH dla obu klientów,
- Na podstawie wspólnych publicznych elementów DH klienci generują klucze publiczne i prywatne,
- Klienci muszą wymienić wygenerowane przez siebie części publiczne schematu DH,
- Na podstawie klucza publicznego i klucza prywatnego tworzony jest wspólny tajny klucz.

a. Wygeneruj wspólne elementy publiczne dla schematu Diffiego-Hellmana dla obu klientów:

```
openssl genpkey -genparam -algorithm DH -out dh_com_pub.pem
```

b. wyświetl wygenerowane wartości parametrów

   - postaci kodowanej

```
cat dh_com_pub.pem
```

- w postaci tekstowej:

```
openssl pkeyparam -in dh_com_pub.pem -text
```

c. Korzystając z wygenerowanych wspólnych parametrów DH, każdy z klientów powinien wygenerować własną część publiczną w schemacie DH (dla obu klientów analogicznie, zmienia się tylko nazwa pliku dh_client1_key.pem):

```
openssl genpkey -paramfile dh_com_pub.pem -out
dh_client1_key.pem
```

- wypisz wygenerowane wartości:

```
openssl pkey -in dh_client1_key.pem -text -noout
```

d. Wyłączenie do rębnego pliku części publicznej wygenerowanej przez klienta1. Analogicznie postępuje klient2.

```
openssl pkey -in dh_client1_key.pem -pubout -out
dh_client1_pub_key.pem
```

e. Strony wymieniają części publiczne pomiędzy sobą (pliki dh_client1(2)_pub_key.pem)

f. Strony generują współdzielony sekret, korzystając z przekazanych przez drugą stronę wartości publicznych i własnego sekretu (poniżej operacja wykonywana przez klienta 1, z wykorzystaniem wartości wygenerowanej przez klienta 2 i przekazanej w pliku **dh_client2_pub_key.pem**:

```
openssl pkeyutl -derive -inkey dh_client1_key.pem -peerkey
dh_client2_pub_key.pem -out secret_key1.bin
```

g. Porównaj współdzielone sekrety przy pomocy komendy `cmp`.

h. Wygeneruj zrzut sekretu korzystając z komendy `xxd`.

Pytania/Wnioski:

1. Który algorytm wymiany kluczy gwarantuje większe bezpieczeństwo? RSA czy DH. Dlaczego?
2. Jakie jest ryzyko dla podmiotów korzystających z protokołu wymiany kluczy DH?
3. Jakie są inne metody określenia wspólnego klucza kryptograficznego?
4. Który element protokołu DH nie jest przesyłany między klientami? Jak to wpływa na kwestie bezpieczeństwa?
5. Sprawdź, czy w ostatnim punkcie udało się ustalić ten sam klucz dla obu klientów. Uwzględnij w raporcie treść uzgodnionego tajnego klucza

6. Raport z przeprowadzonych eksperymentów.

Raport powinien mieć postać dokumentu elektronicznego, w którym zostanie zapisany przebieg realizowanych w trakcie zajęć eksperymentów (np. fragment treści tekstu jawnego, parametry algorytmu szyfrowania, fragment kryptogramu) oraz wnioski, spostrzeżenia, odpowiedzi na pytania umieszczone w instrukcji laboratoryjnej, itp.