Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: Poczta elektroniczna

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

Zadanie przygotowawcze:

W programie pocztowym Thunderbird skonfiguruj konto pocztowe @student.poznan.pl, z którego będziesz korzystać w poniższych ćwiczeniach. Zweryfikuj poprawność konfiguracji wymieniając pocztę z sąsiadem.

1. Bezpieczna komunikacja pocztowa w standardzie S/MIME

1. Pobierz certyfikat ogólnego przeznaczenia wystawiony dla swojego konta @student.poznan.pl. W jakim standardzie jest ten certyfikat zbudowany?

   W jakim formacie pliku został zapisany?

2. W menadżerze certyfikatów klienta pocztowego (Preferences→Privacy&Security→Certificates) zaimportuj swój osobisty certyfikat (w zakładce Your Certificates).
3. Obejrzyj swój osobisty certyfikat w menadżerze certyfikatów. Jaki urząd wystawił certyfikat?

   Jakiej funkcji skrótu użyto do podpisania certyfikatu?

   Jakiego użyto algorytmu kryptograficznego?

4. W zakładce Authorities menadżera certyfikatów wyszukaj certyfikat EDU-CA i upewnij się, że ma zezwolenie (przycisk Edit Trust) na certyfikowanie adresów pocztowych.
5. Sprawdź ścieżkę certyfikacji swojego certyfikatu. Jak nazywa się urząd rootCA dla tej ścieżki?

6. Dokonaj wymiany korespondencji podpisanej elektronicznie przy wykorzystaniu S/MIME i swojego certyfikatu (zwróć uwagę, że musisz wskazać, który certyfikat będziesz wykorzystywać). Przekonaj się czy list odebrany od sąsiada został uznany za poprawnie podpisany. Obejrzyj źródło wiadomości i poszukaj podpisu.

   W jakim standardzie został wykonany podpis?

   Jakiego użyto algorytmu skrótu?

   Skąd klient pocztowy wziął klucz niezbędny do weryfikacji podpisu?

7. Dokonaj wymiany korespondencji szyfrowanej przy wykorzystaniu S/MIME.

2. Bezpieczna komunikacja pocztowa PGP

2.1 OpenPGP w programie Thunderbird

8. W konfiguracji konta pocztowego w ustawieniach szyfrowania "end-to-end" (lub korzystając z menu głównego → Narzędzia) uruchom OpenPGP Key Manager i wygeneruj swoją parę kluczy kryptograficznych PGP. Jakim algorytmem zostały wygenerowane klucze?

   Wygenerowany klucz prywatny wskaż jako klucz osobisty (personal key) dla tego konta.

9. Wyślij podpisany przez PGP list do siebie samego. Sprawdź reakcję klienta pocztowego.
10. Wyślij podpisany list do sąsiada i odbierz jego podpisany list. Czy weryfikacja podpisu przebiegła pomyślnie? Jeśli nie, to dlaczego:
11. Przekaż klucz publiczny sąsiadowi i pozyskaj jego klucz publiczny.
    Zapisz jakim sposobem dokonaliście wymiany kluczy:
12. Sprawdź ponownie efekt weryfikacji podpisu w poprzednim liście od sąsiada (z zad. 10). Zwróć uwagę na to jak został opisany podpis.
13. Zrealizuj komunikację z szyfrowaniem całej przesyłki pocztowej, np. wraz z załącznikami.

14. Zastanów się od czego mógłby zostać uzależniony poziom zaufania do czyjegoś klucza publicznego w systemie takim jak PGP lub podobnym (czy jakieś czynniki mogłyby wpływać na automatyczny wzrost lub spadek poziomu zaufania). Spróbuj przedstawić choć jedną propozycję:

15. Przeanalizuj czy podobnie można by zaproponować jakieś kryteria wielopoziomowego zaufania do certyfikatów kluczy publicznych w S/MIME?

2.2 System GnuPG (GPG)

16. Przećwicz zarządzanie kluczami korzystając z polecenia gpg. Wylistuj pęk swoich kluczy, pobierz klucz publiczny ze wskazanej lokalizacji, przeszukaj serwer kluczy w poszukiwaniu klucza wybranego użytkownika.

17. Jak unieważnić certyfikat swojego klucza publicznego? Zapisz odpowiednie polecenia:

2.2.2 Szyfrowanie plików

18. Zaszyfruj symetrycznie wybrany plik w katalogu domowym. Zapisz użyte polecenie: