Ćwiczenie 04a Techniki kryptograficzne w programie GPG

Celem ćwiczenia jest zapoznanie studentów z wybranymi technikami kryptograficznymi dostępnymi w programie GPG (*GNU Privacy Guard*). Po zainstalowaniu wymaganego oprogramowania studenci zrealizują generowanie kluczy kryptograficznych dla kryptografii asymetrycznej. Następnie dokonują transferu kluczy publicznych. Kolejnym krokiem będzie wymiana zaszyfrowanych i podpisanych cyfrowo wiadomości poczty elektronicznej. Studenci zapoznają się również z możliwości wykorzystania GPG do ochrony lokalnego systemu plików. Ostatnia grupa zadań to eksperyment polegający na sprawdzeniu skuteczności zabezpieczeń integralności oferowanych przez GPG.

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi. Należy również założyć dwa konta pocztowe. Można wykorzystać dowolne 2 konta pocztowe, aktualnie eksploatowane przez studenta realizującego ćwiczenie. Dodatkowo należy zapoznać się z obsługą wszystkich programów, które wykorzystywane będą w trakcie realizacji ćwiczenia. W zasadzie ćwiczenie powinno być realizowane na dwóch przygotowanych wcześniej systemach. W każdym z nich należy wykorzystywać inne konto pocztowe.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

Bezpośrednio przed rozpoczęciem ćwiczenia należy wykonać następujące czynności:

- Zalogować się jako administrator.
- Ustawić poprawną datę i czas systemowy.
- Zainstalować pakiet ***Gpg4win***, wybierając jego komponenty: ***GnuPG*** i ***GPA***. W trakcie instalacji uaktywnić (zakreślić) opcję „*Root certificate defined or skip configuration”*.
- Zainstalować klienta poczty: ***Mozilla Thunderbird***
- Uruchomić program ***Mozilla Thunderbird***. W menu aplikacji (*Application menu*) wybrać funkcję dodawania wtyczek (*Add-ons)*, a następnie przycisnąć przycisk ***Tools for all add-ons*** (przycisk przypominający trybik) i wybrać funkcję instalowania wtyczki programu *GPG* dla klienta poczty.
- Po zamknięciu i ponownym uruchomieniu programu ***Mozilla Thunderbird*** w celu konfiguracji wtyczki wybrać menu aplikacji (*Application menu*) programu ***Thunderbird*** a w nim pozycję ***OpenPGP*** a następnie funkcję określania preferencji (*Preferences)*. Przejść do ustawień eksperckich (*Display Expert Settings*) oraz w zakładce konfiguracji sposobu wyboru klucza (*Key Selection*) wybrać sposób ręczny (*Manually*) i zatwierdzić.
- Skonfigurować konto pocztowe.
- Zrestartować system.

Ćwiczenie 4a. 1 Zarządzanie kluczami kryptograficznymi

Niniejsze ćwiczenie należy zrealizować dla obu kont pocztowych.

1. Uruchomić program ***GNU Privacy Assistant*** (***GPA***). W trakcie uruchamiania odpowiedzieć negatywnie na pytanie dotyczące generowania kluczy.
2. W menu kluczy (*Keys)* wybrać funkcję generowania nowego klucza (*New key*).
3. W oknie generowania klucza, w pasku edycji podać swoje imię i nazwisko oraz w nawiasie słowo *Domowy*. Przejść dalej.
4. W kolejnym oknie podać swój adres email. Przejść dalej.
5. Nie tworzyć kopii zapasowej klucza.
6. Użyć swojego identyfikatora studenckiego jako hasła (*passphrase*) potrzebnego do skorzystania z klucza prywatnego (w przypadku ostrzeżenia dotyczącego niewystarczającej długości hasła, należy wymusić skorzystanie z wprowadzonego hasła przyciskając przycisk ***Take this one away*** i ponownie je wprowadzić).

7. Po wygenerowaniu klucza określić jakiego algorytmu użyto podczas jego generowania, a następnie przejść do menu edycji (*Edit*) i wybrać funkcję zmian preferencji programu (*Preferences*). Ustalić tryb pracy na zaawansowany (*Use advanced mode*) i zatwierdzić zmiany.
8. Wygenerować nowy klucz (por. zadanie 2) dla tego samego adresu e-mail. Czy sposób generowania klucza wygląda tak jak wcześniej? W oknie generowania klucza wybrać algorytm DSA, a następnie ustalić rozmiar klucza (*Key size*) na 3072 bitów. W polu nazwy klucza (*Name*) podać swoje imię i nazwisko oraz w nawiasie słowo *Firmowy*. Pozostałe informacje podać w sposób rzetelny i zatwierdzić. Tak jak poprzednio użyć swojego identyfikatora studenckiego jako hasła (*passphrase*) potrzebnego do skorzystania z klucza prywatnego (por. zadanie 6).
9. Po wygenerowaniu kluczy przejrzeć ich opis w zakładkach: ***Detailes***, ***Signatures*** i ***Subkeys***. Ile kluczy zostało faktycznie wygenerowanych? Czym się różnią poszczególne klucze?
10. Zaznaczyć wygenerowane klucze, a następnie z menu kluczy (*Keys*) wybrać funkcję eksportu (*Export Keys…*). Dokonać eksportu kluczy publicznych do pliku, plik nazwać w sposób następujący: **KLUCZE_PUB_XXXX.TXT**, (gdzie *xxxx* jest identyfikatorem studenta). Zapoznać się z zawartością pliku, za pomocą systemowego notatnika (***Notepad***). Upewnić się, że nie wyeksportowano żadnego klucza prywatnego.
11. Plik z kluczami publicznymi wysłać w załączniku wiadomości e-mail do drugiego konta pocztowego.
12. Odebrać wiadomość pocztową (wysłaną podczas realizacji pkt. 11). Powinna ona zawierać plik o nazwie **KLUCZE_PUB_YYYY.TXT**, (gdzie *xxxx* jest identyfikatorem partnera), z kluczami publicznymi drugiego konta.
13. W oknie programu ***GPA***, w menu kluczy (*Keys*) wybrać funkcję importu (*Import Keys…*).
14. Wskazać miejsce przechowywania pliku pobranego z wiadomości z drugiego konta.
15. Dokończyć proces importu.

Ćwiczenie 4a.2 Zabezpieczanie wiadomości pocztowych

Niniejsze ćwiczenie należy zrealizować wykorzystując jedno konto tylko jako nadawcę, drugie tylko jako odbiorcę.

1. Wysłać do drugiego konta zaszyfrowaną i podpisaną wiadomość pocztową (*Write*). Zarówno szyfrowanie (*Encrypt Message*) jak i podpisywanie (*Sign Message*) włączane są poprzez wciśnięcie przycisku w menu ***OpenPGP***, w oknie tworzonej wiadomości. W przypadku pierwszej próby zabezpieczenia wiadomości powinno pojawić się okno informujące o braku właściwej konfiguracji narzędzi kryptograficznych. W tej sytuacji należy przejść do okna konfiguracji (*Configure*) i włączyć dodatek ***Enigmail*** (*Enable OpenPGP suport (Enigmail) for this identity*). Następnie ustalić domyślny wybór klucza kryptograficznego na podstawie adresu e-mail (*Use email address of this identity to identify OpenPGP key*) i zatwierdzić. W prawym dolnym rogu okna przygotowywanej wiadomości powinny pojawić się stosowne ikony, informujące o zastosowanych zabezpieczeniach. W trakcie wysyłania wybrać do szyfrowania właściwy klucz.
   Jaki klucz został wykorzystany do podpisania tej wiadomości i dlaczego? Obejrzeć treść wysłanej wiadomości (*Sent*) wybierając w menu aplikacji (*Application menu*) programu ***Thunderbird*** menu ***View*** i funkcję podglądu źródła wiadomości (*Message Source*).
2. Odebrać zaszyfrowaną wiadomość pocztową z drugiego konta. Obejrzeć wiadomość w postaci odszyfrowanej i zaszyfrowanej (por. zadanie 1). Zapisać treść wiadomości do pliku tekstowego (*txt*). Następnie w programie ***GPA*** przejść do menadżera plików (*File Manager*),

wybierając z menu ***Windows*** odpowiednią funkcję i otworzyć utworzony przed chwilą plik tekstowy. Dokonać deszyfracji treści tego pliku (*Decrypt*). Porównać treść odszyfrowaną z pliku z treścią wiadomości odszyfrowaną w programie ***Thunderbird***.
Dlaczego klucz publiczny nadawcy wiadomości jest niezaufany (*untrusted, key not valid*)? Co należy zrobić by to zmienić?

3. Wysłać kolejną podpisaną i zaszyfrowaną wiadomość do drugiego konta, wykorzystując drugi z jego kluczy publicznych. Czy partner może odczytać tę wiadomość? Dlaczego?
4. Wysłać jeszcze jedną podpisaną i zaszyfrowaną wiadomość do drugiego konta, tym razem wykorzystując jeden ze swoich kluczy publicznych.
Czy partner może odczytać tę wiadomość? Dlaczego? Wyciągnąć wnioski.

Ćwiczenie 4a.3 Zabezpieczanie plików

Niniejsze ćwiczenie należy zrealizować tylko w jednym systemie, korzystając tylko z jednego konta

1. Utworzyć plik tekstowy o nazwie **PL_XXXX.TXT**, (gdzie *xxxx* jest identyfikatorem studenta). Wpisać do niego swoje imię i nazwisko, następnie zapisać go i zamknąć. W programie ***GPA*** przejść do menadżera plików (*File Manager*), wybierając z menu ***Windows*** odpowiednią funkcję i otworzyć ten plik tekstowy. Zaszyfrować plik (*Encrypt*), wykorzystując jeden z posiadanych kluczy kryptograficznych.
2. Korzystając z systemowego programu ***WordPad,*** otworzyć powstały, zaszyfrowany plik **PL_XXXX.TXT.GPG**, **(**gdzie *xxxx* jest identyfikatorem studenta) i zapoznać się z jego zawartością. Usunąć plik **PL_XXXX.TXT.**
3. Korzystając z programu ***GPA***, odszyfrować zaszyfrowany plik **PL_XXXX.TXT.GPG**, **(**gdzie *xxxx* jest identyfikatorem studenta). W tym celu, w programie ***GPA*** należy zaznaczyć ten plik i przycisnąć przycisk deszyfracji (*Decrypt*). Odczytać nowopowstały plik **PL_XXXX.TXT**, (gdzie *xxxx* jest identyfikatorem studenta)

Ćwiczenie 4a.4 Naruszenia zabezpieczeń

Niniejsze ćwiczenie należy zrealizować tylko w jednym systemie, korzystając tylko z jednego konta

1. Utworzyć plik **DANE_XXXX.TXT**, **(**gdzie *xxxx* jest identyfikatorem studenta) i wpisać do niego swoje imię i nazwisko.
2. Podpisać plik **DANE_XXXX.TXT** przy pomocy następujących poleceń, uruchamianych w oknie wiersza poleceń:

gpg --output **DANE_A_XXXX.SIG** --sign **DANE_XXXX.TXT**

gpg --output **DANE_B_XXXX.SIG** --clearsign **DANE_XXXX.TXT**

gpg --output **DANE_C_XXXX.SIG** --detach-sig **DANE_XXXX.TXT**

3. Korzystając z programu notatnika (*Notepad*) obejrzeć zawartość plików: **DANE_A_XXXX.SIG, DANE_B_XXXX.SIG, DANE_C_XXXX.SIG.**
4. Zweryfikować podpisy przy pomocy następujących poleceń, uruchamianych w oknie wiersza poleceń:

gpg --verify **DANE_A_XXXX.SIG**
gpg --verify **DANE_B_XXXX.SIG**
gpg --verify **DANE_C_XXXX.SIG** **DANE_XXXX.TXT**

5. W pliku **DANE_XXXX.TXT** zmienić dowolny jeden znak w swoim imieniu.
6. Powtórzyć weryfikację podpisów tak jak w zadaniu 4.
7. W plikach **DANE_A_XXXX.SIG** i **Dane_B_xxxx.SIG** zmienić dowolny jeden znak w swoim nazwisku.
8. Zweryfikować podpisy przy pomocy następujących poleceń, uruchamianych w oknie wiersza poleceń:

   gpg --verify **DANE_A_XXXX.SIG**
   gpg --verify **DANE_B_XXXX.SIG**

9. Skasować wszystkie pliki utworzone podczas realizacji ćwiczenia 4a. Korzystając z programu ***GPA*** usunąć wszystkie klucze wygenerowane i importowane w tym ćwiczeniu. Odinstalować program ***Thunderbird*** i pakiet ***Gpg4win***.