ZAKŁAD SYSTEMÓW ROZPROSZONYCH
Politechnika Rzeszowska

EKSPLOATACJA I BEZPIECZEŃSTWO SYSTEMÓW

Laboratorium 5:

Szyfrowanie danych w sieci – szyfry z kluczem publicznym. Oprogramowanie GnuPGP

Cel:

Celem ćwiczenia jest zapoznanie się z mechanizmem PGP

Zainstaluj oprogramowanie GnuPGP. W systemie Windows , uruchomić konsole tekstową i zmień katalog roboczy na *c:\GnuPG*

Wygenerowanie klucza

1. Wyygeneruj klucz o następujących parametrach:
    a. korzystając z algorytmu szyfrowania DSA i Elgamal,
    b. długości 3008 bitów
    c. ważność 10 tygodni
    d. nazwa i hasło dowolne
2. Wyświetlić listę kluczy

Eksportowanie i importowanie klucza publicznego

1. Wyeksportować klucz publiczny do pliku
2. Wymienić się kluczami z innym użytkownikiem – wysłać mailem wygenerowany klucz innemu użytkownikowi.
3. Zaimportować otrzymany klucz i wyświetlić listę posiadanych kluczy. Sprawdzić poprawność klucza (wygenerować „odcisk klucza” i sprawdzić z oryginałem)

Szyfrowanie wiadomości

1. Utworzyć w swoim domowym katalogu plik tekstowy o dowolnej treści, po czym zaszyfrować ten plik otrzymanym kluczem i odesłać nadawcy.
2. Za pomocą odpowiedniej komendy odszyfrować otrzymaną wiadomość.

Podpis cyfrowy

1. Utworzony plik podpisać cyfrowo i wysłać odbiorcy.
2. Otrzymany plik sprawdzić i odkodować.

Szyfrowanie symetryczne

1. Z wykorzystaniem szyfrowania symetrycznego zaszyfrować plik dowolnym hasłem poczym odesłać go drugiemu użytkownikowi.
2. Odkodować otrzymany plik.

Usuwanie kluczy

1. Usunąć wszystkie posiadane klucze
2. Usunąć wszystkie tworzone pliki

PGP

PGP jest oprogramowaniem, które w łatwy sposób pozwala na korzystanie ze współczesnych algorytmów kryptograficznych w celu zabezpieczenia korespondencji a także ochrony wszelkich innych danych w formie elektronicznej. Skrót PGP w języku angielskim rozwijamy jako ”Preety Good Privacy”, co w tłumaczeniu na nasz ojczysty język oznacza „Całkiem niezłą prywatność”. Śmiało można powiedzieć, że stopień prywatności oferowany przez PGP jest o wiele wyższy, niż mogło by to wynikać z samej nazwy.

1. Historia PGP

Pomysłodawcą PGP, którego ideą było udostępnienie wszystkim zainteresowanym możliwość łatwego korzystania ze zdobyczy kryptografii, był Philip Zimmermann. Pierwszą, powszechnie stosowaną wersją PGP było PGP 2.3a, które ukazało się w 1993 roku. W tej wersji (i we wszystkich aż do 5.0) zarządzanie kluczami odbywało się przy użyciu algorytmu RSA. Dodatkowo: IDEA - szyfr symetryczny, MD5 - funkcja jednokierunkowa (z powodzeniem stosowana obecnie do szyfrowania haseł systemów wielodostępnych). Maksymalna długość klucza RSA obsługiwanego przez tą wersje wynosiła 1024 bitów. Po drodze do wersji 2.5, w której dodano wiele nowych funkcji i poprawek a także możliwość generowania kluczy RSA o długości do 2048 bitów, miały miejsce liczne spory patentowe pomiędzy Zimmermannem a RSA DSI Inc. (własnością tej firmy była algorytm RSA). Potem ukazywały się kolejne wersje od 2.6 do 2.6.3, zmieniła się także licencja użytkowania. Od tej pory Massachusetts Institute Of Technology zajął się dystrybucją i ochroną prawną programu. Pojawiła się także wersja międzynarodowa, pozbawiona ograniczeń nakładanych na wersję amerykańską - używała szybszych algorytmów zachowując jednocześnie kompatybilność z wersjami 2.2 i 2.3. Ostatnia wersja z serii 2.x dostępna jest pod 7 systemów operacyjnych (Amiga, Atari, BeOS, Macintosh, MS-DOS, OS/2, Windows) oraz kilkadziesiąt systemów unixowych.
Mniej więcej w 1995 roku Zimmermann założył firmę o nazwie PGP Inc., której dumą była nowa wersja PGP 5.0 (w wersji PGP for Privacy i PGP Freeware - dostępne na platformy Windows, Macintosh, Unix). Właśnie w tej wersji dodano nowy algorytm kluczy DSS/Diffie Hellman, nowe szyfry 3DES i CAST oraz algorytmy służące do generowania funkcji skrótu (używane podczas podpisywania wiadomości, widać to na początku takiego listu jako ”Hash:”) - SHA-1 i RIPEMD-160. Zmiany te zostały spowodowane ograniczeniami patentowymi algorytmu RSA. Dotychczas używany algorytm funkcji skrótu MD5 (używany przy podpisywaniu kluczami RSA) miał zostać zastąpiony przez SHA-1 (tego używamy razem z kluczem DSS/Diffie Hellman).

Aby obejść przepisy eksportowe USA (ITAR), które uznają zaawansowane algorytmy szyfrujące do technik militarnych wykorzystano pewien uciążliwy acz skuteczny sposób. ITAR ogranicza eksport kodu takiego programu jedynie w formie elektronicznej. Drukowano zatem cały kod źródłowy PGP (14 opasłych tomów) na papierze i legalnie przewożono go przez granice. Następnie ok. 70 osób w Europie skanowało wszystkie strony, co zajmowało średnio 1000 godzin. Dzięki takim ”operacjom” będąc w Europie można było bez przeszkód korzystać z kolejnych wersji PGP, a wobec Zimmermanna nie mogły być wysuwane już żadne zarzuty o charakterze prawnym.

W grudniu 1997 roku firma PGP Inc została kupiona przez firmę Network Associates Inc. (NAI). Właśnie wtedy PGP zostało znacznie rozbudowane, pozwalając nie tylko na szyfrowanie poczty elektronicznej ale także na tworzenie szyfrowanych wirtualnych sieci prywatnych VPN (PGPnet, implementacja IPSec), obsługę systemu certyfikatów X.509 oraz szyfrowanie dysków

logicznych (PGPdisk). Najnowsze wersje PGP (serie 6.x i 7.x) dostępne są tylko na platformy Windows i Macintosh. Wersja 7.0.3 wprowadza także obsługę takich kluczy jak RSA V4 (długość do 4096 bitów) i ASE (Advanced Encryption Standard - jest to nowy algorytm NIST używający symetrycznego klucza o długości 256 bitów).

Philip Zimmermann opuścił NAI w lutym 2001 roku. Powodem była nowa polityka co do otwartości kodu programu, który w planach ma być udostępniany jedynie w części. Obecnie P. Zimmermann pracuje on w firmie Hush Communications a także asystuje w projektach realizowanych przez firmę Veridis. Utworzył także specjalne konsorcjum OpenPGP , które ma na celu ułatwienie autorom oprogramowania implementacji OpenPGP w ich projektach, a także będzie wyznaczało dalszy rozwój OpenPGP.

2. Opis działania programu GnuPGP

Poniższy opis powstał w oparciu o linuxową wersję – gpg, jednak poszczególne kroki odnoszą się do wszystkich programów wykorzystujących PGP – co najwyżej poszczególne operacje wykonuje się z wykorzystaniem GUI.

Aby wygenerować nowy klucz wydajemy polecenie na konsoli:
gpg --gen-key

Wyświetlenie listy posiadanych kluczy:
gpg --list-keys

Edytowanie kluczy:
gpg --edit-key [klucz]

Eksportu wybranego klucza dokonujemy poleceniem:
gpg --output [nazwa_pliku] --export [email-osoby]

Aby uzyskać klucz w postaci ASCII trzeba wykonać polecenie:
gpg -a --output [nazwa_pliku] --export [email-osoby]
Aby zaimportować do swojej bazy klucz trzeba użyć polecenia:
gpg --import [nazwa_pliku_z_kluczem]

Do szyfrowania informacji trzeba użyć poniższej komendy:
gpg --output zaszyfrowany.plik --encrypt --recipient adres@odbiorcy plik

Aby odszyfrować informacje trzeba użyć polecenie:
gpg --output odszyfrowany.plik --decrypt zaszyfrowany.plik

Do symetrycznego szyfrowania plików trzeba użyć poniższej komendy:
gpg --output zaszyfrowany.plik --symmetric plik.txt

Odszyfrowanie pliku:
gpg --output odszyfrowany.plik --decrypt zaszyfrowany.plik

Aby podpisać cyfrowo wiadomość należy użyć następującego polecenia:

gpg --output tekst.sig --sign tekst.txt

Do weryfikacji klucza i dekodowanie wiadomości należy użyć następującego polecenia
gpg --verify tekst.sig
gpg --output tekst.txt --decrypt tekst.sig