

# Bezpieczna poczta i PGP

Patryk Czarnik

Bezpieczeństwo sieci komputerowych – MSUI 2009/10

## Poczta elektroniczna – zagrożenia

- ▶ Niechciana poczta (spam)
- ▶ Niebezpieczna zawartość poczty
- ▶ Nieuprawniony dostęp (podśluch)
  - ▶ komunikacja między klientem a serwerem pocztowym
  - ▶ komunikacja między serwerami pocztowymi
  - ▶ poczta składowana na serwerze
  - ▶ poczta składowana u klienta
- ▶ Podszywanie się
  - ▶ w celu wydania nieuprawnionego polecenia, podpisania za kogoś umowy itp.
  - ▶ w celu wyciągnięcia informacji (*phishing*)

# Spam

- ▶ Niechciana poczta, rozsyłana zwykle w celach reklamowych.

## Możliwości ochrony

- ▶ ograniczenia prawne – m.in. w Polsce i generalnie UE
- ▶ filtry antyspamowe
  - ▶ serwer lub klient
  - ▶ „uczące się” lub korzystające z serwerów reguł
  - ▶ zagrożenie – usunięcie pożądaney wiadomości
- ▶ przyjmowanie tylko podpisanej poczty od zaufanych nadawców  
(ale czy na pewno o to chodzi w poczcie elektronicznej? . . . )

## Niebezpieczna zawartość poczty

- ▶ Wirusy, robaki itd.
- ▶ Zagrożenie szczególnie istotne kilka – kilkanaście lat temu.

## Możliwości ochrony

- ▶ filtry antywirusowe na serwerze lub u klienta
- ▶ ostrzeżenia lub blokady otwierania załączników w programach pocztowych
- ▶ mądrzejsi użytkownicy

# Nieuprawniony dostęp do poczty przechowywanej na serwerze/u klienta

## Możliwości ochrony

- ▶ standardowe mechanizmy systemowe ochrony plików i ochrony przed włamaniami
- ▶ przechowywanie poczty w postaci zaszyfrowanej (i ochrona klucza/hasła)
- ▶ szyfrowanie poczty przez nadawcę, deszyfrowanie przez odbiorcę (dotyczy dostępu na serwerze)

## Podśluchiwanie poczty w trakcie komunikacji

- ▶ Poczta narażona na podsłuch:
  1. między wysyłającym a jego serwerem pocztowym,
  2. w drodze między serwerami,
  3. między odbierającym a jego serwerem pocztowym.
- ▶ Można korzystać z transportu po TLS/SSL, jednak:
  - ▶ użytkownicy mają wpływ tylko na 1 i 3,
  - ▶ szyfrowana komunikacja (danych) między serwerami mailowymi jest rzadkością,
  - ▶ nie chroni to przed dostępem do treści w serwerach.
- ▶ Najpewniejszym zabezpieczeniem pozostaje działanie po stronie użytkownika (po obu stronach komunikacji) niezależne od serwerów pocztowych.

# Podszywanie się

## Podszywanie się pod nadawcę

- ▶ w celu zmylenia odbiorcy (*phishing* itp.)
- ▶ w celu wmówienia komuś, że wysłał wiadomość, której nie wysłał

## Możliwości ochrony

- ▶ uwierzytelnianie nadawcy w serwerze poczty (z punktu widzenia odbiorcy wymaga zaufania do serwera nadawcy)
- ▶ podpisywanie wiadomości przez nadawcę, weryfikowanie przez odbiorcę, w oparciu o kryptografię klucza publicznego (np. standard PGP)

# Systemy pochodzące od PEM

- ▶ PEM (*Privacy-enhanced Electronic Mail*):
  - ▶ propozycja IETF (początek lat 90-tych),
  - ▶ nigdy nie wprowadzona w życie,
  - ▶ istotna przeszkoda: założenie o scentralizowanym drzewie jednostek certyfikujących.
- ▶ MOSS (*MIME Object Security Services*):
  - ▶ standard IETF (RFC 1848), idee podobne do PGP i S/MIME, nie używany w praktyce.
- ▶ S/MIME (*Secure MIME*)...:

## S/MIME

- ▶ Idee podobne do PGP:
  - ▶ kryptografia klucza publicznego,
  - ▶ działania kryptograficzne na obu końcach.
- ▶ Specjalny typ MIME `application/pkcs7-mime` dla treści wiadomości.
- ▶ Weryfikacja klucza w CA (opcjonalna).
- ▶ Standard używany w praktyce (alternatywa dla PGP).

## System PGP — historia i status

- ▶ Autor: Phil Zimmermann.
- ▶ Pierwotne założenia:
  - ▶ najlepsze algorytmy szyfrowania,
  - ▶ integracja i ogólność, niezależność od systemu i procesora,
  - ▶ nieodpłatne udostępnienie pakietu, dokumentacji, kodu źródłowego,
  - ▶ (ponadto) wersja komercyjna,
  - ▶ sieć zaufania (*Web of Trust*) zamiast scentralizowanej hierarchii.
- ▶ Obecnie:
  - ▶ PGP – program komercyjny, opatentowane technologie,
  - ▶ standard IETF „Open PGP” opisany w RFC2440, nowe wersje PGP zgodne z tym standardem,
  - ▶ otwarta implementacja GPG (*GNU Privacy Guard*) oraz aplikacje innych firm,
  - ▶ obsługa także certyfikatów typu X.509 (hierarchicznych).

## System PGP — usługi i algorytmy

- ▶ Szyfrowanie komunikatu
  - ▶ asymetryczne: RSA, ElGamal
  - ▶ symetryczne: 3DES, CAST5, Blowfish, Twofish, i AES (128b, 192b i 256b)
- ▶ Sygnatura cyfrowa (RSA, DSA, ElGamal wraz z MD5, SHA-1, SHA-256, RIPEMD-160).
- ▶ Kompresja (ZIP lub ZLIB).
- ▶ Konwersja do ASCII (radix-64).
- ▶ Segmentacja (ograniczenia na długość listu).
- ▶ W PGP 3 wprowadzono wsparcie dla algorytmów CAST5, DSA i ElGamal, aby była możliwość używania nieopatentowanych technologii.

## System PGP — uwierzytelnienie

- ▶ Nadawca tworzy komunikat.
- ▶ Za pomocą MD5 generowany jest wynik haszowania.
- ▶ Wynik haszowania szyfruje się za pomocą RSA kluczem prywatnym nadawcy i dołącza na początku komunikatu.
- ▶ Odbiorca odszyfrowuje wynik haszowania kluczem publicznym nadawcy.
- ▶ Odbiorca generuje własny wynik haszowania i porównuje z odszyfrowanym wynikiem.

## System PGP — szyfrowanie

- ▶ Nadawca tworzy komunikat, a jego system losuje 128-bitową liczbę, która pełni rolę klucza sesji tylko dla tego komunikatu.
- ▶ Komunikat jest szyfrowany za pomocą algorytmu IDEA przy użyciu klucza sesji.
- ▶ Klucz sesji jest szyfrowany za pomocą algorytmu RSA kluczem jawnym odbiorcy i dołączany na początku komunikatu.
- ▶ Odbiorca za pomocą RSA i swego klucza prywatnego odszyfrowuje klucz sesji.
- ▶ Odbiorca za pomocą klucza sesji odszyfrowuje komunikat.

## System PGP — bezpieczeństwo szyfrowania

- ▶ System jest na tyle bezpieczny, na ile stosowane algorytmy są bezpieczne:
  - ▶ AES 256 – praktycznie nie łamalny,
  - ▶ SHA-256 – uważany za bezpieczny,
  - ▶ RSA – łamalność zależy od długości klucza.
- ▶ Stosuje się następujące klucze do RSA:
  - ▶ zwykłe (384 bity) – możliwe do złamania przy dużym wysiłku;
  - ▶ komercyjne (512 bitów) – możliwe do złamania przez wielkie globalne organizacje;
  - ▶ wojskowe (1024 bity) – powszechnie uważane za niełamalne.

## System PGP — kompresja

- ▶ Kompresja jest wykonywana po wygenerowaniu sygnatury, ale przed zaszyfrowaniem.
- ▶ Dlaczego po sygnaturze?
  - ▶ Komunikaty przechowywane są w postaci nieskompresowanej. Dobrze jest mieć jednocześnie pod ręką komunikat i jego sygnaturę.
  - ▶ Zmieniają się parametry algorytmów kompresji.
- ▶ Dlaczego przed szyfrowaniem?
  - ▶ Skompresowany komunikat ma większą entropię – trudniejsza jest kryptoanaliza.

## System PGP — klucze

- ▶ Rodzaje kluczy
  - ▶ Klucz sesji (IDEA / CAST).
  - ▶ Klucz jawny (RSA / DSA).
  - ▶ Klucz prywatny (RSA / DSA).
  - ▶ Klucz oparty na haśle (IDEA / CAST).
- ▶ Konieczny jest mechanizm bezpiecznego generowania kluczy sesji.
- ▶ Użytkownik może mieć wiele par kluczy jawny/prywatny – jedne są starsze, inne nowsze.
- ▶ Potrzebne jest repozytorium kluczy jawnych/prywatnych nadawcy i jawnych korespondentów.



## System PGP — generowanie kluczy

- ▶ Klucze sesji
  - ▶ Generowane za pomocą algorytmu ANSI X9.17
    - ▶ szyfrowanie IDEA,
    - ▶ dane 128 bitowy klucz,
    - ▶ 2 bloki 64-bitowe, które są szyfrowane.
  - ▶ Dane wejściowe – generator liczb pseudolosowych
  - ▶ Generator parametryzowany: napisem oraz odstępami czasowymi między stuknięciami w klawisze. Wynik łączy się z poprzednim wynikiem pracy IDEA.

## System PGP — identyfikatory kluczy

- ▶ Każdy klucz ma ID.
- ▶ ID są z dużym prawdopodobieństwem unikalne dla danego użytkownika.
- ▶ ID klucza jawnego to jego mniej znaczące 64 bity.
- ▶ (Sygnatury zawierają ID klucza jawnego.)

## System PGP — bazy kluczy

- ▶ Tabela z pozycjami:
  - ▶ Datownik,
  - ▶ ID klucza,
  - ▶ Klucz jawny,
  - ▶ Klucz prywatny,
  - ▶ ID użytkownika (e-mail lub inne).

## System PGP — szyfrowanie klucza prywatnego

- ▶ Użytkownik wybiera hasło do szyfrowania kluczy prywatnych.
- ▶ System prosi o podanie hasła.
- ▶ Na podstawie hasła za pomocą MD5 generowany jest 128-bitowy wyciąg.
- ▶ Hasło jest zapominane.
- ▶ System szyfruje klucz za pomocą algorytmu IDEA z wyżej obliczonym kluczem.
- ▶ Wyciąg jest kasowany, zaszyfrowany klucz wędruje do bazy.

## System PGP — zarządzanie kluczami jawnymi

Trzeba zapewnić, że klucze jawne są wiarygodne. Metody:

- ▶ Fizyczne uzyskanie klucza.
- ▶ Weryfikacja klucza przez telefon (można cały, można odcisk).
- ▶ Pobranie przez zaufanego pośrednika.
- ▶ Pobranie z jednostki certyfikującej.

## System PGP — certyfikaty

- ▶ Pierwsza wersja PGP używała „sieci zaufania” (*Web of trust*).
- ▶ Obecnie możliwe także korzystanie z hierarchicznej struktury jednostek certyfikujących.

## System PGP — wiarygodność klucza

- ▶ pole wiarygodności klucza,
- ▶ z pozycją w bazie związana jest lista sygnatur certyfikatu,
- ▶ pole zaufania sygnatury,
- ▶ pole zaufania właściciela.

## System PGP — struktura komunikatu

- ▶ ID klucza jawnego odbiorcy (*R64* – odtąd),
- ▶ Klucz sesji (*Szyfr RSA* – tylko to pole),
- ▶ Datownik (*ZIP+E+I* – odtąd),
- ▶ ID klucza jawnego nadawcy,
- ▶ Pierwsze dwa oktety wyciągu,
- ▶ Wyciąg (*Szyfr RSA* – tylko to pole),
- ▶ Nazwa pliku,
- ▶ Datownik,
- ▶ Dane (*E+I+ZIP+R64* – koniec).