

Bezpieczeństwo systemów komputerowych

Bezpieczeństwo poczty elektronicznej

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

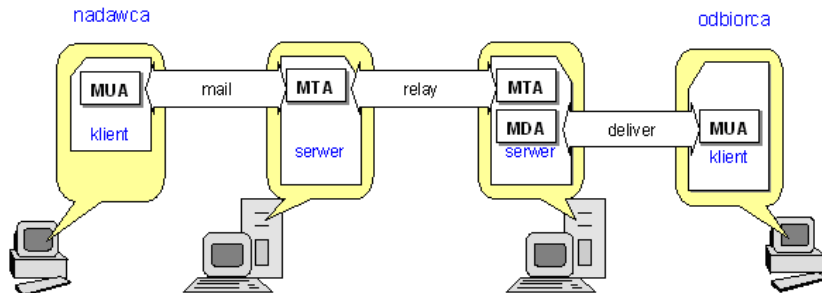
5 grudnia 2010

Wykorzystano materiały Michała Szychowiaka
z <http://wazniak.mimuw.edu.pl>

Poczta elektroniczna

- ▶ Jedna z najstarszych usług internetowych
- ▶ Jedna z dwóch najczęściej używanych usług

Model komunikacji



- ▶ Wykorzystuje protokoły SMTP, POP, IMAP.
- ▶ MUA – Mail User Agent
- ▶ MTA – Mail Transfer Agent
- ▶ MDA – Mail Delivery Agent

Podstawowe problemy bezpieczeństwa

- ▶ Niepożądane przesyłki (spam)
- ▶ Niebezpieczne załączniki (wirusy)
- ▶ Potwierdzanie dostarczenia
- ▶ Naruszanie poufności, integralności, autentyczności

Spam

- ▶ Pojęcie spam dotyczy ogółu niechcianych przesyłek pocztowych zajmujących zasoby pamięciowe (skrzynka pocztowa odbiorcy) i czasowe systemu.
- ▶ Ochrona antyspamowa sprowadza się do odfiltrowania takich przesyłek z całości ruchu pocztowego i może być realizowana na kilku poziomach modelu komunikacji.
- ▶ Na poziomie MTA filtracja jest dokonywana przez analizę adresu nadawcy:
 - ▶ czy jest weryfikowalny w DNS,
 - ▶ czy odpowiada rekordowi MX,
 - ▶ czy nie jest na czarnej liście,
 - ▶ czy można zweryfikować konto nadawcy za pomocą komendy VRFY protokołu SMTP (zwykle nie można).
- ▶ Zaletą jest oszczędność zasobów – odrzucamy spam na pierwszej linii obrony.
- ▶ Wadą jest mała precyzja, bo na tak wczesnym etapie posiadamy mało informacji do dyspozycji.

Spam, cd.

- ▶ Występuje duże prawdopodobieństwo pomyłki – sklasyfikowania niechcianej przesyłki jako pożądanej i odwrotnie.
- ▶ Stosunkowo dużą skuteczność i małe efekty uboczne (opóźnienie) wykazuje tu mechanizm znany jako szare listy (greylisting):
 - ▶ po odebraniu przesyłki MTA odsyła na adres nadawcy kod 452 (czasowa niedostępność) i czeka na powtórny transmisję;
 - ▶ automaty spammerskie z założenia nie retransmitują;
 - ▶ jako pożądane akceptowane są wszystkie retransmitowane listy.
- ▶ Na poziomie MDA stosuje się:
 - ▶ analizę heurystyczną (na podstawie przygotowanej bazy danych charakterystycznych),
 - ▶ analizę statystyczną (samouczące się filtry Bayesa).
- ▶ Klienci pocztowi MUA posiadają wbudowane narzędzia filtrujące, które pozwalają użytkownikowi klasyfikować wybrane listy jako spam.

Ochrona kryptograficzna poczty

- ▶ Tunelowanie za pomocą SSL/TLS:
 - ▶ SMTPS port 465,
 - ▶ IMAPS port 993,
 - ▶ POP3S port 995.
- ▶ Ochrona użytkownik – użytkownik (ang. end to end):
 - ▶ PEM – Privacy Enhanced Mail,
 - ▶ PGP – Pretty Good Privacy,
 - ▶ S/MIME – Secure MIME.
- ▶ Istnieje wiele kompleksowych systemów i standardów pocztowych wykorzystujących kryptografię:
 - ▶ X.400 MHS – Message Handling System,
 - ▶ EDI (EDIFACT X.435) – Electronic Data Interchange.

PEM

- ▶ Jeden z pierwszych standardów zaproponowanych do ochrony przesyłek protokołu SMTP
- ▶ Format zgodny z pierwotnymi wymaganiami, opisanymi w RFC 822
- ▶ Kontrola integralności przy wykorzystaniu MD2 lub MD5
- ▶ Opcjonalne szyfrowanie wiadomości za pomocą DES-ECB, 3DES
- ▶ Wsparcie dla zarządzania kluczami i certyfikatami wg ISO X.509
- ▶ Przykładowe implementacje: RIPEM, TIS-PEM
- ▶ Niewielka popularność

PEM, format wiadomości

From:
To:
Subject:
Date:

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 4, ENCRYPTED
Content-Domain: RFC822
* * * * *

Jdb%\$d+\$bnc/dsf=-905wn@dj~`fj^5%*dkf
nvkvkffMkjGUYgjw=\&uye flbv\
vj*7fd#mM>)ckcj`d[ff.dk>?
<"sd{dk{TR&+5@
* * * * *

-----END PRIVACY-ENHANCED MESSAGE-----

PEM, wysyłanie

► Wysyłanie

- konwersja komunikatu do postaci kanonicznej
 - tylko znaki z 7-bitowego ASCII
 - konwersja znaków końca wiersza na sekwencję CR, LF
 - wiersze nie dłuższe niż 1000 znaków
- podpisanie
- szyfrowanie (opcjonalne)
- konwersja do kodowania drukowalnego, Radix-64/Base64 (opcjonalna)

► Odbieranie

- konwersja do kodowania binarnego (opcjonalna)
- deszyfrowanie (opcjonalne)
- weryfikowanie podpisu
- konwersja komunikatu do kodowania lokalnego

PEM, klucze

- ▶ DEK (data encryption key) – jednorazowy klucz sesji dla algorytmów symetrycznych
- ▶ IK (interchange key) – symetryczny klucz wymiany lub para kluczy publiczny i prywatny
- ▶ Asymetryczne zarządzanie kluczami:
 - ▶ DEK – szyfruje tekst komunikatu i jego skrót;
 - ▶ IK – szyfruje DEK.
- ▶ Symetryczne zarządzanie kluczami:
 - ▶ DEK – szyfruje tekst komunikatu;
 - ▶ IK – szyfruje skrót komunikatu i DEK.

PEM, listy dyskusyjne

- ▶ Metoda jednego klucza IK na odbiorcę
 - ▶ tekst wiadomości jest szyfrowany wspólnym kluczem DEK;
 - ▶ dla każdego asymetrycznego klucza IK klucz DEK jest szyfrowany kluczem publicznym odbiorcy i włączany do nagłówka w polu odpowiedniego odbiorcy;
 - ▶ dla każdego symetrycznego klucza IK klucz DEK oraz skrót wiadomości są szyfrowane i włączane do nagłówka w polu odpowiedniego odbiorcy.
- ▶ Metoda jednego klucza IK na każdą listę – IK musi być znany wszystkim uczestnikom komunikacji.

PEM, certyfikaty kluczy publicznych, unieważnianie certyfikatów

- ▶ Nagłówek komunikatu może zawierać identyfikator nadawcy, instytucji wydającej klucz publiczny, identyfikator klucza, numer wersji, datę ważności.
- ▶ Nagłówek komunikatu może zawierać klucz publiczny wraz z certyfikatem.
- ▶ CRL (certificate revocation list) – lista unieważnień certyfikatów, jest opcjonalnie dołączana do komunikatu.

PGP

- ▶ Stworzono jako projekt akademicki prowadzony przez Phila Zimmermanna z MIT
- ▶ Wersje darmowe i komercyjne
- ▶ Wersja GnuPG dystrybuowana na licencji GNU
- ▶ Umożliwia:
 - ▶ podpisanie wiadomości,
 - ▶ zaszyfrowanie wiadomości,
 - ▶ kompresję,
 - ▶ zachowanie zgodności ze standardami poczty elektronicznej – przekształcanie do formatu ASCII (konwersja do Radix-64/Base64),
 - ▶ segmentację w celu ominięcia ograniczeń dotyczących maksymalnych rozmiarów.

PGP, uwierzytelnianie

- ▶ Alicja (nadawca) podpisuje wiadomość za pomocą swojego klucza prywatnego

$$h = E_{KS_A}(H(M)).$$

- ▶ Alicja wysyła skompresowaną konkatencję wiadomości i podpisu

$$C = Z(M \parallel h).$$

- ▶ Bob (odbiorca) dekompresuje otrzymaną wiadomość

$$(M, h) = Z^{-1}(C).$$

- ▶ Bob weryfikuje poprawność podpisu, używając klucza publicznego Alicji, sprawdza, czy

$$D_{KP_A}(h) = H(M)?$$

PGP, poufność

- ▶ Alicja szyfruje skompresowaną wiadomość za pomocą losowo wybranego klucza sesji

$$C = E_{K_S}(Z(M)).$$

- ▶ Alicja wysyła konkatencję klucza sesji, zaszyfrowanego kluczem publicznym Boba, i szyfrogramu

$$E_{K_{P_B}}(K_S) \parallel C.$$

- ▶ Bob odszyfrowuje klucz sesji za pomocą swojego klucza prywatnego

$$K_S = D_{K_{S_B}}(E_{K_{P_B}}(K_S)).$$

- ▶ Bob deszyfruje i dekompresuje wiadomość

$$M = Z^{-1}(D_{K_S}(C)).$$

PGP, poufność i uwierzytelnianie

- ▶ Alicja podpisuje wiadomość, kompresuje ją i szyfruje

$$C = E_{K_S}(Z(M \parallel E_{K_{S_A}}(H(M)))).$$

- ▶ Alicja wysyła wiadomość

$$E_{K_{P_B}}(K_S) \parallel C.$$

- ▶ Bob odzyskuje klucz sesji

$$K_S = D_{K_{S_B}}(E_{K_{P_B}}(K_S)).$$

- ▶ Bob deszyfruje wiadomość wraz z podpisem

$$(M, h) = Z^{-1}(D_{K_S}(C)).$$

- ▶ Bob sprawdza, czy

$$D_{K_{P_A}}(h) = H(M)?$$

PGP, uwagi

- ▶ Do szyfrowania wiadomości używa się algorytmu symetrycznego, np. IDEA.
- ▶ Do podpisywania i szyfrowania klucza sesji używa się algorytmu asymetrycznego, np. RSA.
- ▶ Podpis generuje się przed kompresją, gdyż
 - ▶ umożliwia stosowanie niedeterministycznych algorytmów kompresji;
 - ▶ nie wymaga przechowywania lub wyliczania skompresowanej wersji wiadomości w celu weryfikacji.
- ▶ Aby uniknąć ataku powtórzeniowego, do wiadomości, przed jej podpisaniem, dodaje się datownik.

PGP, klucze

- ▶ Klucz sesji K_S jest
 - ▶ używany do szyfrowania wiadomości szyfrem symetrycznym;
 - ▶ generowany losowo;
 - ▶ używany tylko jeden raz.
- ▶ Klucz prywatny nadawcy KS_A jest używany do generowania podpisu.
- ▶ Klucz publiczny nadawcy KP_A jest używany do weryfikacji podpisu.
- ▶ Klucz publiczny odbiorcy KP_B jest używany do szyfrowania klucza sesji algorytmem asymetrycznym.
- ▶ Klucz prywatny odbiorcy KS_B jest używany do odszyfrowania klucza sesji.
- ▶ Klucz oparty na haśle jest używany do szyfrowania algorytmem symetrycznym lokalnie przechowywanych kluczy prywatnych.

PGP, identyfikatory kluczy

- ▶ Pary kluczy prywatny i publiczny należy okresowo zmieniać.
- ▶ Można odebrać wiadomość używając klucza, którego termin ważności właśnie upłynął.
- ▶ Można chcieć używać różnych par kluczy z różnymi osobami.
- ▶ Odbiorca musi wiedzieć, którego klucza publicznego użyto.
- ▶ Identyfikator pary kluczy to 64 najmniej znaczących bitów klucza publicznego.
- ▶ Identyfikatory kluczy są przesyłane wraz z wiadomościami.

PGP, przechowywanie kluczy

▶ Baza kluczy prywatnych

- ▶ przechowuje pary kluczy publiczny/prywatny należące do lokalnego użytkownika;
- ▶ rekord zawiera:
 - ▶ datownik,
 - ▶ identyfikator pary kluczy (64 najmniej znaczące bity klucza publicznego),
 - ▶ klucz publiczny,
 - ▶ zaszyfrowany klucz prywatny,
 - ▶ identyfikator użytkownika.

▶ Baza kluczy publicznych

- ▶ przechowuje klucze publiczne innych użytkowników;
- ▶ rekord zawiera:
 - ▶ datownik,
 - ▶ identyfikator klucza (64 najmniej znaczące bity),
 - ▶ klucz publiczny,
 - ▶ identyfikator użytkownika.

PGP, zarządzanie kluczami publicznymi

- ▶ Jak nabrać przekonania o autentyczności klucza publicznego?
- ▶ Uzyskać go bezpośrednio od właściciela, bez przesyłania przez sieć.
- ▶ Zweryfikować klucz lub jego odcisk palca przez telefon.
- ▶ Uzyskać sygnowany certyfikat od zaufanej osoby.
- ▶ Uzyskać sygnowany certyfikat od instytucji certyfikującej.

PGP, poziomy zaufania

- ▶ OWNERTRUST – poziom zaufania przypisywany przez użytkownika każdemu właścielowi klucza publicznego
 - ▶ nieokreślony poziom zaufania
 - ▶ nieznany użytkownik
 - ▶ zwykle nie obdarzany zaufaniem jako sygnujący inne klucze
 - ▶ zwykle obdarzany zaufaniem jako sygnujący inne klucze
 - ▶ zawsze obdarzany zaufaniem jako sygnujący inne klucze
 - ▶ nieograniczone zaufanie
- ▶ SIGTRUST – poziom zaufania sygnatury certyfikującej dany klucz publiczny, kopia pola OWNERTRUST osoby sygnującej
- ▶ KEYLEGIT – poziom wiarygodności klucza, obliczany przez PGP
 - ▶ poziom zaufania nie znany lub nie zdefiniowany
 - ▶ brak zaufania co do własności klucza
 - ▶ ograniczone zaufanie co do własności klucza
 - ▶ pełne zaufanie co do własności klucza

PGP, obliczanie poziomu wiarygodności klucza

- ▶ Jeśli co najmniej jedna sygnatura ma w polu SIGTRUST nieograniczone zaufanie, kluczowi przypisuje się pełne zaufanie.
- ▶ W p.p. oblicza się średnią ważoną z liczby certyfikatów od osób zwykłe i zawsze obdarzanych zaufaniem.
- ▶ Jeśli obliczona wartość osiągnie co najmniej 1, klucz obdarza się pełnym zaufaniem.

PGP, unieważnianie kluczy publicznych

- ▶ Odbywa się przez wydanie przez właściciela sygnowanego przez siebie certyfikatu unieważnienia klucza.
- ▶ Taki certyfikat powinien być rozpowszechniony możliwie szybko i do jak największej liczby odbiorców.
- ▶ Agresor, któremu udało się poznać klucz prywatny, również może wydać taki certyfikat, ale zwykle nie ma w tym żadnego interesu.

S/MIME

- ▶ Secure/Multipurpose Internet Mail Extensions
- ▶ Integruje kryptografię z kluczem publicznym (szyfrowanie i podpisywanie) z mechanizmami MIME obsługi załączników.
- ▶ Pierwotna wersja została opracowana przez RSA Data Security Inc.
- ▶ Integracja z PKI
- ▶ Protokoły PGP/MIME i OpenPGP/MIME

Problemy

- ▶ Klienci pocztowe korzystające z przeglądarki internetowej (ang. webmail clients):
 - ▶ klucz prywatny musi być przekazany do kodu wykonywanego przez przeglądarkę;
 - ▶ dostęp do skrzynki pocztowej z dowolnego komputera wymaga, aby klucz prywatny był przechowywany w serwerze;
 - ▶ możliwość przechwycenia jawnej postaci wiadomości przy przesyłaniu z serwera do przeglądarki.
- ▶ Szyfrowanie załączników, oprócz pożądaných informacji, ukrywa także złośliwe oprogramowanie (ang. malware), uniemożliwiając skanowanie poczty w bramach pocztowych (ang. mail gateway).
- ▶ Oprogramowanie list dyskusyjnych notorycznie zmienia tekstową część wiadomości, unieważniając jej podpis.