Bezpieczeństwo poczty elektronicznej

Główne zagadnienia wykładu

Bezpieczeństwo systemów informatycznych

Bezpieczeństwo poczty elektronicznej

Bezpieczna poczta elektroniczna

- Bezpieczeństwo wewnętrzne
  - Poufność korespondencji
  - Spójność korespondencji
  - Dostępność przesyłki i systemu pocztowego
  - Niezaprzeczalność autorstwa
- Bezpieczeństwo zewnętrzne

Bezpieczeństwa systemu przekazywania poczty

<u>Zagrożenia wymierzone w poufność korespondencji</u>

- Podsłuch w sieci
- Podgląd korespondencji podczas jej obsługi przez system pocztowy
- Podgląd informacji w skrzynce pocztowej odbiorcy
- Możliwość ujawnienia informacji podczas działania klientów pocztowych
- Atak kryptoanalityczny na zawartość przesyłki

Bezpieczeństwa systemu przekazywania poczty

<u>Zagrożenia wymierzone w spójność przesyłki</u>

- Robaki internetowe oraz wirusy rozpowszechniane poprzez pocztę elektroniczną
- Modyfikacja korespondencji poprzez zmianę treści wiadomości na jednym z serwerów
- Darmowe serwisy obsługujące pocztę elektroniczną

Bezpieczeństwa systemu przekazywania poczty

<u>Zagrożenia umożliwiające manipulację autorstwem przesyłki</u>

- Brak wymagania autoryzacji użytkownika podczas wysyłania korespondencji
  - Rozsyłanie tzw. spamu
  - Wysyłanie tzw. bomb pocztowych
  - Zapisywanie ofiary do wielu list dyskusyjnych
- Ataki na narzędzia kryptograficzne do tworzenia podpisów cyfrowych
- Fałszowanie poczty przy użyciu błędów w programach pocztowych

Bezpieczeństwa systemu przekazywania poczty

Zagrożenia dla dostępności przesyłki lub systemu pocztowego

- Brak systemu podtrzymywania napięcia
- Ataki typu „odmowa usługi”
- Spowolnienie działania systemu w skutek zbytniego obciążenia zasobów
- Przerwy w działaniu systemu operacyjnego

Zbigniew Suski BSI – bezpieczeństwo poczty 6

Zagrożenia bezpieczeństwa „*na zewnątrz*”

- Ataki aktywną zawartością (*active content attacks*)
- Ataki przepełnienia buforu (*buffer overflow attacks*)
- Konie trojańskie (*Trojan horse attacks*)
- Ataki z wykorzystaniem skryptów powłoki (*shell script attacks*)
- Ataki w oparciu o błąd sieci (*web bug privacy attack*)

Zbigniew Suski BSI – bezpieczeństwo poczty 7

Inne zagrożenia

- Ataki z wykorzystaniem luk w agentach przesyłania poczty
- Podawanie się za przełożonego lub administratora
- Atak na prywatność adresu pocztowego użytkowników
- Zagrożenia związane z protokołem POP3
- Zagrożenia związanie z protokołem IMAP4
- Zagrożenia związane z protokołem SMTP

Zbigniew Suski BSI – bezpieczeństwo poczty 8

Zagrożenia związane z protokołem SMTP

- Brak szyfrowania
- Brak autoryzacji nadawcy przy wysyłaniu
- Brak kontroli spójności przesyłki na poziomie transportowym
- Polecenia RCPT, VRFY, EXPN, HELP

Zbigniew Suski BSI – bezpieczeństwo poczty 9

Pretty Good Privacy (PGP)

- Poufność
- Uwierzytelnienie źródła
- Integralność (spójność) wiadomości
- Niezaprzeczalność nadania
- Zarządzanie kluczami
  - IDEA – szyfrowanie danych
  - RSA – zarządzanie kluczami
  - MD5 i RSA – spójność i podpisy cyfrowe

Zbigniew Suski BSI – bezpieczeństwo poczty 10

Pretty Good Privacy (PGP)

- Opcjonalny podpis cyfrowy
- Kompresja
- Opcjonalne szyfrowanie
- Opcjonalne kodowanie do transmisji

Zbigniew Suski BSI – bezpieczeństwo poczty 11

Privacy Enhanced Mail (PEM)

- RFC 1421
- RFC 1422
- RFC 1423
- RFC 1424

- Poufność
- Uwierzytelnienie źródła
- Integralność (spójność) wiadomości
- Niezaprzeczalność nadania
- Zarządzanie kluczami

Privacy Enhanced Mail (PEM)

- Typy wiadomości:
  - MIC-CLEAR
  - MIC-ONLY
  - ENCRYPTED
- Standaryzacja (kanonizacja)
- Zapewnienie integralności i wstawienie podpisu
- Opcjonalne szyfrowanie.
- Opcjonalne kodowanie do transmisji

Mechanizmy ochronne

- Ochrona przed utratą poufności przesyłki
  - Bezpieczna topologia
  - Szyfrowanie
  - Produkty wykrywające programy podsłuchujące
- Zapewnianie spójności przesyłki
  - Oprogramowanie umożliwiające generowanie i sprawdzanie sum kontrolnych - *md5sum, sum*
  - *Program ccrypt* i inne programy szyfrujące
  - Stosowanie oprogramowania antywirusowego
  - Stałe wiązanie adresów MAC

Mechanizmy ochronne

- Ochrona przed „*niechcianą*” pocztą
  - *Procmail*
  - Restrykcje w przekazywaniu poczty
  - Bazy RBL
  - Programy *Advanced E-mail Protector, Spam Exterminator, EmC* itp.
  - *Mailfilter*
  - *Sam Spade*
  - *BombSquad, MailDeleter*

Mechanizmy ochronne

- Ochrona przed atakami zagrażającymi dostępności systemu pocztowego
- Ochrona przed atakami wyprowadzanymi poprzez system pocztowy
  - Oprogramowanie antywirusowe
  - *Procmail sanitizer*
  - Uaktualnianie oprogramowania i staranna konfiguracja
  - Niestandardowe oprogramowanie i niestandardowe instalacje