Bezpieczeństwo poczty elektronicznej

Mariusz Goch

Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

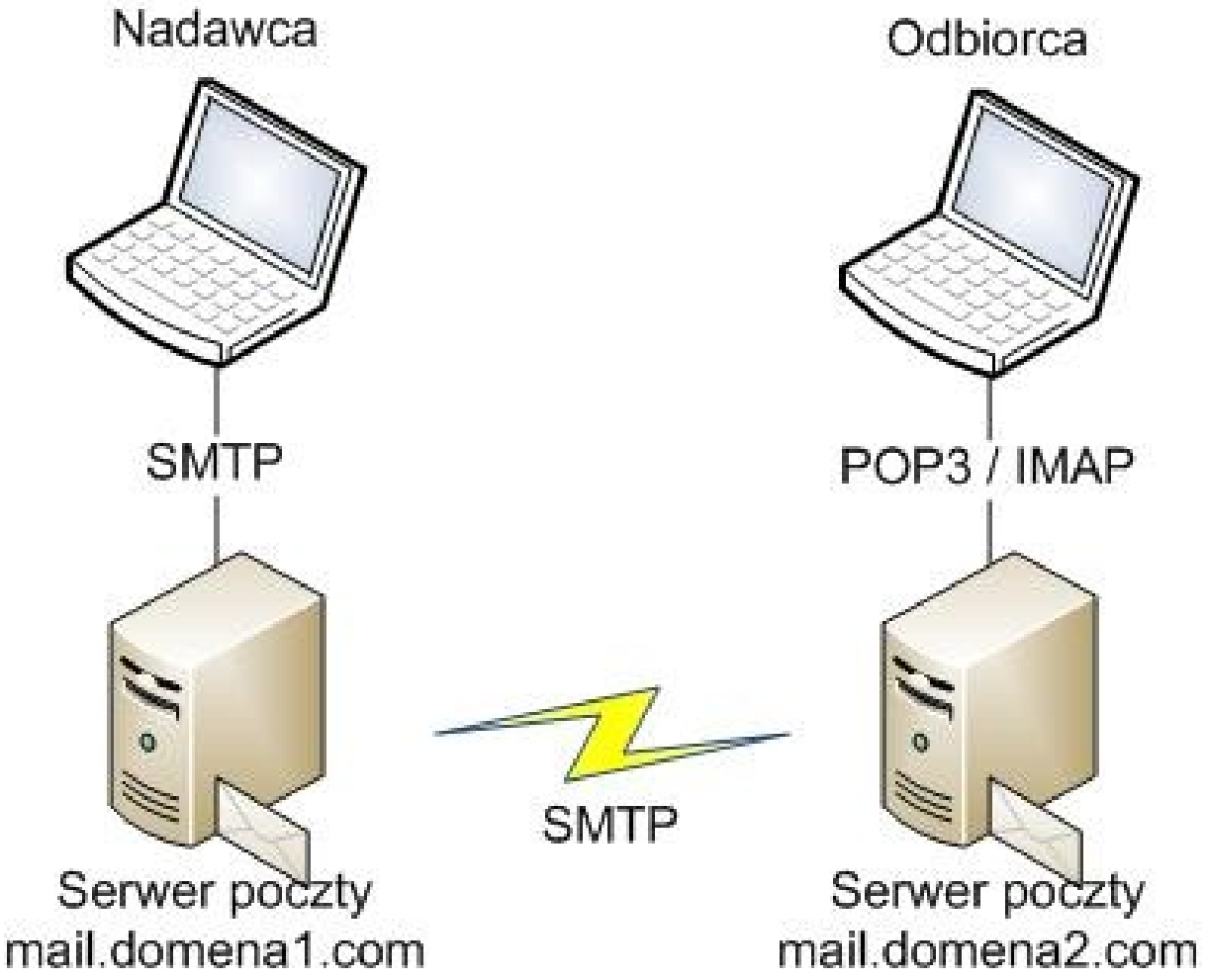
Plan prezentacji

- Bezpieczeństwo transportu wiadomości
- Problemy serwera pocztowego
- Niechciana poczta

Transport wiadomości

- Przesyłanie wiadomości
- Protokół SMTP
- Protokoły POP3/IMAP

Przesyłanie wiadomości



Protokół SMTP

- Simple Mail Transfer Protocol
- Komunikacja pomiędzy klientem poczty a serwerem
- Komunikacja pomiędzy serwerami
- Czy wymagać uwierzytelnienia, a jeśli tak to od kogo?

Protokół SMTP

```
220 test.com ESMTP Easy.Server
EHLO dom
250-test.com
250-PIPELINING
250-SIZE 22000000
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-AUTH=LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-8BITMIME
250 DSN
AUTH LOGIN
334 VXNlcm5hbWU6                          [Username:]
cG9jenRhQHRlc3QuY29tCg==                [poczta@test.com]
334 UGFzc3dvcmQ6                          [Password:]
dGVzdAo=                                        [test]
235 2.0.0 Authentication successful
```

Protokół SMTP

```
MAIL FROM:<poczta@test.com>
250 2.1.0 Ok
RCPT TO:<poczta@test2.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Wiadomość
.
250 2.0.0 Ok: queued as 723F62090F1
QUIT
221 2.0.0 Bye
```

Uwierzytelnianie w protokole SMTP

- PLAIN
  - Jeden komunikat (base64):

    base64('authid', 0, 'userid', 0, 'password')
- LOGIN
  - Oddzielnie login i hasło (base64)
- Base64 – kodowanie umożliwiające zapis danych binarnych w formie znaków drukowanych
- Brak zabezpieczenia przed podsłuchem

Uwierzytelnianie w protokole SMTP

- CRAM-MD5
  - Bazuje na funkcji haszującej MD5
  - Serwer generuje losowy ciąg bajtów
  - Klient tworzy odpowiedź na podstawie funkcji XOR i MD5 na znanym haśle i otrzymanym ciągu znaków
- DIGEST-MD5
  - Dokonuje uwierzytelnienia nie tylko klienta, ale i serwera

Zabezpieczenie przed posłuchem

- Szyfrowanie komunikacji poprzez TLS - Transport Layer Security
- Komenda STARTTLS po przywitaniu

```
STARTTLS
220 2.0.0 Ready to start TLS
```

- Szyfrowanie zarówno komunikacji z klientem poczty jak i pomiędzy serwerami
- Komunikacja cały czas poprzez port 25

Protokoły POP3/IMAP

- Oddzielne usługi serwera
- Wiadomości pobierane bezpośrednio z dysku serwera
- Metody uwierzytelniania podobne jak w SMTP
- Można niezależnie uruchomić usługi z szyfrowaniem połączenia SSL
- Porty:

POP3 – 110	POP3S – 995
IMAP – 143	IMAPS – 993

Protokół POP3

- Komendy:
  - **AUTH** – wybór sposobu uwierzytelniania
  - **USER** – identyfikator użytkownika
  - **PASS** – hasło
  - **LIST** – pobierz listę wiadomości
  - **RETR** – pobierz wiadomość
  - **DELE** – usuń wiadomość
  - **QUIT** – koniec

Zagrożenia transportu wiadomości

- Podsłuch hasła dostępowego do skrzynki
- Podsłuchanie treści wiadomości
- Modyfikacja wiadomości

Problemy serwera pocztowego

- OpenRelay
- Kontrola podanych adresów
- Weryfikacja nadawców
- Konta systemowe
- Odporność na awarie

OpenRelay

- Serwer pocztowy niezabezpieczony przed nieautoryzowanym dostępem
  - Rozsyłanie spamu
  - Podszywanie się
- Wymuszenie uwierzytelniania przed wysłaniem wiadomości
- Blokada przekazywania wiadomości
  - Odblokowanie tylko dla znanych serwerów wspólnie realizujących obsługę poczty

Kontrola podanych adresów

- Kontrola komend protokołu SMTP:
  - **MAIL FROM**
  - **RCPT TO**
- Poprawność podanych adresów

  FQDN - Fully Qualified Domain Name
- Zgodność z danymi podanymi w trakcie uwierzytelniania

Weryfikacja nadawcy

- Odnalezienie serwera nadawcy (na podstawie danych w DNS)
- Komunikacja z serwerem i próba wysłania wiadomości do nadawcy
- Gdy serwer nadawcy przyjmie wiadomość testową, zakończenie połączenia i akceptacja wiadomości
- Operacja kosztowna
- Cachowanie wyników

Konta systemowe

- Skrzynka pocztowa = Konto pocztowe ??
- Wirtualne skrzynki pocztowe:
  - Informacje o kontach w bazie danych
  - Ograniczenie dostępu do systemu
  - Możliwość utrzymywania poczty z wielu domen na pojedynczym serwerze

Odporność na awarie

- Podstawowe lekarstwo na awarie – redundancja
- Za pomocą rekordów MX w DNS można ustawić wiele serwerów SMTP
- Awaria głównego serwera uniemożliwia odbiór wiadomości poprzez POP3/IMAP
- Ustawienie bramki pocztowej
  - Wiadomości trzymane poza serwerem odpowiedzialnym za komunikacje z resztą sieci

Niechciana poczta

- Rodzaje niepożądanej poczty
- Filtry antyspamowe i antywirusowe
- RBL
- Greylist

Rodzaje niepożądanej poczty

- Wirusy, exploity
- Spam
- Ataki Denial of Service - DoS

Filtry antyspamowe i antywirusowe

- Lokalna kontrola wiadomości
- Analiza sygnatur
  - Blokowanie słów kluczowych
- Analiza heurystyczna
- Filtrowanie załączników

RBL

- RBL – Realtime Blackhole Lists
- Globalne bazy danych o hostach podejrzanych o rozsyłanie spamu
- Dane udostępniane poprzez DNS
  - Adres IP: a.b.c.d
  - Zapytanie o rekord TXT: d.c.b.a.serwer.list.rbl.

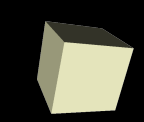
Greylist

- Wysłanie pojedynczego spamu nie jest ponawiane
- Serwer pocztowy zrywa połączenie za pierwszym razem i zapisuje sygnaturę listu
- Jeśli wysyłka zostanie ponowiona serwer zaakceptuje wiadomość
- Wprowadza opóźnienie w dostarczeniu przesyłki

Literatura

- Ralf Hildebrandt, Patrick Koetter

  „The Book of Postfix”



Dziękuję za uwagę

Pytania?