Metody uwierzytelniania nadawców w protokole SMTP

Seminarium: Protokoły komunikacyjne
dr Sławomir Lasota, dr hab. Jerzy Tyszkiewicz
[1000-2D02PK], SOCRATES: 11304

2006-02-28

Tomasz Andrzej Nidecki
tomasz.nidecki@students.mimuw.edu.pl
nr indeksu 136413

Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Plan ogólny referatu

- Jedna z najpoważniejszych wad protokołu SMTP: brak uwierzytelnienia nadawcy.
- Zagrożenia i nadużycia związane z brakiem uwierzytelnienia nadawcy.
- Proponowane metody rozszerzenia protokołu SMTP o uwierzytelnienie nadawcy.
- Opis zasad działania SPF.
- Opis zasad działania DKIM.
- Opis zasad działania CSV.
- Opis zasad działania Sender ID.
- Problemy i ograniczenia związane ze stosowaniem mechanizmów uwierzytelnienia nadawcy oraz metody ich rozwiązania.
- Czy warto stosować uwierzytelnienie nadawcy?

Brak uwierzytelnienia nadawcy w protokole SMTP

- Protokół SMTP w podstawowej formie nie uwzględnia żadnego mechanizmu uwierzytelnienia nadawcy (RFC 2821).
- Rozszerzenie ESMTP (RFC 2554) wprowadza uwierzytelnienie nadawcy, ale jest ono przeznaczone tylko do relayowania poczty.
- Nadal brak żadnych mechanizmów gwarantujących, że adres i dane nadawcy są prawdziwe.
- Budowa protokołu SMTP uniemożliwia wprowadzenie uwierzytelnienia każdego nadawcy w oparciu o login i hasło, ponieważ SMTP jest również wykorzystywane do komunikacji między serwerami.
- Sytuacja patowa: wymaga rozszerzenia lub poważnej zmiany protokołu, albo uwierzytelnienia w treści.

Brak uwierzytelnienia nadawcy w protokole SMTP

```
< 220 server.com ESMTP
> HELO host.com
< 250 server.com

> MAIL FROM: <nobody@nowhere.com>
< 250 ok

> RCPT TO: <someone@server.com>
< 250 ok
> DATA
< 354 go ahead

> From: Nobody <nobody@nowhere.com>
> Subject: Test
>
> This is a test
> .
< 250 ok 1140874002 qp 10140
```

- Na żadnym etapie komunikacji SMTP nie ma konieczności uwierzytelnienia adresu ani danych nadawcy.
- Na etapie HELO nie jest sprawdzana poprawność nazwy domenowej.
- Na etapie MAIL FROM adres nie jest weryfikowany.
- Na etapie nagłówków wiadomości adres również nie jest weryfikowany (i może być różny od MAIL FROM).
- Jedynym wymaganiem może być, by adres RCPT TO należał do domeny lokalnej serwera.

Nadużycia związane z brakiem uwierzytelnienia

- Brak uwierzytelnienia prowadzi do wielu nadużyć:
  - Brak jakiejkolwiek pewności, że list pochodzi od osoby, za którą podaje się nadawca.
  - Phishing — podszywanie się pod instytucje finansowe.
  - Joe-job — zrzucanie winy za nadużycia (np. spam) na kogoś innego.
  - Możliwość wykorzystania nieistniejących, przypadkowych adresów przy rozsyłaniu spamu i wirusów.
  - Uwiarygodnienie wirusów przez stosowanie istniejących adresów z książki adresowej ofiary.
- Brak uwierzytelnienia jest podstawą większości problemów występujących obecnie przy stosowaniu poczty elektronicznej.

Rozszerzenia protokołu SMTP — uwierzytelnienie

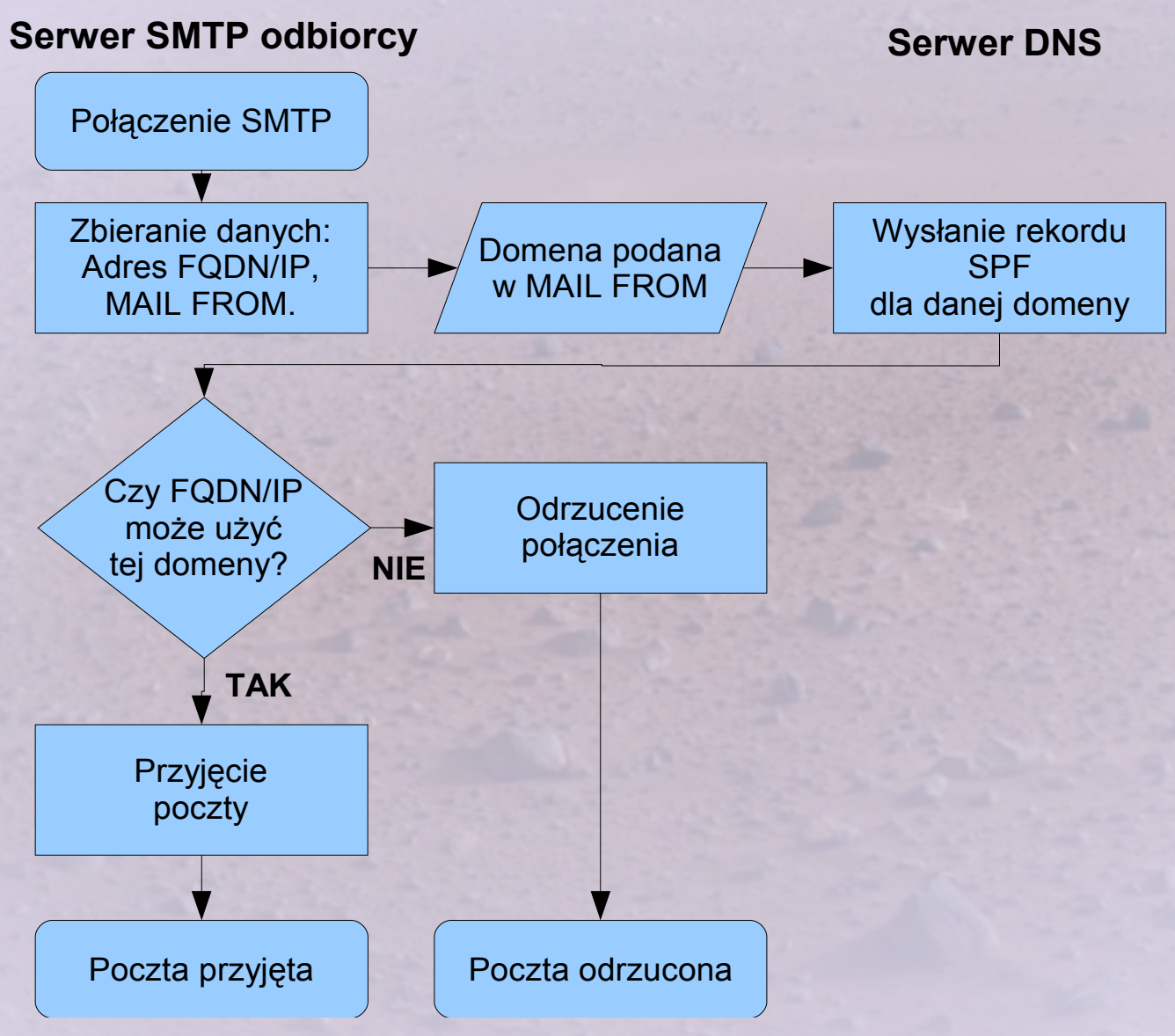
- **SPF — Sender Policy Framework**
  - **Uwierzytelnia tylko adres MAIL FROM.**
  - Sprawdza, czy e-mail przychodzący z danego serwera pocztowego może stosować określoną nazwę domenową w MAIL FROM. Opiera się na infrastrukturze DNS oraz rekordach TXT.
- **DKIM — DomainKeys Identified Mail**
  - **Uwierzytelnia treść i niektóre nagłówki wiadomości.**
  - Opiera się na cyfrowym podpisywaniu treści wiadomości i części nagłówków (podpis w oddzielnym nagłówku) oraz infrastrukturze DNS do dystrybucji kluczy publicznych.
  - Powstał z połączenia Yahoo! DomainKeys i Cisco Identified Internet Mail.
- **CSV — Certified Server Validation**
  - **Uwierzytelnia tylko parametr polecenia HELO/EHLO.**
  - Określa poziom zaufania przy połączeniu nadchodzącym z innego MTA na podstawie jego adresu IP oraz parametru polecenia HELO lub EHLO. Stosuje infrastrukturę DNS oraz rekordy SRV.
- **Microsoft Sender ID**
  - **Uwierzytelnia MAIL FROM oraz From.**
  - Syntaktycznie zgodny z SPF. Rozszerza użycie SPF do nagłówków From:.
  - Oparty na SPF oraz propozycji Microsoftu z 2004 r.: *Caller ID for E-Mail*.

Rozszerzenia protokołu SMTP — uwierzytelnienie

Rozszerzenia umożliwiające uwierzytelnianie w protokole SMTP działają na różnych poziomach:

Poziom	Parametr	Podstawa	Mechanizm
Łączący się host	Warstwa IP	Sieć IP	
Łączący się MTA	Warstwa IP	Adres IP	
Administrator MTA	HELO/EHLO	Domena	CSV
Pośrednik MTA	Received:	Domena	
Nadawca	MAIL FROM	E-mail/Domena	SPF
Nadawca	From:	E-mail/Domena	Sender ID, DKIM (DomainKeys)
Autor	Autor treści	E-mail/Domena	DKIM (IIM)

SPF — Sender Policy Framework



SPF — Sender Policy Framework

- Rekordy SPF dla danej domeny publikowane są przez serwer DNS dla tej domeny.
- Rekordy SPF publikowane są w postaci rekordów TXT (IN TXT w BIND).
- Przykładowe rekordy SPF:
  - `V=spf1 a:example.com -all`
    IP z rekordu A dla example.com ma prawo do domeny example.com (a:example.com), pozostałe mają być odrzucone (-all).
  - `V=spf1 mx ~all`
    IP z rekordu MX dla aktualnej domeny ma prawo do tej domeny (mx), pozostałe mają być odrzucone tymczasowo (~all).
  - `V=spf1 +all`
    Wszyscy mają prawo korzystać z aktualnej domeny (+all).
- Sposób reakcji jest sugerowany (decyzja po stronie serwera MTA, również w wypadku braku rekordu).
- Pełna specyfikacja formatu rekordów SPF: *http://www.openspf.org/mechanisms.html*

SPF — Sender Policy Framework

- Sender Policy Framework jest najbardziej rozpowszechnionym mechanizmem:
  - stosowany przez np. AOL,
  - stosowany przez większość polskich portali (np. WP, Interia),
  - większość znanych domen publikuje rekordy w DNS.
- Zdecydowana większość (liczbowa) domen nie ma rekordów SPF.
- W przypadku braku rekordu SPF do serwera MTA należy decyzja, czy mimo to przyjąć list, czy też go odrzucić.
- Odrzucanie listów z domen bez rekordów SPF może spowodować odrzucanie większości poczty.
- Nowa wersja SPF zwana SPF Classic (z czerwca 2005 r.) obejmuje ochroną dodatkowo parametr HELO.

DKIM — DomainKeys Identified Mail

- Właściciel domeny publikuje w serwerze DNS klucz publiczny dla tej domeny.
- E-mail (treść i część nagłówków) wychodzący z serwera mającego prawo do wysyłania listów z danej domeny jest podpisywany odpowiednim dla tej domeny kluczem prywatnym (na poziomie MTA).
- Podpis jest dołączany w dodatkowym nagłówku DKIM-Signature:.
- Odbiorca listu (MTA) pobiera z serwera DNS klucz publiczny dla domeny podanej w nagłówku From:.
- Odbiorca weryfikuje prawidłowość podpisu zawartego w nagłówku DKIM-Signature w oparciu o klucz publiczny z DNS.

DKIM — DomainKeys Identified Mail

- Przykładowa zawartość nagłówka DKIM-Signature:

```
DKIM-Signature: a=rsa-sha1; q=dns;
d=example.com;
i=user@eng.example.com;
s=jun2005.eng; c=relaxed;
t=1117574938; x=1118006938;
h=from:to:subject:date;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
  av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- Znaczenie poszczególnych pol:
  - a — użyty algorytm (hash SHA1 zaszyfrowany RSA),
  - q — zapytanie kierować do serwera DNS,
  - d — uwierzytelniana domena,
  - i — właściciel klucza,
  - s — poddomena w której przechowywane są rekordy (jun2005.eng._domainkey.example.com),
  - c — kanonizacja (usuwanie znaków pustych, konwersja wielkości liter itp.),
  - t,x — znaczniki czasowe (podpisu i ważności),
  - h — uwzględniane (podpisane) nagłówki
  - b — właściwy podpis

DKIM — DomainKeys Identified Mail

- DKIM nie jest tak rozpowszechnione, jak SPF, ale koncepcję wspierają firmy takie jak: AOL, Cisco, EBay, PayPal, Habeas, IBM, PGP, Verisign czy Yahoo!
- Mechanizm został stworzony w oparciu o projekt Cisco (IIM) i Yahoo (DomainKeys).
- W IETF powstała grupa robocza DKIM, a więc mechanizm jest na drodze do standaryzacji.
- Więcej informacji o DKIM można uzyskać pod adresami:
  http://mipassoc.org/dkim/index.html
  http://mipassoc.org/dkim/specs/draft-allman-dkim-base-01.html
  http://antispam.yahoo.com/domainkeys

CSV — Certified Server Validation

- Bardzo prosty mechanizm stworzony do uwierzytelniania nie nadawcy lub treści listu, lecz jedynie serwera SMTP z którego nadchodzi połączenie.
- CSV opiera się na trzech metodach, by sprawdzić, czy serwer SMTP z którego nadchodzi połączenie jest wiarygodny:
  - Porównanie IP łączącego się serwera do IP uzyskanego z DNS w wyniku zapytania o parametr (FQDN) polecenia HELO lub EHLO.
  - Uzyskanie z serwera DNS odpowiedzialnego za domenę podaną jako parametr polecenia HELO/EHLO wpisu SRV (RFC 2782) informującego, czy dany IP ma prawo przedstawiać się jako ta domena.
  - Uzyskanie od ewentualnych stron trzecich potwierdzenia, że podana domena jest wiarygodna (np. nie należy do spamera).
- Na podstawie wyników uzyskanych za pomocą tych trzech metod, serwer określa poziom wiarygodności i w zależności od niego podejmuje dalsze decyzje.

CSV — Certified Server Validation

- CSV może być zaimplementowane wspólnie z dwoma innymi mechanizmami: CSA i DNA:
  - CSA (Client SMTP Authentication) posługuje się rekordami SRV, aby określić, czy serwer ma prawa do wysyłania poczty na podstawie zwróconych parametrów: Priority, Weight i Port.
  - DNA (Domain Name Accreditation) posługuje się rekordami SRV, by określić, jakie strony trzecie mogą potwierdzić wiarygodność serwera nawiązującego połączenie.
- Więcej informacji nt. CSV, CSA i DNA:
  http://mipassoc.org/csv/
  http://mipassoc.org/csv/draft-ietf-marid-csv-intro-02.html
  http://mipassoc.org/csv/draft-ietf-marid-csv-csa-02.html
  http://mipassoc.org/csv/draft-ietf-marid-csv-dna-02.html

Microsoft Sender ID

- Sender ID jest oparte na oryginalnej propozycji Microsoftu opublikowanej pod nazwą Caller ID i łączy funkcjonalność zawartą w tej propozycji z mechanizmami SPF.
- Sender ID jest w zasadzie syntaktycznie zgodne z SPF. Różnica polega na stosowanym przedrostku:
  - W SPF przedrostkiem jest **v=spf1**.
  - W Sender ID przedrostki mogą mieć postać: **spf2.0/mfrom**, **spf2.0/mfrom,pra**, **spf2.0/pra,mfrom** lub **spf2.0/pra**.
  - Przedrostki informują, do jakich parametrów należy stosować uwierzytelnienie. Przedrostek **mfrom** — do MAIL FROM, natomiast **pra** oznacza Purported Responsible Address i obejmuje nagłówki poczty: **From**, **Sender**, **Resent-From** i **Resent-Sender**.

Microsoft Sender ID

- Podstawowym problemem związanym z Sender ID jest licencja, na której może być stosowany. Jego użycie wymaga uzyskania pozwolenia od Microsoftu. Powoduje to, że istnieje niewielka szansa na to, aby Sender ID mógł zostać przyjęty jako standard internetowy, a także zachęca do bojkotowania tego rozwiązania przez zwolenników wolnych licencji.
- Organizacje takie jak Apache Software Foundation i Debian Project opublikowały informacje o niemożliwości zastosowania tego mechanizmu w swoich rozwiązaniach z powodów licencyjnych.
- Więcej informacji o Sender ID:
  http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
  http://www.maawg.org/about/whitepapers/spf_sendID/

Problemy i ograniczenia

- Większość proponowanych rozwiązań wprowadzających uwierzytelnianie nadawcy **uniemożliwia stosowanie popularnych i przyjętych mechanizmów pocztowych, a także wymusza na innych stosowanie tego samego standardu!**
- Jeśli serwer odbierający pocztę stosuje SPF lub SenderID/mfrom do ochrony MAIL FROM:
  - nadawcy nie mogą stosować forwardowania (pre-delivery forwarding),
  - domena nadawcy musi publikować rekord w DNS-ie (jeśli serwer odbierający pocztę odrzuca e-maile z domen bez stosownych wpisów).
- Z kolei DKIM oraz SenderID/pra utrudniają lub nawet uniemożliwiają stosowanie list dyskusyjnych.
- DKIM powoduje znaczne obciążenie serwerów z powodu konieczności stosowania kryptografii.

Problemy i ograniczenia

- Czemu SPF uniemożliwia stosowanie forwardowania?
  - Jan Abacki używa aliasu *abacki@mail.com* do swojego konta *abacki@wp.pl* i chce wysłać e-mail do kolegi: *babacki@interia.pl*
  - Serwer *interia.pl* jest chroniony SPF-em.
  - Domena *mail.com* nie publikuje rekordu SPF.
  - Abacki wysyła e-mail przez *smtp.wp.pl* z adresem *abacki@mail.com* do *babacki@interia.pl*.
  - MTA *interia.pl* odrzuca mail, ponieważ nie znajduje rekordu SPF dla domeny *mail.com*.
- Rozwiązania:
  - Domena *mail.com* musiałaby opublikować rekord SPF umożliwiający każdemu korzystanie z tej domeny (v=spf1 +all).
  - MTA *smtp.wp.pl* musiałoby stosować SRS.

Problemy i ograniczenia

- SRS — Sender Rewriting Scheme
  - Jest to mechanizm do zaimplementowania w serwerach SMTP, które chcą umożliwić swoim użytkownikom stosowanie forwardowania do serwerów używających SPF lub Sender ID/mfrom.
  - Polega na zmianie adresu podawanego w MAIL FROM na adres w formacie:
    SRS0=*HHH*=*TT*=host=localorig@hostnew
    - SRS0 — ciąg stały,
    - HHH — hash z pól hostname, TT i localorig,
    - TT — znacznik czasowy określający ważność adresu SRS,
    - host — oryginalna nazwa domenowa,
    - localorig — oryginalna nazwa lokalna,
    - hostnew — nazwa domenowa należąca do serwera forwardującego.
  - Przykład: *abacki@mail.com* i *smtp.wp.pl*:
    - **SRS0=*HHH*=*TT*=mail.com=abacki@wp.pl**
- SRS nie jest dobrym rozwiązaniem, bo wymusza poważne zmiany w serwerach nadawców.
- Więcej o SRS: *http://www.libsrs2.org/*

Czy warto stosować uwierzytelnianie nadawcy?

- W obecnej formie każda propozycja (prócz mało efektywnego i praktycznie niestosowanego CSV) wprowadza poważne ograniczenia w używaniu poczty.
- Większość propozycji wymusza stosowanie wybranych rozwiązań na administratorach serwerów, które kontaktują się z chronionym serwerem. Żadna z propozycji nie jest natomiast standardem, a implementacja zmian jest często kłopotliwa (np. nie każdy MTA umożliwia stosowanie SRS).
- Skuteczność powyższych rozwiązań jest zbyt niska w porównaniu z ograniczeniami, jakie wprowadzają. Redukują spam i ataki wirusów w stopniu mniejszym, niż inne rozwiązania które nie mają tak poważnych efektów ubocznych (np. greylisting).

Czy warto stosować uwierzytelnienie nadawcy?

- Przy obecnym stanie rzeczy stosowanie jakichkolwiek mechanizmów gwarantujących uwierzytelnienie nadawcy w SMTP jest **bardzo złym pomysłem**.
- **Najlepszym wyjściem wydaje się podpisywanie e-maili (S/MIME).**

- Bibliografia:

Magazyn *hakin9* 2/2006 — artykuł o SPF i jego wadach,
http://homepages.tesco.net/J.deBoynePollard/FGA/smtp-spf-is-harmful.html,
http://www.taugh.com./mp/lmap.html,
http://bradknowles.typepad.com./considered_harmful/2004/05/spf.html,
http://www.circleid.com/posts/sender_id_a_tale_of_open_standards_and_corporate_greed_part_i/.