

# DNSSEC

## Brakujące ogniwo w bezpieczeństwie Internetu

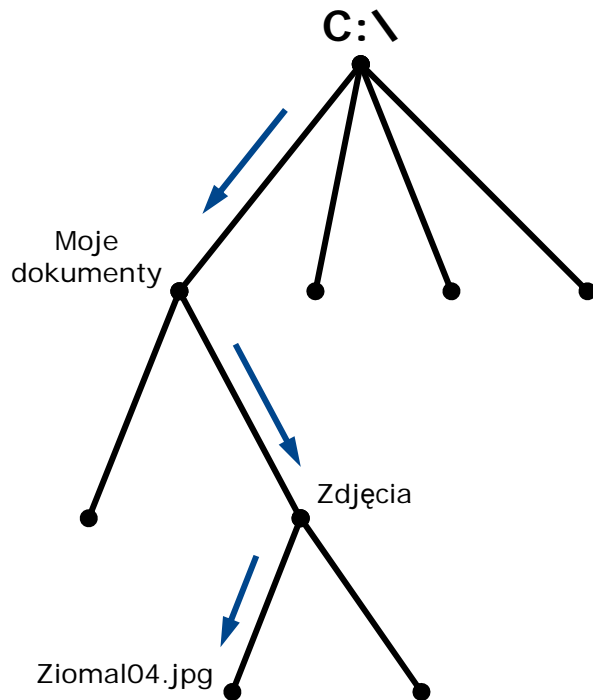
- **Domain Name System**
- **Rozproszona baza danych**  
informacje o komputerach w sieci znajdują się na wielu serwerach DNS rozproszonych po całym świecie
- **Główne zastosowanie: mapowanie nazw domenowych na adresy IP hostów**
- **Doskonałe środowisko do przechowywanie innych informacji, np. danych teleadresowych - ENUM**
- **Duża niezawodność**  
osiągnięta dzięki nadmiarowości serwerów DNS (minimalnie dwa)
- **Doskonała skalowalność**

## **DNS jest podstawą Internetu**

Z DNS korzysta wiele protokołów i usług sieciowych

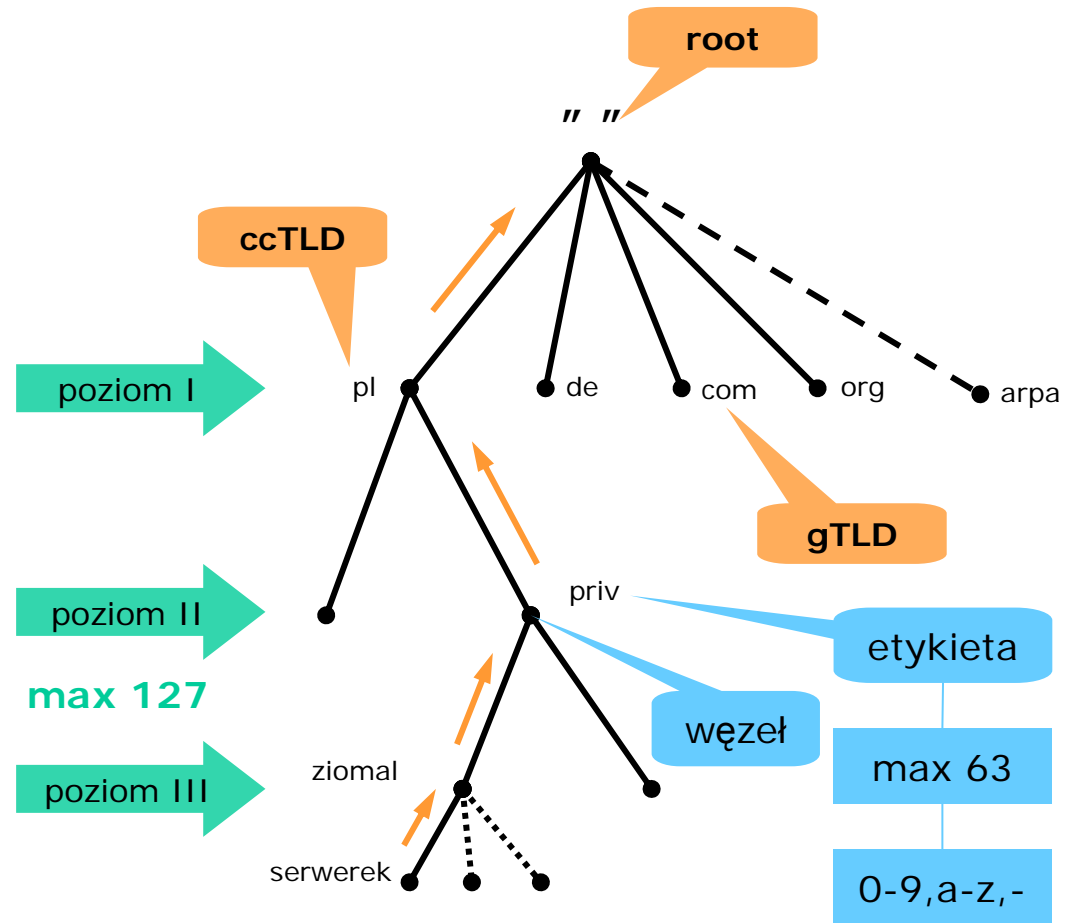
# Struktura DNS

## Struktura plików w systemach operacyjnych Windows



C:\Moje dokumenty\Zdjęcia\Zioma104.jpg

## Baza danych DNS



serwerek.ziomal.priv.pl

# DNS

---

- DNS ma już ponad 20 lat; wymyślony w 1986r
- DNS (RFC 1034, RFC 1035) nie jest doskonały  
pierwsza luka odkryta w 1990
- Wiele aplikacji zależy od DNS'u
- Zagrożenia w DNS są rozpoznane  
RFC3833
- W sieci istnieją gotowe narzędzia do pobrania,  
umożliwiające przeprowadzenie różnych ataków na  
infrastrukturę DNS

# Zagrożenia w DNS

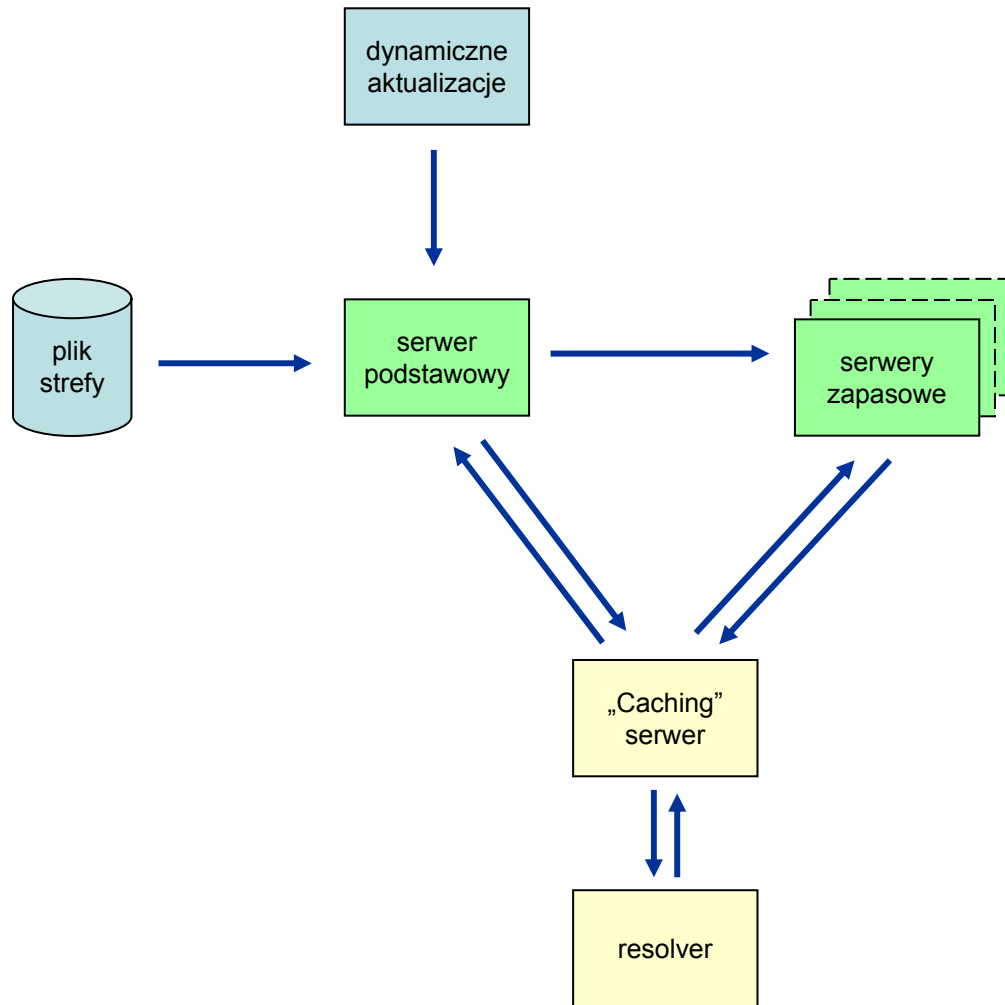
---

- Amplification Attacks
- Cache Poisoning
- Distributed Denial of Service (DDoS) Attack
- Monkey-in-the-Middle Attack
- Pharming Attacks
- Spoofing

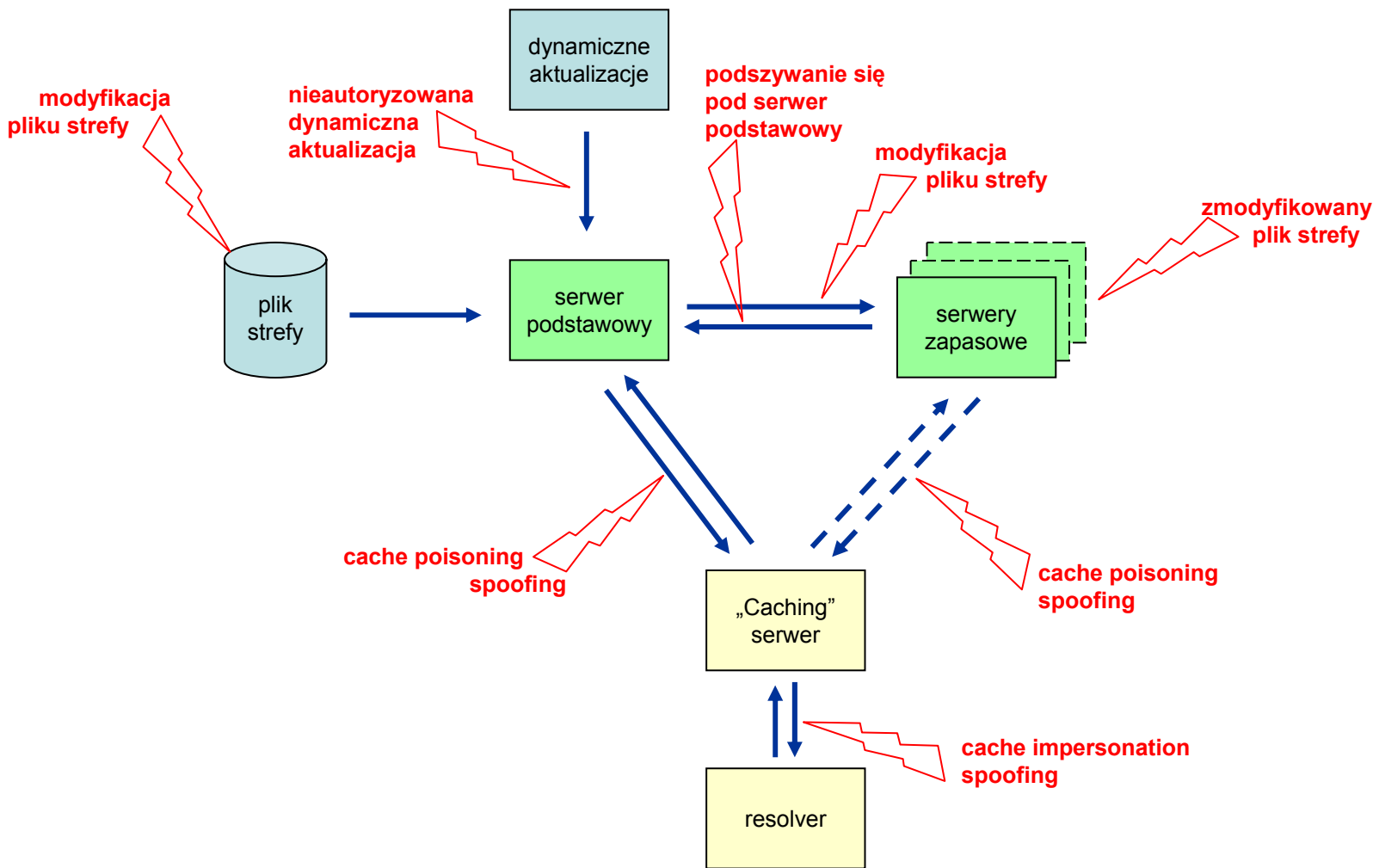
Literatura:

- RFC 3833 Threat Analysis of the Domain Name System (DNS)
- Schuba, C., "Addressing Weaknesses in the Domain Name System Protocol", Master's thesis, Purdue University Department of Computer Sciences, August 1993.
- <http://www.dnssec.net/dns-threats>

# Przepływ danych w DNS



# Zagrożenia w DNS

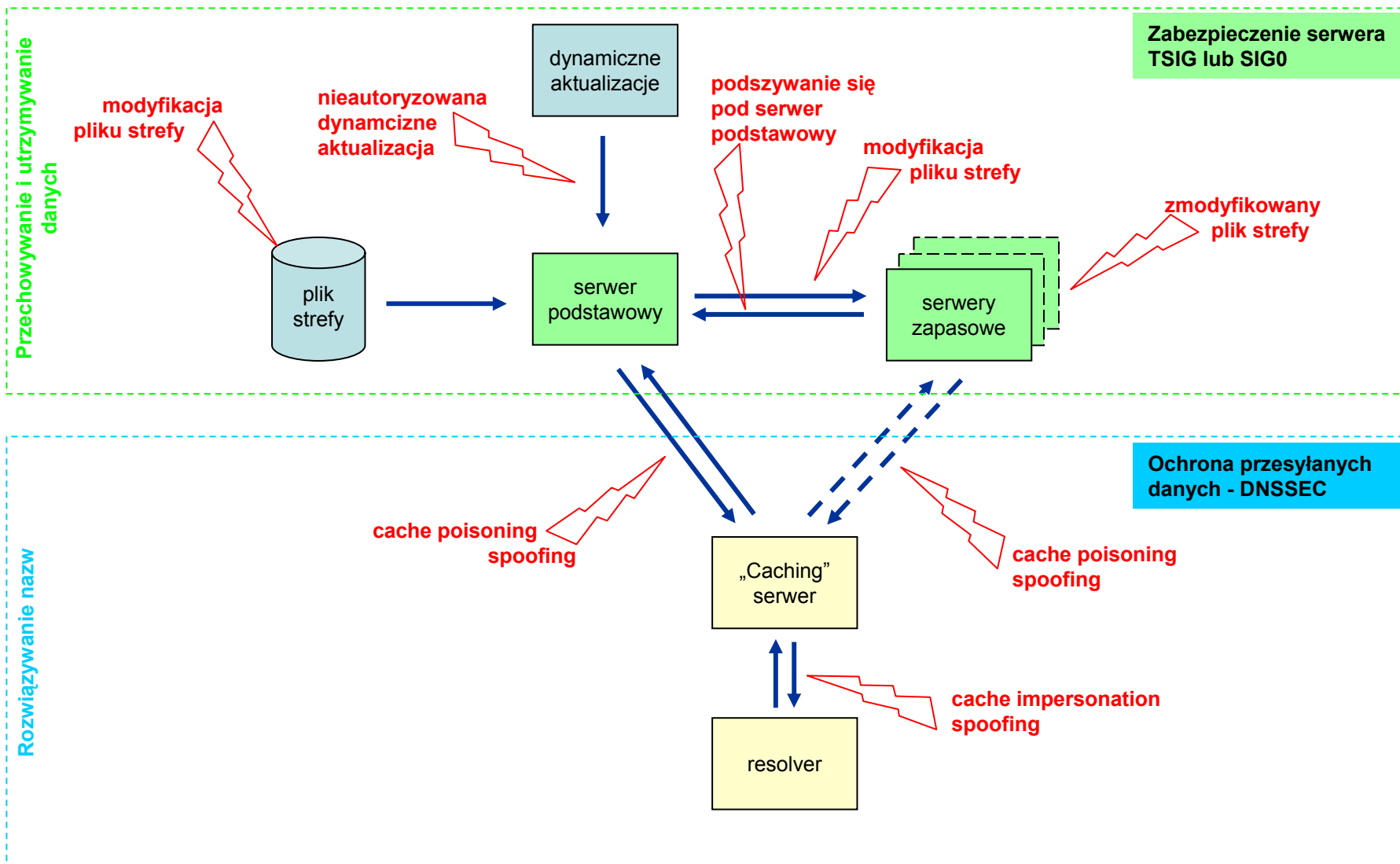


# Przepływ danych w DNS

---

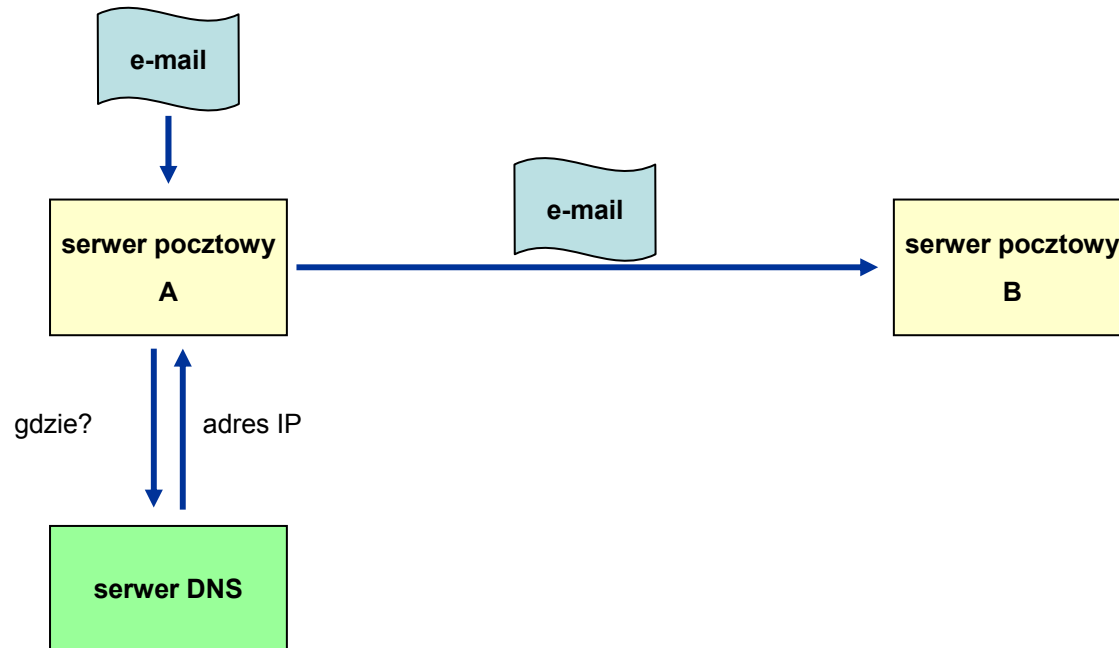
- Komunikacja między elementami systemu odbywa się za pośrednictwem sieci Internet.
- Przesyłane informacje nie są utajnione, ani zabezpieczone przed podrobieniem czy modyfikacją.
- Potencjalnie, dane DNS mogą zostać sfałszowane bądź zmienione w wielu miejscach
- Sfałszowane dane wprowadzone do pamięci cache serwerów zostają w systemie przez dłuższy czas.  
To powoduje, że skutki ataku długo odbijają się echem.
- W kontekście istotności przesyłanych informacji wprowadzenie mechanizmów zapewniających bezpieczeństwo jest bardzo pożądane.

# Zabezpieczenia

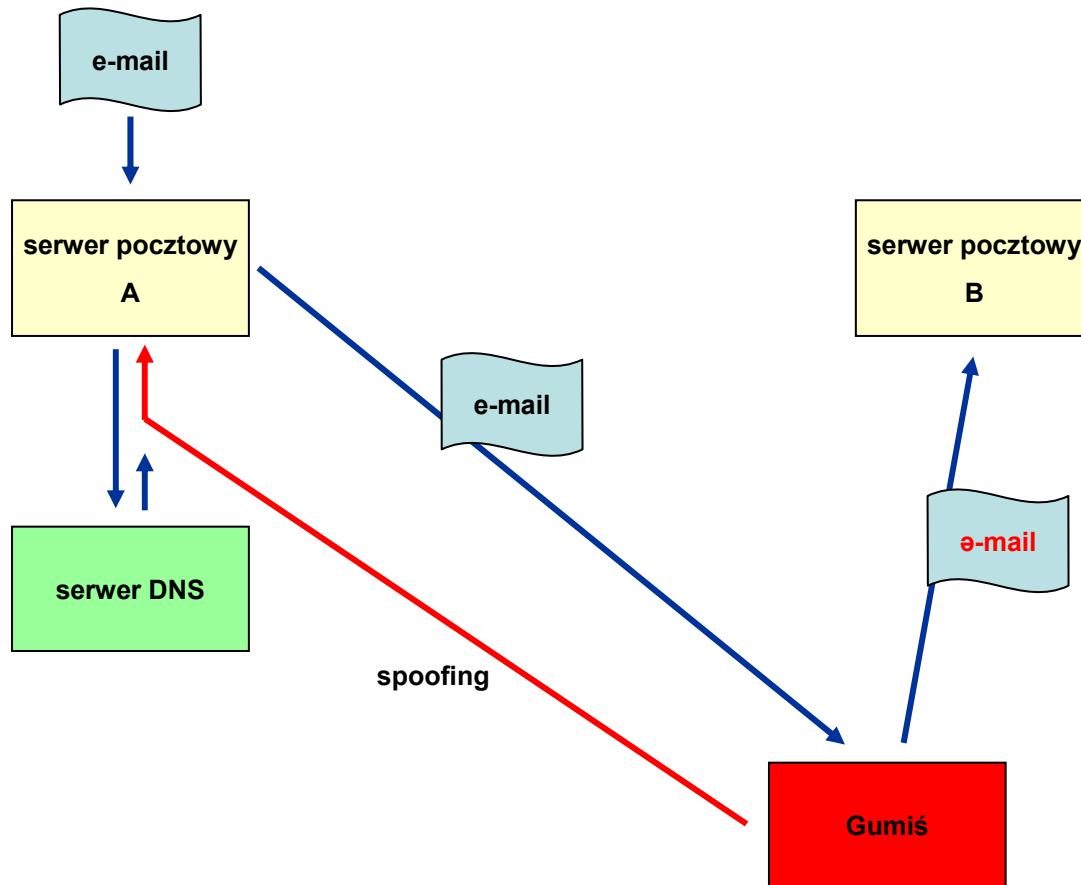


# Jeszcze jeden przykład

---



# Jeszcze jeden przykład



- Za pomocą fałszywych danych w DNS możemy połączyć się z fałszywą stroną www
- List elektroniczny może zostać przekierowany w inne miejsce bądź wogóle nie dostarczony.
- Nasz *login* może zostać przechwycony podczas ataku man-in-the-middle

# Dlaczego DNSSEC?

---

- Otrzymując odpowiedź z serwera DNS nie możemy być pewni, że:
  - ✓ otrzymana wiadomość pochodzi z właściwego źródła, oraz
  - ✓ nie została zmodyfikowana w czasie przesyłania

# Dlaczego DNSSEC?

---

- DNSSEC wprowadza mechanizmy umożliwiające:
  - ✓ zapewnienie **integralności** wiadomości DNS
  - ✓ weryfikację **autentyczności** pozyskanych danych
- DNSSEC daje możliwość weryfikacji odpowiedzi negatywnych  
(ang. authenticated denial of existence of DNS data).

- **Autentyczność**

DNSSEC dostarcza mechanizm, który umożliwia zweryfikowanie źródła informacji.

- **Integralność**

DNSSEC zapewnia integralności komunikacji, umożliwiając stwierdzenie czy odebrana informacja jest w takiej postaci, w jakiej została wysłana.

# Autentyczność i integralność danych

---

## podsumowanie

- Klient systemu może mieć pewność, że otrzymane przez niego dane są:
  - ✓ wiarygodne
  - ✓ i nie zostały zmienione w trakcie transportu ze źródła.

- DNSSEC wprowadza nam mechanizmy bezpieczeństwa już na poziomie DNS
- Następną warstwę zabezpieczeń stanowią takie protokoły jak TLS, SSL oraz PKI.

- **Bezkonfliktowo współistnieje z niezabezpieczoną częścią systemu DNS**

# Czego nie zapewnia DNSSEC?

---

- DNSSEC nie dostarcza:
  - ✓ mechanizmów autoryzacji
  - ✓ poufności danych

# Jak działa DNSSEC?

---

- DNSSEC opiera się na kryptografii klucza publicznego (kryptografia asymetryczna)
- zabezpieczona strefa ma swój **klucz prywatny i publiczny**
- klucz prywatny wykorzystywany jest do podpisywania danych przechowywanych w DNS
- klucz publiczny jest używany do weryfikacji podpisanych danych; jest opublikowany w zabezpieczonej strefie

# Nowe rekordy DNS

---

DNSSEC wprowadza następujące nowe rekordy zasobów:

- **DNSKEY**  
rekord przechowujący klucz publiczny do weryfikacji podpisów (rekordów RRSIG)
- **RRSIG**  
podpis grupy rekordów
- **NSEC**  
zapewnienie spójności danych strefy i umożliwienie weryfikacji informacji o nieistnieniu rekordu lub o braku zabezpieczeń (**authenticated denial of existence of data**); rekord wskazuje, na następną dostępną nazwę w pliku stref (dane posortowane kanonicznie) oraz wskazuje, które typy rekordów są dostępne dla danej nazwy domenowej.
- **DS**  
wskazanie na klucz podpisujący dane w strefie podrzędnej (delegation signer)

# Łańcuch zaufania

## weryfikacja danych

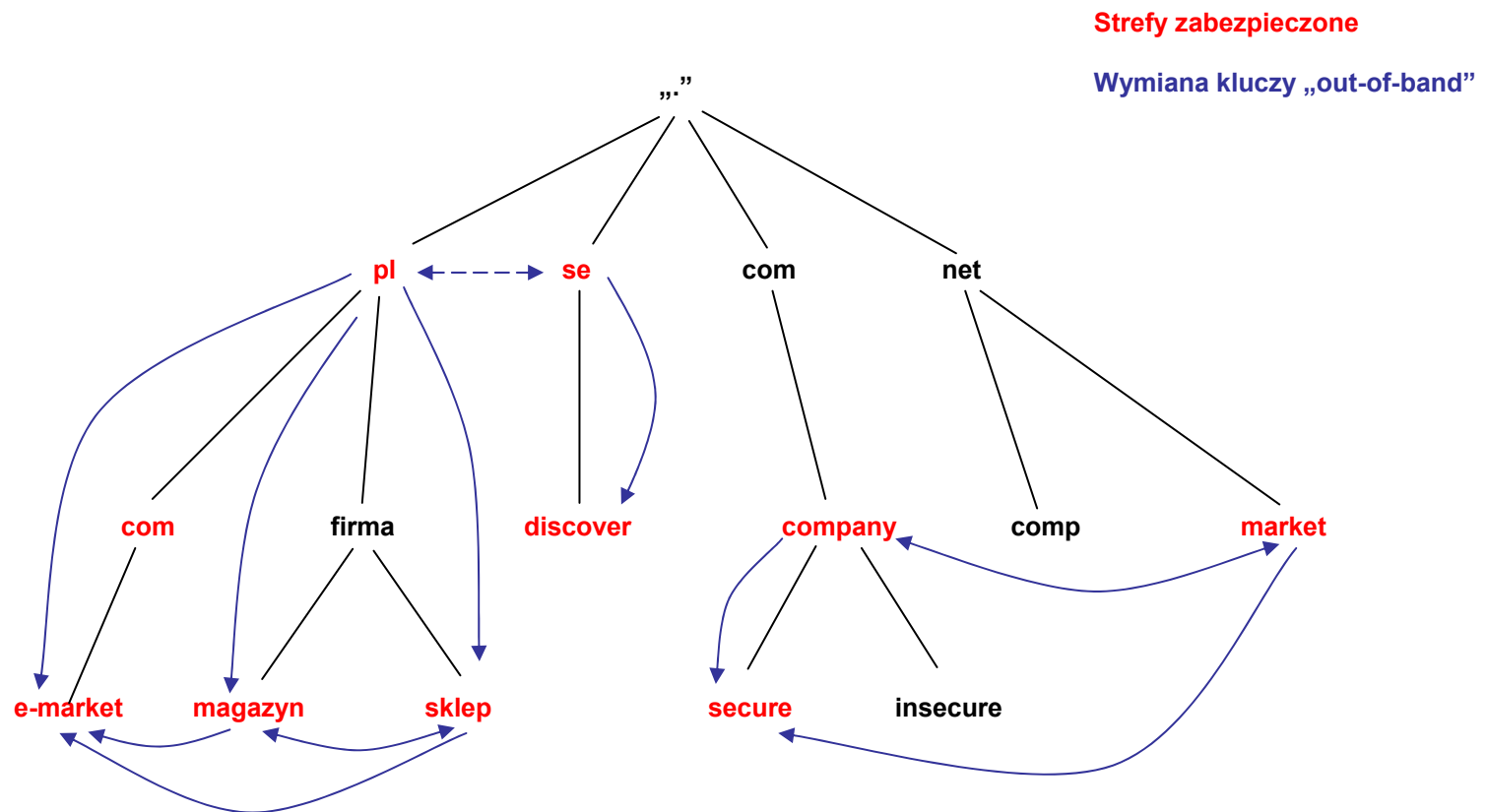


# Łańcuch zaufania

---

- Ufamy danym podpisanym przez ZSK
- Możemy zaufać ZSK jeśli jest podpisany przez KSK
- Ufamy KSK, jeśli jest wskazany przez rekord DS w strefie nadrzędnej
- Ufamy rekordowi DS ze strefy nadrzędnej jeśli jest podpisany przez klucz ZSK z tej strefy, itd.
- Jeśli trafimy na klucz (SEP - Secure Entry Point), któremu ufamy (tzn. jest zapisany w pliku named.conf, dyrektywa trusted-keys), to oznacza, że zbudowaliśmy łańcuch zaufania i dane są zweryfikowane poprawnie.

# Wyspy bezpieczeństwa



- Prace nad DNSSEC rozpoczęto w 1995
- W 1999 opublikowano RFC 2535
- W marcu 2005 opublikowano tzw. **DNSSECBis**  
RFC 4033, RFC 4034, RFC 4035

## Obecna sytuacja

---

- Istnieje oprogramowanie wspierające DNSSEC  
serwery DNS
- Brak jeszcze aplikacji-klientów, potrafiących  
wykorzystać w pełni zalety DNSSEC
- Potrzebne jest zabezpieczenie kanałów  
przesyłania informacji na drodze klient - serwer
- Prace nad DNSSEC wciąż trwają  
rekord NSEC3
- Budowanie świadomości
- Zabezpieczanie całej drzewiastej struktury DNS

---

KONIEC