Wykrywanie i zapobieganie atakom na protokół BGP

praca magisterska

opiekun: prof. dr hab. inż. Zbigniew Kotulski
autor: Łukasz Chmielarski

Agenda

- Zasada działania BGP
- Rodzaje ataków
- Metody obrony
- System wykrywania ataków

Co to jest BGP ?

- Border Gateway Protocol
- Protokół routingowy pomiędzy domenami lub wewnątrz domeny (Autonomous System)
- Powszechnie używana BGPv4
- Stworzony na podstawie ARPANET EGP
- Pierwsze RFC:
  - 1105 (BGP) -> czerwiec 1989
  - 1771 (BGPv4) -> marzec 1995
- Aktualne RFC:
  - 4271 (BGPv4) -> styczeń 2006

Zasada działania

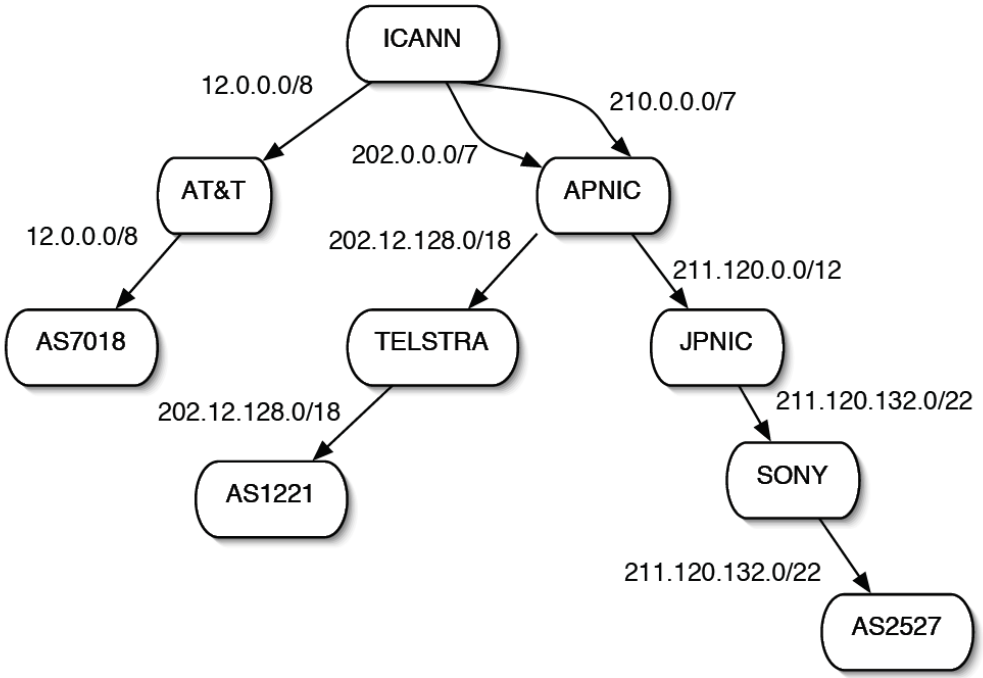
- BGP speaker – router używający protokołu BGP
- Komunikacja z wykorzystaniem TCP port 179
- Rodzaje wiadomości:
  - Open
  - Keep-alive
  - Update
  - Notification
- Zasady wyboru ścieżki:
  - Longest prefix matching
  - Liczba hop-ów

Autonomous System

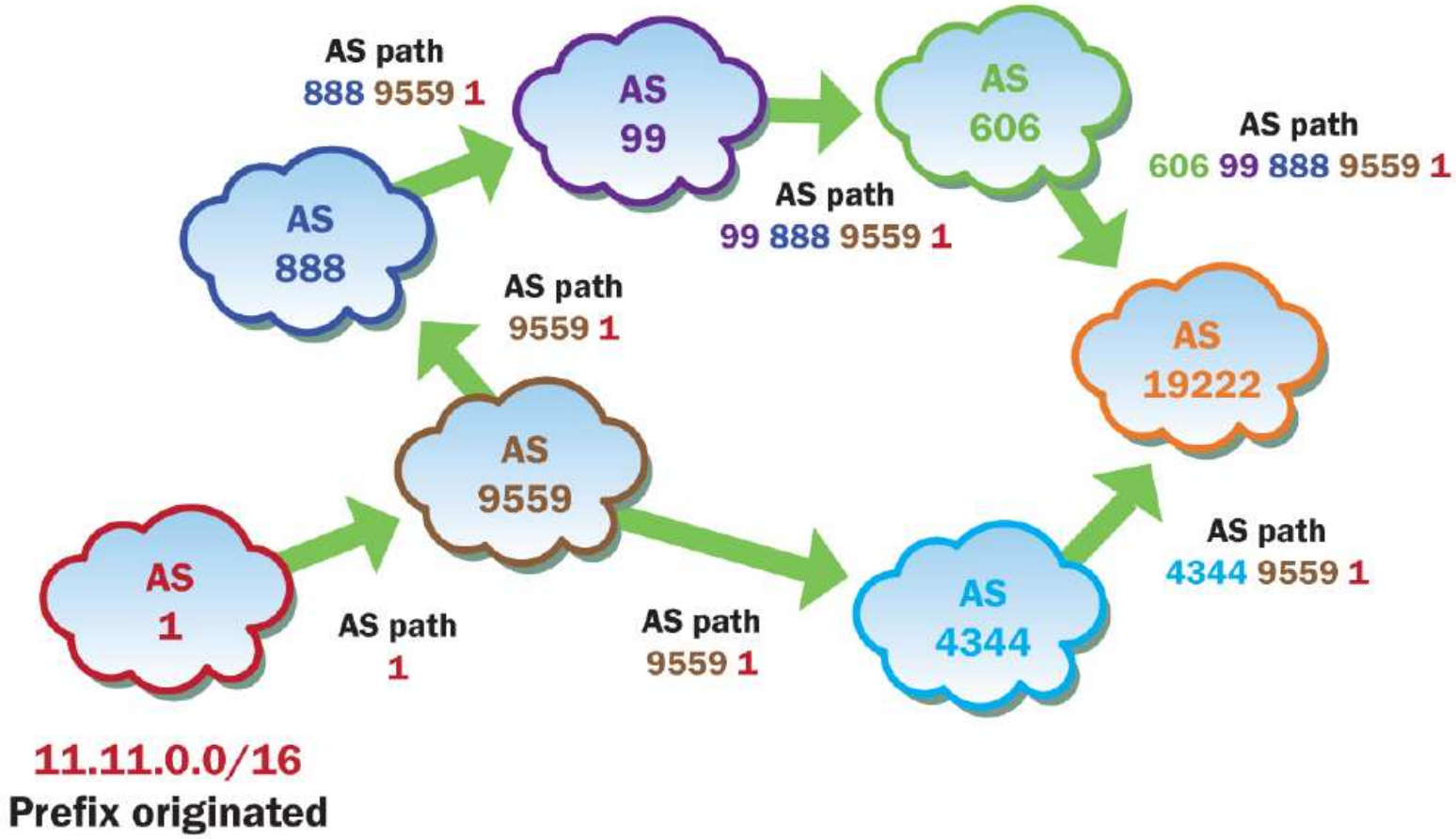
- AS - sieć zarządzana przez jednego operatora
- Każdy AS ma przypisany:
  - Identyfikator AS
  - Jeden lub więcej prefiksów (zakresów IP)
- Przykłady AS-ów:

Zarządzanie adresami

- ICANN- centralny zarządca prefiksów
- Regionalni zarządcy: ARIN, RIPE, APNIC



Przykład rozgłoszenia BGP

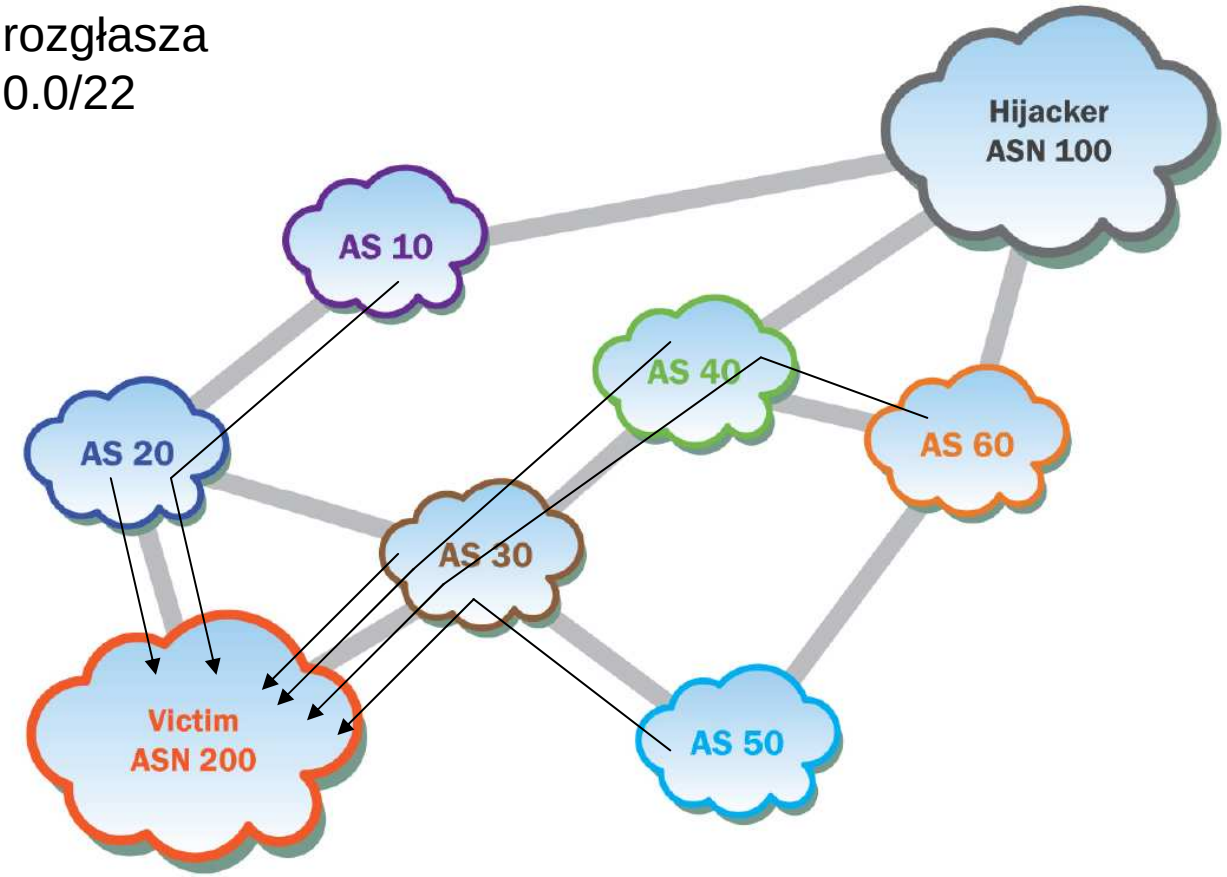


Rodzaje ataków

- Atak lokalny na parę BGP speaker-ów:
  - Atak na integralność
  - Wiadomości nie są szyfrowane
  - Możliwość zakończenia sesji
  - Możliwy atak SYN flooding
- Atak globalny
  - Prefix hijacking
  - Sub-Prefix hijacking
  - Unused prefix hijacking
  - Atak typu MItM
- Błędna konfiguracja

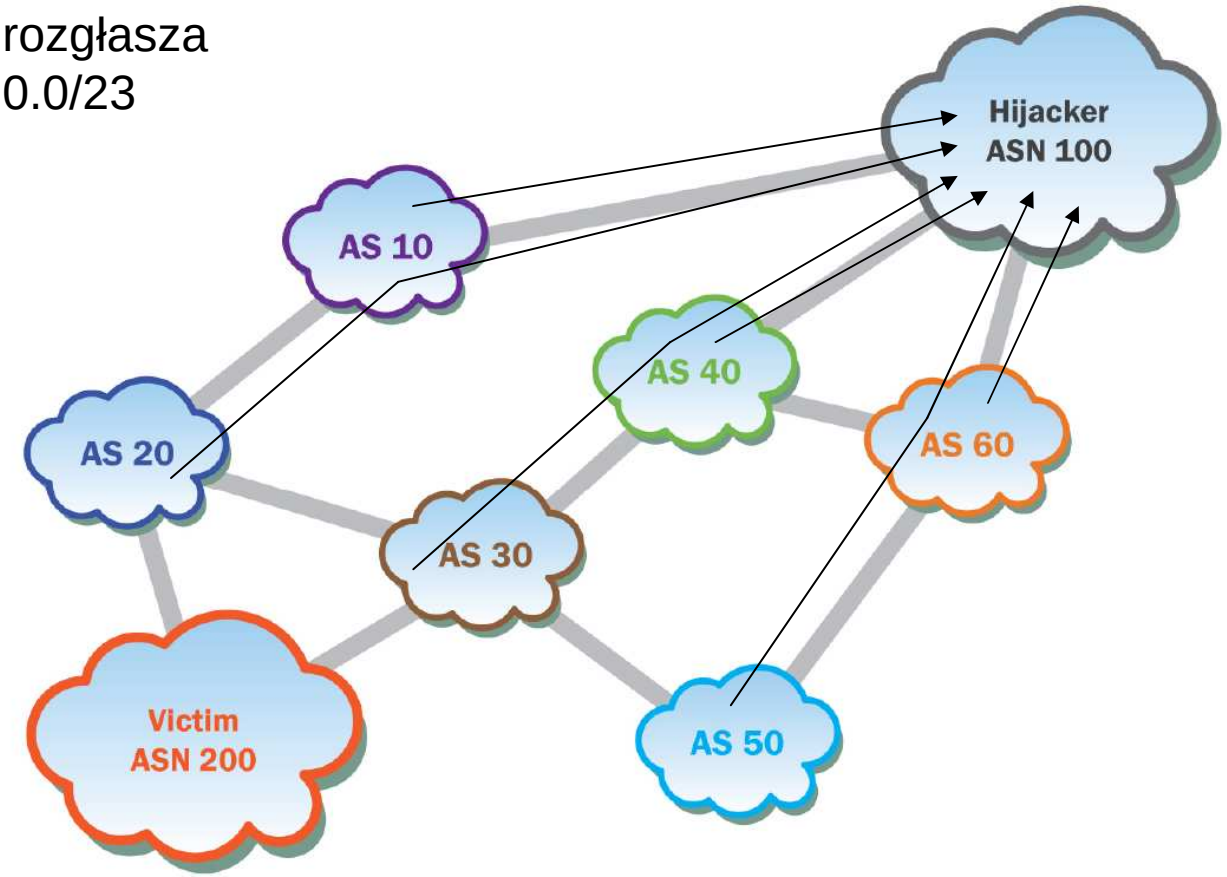
Sub-prefix hijacking (1)

ASN 200 rozgłasza
sieć 10.0.0.0/22



Sub-prefix hijacking (2)

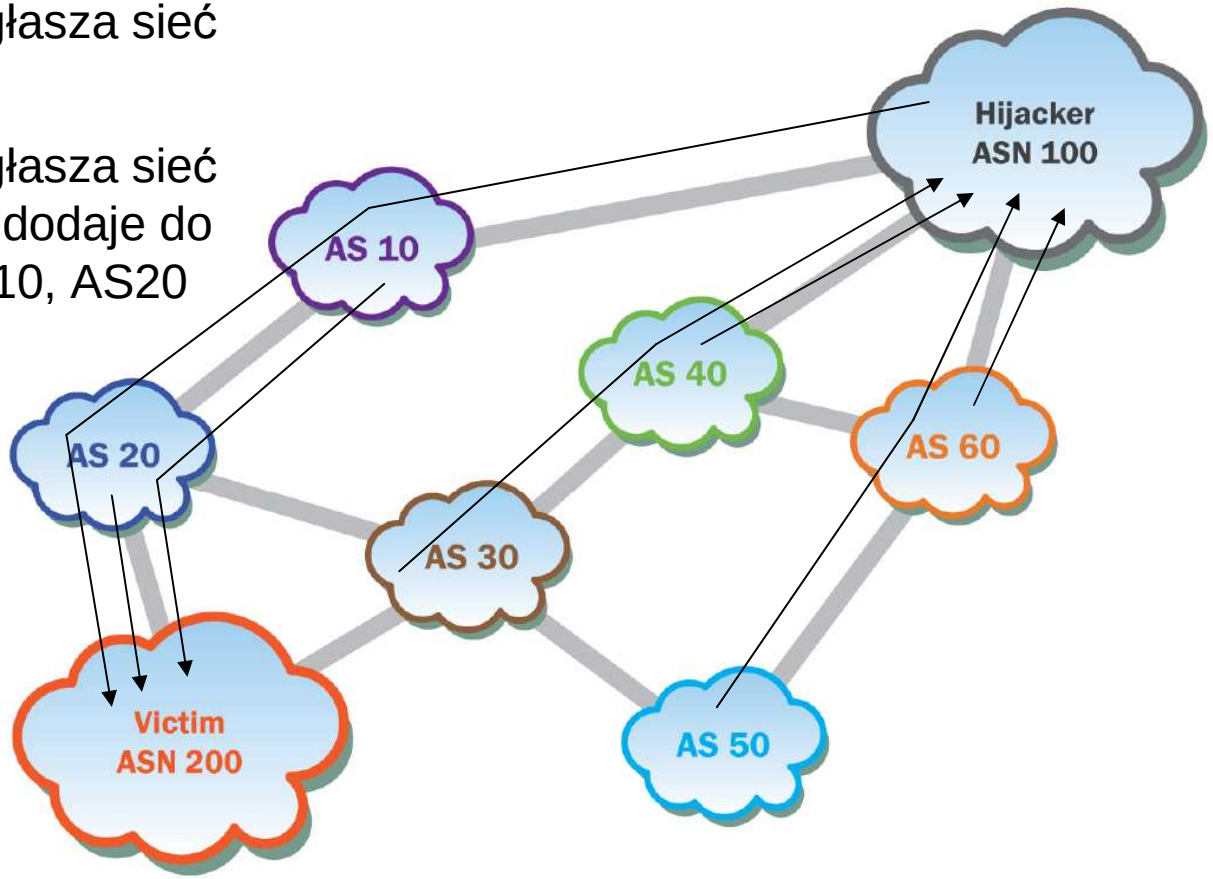
ASN 100 rozgłasza
sieć 10.0.0.0/23



Atak MItM

ASN 200 rozgłasza sieć 10.0.0.0/22

ASN 100 rozgłasza sieć 10.0.0.0/23 + dodaje do ASPATH: AS10, AS20

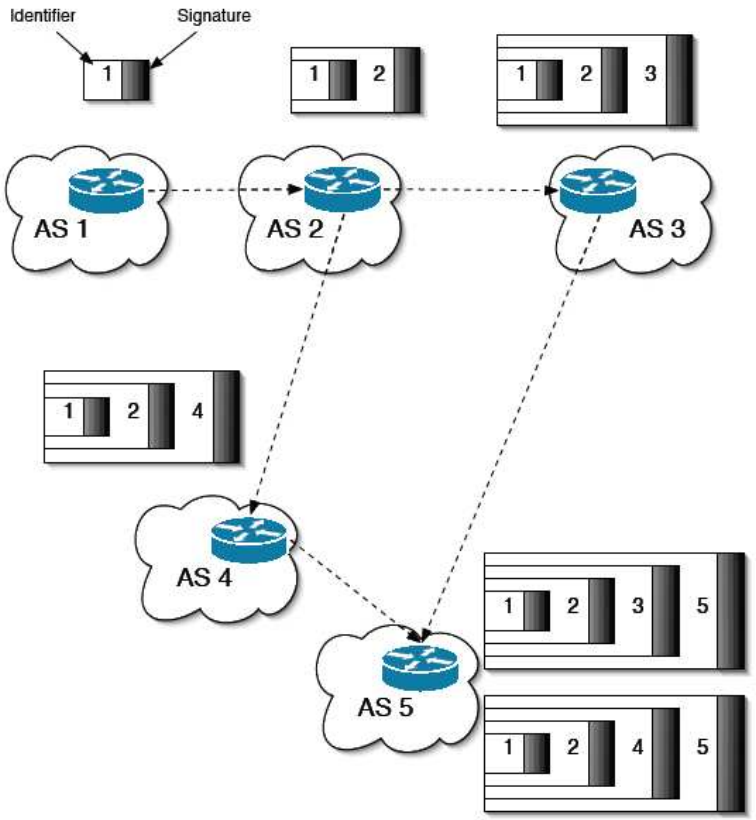


Metody ochrony

- Mechanizmy ochrony na ataki lokalne:
  - IPsec
  - MD5
  - General TTL Security Mechanism
- Mechanizmy ochrony na ataki globalne:
  - filtrowanie
  - SBGP
  - soBGP
  - IRV

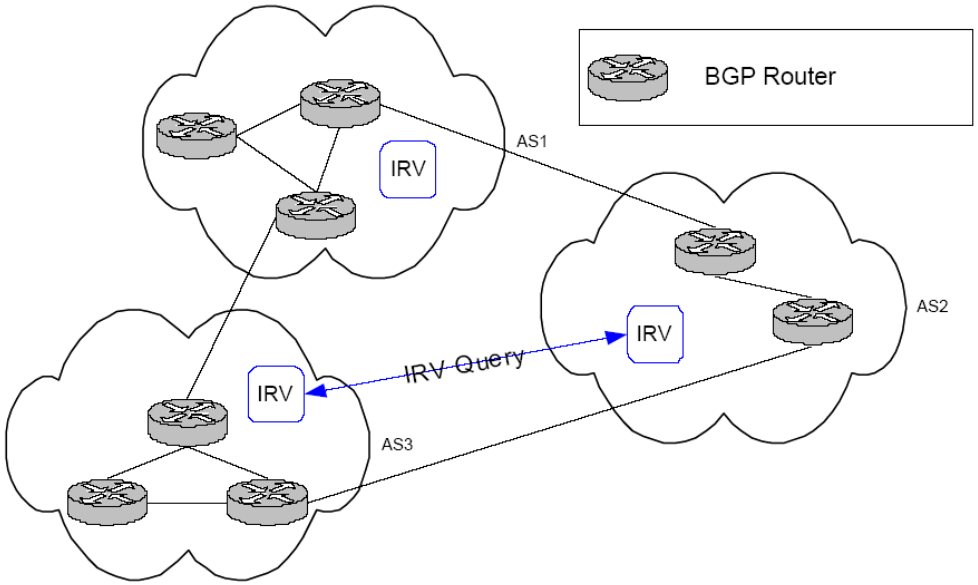
Secure BGP (S-BGP)

- Standard IETF
- Wykorzystanie PKI
- Duże obciążenie procesora
- Różnice względem soBGP:
  - S-BGP „onion-style”
  - soBGP topology database



Interdomain Route Validation

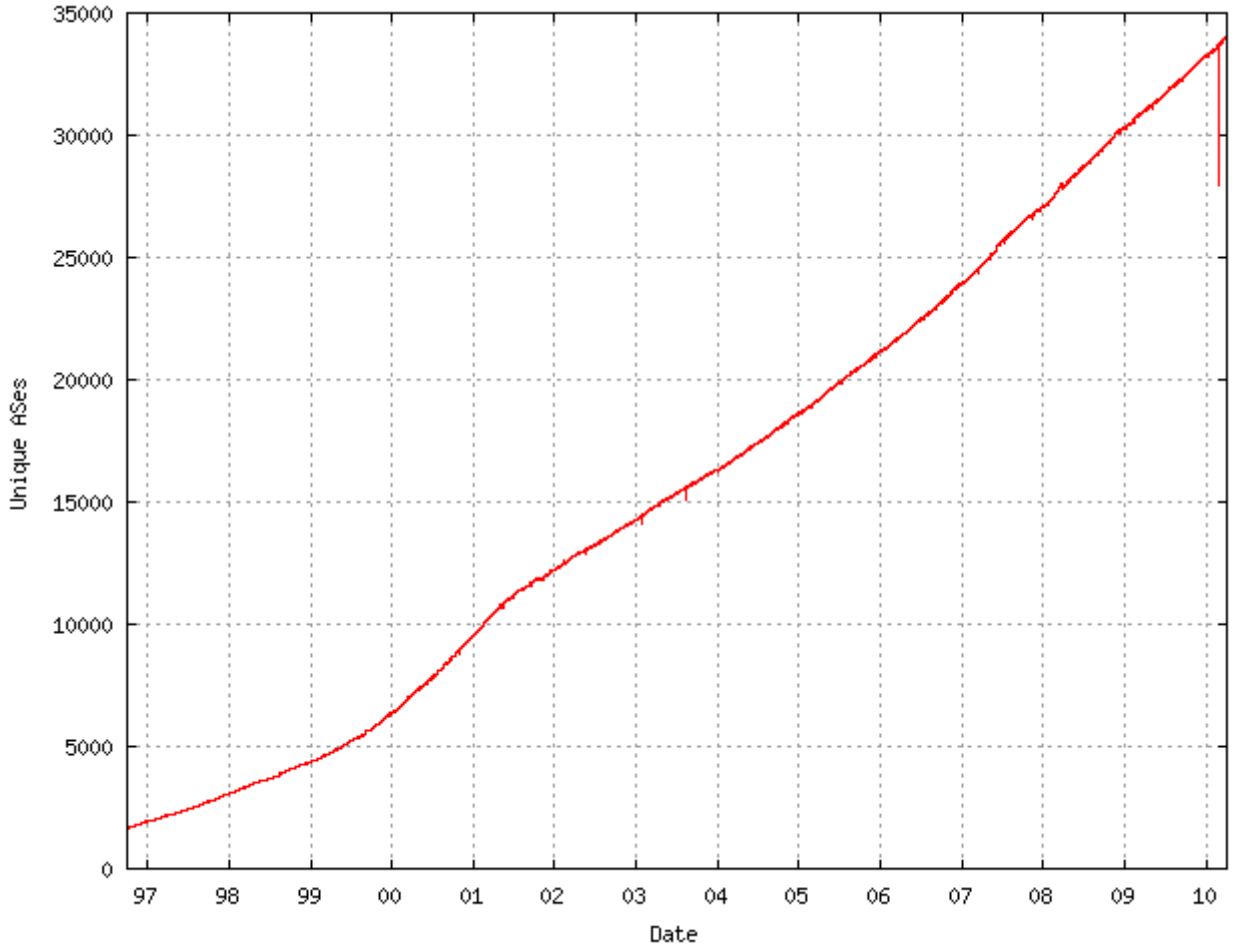
- Protokół niezależny od BGP
- Każdy AS posiada IRV serwer
- Każda wiadomość jest sprawdzana na serwerze IRV



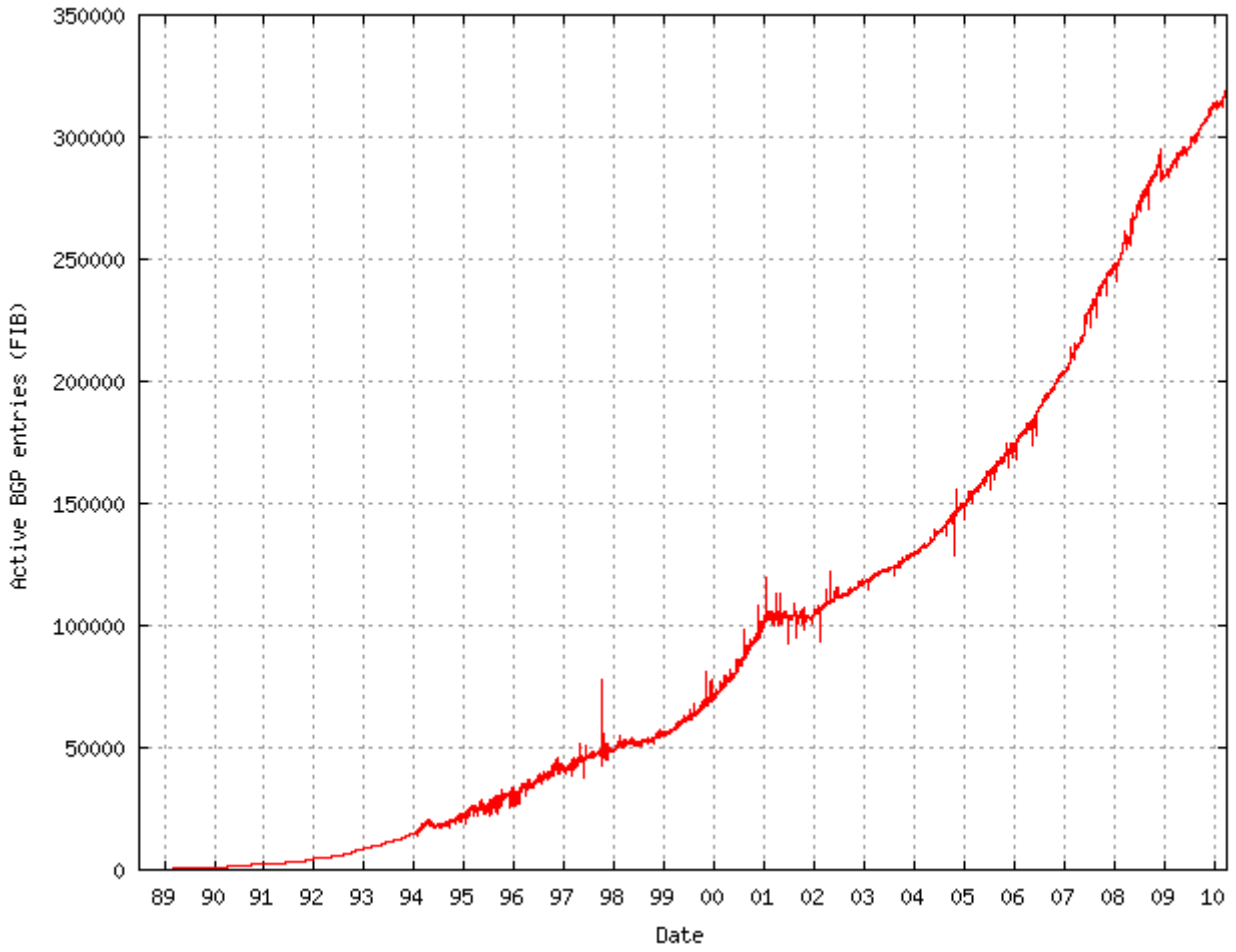
Eksperymentalne implementacje

- Multiple origin AS – MOAS
- Origin Authentication
- Path Authentication
- Pretty secure BGP – psBGP
- Secure Path Vector Protocol – SPV
- Whisper protocol

Liczba AS-ów


35000
30000
25000
20000
15000
10000
5000
0
Unique ASes
97
98
99
00
01
02
03
04
05
06
07
08
09
10
Date

Liczba rekordów w FIB



System wykrywania ataków

- Założenia systemu:
  - Monitor pobiera pliki zawierające wiadomości Update i tablice routingu z repozytorium
  - Pliki są analizowane poprzez pakiet Quagga
  - Zawartość plików jest umieszczana w baze danych
  - Każdy nowy pakiet danych jest przeszukiwany pod względem ewentualnych ataków
  - Przeszukiwanie odbywa się zgodnie z określoną logiką programu
  - Wysyłanie powiadomień o ataku
  - Graficzny dostęp poprzez WWW

Jak zebrać dane ?

- Wykorzystanie danych RIPE lub RouteViews
- Tablice routingu routerów znajdujących się w Tier-1
- Tablice routingu i wiadomości Update kopiowane są do plików
- Wykorzystanie pakietu **Quagga**
- Dane z 16 routerów na świecie
- Dane można wykorzystywać nieodpłatnie do celów naukowych

Logika działania

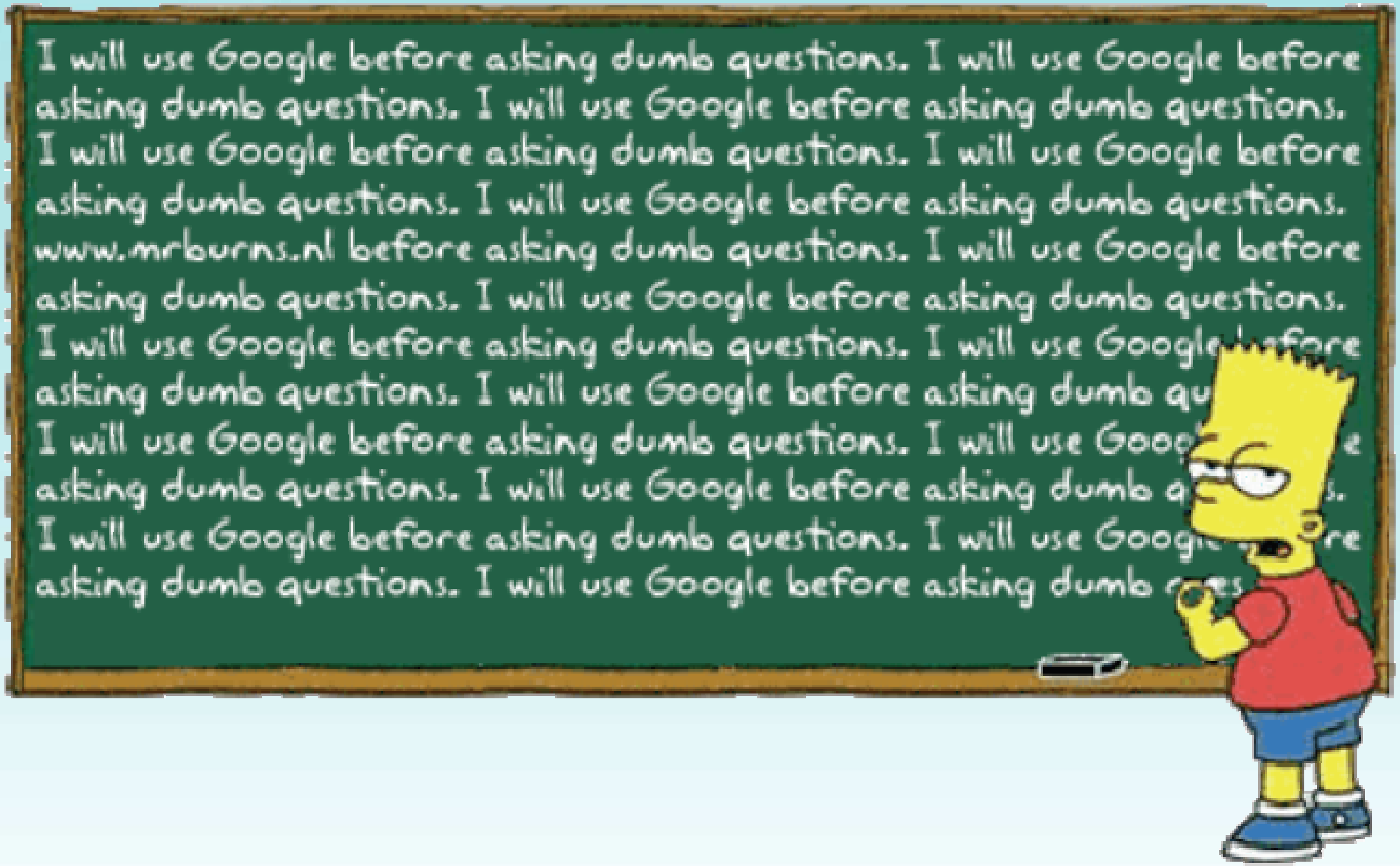
- Przeglądamy wszystkie prefiksy p w tablicy routingu
- Sprawdzamy czy ten prefiks jest przypisany do AS
- Sprawdzenie kto rozgłosił ten prefiks:
  - Porównanie z ICANN
  - Porównanie z poprzednimi pomiarami
- Sprawdzenie czy istnieje prefiks bardziej znaczący zawierający się w p:
  - Jeśli tak sprawdzamy kto go rozgłosił
  - Jeżeli oba prefiksy są rogłoszone przez ten sam AS sprawdzamy AS_PATH
- Wysłanie powiadomienia do właściciela AS

Istniejące rozwiązania

- MyASN service
- BGPmon
- WatchMy.Net
- Prefix Hijacked Alert System (PHAS)
- Internet Alert Registry (IAR)

- Różnice:
  - koszt, darmowy czy komercyjny
  - źródło danych, własne czy ze wspólnego repozytorium
  - czas odpowiedzi, rodzaj wsparcia, typy alarmów

Pytania ?


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google
asking dumb questions. I will use Google before asking dumb
I will use Google before asking dumb questions. I will use
asking dumb questions. I will use Google before asking dumb
I will use Google before asking dumb questions. I will use
asking dumb questions. I will use Google before asking dumb