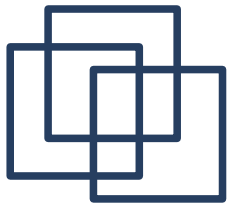


Paweł Pokrywka, Ispara.pl

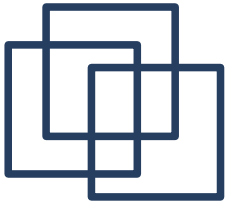


**multispoof: Zaawansowany mac
spoofing w sieciach lokalnych**



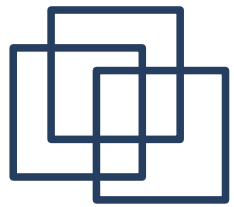
Plan prezentacji

- Obszar zainteresowania
- Problem uwierzytelniania w sieciach LAN
- Wykorzystanie podatności: multispoof
- Detekcja nadużyć
- Środki prewencyjne



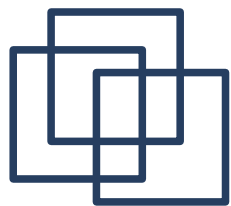
Sieci LAN

- Obszar zainteresowania:
 - Sieć lokalna z dostępem do Internetu (tzw. *sieć osiedlowa*)
 - Dostęp do zasobów globalnej sieci jest płatny
- Problem:
 - *Jak powiązać transmisje sieciowe przepływające przez router operatora z człowiekiem, którego komputer je wygenerował?*

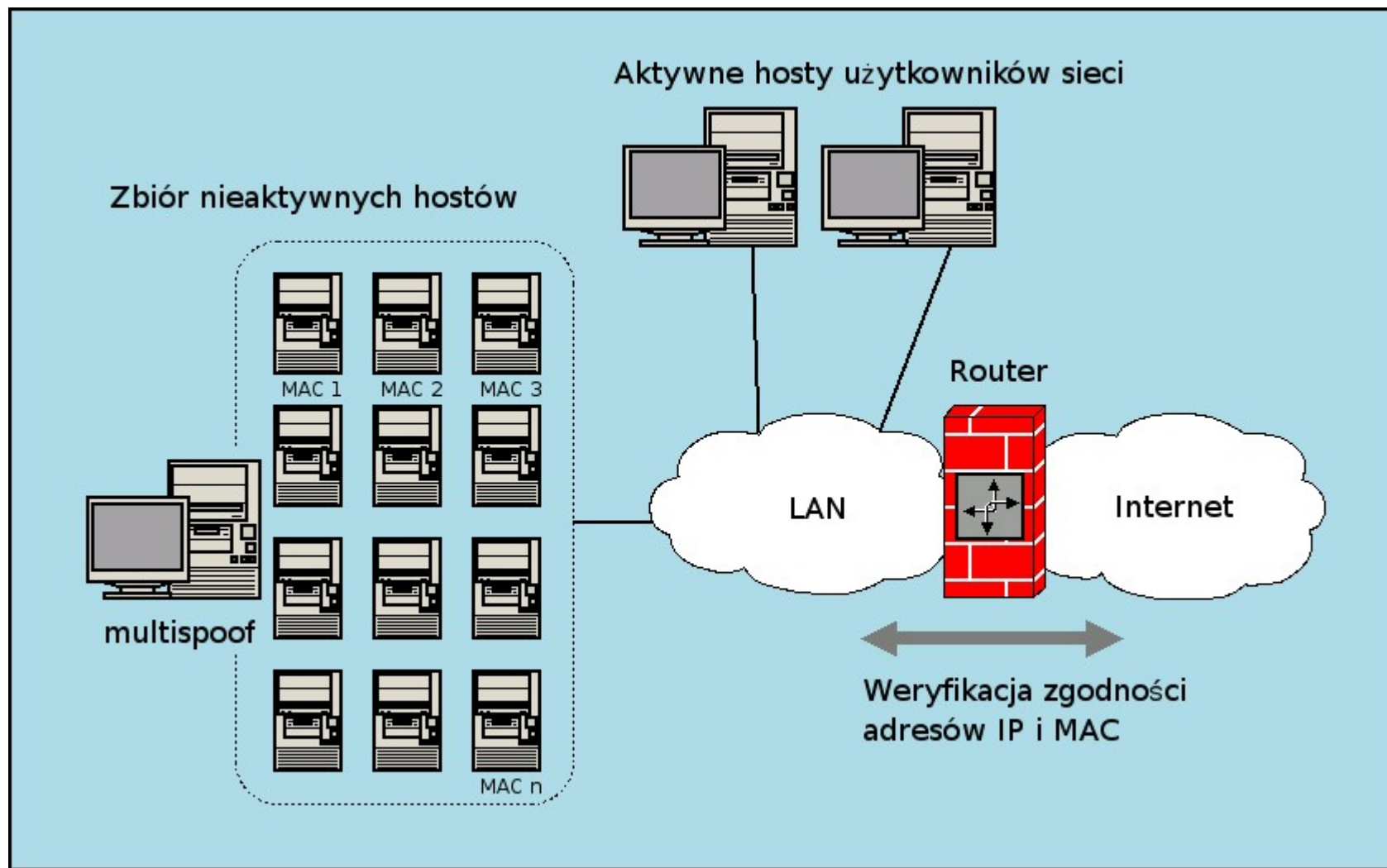


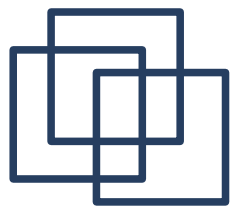
Uwierzytelnianie w LAN

- Uwierzytelnianie na podstawie adresów MAC
- Adres można zmienić
 - I podszywając się w ten sposób pod legalnego, nieaktywnego użytkownika wykorzystywać jego pasmo transmisyjne
- Czy można się podszywać pod wiele komputerów jednocześnie?
 - IP – można zdefiniować wiele aliasów
 - MAC – tylko jeden na interfejsie

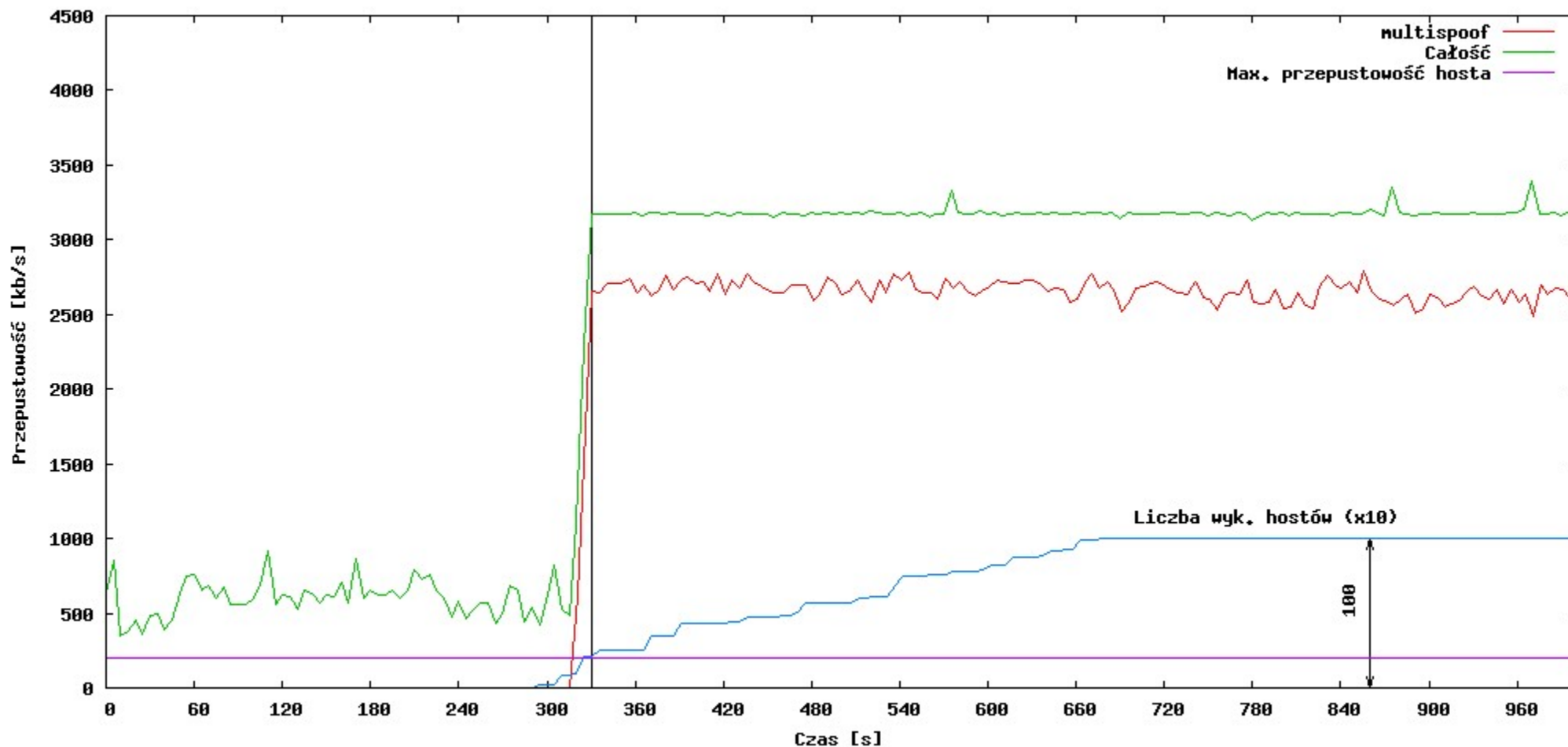


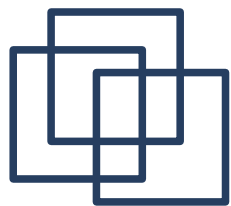
multispoof: Idea





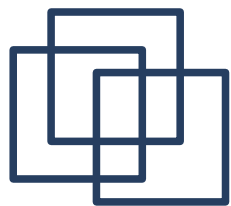
multispoof: Wyniki



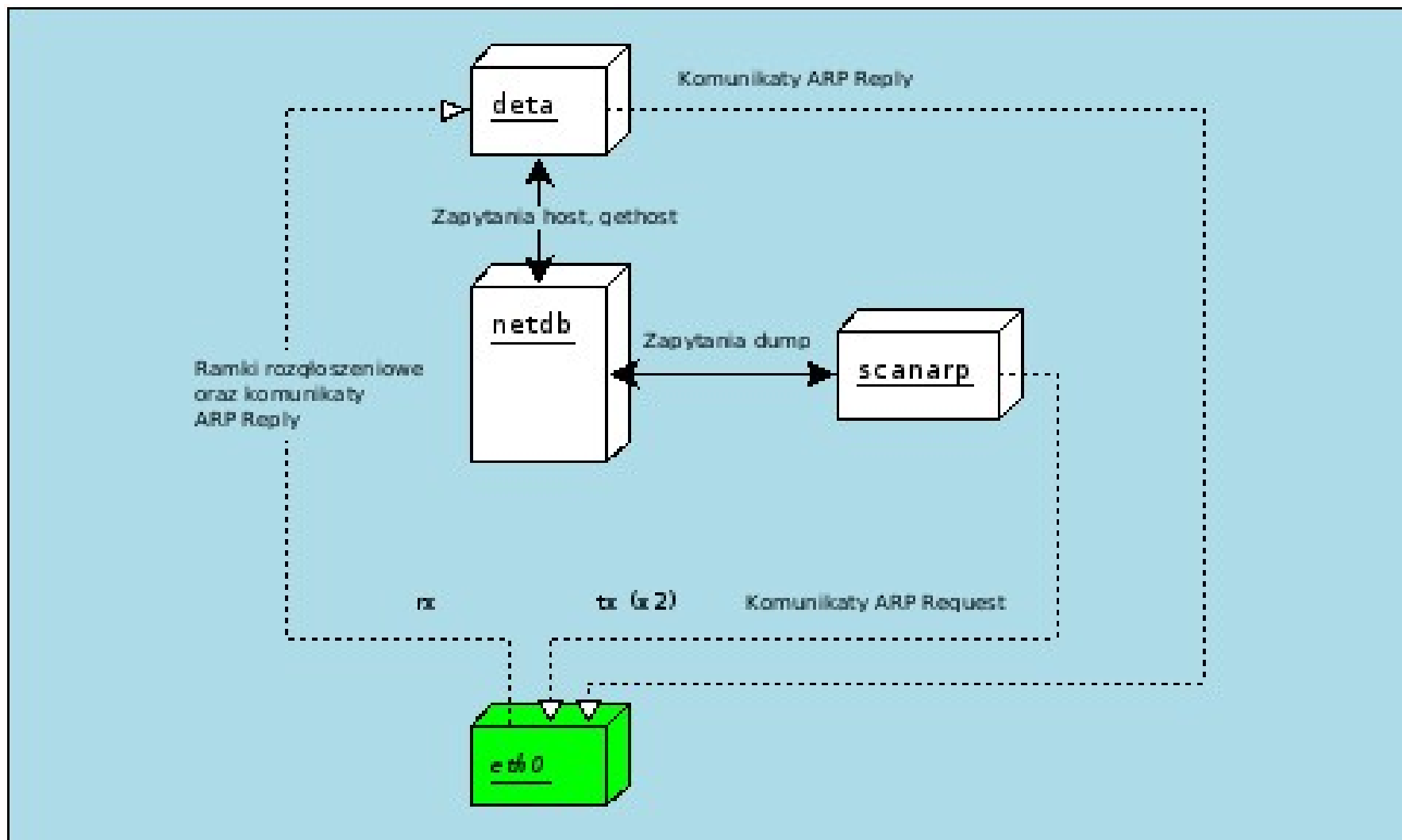


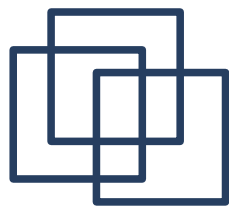
multispoof: Budowa

- Architektura:
 - Procesy uniksowe
 - IPC
- Niskopoziomowa komunikacja z siecią
 - Wstrzykiwanie ramek
 - Podśluchiwanie transmisji
- Wirtualny interfejs sieciowy *tap*
- Rozkładanie obciążenia

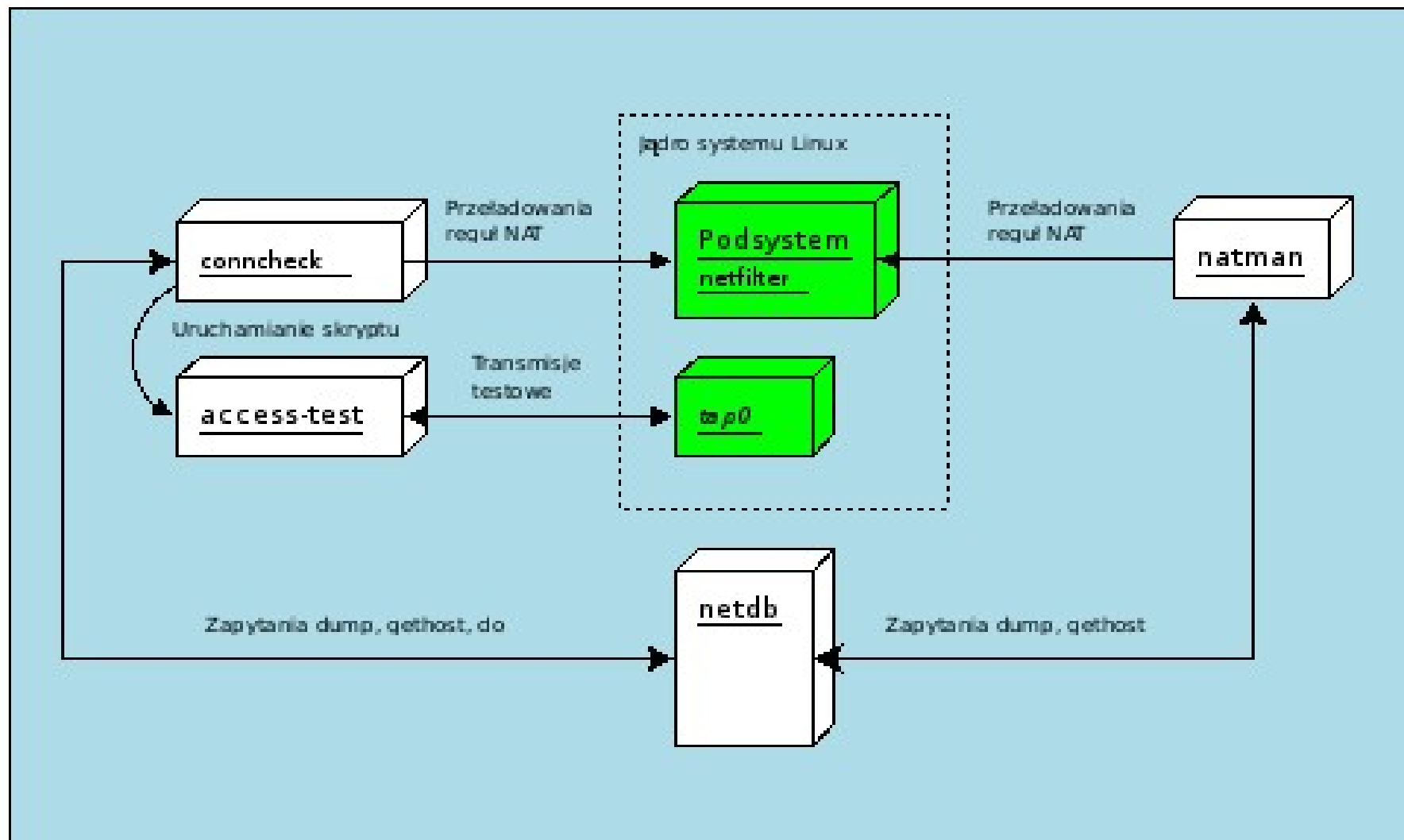


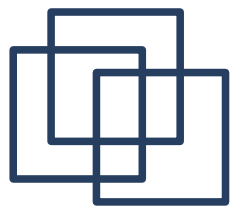
Zbieranie danych o sieci



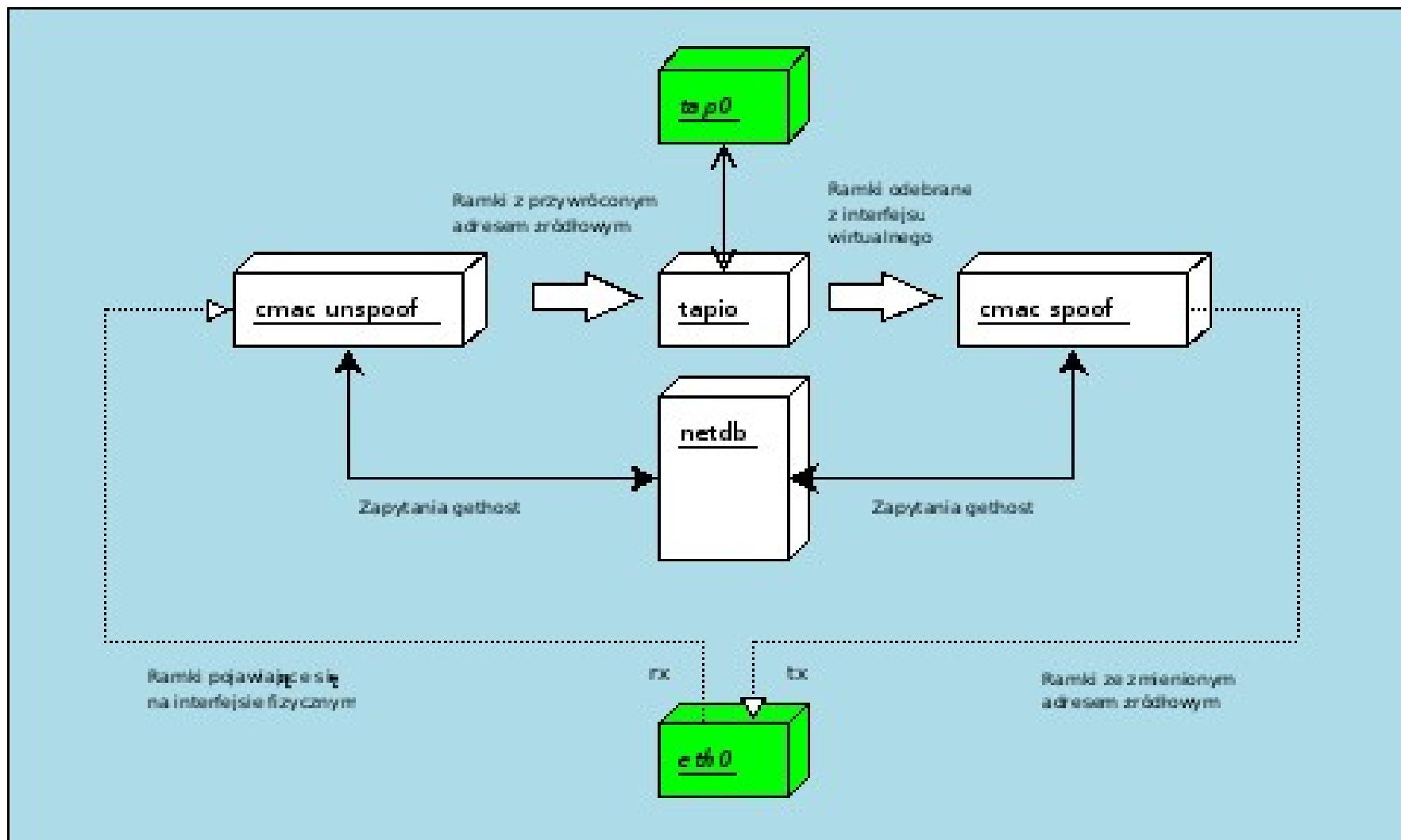


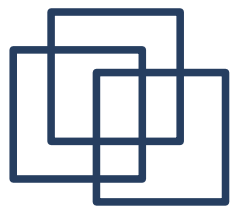
Rozkładanie obciążenia





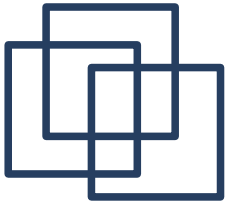
Podmiana MAC



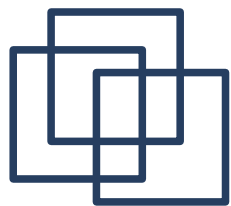


Więcej informacji

- Szczegółowa dokumentacja jak i sam program multispoof są dostępne na:
 - <http://multispoof.cryptonix.org/>
 - <http://cryptonix.org/>



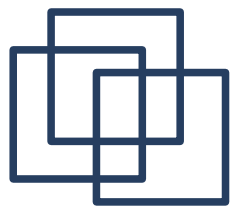
Demonstracja



Obrona przed spoofingiem

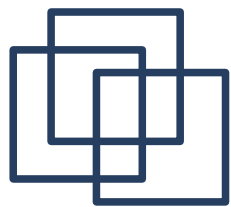
- Metody reaktywne
 - Wykrywanie nadużyć i lokalizowanie sprawców
 - Zazwyczaj tanie
 - Trzeba wykonywać wielokrotnie
- Metody prewencyjne
 - Wprowadzanie zabezpieczeń uniemożliwiających podszywanie się
 - Kosztowne
 - Jednorazowo

Nie można jednoznacznie stwierdzić które podejście jest bardziej korzystne.

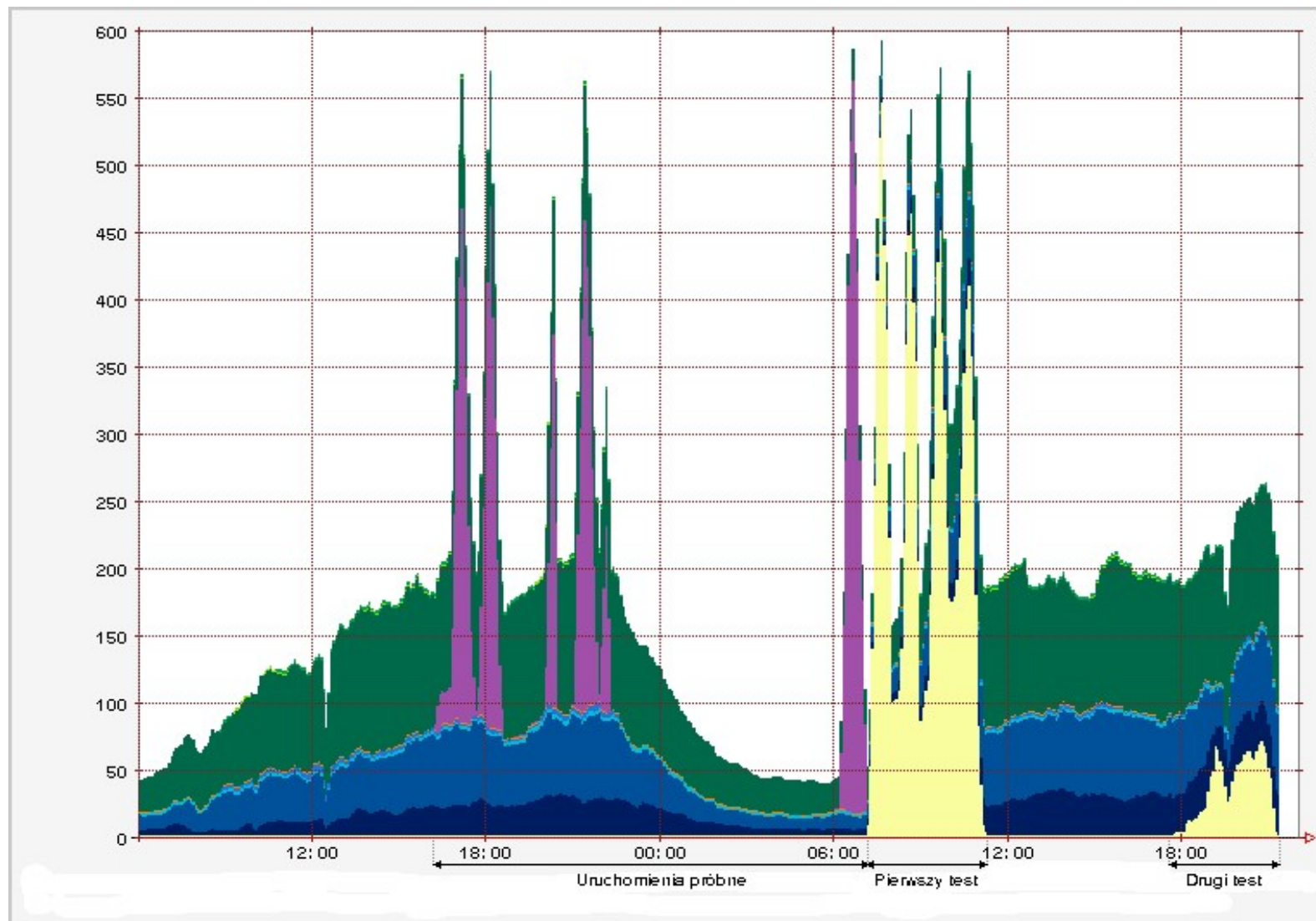


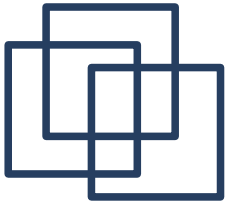
Metody detekcji

- Metody słabe (tylko multispooof):
 - Skanowania ARP, testowanie łączności
 - Brak standardowych transmisji
 - Skanowanie i monitorowanie hostów
- Metody silne (wykrywanie spoofingu):
 - Hosty pułapki
 - Korelacja transmisji sieciowych
 - Moment pojawienia się hosta w sieci
 - Analiza wykorzystania portów przełączników



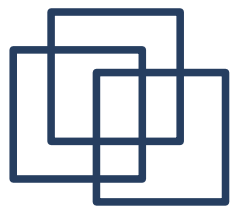
Analiza wyk. portów switcha





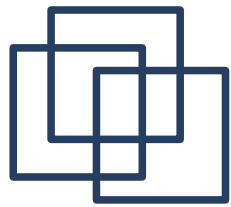
Lokalizacja

- Metoda detekcji dająca odpowiedź na pytanie:
 - „Czy w danej chwili w sieci można zaobserwować mac-spoofing?“
- Dwóch ludzi
- Telefon komórkowy/krótkofalówka
- Mapa sieci
- Samochód i drabina



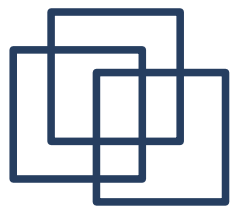
Prewencja sprzętowa

- Inteligentne przełączniki sieciowe
 - Port Security
 - 802.1x
- Bardzo duża skuteczność
- Wysoki koszt
 - urządzeń
 - administracji (Port Security)



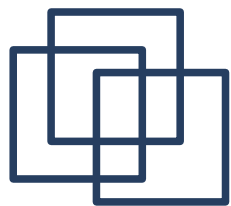
Prewencja programowa

- Model dostępu do usługi w sesjach
 - Rozpoczęcie sesji
 - zabezpieczone przed przechwyceniem danych uwierzytelniających
 - ochrona przed atakiem powtórzeniowym
 - Czas trwania sesji
 - wszystkie transmisje powinny być uwierzytelnione
 - Zakończenie sesji
 - tylko na życzenie użytkownika lub
 - timeout



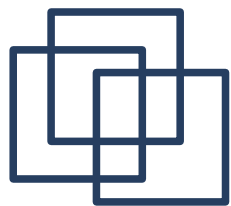
Metody programowe 1

- Autoryzujące serwery proxy
 - Proxy aplikacyjne
 - Każda aplikacja wymaga proxy
 - SOCKS4
 - SOCKS5
 - UDP
 - uwierzytelnianie (silne – ale tylko na papierze)



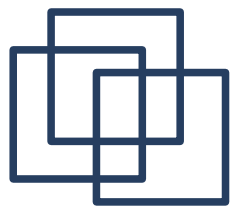
Metody programowe 2

- Portale
 - Słabe uwierzytelnianie
 - Możliwość przedłużania sesji w nieskończoność
- Authpf
 - Silne uwierzytelnianie
 - Przy braku dodatkowych zabezpieczeń możliwe „pasożytnicze“ korzystanie z usługi



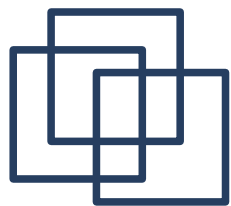
Metody programowe 3

- VPN
 - IPSec (ESP/AH)
 - PPTP (popularność)
 - PPPoE (wykluczenie IP!)
 - L2TP
 - OpenVPN (tokeny, karty chipowe)
 - inne:
 - Peter Gutmann, Linux's answer to MS-PPTP
<http://diswww.mit.edu/bloom-picayune/crypto/14238>



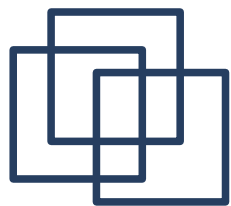
Metody programowe 4

- Metody pomocnicze
 - Firewall
 - DHCP
 - ARP
 - Sprawdzanie zgodności IP-MAC



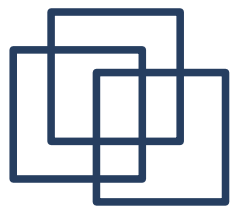
Skuteczność

- Proxy
- Portale, Authpf
- VPN
- Metody pomocnicze



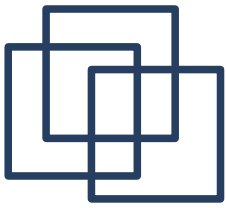
Kierunki dalszego rozwoju

- Utrudnianie wykrywania:
 - Randomizacja (kolejność skanowania, odstępy czasowe, metody testowania)
 - Symulacja normalnej aktywności (klient i serwer)
 - Kontrola wykorzystania adresów
- Antyradar
- Wybór trybu pracy:
 - Wydajność transmisji typu *bulk*
 - Wygoda przy normalnym użytkowaniu
 - Anonimowość (brak skanowania, tylko jedno IP)



Kierunki dalszego rozwoju

- Przełamywanie innych, słabych metod uwierzytelniania:
 - Przechwytywanie danych uwierzytelniających:
 - Proxy
 - Portale
 - Pasożytnicze korzystanie z usługi:
 - Portale
 - Authpf
- Przełamywanie metod dodatkowo zabezp.



Dziękuję za uwagę