System anonimowej i poufnej poczty elektronicznej

Jakub Piotrowski

Plan prezentacji

- Wprowadzenie
- Systemy ochrony poczty elektronicznej
- Anonimowa poczta elektroniczna
- Projekt systemu pocztowego
- Podsumowanie

Wprowadzenie

- Usługi bezpieczeństwa w kontekście poczty elektronicznej
- Anonimowość, niewykrywalność…
- Niewykrywalność???

Usługi bezpieczeństwa

- Integralność
- Poufność
- Autentyczność
- Dostępność
- Niezawodność

Dodatkowe usługi

- Anonimowość:
  - Anonimowość osoby
  - Anonimowość przekazu
- Niewykrywalność

Niewykrywalność

- Ukryta czy niewykrywalna?
- „Użytkownik być może korzysta z systemu komunikacji”
- Jak uzyskać niewykrywalność?
  - Izolacja kanału
  - Ruch nadmiarowy
  - Steganografia

Steganografia

- Ukrywanie komunikatu w innym komunikacie (zatajamy sam fakt porozumiewania się)
- Steganografia sieciowa
- Mała eleastyczność (ograniczona ilość danych + im szersza skala stosowania, tym mniejsza wartość ukrywania)

Systemy ochrony poczty elektronicznej

- Zapewniają integralność, poufność, niezaprzeczalność
- Dodatkowo, oferują możliwość wykorzystania podpisu cyfrowego
- Współpracują ze standardowymi systemami certyfikatów i dystrybucji kluczy

PEM

- Pierwszy standard bezpiecznej poczty
- Wykorzystuje certyfikaty X.509
- Obecnie wyparty przez PGP i S/MIME

PGP

- Popularne narzędzie do szyfrowania poczty elektronicznej
- Wiele odmian (OpenPGP, iPGP, GPG)
- PGP Web of Trust

S/MIME

- Rozszerzenie bezpieczeństwa dla Multipurpose Internet Mail Extensions
- Wykorzystuje X.509
- Kilka trybów pracy (Enveloped-only, Signed-only,Compressed-only, Multiple operations, Certificate management)

Anonimowa poczta elektroniczna

- Ochrona tożsamości nadawcy
- Ryzyko nadużyć (spam, niedozwolona zawartość…)
- Zastosowanie w krajach łamiących wolność słowa

Anonimowość poczty – środki techniczne

- Serwery anonimizujące
- Routing cebulowy
- Mix-y
- Połączenia teleskopowe

Routing cebulowy

- Pakiet zawiera wiele zaszyfrowanych nagłówków
- Każdy z węzłów odczytuje tylko część nagłówka przeznaczoną dla niego
- Węzły znają tylko swoich bezpośrednich sąsiadów
- Nagłówek generowany jest przez nadawcę lub przez pierwszy węzeł

Mix

- Celem mixa jest ukrycie związku między wiadomościami przychodzącymi i wychodzącymi z serwera
- Aby to osiągnąć, wiadomości są dzielone na pakiety, szyfrowane, wysyłane w losowej kolejności
- Każda wiadomość powinna być przetwarzana dokładnie raz

Połączenia teleskopowe

- Nadawca tworzy szyfrowaną sesję z pierwszym węzłem…
- … z drugim…
- … aż do odbiorcy
- Wykorzystywane w systemie TOR
- Nadawca może komunikować się z odbiorcą jak i węzłami pośredniczącymi z zachowaniem poufności względem pozostałych węzłów

Systemy poczty anonimowej

- Anon.penet.fi – remailer Helsingiusa
- Cypherpunk
- Mixmaster
- Mixminion

Remailer Helsingiusa

- Zamiana adresu nadawcy na „*anXXXX@anon.penet.fi*”
- Łatwość wykorzystania (sterowanie za pomocą nagłówka wiadomości)
- Brak szyfrowania
- Jeden serwer

Cypherpunk

- Podstawowa wersja to jeden serwer
- Wykorzystuje PGP do szyfrowania wiadomości między nadawcą a serwerem
- Przy odrobinie wysiłku możliwość wykorzystania wielu serwerów
- Natychmiastowy przekaz wiadomości

Mixmaster

- Oparty o sieć mixów
- Przekazywanie wiadomości podzielonych na zaszyfrowane pakiety o stałej długości, z odpowiednim odstępem czasowym
- Treść wiadomości szyfrowana algorytmem symetrycznym, nagłówek – algorytmem klucza publicznego
- Wykorzystanie routingu cebulowego

Mixminion

- Podstawowe elementy takie jak w Mixmasterze, ale…
- Istnieje możliwość odpowiadania na anonimowe wiadomości (również anonimowego)
- Dwupoziomowa hierarchia sieci
- Brak funkcjonalnych bram wyjściowych

Mixminion

- „Exit Policy”
- Zróżnicowane typy węzłów (otwarte, pośredniczące, lokalne)
- Możliwość włączenia do kaskady mixów serwerów typu Mixmaster

Freenet

- W pełni rozproszony system p2p, oferujący poufność i anonimowość komunikacji
- Szyfrowanie komunikacji, szyfrowanie zawartości buforów
- Każdy węzeł to serwer i proxy
- Routing cebulowy
- Przeszukiwanie zasobów na podstawie skrótów plików

Projektowany system pocztowy

- Nazwa
- Motywacja
- Architektura sieci
- Usługi bezpieczeństwa
- Przyszłość…

Hermod?

- *„W mitologii nordyckiej Hermod był bogiem-posłańcem. Czasem opisywany jest jako jeden z synów Odyna, boga wojny i wojowników, a czasem jako deifikowany heros. Zasłynął mityczną wyprawą do bogini Hel, władającej krainą umarłych śmiercią niechwalebną, której miał bezpiecznie dostarczyć prośbę swojego ojca o uwolnienie Baldura, boga dobra.”*

Hermod - motywacja

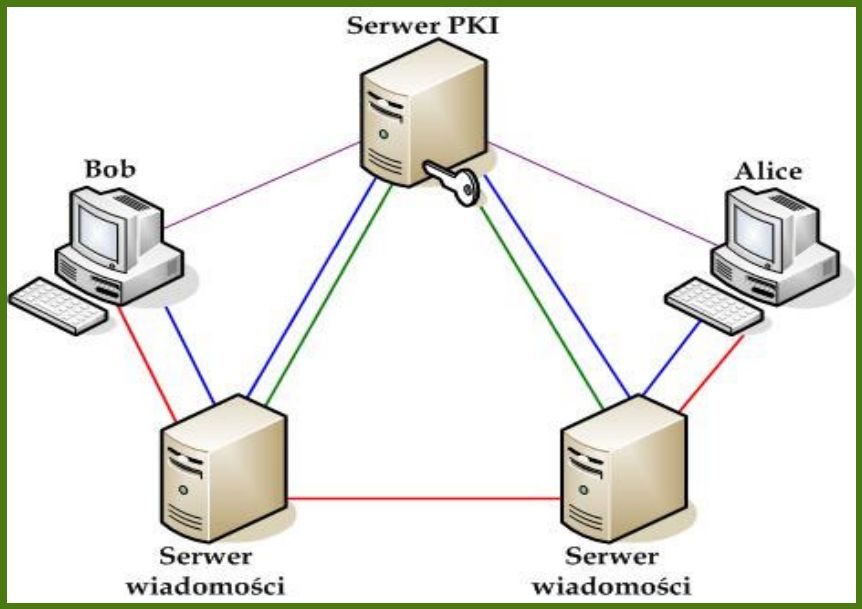
- Oferowanie usług bezpieczeństwa + anonimowości + …- w ramach jednego rozwiązania
- Rozsądna ilość węzłów
- Niewykrywalność

Hermod – architektura sieci

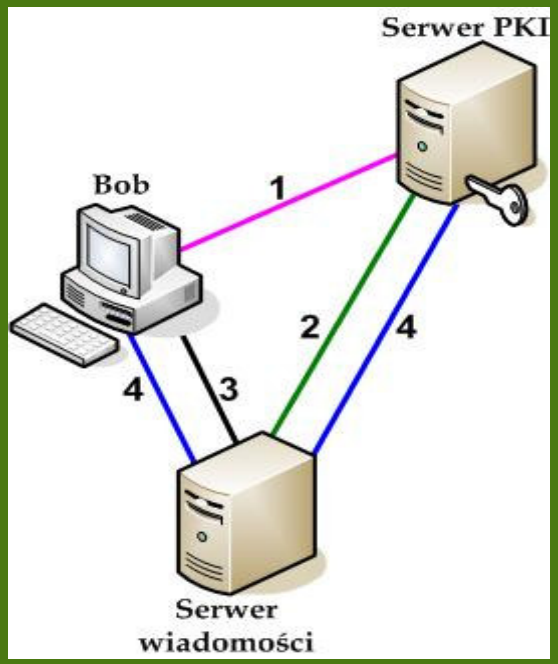
- 3 rodzaje węzłów
- Hierarchiczny układ sieci
- Kontrola obciążenia

Hermod – rodzaje węzłów

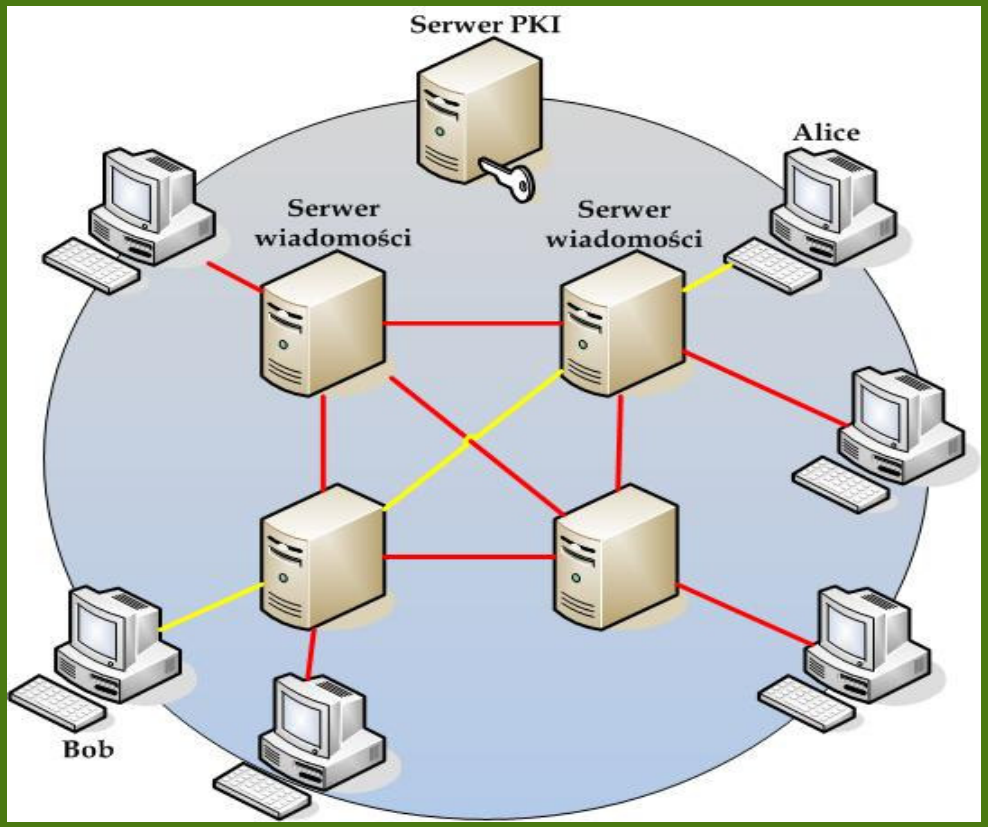
- Serwer kluczy
- Serwer wiadomości
- Serwer lokalny



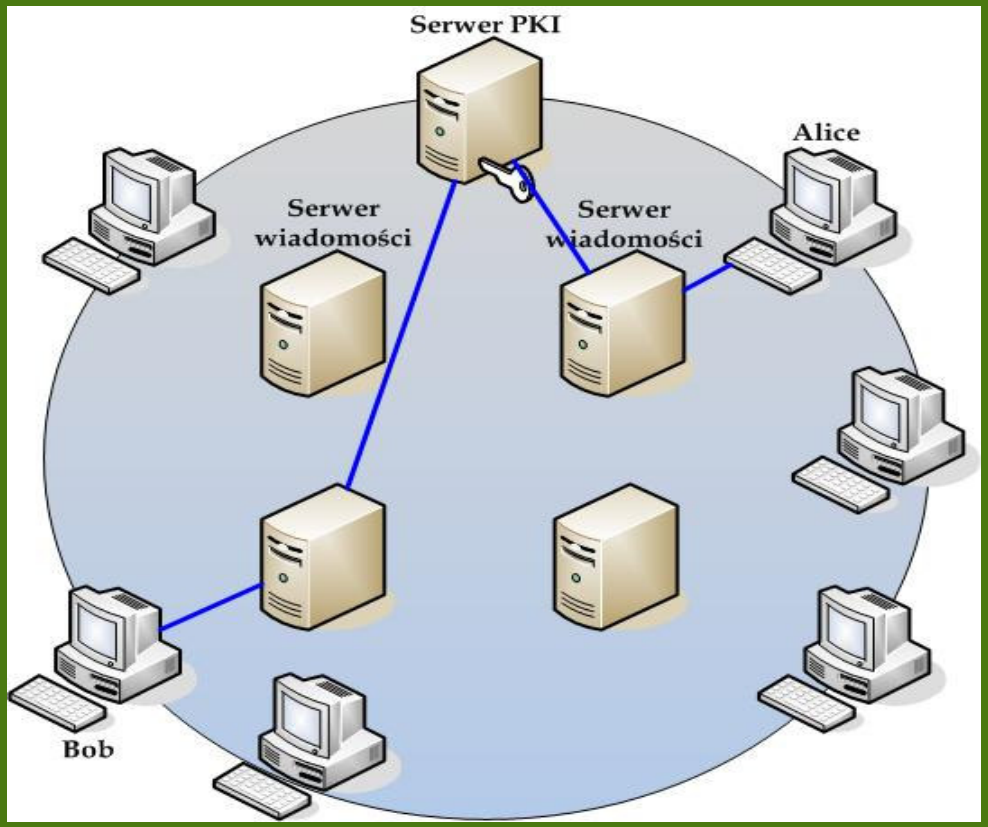
Hermod – rejestracja użytkowników



Sposób przesyłania wiadomości



Sposób przesyłania kluczy



Hermod – z punktu widzenia użytkownika

- SnowMail zaimplementowanym klientem pocztowym
- Możliwość rozszerzenia możliwości przez włączenie lokalnego serwera pocztowego

Hermod – oferowane usługi

- Poufność
- Szyfrowanie e2e
- Szyfrowanie komunikacji między każdą parą węzłów
- Połączenia teleskopowe

Hermod – oferowane usługi

- Anonimowość
- Wiedza o nadawcy kontrolowana przez nadawcę
- „zwykłe” usuwanie nadawcy z nagłówka
- Szyfrowanie + ruch nadmiarowy metodą ochrony tożsamości

Hermod – usługi bezpieczeństwa

- Niewykrywalność
- Ruch nadmiarowy – pakiety o stałym rozmiarze, wysyłane w stałych odstępach czasu, zaszyfrowane

Hermod – możliwości rozwoju

- Dodanie bram łączących ze „światem zewnętrznym”
- Konieczność stworzenia wydajnego mechanizmu zarządzania kluczami i obciążeniem sieci

Podsumowanie

- Hermod daje połączenie anonimowości z poufnością w jednym systemie, a dodatkowo – niewykrywalność
- Anonimowość i niewykrywalność uzyskiwana jest kosztem opóźnień i ograniczenia funkcjonalności

Dziękuję za uwagę