Sieci Komputerowe

Grzegorz Gutowski

Uniwersytet Jagielloński

2023/24

Bezpieczne sieci

IPsec

Bezpieczne sieci

IPsec

VPN

IPSec

- Szyfrujmy cały ruch IP

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared
  - IKE : wersje Needham-Schroeder

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared
  - IKE : wersje Needham-Schroeder
  - IKE : IPSECKEY w DNS (RFC 4025)

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared
  - IKE : wersje Needham-Schroeder
  - IKE : IPSECKEY w DNS (RFC 4025)
- Transmisje
  - Authentication Header
  - Encapsulating Security Payload

THEORETICAL COMPUTER SCIENCE Jagiellonian University

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared
  - IKE : wersje Needham-Schroeder
  - IKE : IPSECKEY w DNS (RFC 4025)
- Transmisje
  - Authentication Header
  - Encapsulating Security Payload
- Tunele
- Czy DNS jest bezpieczny?
- Komu zaufać?

IPSec

- Szyfrujmy cały ruch IP
- Wymiana kluczy (Security Associations)
  - pre-shared
  - IKE : wersje Needham-Schroeder
  - IKE : IPSECKEY w DNS (RFC 4025)
- Transmisje
  - Authentication Header
  - Encapsulating Security Payload
- Tunele
- Czy DNS jest bezpieczny?
- Komu zaufać?
- Ile to wszystko kosztuje?

OpenVPN

Sieci P2P

- BitTorrent

Modele

- Klient – serwer
- Centralny serwer
- Sieci bez centrum
- Sieci hybrydowe

Połączenia

- Sieci nad sieciami
- Skąd się biorą adresy
- Jak łączyć komputery bez publicznych adresów
  - SOCKS, etc.
  - NAT
  - IGD w uPNP
  - IPv6

Połączenia

- Sieci nad sieciami
- Skąd się biorą adresy
- Jak łączyć komputery bez publicznych adresów
  - SOCKS, etc.
  - NAT
  - IGD w uPNP
  - IPv6 ?

BitTorrent

- plik torrent

BitTorrent

- plik torrent
- tracker

BitTorrent

- plik torrent
- tracker
- ściągaj po kawałku

BitTorrent

- plik torrent
- tracker
- ściągaj po kawałku
- ściągaj najrzadsze fragmenty

BitTorrent

- plik torrent
- tracker
- ściągaj po kawałku
- ściągaj najrzadsze fragmenty
- szukaj dobrych partnerów
  - współpracuj z dobrymi
  - duś złych

BitTorrent

- plik torrent
- tracker
- ściągaj po kawałku
- ściągaj najrzadsze fragmenty
- szukaj dobrych partnerów
  - współpracuj z dobrymi
  - duś złych
- magnet
- DHT

THEORETICAL COMPUTER SCIENCE
Jagiellonian University

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać” o potęgi dwójki

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać” o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać” o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać” o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać” o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać" o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność
- replikacja (wgraj dane do k następników)

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać" o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność
- replikacja (wgraj dane do k następników)
- ponowne rozgłaszanie zasobów (przygotowanie na wyłączenia)

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać" o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność
- replikacja (wgraj dane do k następników)
- ponowne rozgłaszanie zasobów (przygotowanie na wyłączenia)
- trudno wyszukiwać czymś innym niż haszem

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać" o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność
- replikacja (wgraj dane do k następników)
- ponowne rozgłaszanie zasobów (przygotowanie na wyłączenia)
- trudno wyszukiwać czymś innym niż haszem
- czy możemy wierzyć w przechowywane wartości?

DHT, Chord

- m-bitowe identyfikatory komputerów i danych
- dane o k przechowywane w $succ(k)$
- wystarczy umieć się komunikować z następnikiem
- ale lepiej umieć „skakać" o potęgi dwójki
- Podłączanie się do sieci
  - wystarczy znać jeden komputer
  - trzeba wybrać identyfikator
  - wstawić się do sieci
  - przejąć swoją odpowiedzialność
- replikacja (wgraj dane do k następników)
- ponowne rozgłaszanie zasobów (przygotowanie na wyłączenia)
- trudno wyszukiwać czymś innym niż haszem
- czy możemy wierzyć w przechowywane wartości?
- od czasu do czasu zapytaj następnika o poprzednika

TOR

- problemy z anonimowością

TOR

- problemy z anonimowością
- routing

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL
- ukrywanie klienta

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL
- ukrywanie klienta
- ukrywanie serwera

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL
- ukrywanie klienta
- ukrywanie serwera
- Z kim się łączę wpisując

  https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL
- ukrywanie klienta
- ukrywanie serwera
- Z kim się łączę wpisując

  https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
- HSDir oparte o DHT

TOR

- problemy z anonimowością
- routing
- SOCKS + SSL
- ukrywanie klienta
- ukrywanie serwera
- Z kim się łączę wpisując

  https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
- HSDir oparte o DHT
- https://facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion