ANONYMITA V POČÍTAČOVÝCH SIEŤACH S VYUŽITÍM ONION ROUTINGU

Peter Csiba
Vedúci: Mgr. Peter Gaži PhD.

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

25.06.2012

Obsah prezentácie

- Motivácia a ciele práce.
- Úvod do problematiky.
- Prínos a záver.

Motivácia anonymity

- Prehľadávanie na Internete neskrýva identitu užívateľa.
- Ochrana súkromia.
- Obchádzanie cenzúry.

Anonymný prístup k verejným zdrojom.

Ciele práce

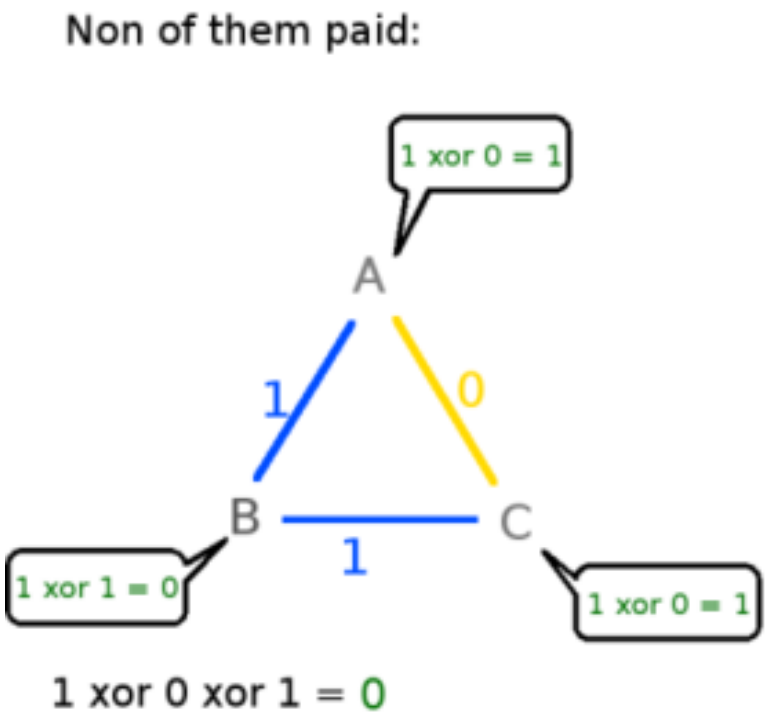
- Poskytnúť prehľad používaných systémov na dosiahnutie anonymity v počítačových sieťach.
- Zamerať sa na systém Tor.
- Slovenčina.
- Diskutovať o možných útokoch.
- Implementovať niektoré z nich.

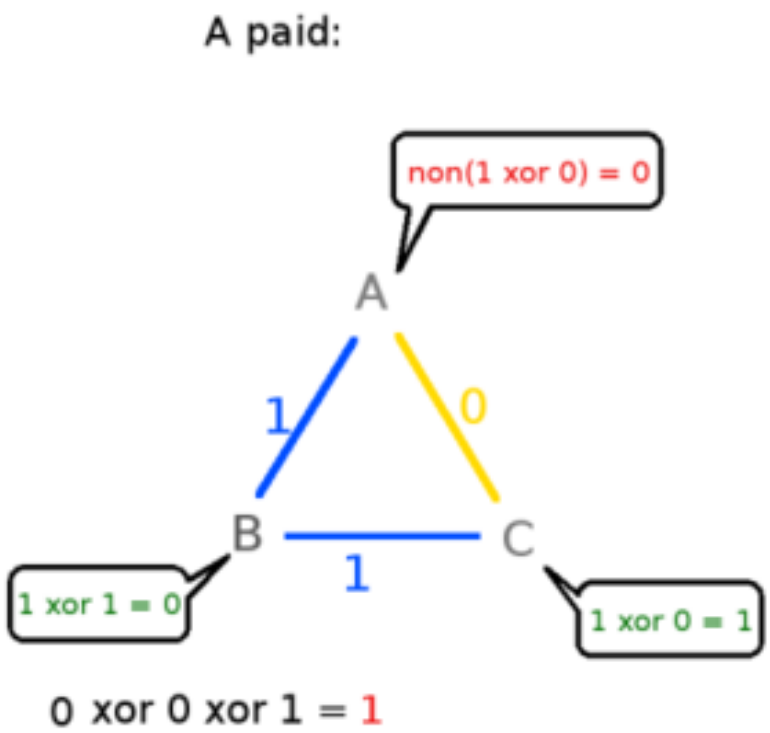
Anonymné počítačové siete

- Za anonymnú komunikáciu považujeme výmenu informácií medzi dvoma účastníkmi, ktorú "je ťažké" vystopovať.
- Najčastejšie predpokladáme verejnú sieť so špeciálnymi zariadeniami.
- Rozlišujeme ich podľa času odozvy a podľa toho prepokladáme aj schopnosti účastníka.

Problém večerajúcich kryptológov

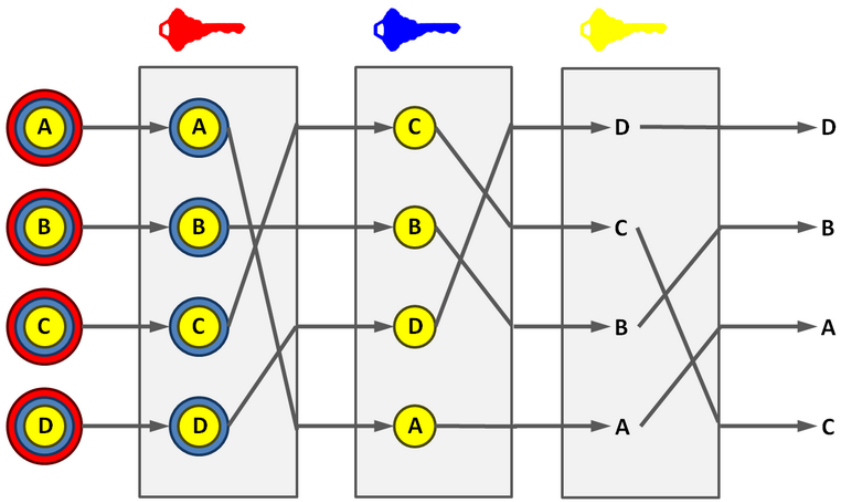
- Teoretický protokol.
- Dokázateľná absolútna anonymita.





Mixy

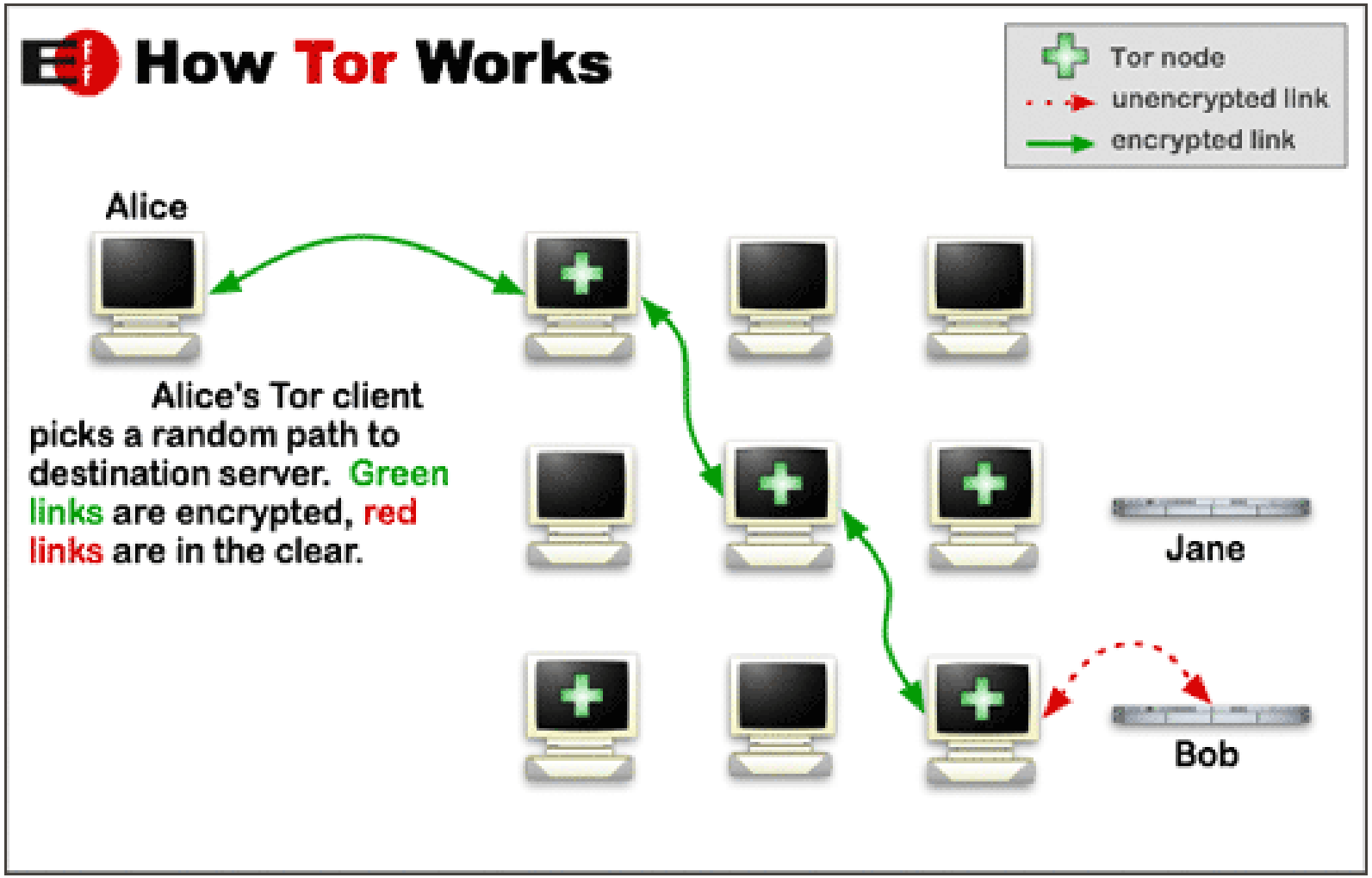
- Prvý anonymný systém navrhnutý Chaumom v roku 1981.
- S veľkou odozvou.
- V prípade pasívneho útočníka vie zabezpečiť absolútnu anonymitu.



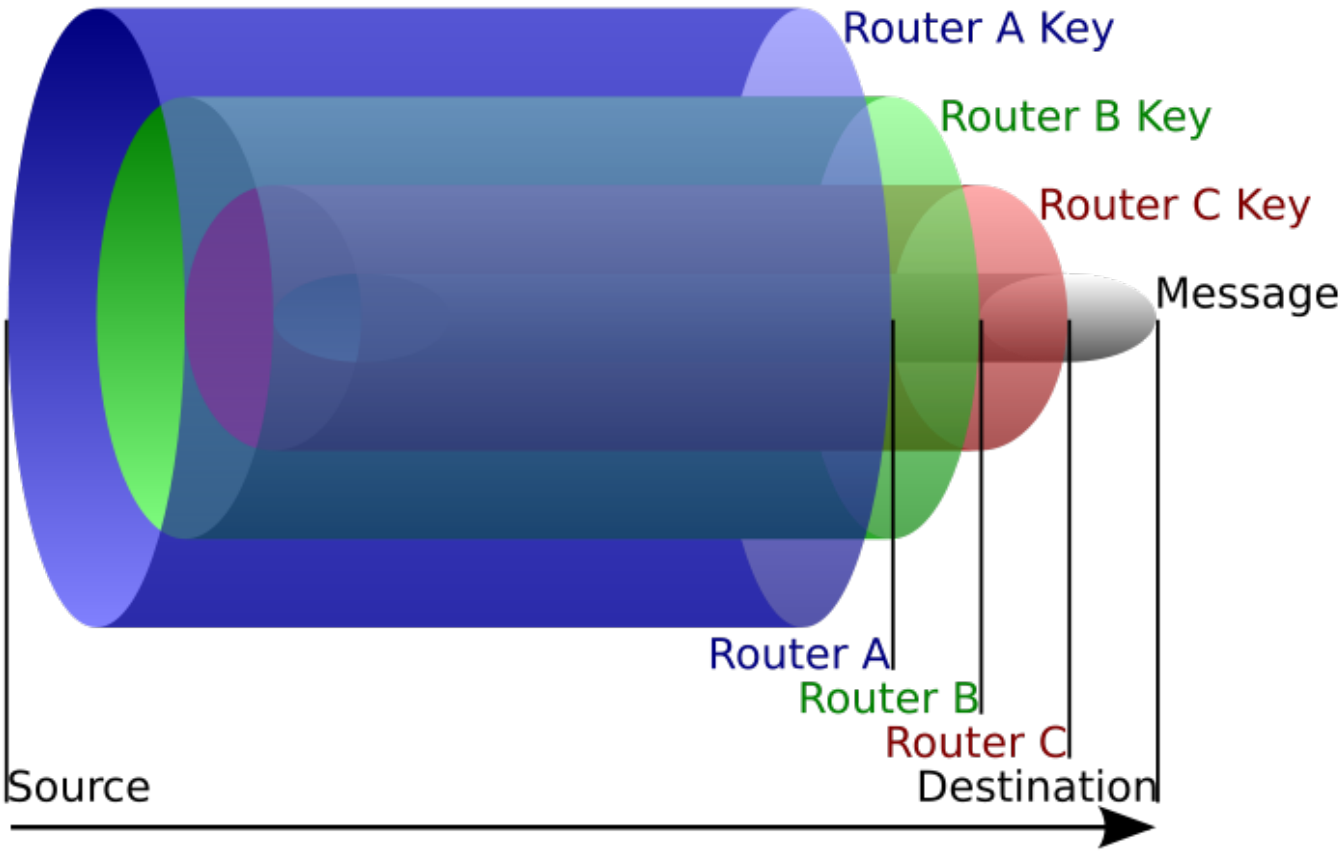
Tor - The Onion Router

- Peer-to-peer systém vytvárajúci náhodné obvody cez sieť routrov.
- Open source.
- Anonymita, integrita, šifrovanie.
- Jednoduché na používanie.

Tor - The Onion Router



Tor - The Onion Router



Tor - The Onion Router

- Incremental path building.
- Hidden services and rendezvous points.
- Bridges.

Útoky

- Potenciálne útoky.
  - Odtlačky webových servrov.
  - Útok zahltením.
- Zamedzené útoky.
  - Tagging attack.
  - Replay attack.

Prínos

- Aktuálny prehľad anonymných sietí.
- Slovenčina.

Priestor na otázky

Ďakujem za pozornosť!

Ďakujem za pozornosť!