# Mixy a systémy pro poskytování anonymity

Marek Kumpošt, Vašek Matyáš
Fakulta informatiky, MU Brno
{xkumpost|matyas}@fi.muni.cz

# Obsah přednášky

- Motivace
- Charakteristiky anonymity
- Typy mixů – prezentace Mixminionu
  - kterak odeslat anonymní emailovou zprávu
- Měření anonymity
- Onion routing – jiný přístup pro poskytování anonymity

# Motivace pro anonymitu

- Ochrana osobních dat
- Anonymita uživatele, lokace, transakce
- Anonymita je prvkem funkčnosti pro systémy poskytující ochranu informačního soukromí (privacy)
  - pseudonymita
  - nespojitelnost
  - nesledovatelnost
- Nutnost zajistit anonymitu v mnoha případech
  - informace o zdravotním stavu (anonymita vs. pseudonymita)
  - elektronické volby
  - svoboda slova
  - udání informací o trestné činnosti apod.

# Anonymita – rub a líc

- anonymní zneužití útočníkem pro vedení útoků
  - útočník je nezjistitelný
- využití systémů poskytujících anonymitu chrání uživatele před krádeží jeho identity

# Definice anonymity

- *CC:* Uživatel může využít zdroj nebo službu bez odhalení své identity.
- *Mixy:* Stav bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině.
  - Anonymitní množina je množinou všech možných subjektů (obvyklí podezřelí ☺)
    - s ohledem na odesilatele možných odesilatelů,
    - s ohledem na příjemce možných příjemců atd.
- Význam modelu útočníka
  - pasivní/aktivní, lokální/globální
  - anonymita se vyjadřuje v závislosti na daném modelu

# Charakteristika anonymity

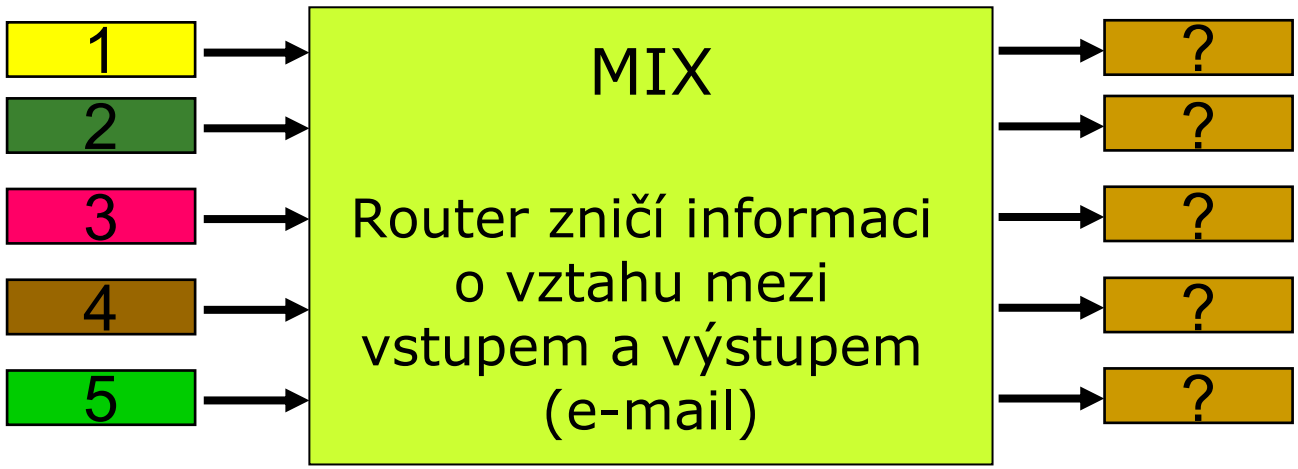
- Kvantitativní
  - velikost anonymitní množiny
    - různá pro odesílatele / příjemce
    - různé přístupy při určování anonymitní množiny
    - nelze brát v úvahu pouze velikost množiny
    - potřeba zohlednit i „chování“ subjektů
- Kvalitativní
  - odolnost proti různým typům útoků
- Analýza provozu
  - snaha útočníka získat identifikační údaje účastníků komunikace
- Falešný provoz v síti
  - kompenzace malého provozu v síti

# Motivace pro mixy

- Internetový provoz je vysledovatelný a data jsou svázána s jejich odesílatelem
- Mixy jsou routery měnící tok a výskyt dat na komunikačním kanálu
  - vstupy nelze jednoduše spojit s výstupy
  - skrytí obsahu zprávy: kryptografie
  - změna toku zpráv: prodlevy, přeuspořádání, falešné zprávy
  - je třeba vyvážit hladinu přípustné latence/ceny vs. míry poskytnuté anonymity
- Anonymitní komunikační sítě
  - Mixovací sítě/ mixovací kaskády (vodopády)
  - Peer-to-peer systémy

# Typy mixů

- Chaum / prahový (threshold) mix (1981)
  - shromáždí N zpráv
  - přeuspořádání zpráv
  - odeslání zpráv (fire/flush)



# Typy mixů (2)

- Pool mixy: rozšíření původního návrhu (Chaum) přidáním vnitřní paměti (pool)
- Zprávy jsou zpracovány v dávkách (batches)
- Podmínka pro odeslání zpráv
  - časová/prahová
  - deterministická/náhodná
- Algoritmus pro výběr zpráv z paměti
  - není paměť / statická paměť / dynamická paměť
  - ovlivňuje výkon a poskytovanou míru anonymity

# Typy mixů (3)

- continuous / stop-and-go mixy
- mixování založené na prodlevách
- zprávy jsou po určitou dobu pozastaveny v mixu
- problém při malém provozu v síti
- musí existovat služba poskytující informace pro uživatele

# Typy mixovacích sítí

- při anonymní komunikaci se nespoléhá pouze na jeden mixovací uzel
- uzly se spojují do mixovacích sítí
  - zapojení jako síť mixů – nerestriktivní směrování (uživatel si cestu zvolí sám)
  - zapojení jako „kaskáda“ mixů – omezení na směrování (uživatel použije cestu v závislosti na zapojení mixů)
  - hybridní zapojení:
    - několik „kaskádových“ cest sítí – uživatel si může vybrat
    - volba sousedních mixů – mix určí množinu svých možných následníků, uživatel si náhodně jeden zvolí

# Dummy traffic (umělý provoz)

- potřeba pro:
  - zvýšení odolnosti proti vybraným útokům
  - kompenzace malého provozu na síti
  - zvýšení anonymity
  - poskytnutí nevystopovatelnosti
- falešné zprávy (fake messages)
  - generují uživatelé / mixy, mixy je zahazují
  - útočník nerozezná falešnou zprávu od skutečné

# Mixminion

- www.mixminion.net
- informace o serverech v síti
- odeslání anonymního emailu
  - specifikace cesty skrz mixovací síť
- SURB – Single Use Reply Block – odpověď na anonymní emailovou zprávu
  - omezená platnost
  - zašifrovaná struktura s popisem cesty „zpět“
  - odpověď je v síti nerozlišitelná
- doručená anonymní zpráva

# Měření anonymity

- Anonymitní množina
  - množina všech uživatelů, kteří mohli poslat danou zprávu – anonymitní množina odesílatele
- Velikost množiny není příliš dobrý ukazatel
  - různé chování uživatelů odesílatelů/příjemců zpráv
- Entropie – použití mj. i pro určení velikosti anonymitní množiny
- Je vhodné zohlednit i kontextové informace se vztahem ke zkoumanému systému
  - časy odesílání zpráv, četnost zpráv, velikost zpráv, IP a MAC adresy…

# Onion Routing - Úvod

- Co to je Onion Routing?
  - systém pro zabezpečenou komunikaci při použití veřejné sítě
  - systém pro obousměrné anonymní spojení
  - poskytuje téměř real-time anonymní spojení pro různé služby na Internetu (www, ssh, ftp, …)
  - volně dostupný systém
- TOR – The Onion Routing
  - onion routing systém druhé generace

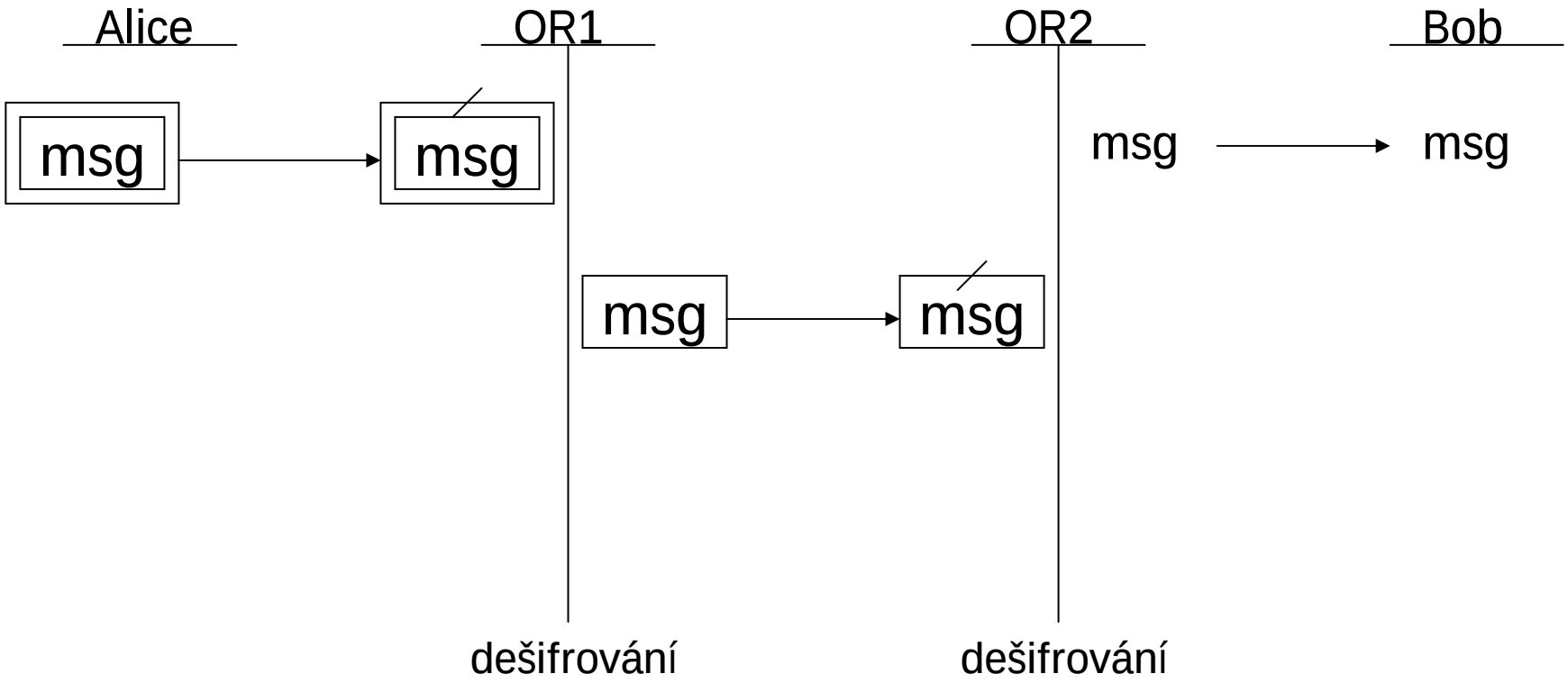
# Proč Onion Routing systémy?

- máme přece mixovací systémy
  - zpoždění je pro některé aplikace nepřípustné
- lze vysledovat odesílatele zašifrované zprávy a odhalit, kdo s kým komunikuje
  - zabezpečit jak obsah zprávy, tak informaci o komunikujících stranách
- zamezit prozrazení identity subjektu do sítě
- systém poskytující anonymní přenos dat pro různé služby Internetu bez nutnosti modifikace těchto služeb (ssh, rlogin, VPN, …)
  - pracující jako proxy server

# Odstranění identif. informace

- data jsou před odesláním do sítě filtrována
  - dojde k odstranění informace o odesílateli dat
  - útočník nemá možnost vystopovat účastníky komunikace
  - není možný útok analýzou datového toku (traffic analysis)
- identifikační data o účastnících komunikace je nutné poslat zabezpečeným kanálem
  - pokud je přenos těchto dat potřeba

# Schéma zpracování zprávy



# Symetrická vs. asymetrická kryptografie

- Symetrická kryptografie
  - používá se tajní klíč pro šifrování i dešifrování (AES, DES)
  - obě strany musí tento klíč zdát – problematická distribuce
- Asymetrická kryptografie nebo kryptografie s veřejným klíčem
  - různé klíče pro šifrování/dešifrování (veřejný a privátní klíč)
  - veřejný klíč je všem dostupný (keyservery)
  - př. RSA, ElGamal, …

# Zpracování dat

- přes sérii Onion Routerů (OR) namísto přímého spojení klient <-> server
  - OR síť umožňuje anonymní spojení klienta a serveru přes veřejnou síť
  - každý OR zná pouze svého předchůdce a následníka
  - vzájemné spojení OR je permanentní
  - komunikační cesta (okruh) je definována při sestavení komunikačního kanálu
  - data putující tímto kanálem jsou při každém průchodu přes OR „změněna“ v důsledku dešifrování

# Zpracování dat (2) – proxy

- k OR síti se přistupuje přes spec. proxy
  - v původním návrhu musí být pro každou aplikaci speciální proxy – podpora omezeného množství aplikací
  - aplikace se spojí s aplikační proxy
  - aplikační proxy data upraví do podoby srozumitelné pro OR síť
  - aplikační proxy vytvoří spojení s OR proxy
    - dojde k vytvoření komunikačního okruhu
  - okruh je připraven přenášet data

# Zpracování dat (3) – k. okruhy

- OR proxy vytvoří vrstvenou datovou strukturu – Onion a pošle ji do sítě (využití PK)
- každý OR odstraní vrchní vrstvu (dešifruje); získá materiál pro ustavení symetrického klíče; pošle data na další OR
- poslední OR na cestě předá data příjemci
- výsledkem je vytvořený komunikační okruh (ustanovení symetrických klíčů mezi OR a odesílatelem)

# Zpracování dat (4)

- každý OR si ukládá seznam přeposlaných „paketů“ dokud nevyprší jejich platnost
  - takové pakety OR zahazuje
- data jsou šifrována proudovou šifrou se symetrickým klíčem
  - při každém průchodu přes OR se z pohledu útočníka tato data „změní“

# TOR

- systém pro poskytování anonymity založený na komunikačních okruzích s malou latencí
  - TOR je následníkem původního návrhu OR
  - do původního návrhu nebyly zahrnuty nové požadavky na funkcionalitu systému
- TOR přináší následující vylepšení funkcionality
  - dokonalé „dopředné“ utajení
  - není nutné vyvíjet specializované aplikační proxy
    - podpora většiny TCP-based aplikací bez jejich modifikace
  - více TCP proudů může sdílet komunikační okruh
  - data mohou OR síť opustit v libovolném místě
  - kontrola možného zahlcení OR sítě

# TOR (2)

- podpora adresářových serverů
  - informace o routerech a jejich stavu
  - uživatelé si mohou tyto informace vyžádat
- end-to-end testování integrity přenesených dat
  - původní návrh vůbec neprováděl testování integrity
  - ochrana proti tzv. tagging útokům
- „místa setkání“ a skryté služby
- nevyžaduje změny v jádře OS
- volně dostupný systém

# Perfect forward secrecy

- v původním návrhu si mohl útočníkův uzel ukládat datový tok a poté útokem donutit následující uzly dešifrovat tato dat
- TOR používá jiný přístup při budování komunikačního okruhu – teleskopické ustavení cesty
  - odesílatel ustanoví symetrické klíče se všemi uzly v okruhu
  - po smazání těchto klíčů již není možné dešifrovat starší data
- celý proces budování komunikační cesty je více spolehlivý

# Místa setkání a skryté služby

- novinka TORu – v původním návrhu tato služba nebyla
- pro zajištění anonymity příjemce (serveru, služby apod.)
  - možnost řízení příchozího datového toku
- zabrání Denial of Service útokům
  - útočník neví, kde je daný server, protože ten je schovaný za několika OR
- klient zvolí místo setkání v OR síti, přes které se spojí se „serverem“ – resp. na OR, které server zveřejní
  - server prostřednictvím adr. služby zveřejní uzly, kde čeká na spojení od klientů

# Několik užitečných odkazů

- www.freehaven.net
  - Stránky projektu
- www.mixminion.net
  - Mixminion
- tor.freehaven.net
  - TOR – OR
- www.anonymizer.com
  - Existující systém pro poskytování anonymity, nutnost registrace
- …

# Otázky?

Marek Kumpošt
Vašek Matyáš