Bezpečnost v IT

9. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

11. 4. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- VPN
- IPSsec
- WireGuard
- Tor

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Výroční zpráva Českého bezpečnostního týmu CSIRT.cz

Virtuální privátní sítě (VPN)

- Virtuální sítě využívající infrastrukturu větší sítě (např. Internet)
- (většinou) přidává bezpečnostní prvky pro přenos nezabezpečeným kanálem

Virtuální privátní sítě (VPN)

- Virtuální sítě využívající infrastrukturu větší sítě (např. Internet)
- (většinou) přidává bezpečnostní prvky pro přenos nezabezpečeným kanálem
- Privátní adresace
  - Podsíť oddělená od větší sítě
  - Neveřejný rozsah (10.x.x.x), neroutovatelný
  - Potřeba oddělit od ostatních sítí (filtrace)

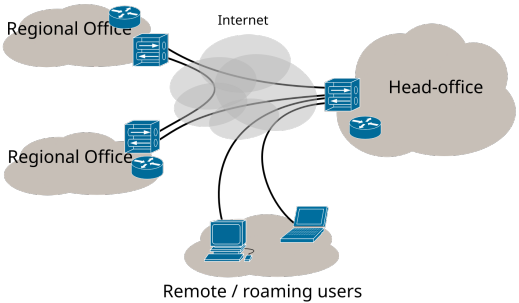
Virtuální privátní sítě (VPN)

- Virtuální sítě využívající infrastrukturu větší sítě (např. Internet)
- (většinou) přidává bezpečnostní prvky pro přenos nezabezpečeným kanálem
- Privátní adresace
  - Podsíť oddělená od větší sítě
  - Neveřejný rozsah (10.x.x.x), neroutovatelný
  - Potřeba oddělit od ostatních sítí (filtrace)
- Tunel
  - Zapouzdření privátních IP paketů do paketů transportní sítě
  - Protokol GRE RFC-1701
  - „IP over IP“ v transportním paketu GRE hlavička, pak privátní IP paket
  - Zapouzdření privátních IP paketů do TCP/UDP transportní sítě (OpenVPN)
  - Velmi časté použití, např. IPsec
  - Propojení geograficky oddělených lokací do jedné sítě

VPN Tunel

- Základní módy
  - Počítač – počítač (např. WireGuard)
  - Router – Router – spojení dvou sítí přes nezabezpečenou (klienti nemusí vědět)
  - Počítač – router – připojení jednoho klienta do interní sítě

Internet VPN



Obrázek: https://en.wikipedia.org/wiki/Virtual_private_network

VPN – základní požadavky

- Řízení přístupu – „Kdo může mít přístup do privátní sítě?“
- Zajištění integrity dat – Nikdo po cestě nemůže data podvrhnout
- Zajištění důvěrnosti dat
  - Privátní pakety putují nezabezpečenou/veřejnou sítí
  - Potřeba zajistit, aby si data nikdo nežádoucí nepřečetl
  - $\Rightarrow$ šifrování
- Zajištění původu paketů
  - Kdo je uveden jako zdroj paketů, je pravým zdrojem

Point to Point Tunneling protocol (PPTP)

- Publikován $\approx$ 1999 v RFC-2637
- Podílelo se více společností (3Com, Microsoft – součástí Windows)
- Šifrování a autentizace není součástí standardu
  - Přenecháno na konkrétní implementace a vrstvu PPP

Point to Point Tunneling protocol (PPTP)

- Publikován $\approx$ 1999 v RFC-2637
- Podílelo se více společností (3Com, Microsoft – součástí Windows)
- Šifrování a autentizace není součástí standardu
  - Přenecháno na konkrétní implementace a vrstvu PPP
- Původní paket obalen PPP hlavičkou, ta následně GRE hlavičkou
  - Takto obalený paket putuje do transportní sítě

Point to Point Tunneling protocol (PPTP)

- Publikován $\approx$ 1999 v RFC-2637
- Podílelo se více společností (3Com, Microsoft – součástí Windows)
- Šifrování a autentizace není součástí standardu
  - Přenecháno na konkrétní implementace a vrstvu PPP
- Původní paket obalen PPP hlavičkou, ta následně GRE hlavičkou
  - Takto obalený paket putuje do transportní sítě
- Implementace obsahují mnoho zranitelností
  - Slabé autentizační mechanismy (MSCHAPv1, v2)
  - Slabá RC4 šifra

Point to Point Tunneling protocol (PPTP)

- Publikován $\approx$ 1999 v RFC-2637
- Podílelo se více společností (3Com, Microsoft – součástí Windows)
- Šifrování a autentizace není součástí standardu
  - Přenecháno na konkrétní implementace a vrstvu PPP
- Původní paket obalen PPP hlavičkou, ta následně GRE hlavičkou
  - Takto obalený paket putuje do transportní sítě
- Implementace obsahují mnoho zranitelností
  - Slabé autentizační mechanismy (MSCHAPv1, v2)
  - Slabá RC4 šifra
- Neměl by se používat, považován za nebezpečný

Layer Two Tunneling Protocol (L2TP)

- Nástupce PPTP a Cisco Layer 2 Forwarding Protocol – RFC-2661
- Spolupráce s PPP protokolem (autentizace)

Layer Two Tunneling Protocol (L2TP)

- Nástupce PPTP a Cisco Layer 2 Forwarding Protocol – RFC-2661
- Spolupráce s PPP protokolem (autentizace)
- Hlavička a data posílány UDP protokolem
- Neřeší důvěrnost a autentizaci
- Velmi často používán ve spojení s IPsec – RFC-3193

Layer Two Tunneling Protocol (L2TP)

- Nástupce PPTP a Cisco Layer 2 Forwarding Protocol – RFC-2661
- Spolupráce s PPP protokolem (autentizace)
- Hlavička a data posílány UDP protokolem
- Neřeší důvěrnost a autentizaci
- Velmi často používán ve spojení s IPsec – RFC-3193
- Bez zabezpečení pomocí IPsec nebezpečné

VPN

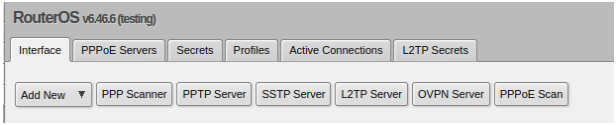
- Oba předchozí protokoly považovány za zastaralé
- Bohužel v praxi je stále můžeme potkat

VPN

- Oba předchozí protokoly považovány za zastaralé
- Bohužel v praxi je stále můžeme potkat
- Naštěstí již velmi často L2TP/IPsec (např. univerzitní VPN)

VPN

- Oba předchozí protokoly považovány za zastaralé
- Bohužel v praxi je stále můžeme potkat
- Naštěstí již velmi často L2TP/IPsec (např. univerzitní VPN)
- Spousta routerů stále nabízí tuto možnost
  - Např. Mikrotik – umožňuje šifrované i nešifrované
  - Umožňuje L2TP bez IPsec



IPsec – Úvod

- = soustava protokolů zabezpečující IP komunikaci přes nezabezpečenou síť
- RFC-2401 až RFC-2412

IPsec – Úvod

- = soustava protokolů zabezpečující IP komunikaci přes nezabezpečenou síť
- RFC-2401 až RFC-2412
- Řeší komunikaci mezi jednotlivými počítači
  - Neřeší zabezpečení mezi uživateli či aplikacemi jednoho stroje
  - Toto přenechává vyšším vrstvám, OS

IPsec – Úvod

- = soustava protokolů zabezpečující IP komunikaci přes nezabezpečenou síť
- RFC-2401 až RFC-2412
- Řeší komunikaci mezi jednotlivými počítači
  - Neřeší zabezpečení mezi uživateli či aplikacemi jednoho stroje
  - Toto přenechává vyšším vrstvám, OS
- IPsec nemusí implementovat koncové uzly
  - Můžou např. hraniční směrovače dvou poboček
  - Aplikace, počítače o tom nemusí vědět

IPsec – Úvod

- = soustava protokolů zabezpečující IP komunikaci přes nezabezpečenou síť
- RFC-2401 až RFC-2412
- Řeší komunikaci mezi jednotlivými počítači
  - Neřeší zabezpečení mezi uživateli či aplikacemi jednoho stroje
  - Toto přenechává vyšším vrstvám, OS
- IPsec nemusí implementovat koncové uzly
  - Můžou např. hraniční směrovače dvou poboček
  - Aplikace, počítače o tom nemusí vědět
- Původně „nativní“ součástí IPv6, později backportován do IPv4
  - Složitý, komplexní návrh
  - Možné implementovat jen podmnožinu $\Rightarrow$ široké a rychlé rozšíření
  - Jak je na tom IPv6?

IPsec – režimy zabezpečení

- Transportní režim
  - Jednodušší případ
  - Mezi záhlaví IP a záhlaví vyšší vrstvy vloženo *bezpečnostní záhlaví*
  - Specifikace, jak jsou data zabezpečena
  - Pakety poté putují „normálně internetem“

IPsec – režimy zabezpečení

- Transportní režim
  - Jednodušší případ
  - Mezi záhlaví IP a záhlaví vyšší vrstvy vloženo *bezpečnostní záhlaví*
  - Specifikace, jak jsou data zabezpečena
  - Pakety poté putují „normálně internetem“
- Tunelovací režim
  - Zabezpečuje celý (původní) IP-datagram
  - Tento je vložen do nového s bezpečnostním záhlavím a přenesen nezabezpečenou sítí
  - Internet jen jako přenosové médium

IPsec – režimy zabezpečení

- Transportní režim
  - Jednodušší případ
  - Mezi záhlaví IP a záhlaví vyšší vrstvy vloženo *bezpečnostní záhlaví*
  - Specifikace, jak jsou data zabezpečena
  - Pakety poté putují „normálně internetem“
- Tunelovací režim
  - Zabezpečuje celý (původní) IP-datagram
  - Tento je vložen do nového s bezpečnostním záhlavím a přenesen nezabezpečenou sítí
  - Internet jen jako přenosové médium
- Modely komunikace: dvě koncové stanice, dva routery, stanice-router
  - Kombinace integrity, autorizace na stanicích a šifrování mezi routery „IPsec over IPsec“
  - Obrázky
- Zabezpečení rozděleno na dva „podprotokoly“

Protokol IP Authentication Headeer (AH)

- Zajišťuje integritu IP datagramů
- Autentizuje odesílatele
- Chrání proti útoku *zopakováním dat*

Protokol IP Authentication Headeer (AH)

- Zajišťuje integritu IP datagramů
- Autentizuje odesílatele
- Chrání proti útoku *zopakováním dat*
- Bezpečnostní záhlaví:
  - *Další záhlaví* – 1B – číslo zabezpečovaného protokolu, stejná čísla jako *Protokol vyšší vrstvy* v IP záhlaví(1 – ICMP, 4 – IP(tunel), 6 a 17 pro TCP a UDP(transport))
  - *Délka záhlaví* – 1B – jednotkou jsou 4B, hodnota - 2 jednotky
  - *Rezerva* – 2B – pro budoucí použití
  - *Security Parameter Index (SPI)* – 4B – Index použitých zabezpečení (nespojová služba), viz dále.
  - *Pořadové číslo* – 4B – Čítač přenesených paketů – ochrana proti zopakování, inkrementace
  - *Autentizační data* – variabilní délka – kontrolní součet z IP záhlaví, AH, přenášených dat
- Obrázek

IP Encapsulating Security Payload (ESP)

- Zajišťuje šifrování dat, integrita dat je volitelná(není počítána ze záhlaví IP datagramu)
- Ve „vnějším“ IP paketu uvedeno jako *Protokol vyšší vrstvy* – 50
- Kvůli šifrování jsou data zarovnána do bloku, mírná komplikace hlavičky

IP Encapsulating Security Payload (ESP)

- Zajišťuje šifrování dat, integrita dat je volitelná(není počítána ze záhlaví IP datagramu)
- Ve „vnějším“ IP paketu uvedeno jako *Protokol vyšší vrstvy* – 50
- Kvůli šifrování jsou data zarovnána do bloku, mírná komplikace hlavičky
- Struktura záhlaví:
  - *SPI* – 4B – viz dále
  - *Pořadové číslo* – 4B – čítač paketů, ochrana proti zopakování

IP Encapsulating Security Payload (ESP)

- Zajišťuje šifrování dat, integrita dat je volitelná(není počítána ze záhlaví IP datagramu)
- Ve „vnějším“ IP paketu uvedeno jako *Protokol vyšší vrstvy* – 50
- Kvůli šifrování jsou data zarovnána do bloku, mírná komplikace hlavičky
- Struktura záhlaví:
  - *SPI* – 4B – viz dále
  - *Pořadové číslo* – 4B – čítač paketů, ochrana proti zopakování
- Data – variabilní délka

IP Encapsulating Security Payload (ESP)

- Zajišťuje šifrování dat, integrita dat je volitelná(není počítána ze záhlaví IP datagramu)
- Ve „vnějším“ IP paketu uvedeno jako *Protokol vyšší vrstvy* – 50
- Kvůli šifrování jsou data zarovnána do bloku, mírná komplikace hlavičky
- Struktura záhlaví:
  - *SPI* – 4B – viz dále
  - *Pořadové číslo* – 4B – čítač paketů, ochrana proti zopakování
- Data – variabilní délka
- Zápatí
  - *Zarovnání* – 0 - 255B – kvůli blokové šifře
  - *Délka zarovnání* – 1B
  - *Další hlavička* – číslo protokolu přenášených dat

IP Encapsulating Security Payload (ESP)

- Zajišťuje šifrování dat, integrita dat je volitelná(není počítána ze záhlaví IP datagramu)
- Ve „vnějším“ IP paketu uvedeno jako *Protokol vyšší vrstvy* – 50
- Kvůli šifrování jsou data zarovnána do bloku, mírná komplikace hlavičky
- Struktura záhlaví:
  - *SPI* – 4B – viz dále
  - *Pořadové číslo* – 4B – čítač paketů, ochrana proti zopakování
- Data – variabilní délka
- Zápatí
  - *Zarovnání* – 0 - 255B – kvůli blokové šifře
  - *Délka zarovnání* – 1B
  - *Další hlavička* – číslo protokolu přenášených dat
- *ESP Authentication Data* – volitelné zápatí obsahující kontrolní součet

SPI

- Protokol IP je datagramová služba – každý paket je nezávislý
- Připojovat zabezpečovací informace ke každému paketu by nebylo efektivní
  - Metody autentizace
  - Sdílená tajemství
  - algoritmy kontrolního součtu, šifrování
  - Klíče, . . .

SPI

- Protokol IP je datagramová služba – každý paket je nezávislý
- Připojovat zabezpečovací informace ke každému paketu by nebylo efektivní
  - Metody autentizace
  - Sdílená tajemství
  - algoritmy kontrolního součtu, šifrování
  - Klíče, . . .
- *Security Policy (SP)* – konkrétní pravidla specifikující použitá zabezpečení
  - Uložená v *Security Policy Database (SPD)* v konfiguraci zapojených uzlů
  - Každý spoj dostane své číslo – Index $\Rightarrow$ SPI

SPI

- Protokol IP je datagramová služba – každý paket je nezávislý
- Připojovat zabezpečovací informace ke každému paketu by nebylo efektivní
  - Metody autentizace
  - Sdílená tajemství
  - algoritmy kontrolního součtu, šifrování
  - Klíče, . . .
- *Security Policy (SP)* – konkrétní pravidla specifikující použitá zabezpečení
  - Uložená v *Security Policy Database (SPD)* v konfiguraci zapojených uzlů
  - Každý spoj dostane své číslo – Index $\Rightarrow$ SPI
- *Security Association(SA)* – trojice SPI, IP adresa, protokol (AH, ESP)
  - SA ukazuje do databáze, kde nalezneme konkrétní hodnoty nastavení (klíč, tajemství)

SPI

- Protokol IP je datagramová služba – každý paket je nezávislý
- Připojovat zabezpečovací informace ke každému paketu by nebylo efektivní
  - Metody autentizace
  - Sdílená tajemství
  - algoritmy kontrolního součtu, šifrování
  - Klíče, . . .
- *Security Policy (SP)* – konkrétní pravidla specifikující použitá zabezpečení
  - Uložená v *Security Policy Database (SPD)* v konfiguraci zapojených uzlů
  - Každý spoj dostane své číslo – Index $\Rightarrow$ SPI
- *Security Association(SA)* – trojice SPI, IP adresa, protokol (AH, ESP)
  - SA ukazuje do databáze, kde nalezneme konkrétní hodnoty nastavení (klíč, tajemství)
  - Jak tuto tabulku naplníme?

Internet Security Asssociation And Key Management Protocol (ISAKMP)

- = aplikační protokol pro dynamické naplnění databází SA obou uzlů – port 500/UDP
  - šlo by dělat i ručně, zdlouhavé

Internet Security Asssociation And Key Management Protocol (ISAKMP)

- = aplikační protokol pro dynamické naplnění databází SA obou uzlů – port 500/UDP
  - šlo by dělat i ručně, zdlouhavé
- Architektura *initiator/responder*
- Dvě fáze komunikace:
  - Vytvoření SA pro svou další (zabezpečenou) komunikaci – šifrovány oba směry, bez SPI
  - Vytváření SA pro IPsec

Internet Security Asssociation And Key Management Protocol (ISAKMP)

- = aplikační protokol pro dynamické naplnění databází SA obou uzlů – port 500/UDP
  - šlo by dělat i ručně, zdlouhavé
- Architektura *initiator/responder*
- Dvě fáze komunikace:
  - Vytvoření SA pro svou další (zabezpečenou) komunikaci – šifrovány oba směry, bez SPI
  - Vytváření SA pro IPsec
- Poté již mohou strany komunikovat pomocí IPsec
- Struktura paketu poměrně složitá (více zpráv v jednom)
  - Možné i vnořené zprávy

ISAKMP – typy zpráv

- Security Association(1)– vyjednání autentizační metody, algortml, . . .
  - Počítá s využitím i jinými protokoly než IPsec
- Proposal(2) – vnořeny do předchozí
  - Odesílatel nabízí podporované algoritmy žadateli (pro protokoly AH, ESP, ISAKMP)
  - Nabídky vloženy ve zprávách *Transform(3)*
  - Seřazeny podle preference
- Key Exchange(4) – informace pro vytvoření šifrovacíích klíčů
  - Pro IPsec nejčastěji čísla pro Diffie-Hellman
- Indetification(5) – identifikace odesilatele protokolu vyšší vrstvy (IP adresa, DNS jméno, email)
- Certificate(6) – certifikát odesilatele
- Certificate request(7) – žádost o certifikát druhé strany
- Hash(8) – kontrolní součet ze zpráv a náhodného čísla
- Signature(9) – podpis zprávy
- Nonce(10), Notification(11)

Protokol Internet Key Exchange

- Samotný protokol výměny klíču, vystavěn nad ISAKMP
- 1. fáze – vytvoření zabezpečeného ISAKMP kanálu
  - Autentizace pomocí digitálního podpisu, veřejného šifrovacího klíče či sdíleným tajemství
  - Výměna veřejných DH čísel (Key Exchange a Nonce)
  - Zprávy SA, Transform, Proposal

Protokol Internet Key Exchange

- Samotný protokol výměny klíču, vystavěn nad ISAKMP
- 1. fáze – vytvoření zabezpečeného ISAKMP kanálu
  - Autentizace pomocí digitálního podpisu, veřejného šifrovacího klíče či sdíleným tajemství
  - Výměna veřejných DH čísel (Key Exchange a Nonce)
  - Zprávy SA, Transform, Proposal
- Dále již šifrované

Protokol Internet Key Exchange

- Samotný protokol výměny klíču, vystavěn nad ISAKMP
- 1. fáze – vytvoření zabezpečeného ISAKMP kanálu
  - Autentizace pomocí digitálního podpisu, veřejného šifrovacího klíče či sdíleným tajemství
  - Výměna veřejných DH čísel (Key Exchange a Nonce)
  - Zprávy SA, Transform, Proposal
- Dále již šifrované
- 2. fáze – Vytváření SA pro AH a ESP
  - používá se také pro obnovování SA po vypršení času či čítače
  - Zprávy: hash, SA, Nonce
- Obrázky

IPsec

- Protokoly kolem IPsec jsou poměrně komplikované
- Některé systémy nemusí implementovat vše, či vůbec podporovat
- Poměrně složité nastavování, výměna klíčů
- Někdy pomalejší (šifrování, podpora v HW)
- Pomalejší „start spojení“ (např. ping čeká na celý ISAKMP „handshake“)
- Částečnou odpovědí je WireGuard

WireGuard

- WireGuard – „Odlehčený nástupce IPsec“
- Citace z webu: „WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache.“

WireGuard

- WireGuard – „Odlehčený nástupce IPsec“
- Citace z webu: „WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache.“
- Od počátků součástí Linuxového jádra
- Později implementace pro Windows, BSD, macOS, iOS, Android, . . .
- Důraz na krátký, jednoduchý kód (lehká auditovatelnost)

WireGuard

- WireGuard – „Odlehčený nástupce IPsec“
- Citace z webu: „WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache.“
- Od počátků součástí Linuxového jádra
- Později implementace pro Windows, BSD, macOS, iOS, Android, ...
- Důraz na krátký, jednoduchý kód (lehká auditovatelnost)
- Pro systém se jeví jako další síťové rozhraní
- Handshake vyžaduje pouze dvě zprávy (1 v každém směru)
- Doporučuji pročíst `https://www.wireguard.com/protocol/`

Ukázka WireGuard VPN

- Na obou strojích vygenerujeme privátní a soukromé klíče

```
wg genkey > private
wg pubkey < private
```

- přidáme síťové rozhraní

```
ip link add wg0 type wireguard
ip addr add 10.0.0.1/24 dev wg0
wg set wg0 private-key ./private
ip link set wg0 up
```

- Zkontrolujeme nastavení a zjistíme port

```
wg
```

WireGuard ukázka

- Na obou strojích přidáme povolené klienty

```
wg set wg0 peer VEREJNY KLIC allowd-ips 10.0.0.2/32
                                endpoint IP_KLIENTA:PORT
```

- Můžeme zkusit ping

```
ping 10.0.0.2
```

- Můžeme zase zkontrolovat status

```
wg
```

Tor

- *The Onion Router* – anonymní šifrovaná komunikace skrze internet
- https://www.torproject.org/
- Nastíníme si pouze síťovou část, složitý distribuovaný systém

Tor

- *The Onion Router* – anonymní šifrovaná komunikace skrze internet
- https://www.torproject.org/
- Nastíníme si pouze síťovou část, složitý distribuovaný systém
- Efektivita komunikace není důležitá, důraz na anonymitu

- Doména `.onion` funkční pouze v síti Tor

Tor

- *The Onion Router* – anonymní šifrovaná komunikace skrze internet
- https://www.torproject.org/
- Nastíníme si pouze síťovou část, složitý distribuovaný systém
- Efektivita komunikace není důležitá, důraz na anonymitu
- V Internetu běží mezilehlé Tor uzly (relays), provozované dobrovolníky
  - Guard relay – první uzel s kterým komunikuje klient. Jako jediný zná uživatelovu IP, nezná ale cíl komunikace
  - Middle relay – pouze jako prostředník komunikace, ví jen komu má poslat data dál
  - Exit relay – koncový článek, komunikuje s cílem, výstupní bod
- Doména `.onion` funkční pouze v síti Tor
- Tor WebTunnel – skrývání Tor komunikace za https provoz

Tor – komunikace

- Klient z veřejného seznamu uzlů (náhodně) vybere 3 (A, B, C) splňující potřebné vlastnosti
- Svůj požadavek na cílový server zabalí „do cibule“ s vrstvami
  - Šifrováno veřejným klíčem A
  - Šifrováno veřejným klíčem B
  - Šifrováno veřejným klíčem C
  - Data

Tor – komunikace

- Klient z veřejného seznamu uzlů (náhodně) vybere 3 (A, B, C) splňující potřebné vlastnosti
- Svůj požadavek na cílový server zabalí „do cibule“ s vrstvami
  - Šifrováno veřejným klíčem A
  - Šifrováno veřejným klíčem B
  - Šifrováno veřejným klíčem C
  - Data
- Uzel A – dešifruje svým soukromým klíčem, zjistí komu má poslat dál – „sloupne vrstvu“
- Uzel B – dešifruje svým soukromým klíčem, zjistí komu poslat dál – „sloupne vrstvu“
- Uzel C – udělá totéž, kontaktuje cílový server

Tor – komunikace

- Klient z veřejného seznamu uzlů (náhodně) vybere 3 (A, B, C) splňující potřebné vlastnosti
- Svůj požadavek na cílový server zabalí „do cibule“ s vrstvami
  - Šifrováno veřejným klíčem A
  - Šifrováno veřejným klíčem B
  - Šifrováno veřejným klíčem C
  - Data
- Uzel A – dešifruje svým soukromým klíčem, zjistí komu má poslat dál – „sloupne vrstvu“
- Uzel B – dešifruje svým soukromým klíčem, zjistí komu poslat dál – „sloupne vrstvu“
- Uzel C – udělá totéž, kontaktuje cílový server
- Pro opačnou cestu musí proběhnout dohoda mezi klientem a uzly na klíči
- „Cibule“ se tvoří postupně, každý Uzel přidá svoji vrstvu

Tor z pohledu aplikací

- Standardním postupem je, že na počítači spustíme Tor proxy
- Tato proxy je SOCKS5 – většina aplikací ji umí používat
- Aplikace ani nemusí vědět, že putují přes Tor

Tor z pohledu aplikací

- Standardním postupem je, že na počítači spustíme Tor proxy
- Tato proxy je SOCKS5 – většina aplikací ji umí používat
- Aplikace ani nemusí vědět, že putují přes Tor
- Předchozí je uživatelsky nepřívětivé

Tor z pohledu aplikací

- Standardním postupem je, že na počítači spustíme Tor proxy
- Tato proxy je SOCKS5 – většina aplikací ji umí používat
- Aplikace ani nemusí vědět, že putují přes Tor
- Předchozí je uživatelsky nepřívětivé
- Specializované prohlížeče podporující Tor
  - Tor browser
  - Brave – ukázka

Tor z pohledu aplikací

- Standardním postupem je, že na počítači spustíme Tor proxy
- Tato proxy je SOCKS5 – většina aplikací ji umí používat
- Aplikace ani nemusí vědět, že putují přes Tor
- Předchozí je uživatelsky nepřívětivé
- Specializované prohlížeče podporující Tor
  - Tor browser
  - Brave – ukázka
- Mobilní aplikace

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje
- Relativně snadná blokace exit relay – seznam je veřejný

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje
- Relativně snadná blokace exit relay – seznam je veřejný
- Důvěra v exit node – probíhá distribuované hlasování
  - Může nahlížet do nešifrované komunikace – používejte SSL/TLS

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje
- Relativně snadná blokace exit relay – seznam je veřejný
- Důvěra v exit node – probíhá distribuované hlasování
  - Může nahlížet do nešifrované komunikace – používejte SSL/TLS
- Pomůže navýšení mezilehlých uzlů vyšší bezpečnosti?

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje
- Relativně snadná blokace exit relay – seznam je veřejný
- Důvěra v exit node – probíhá distribuované hlasování
  - Může nahlížet do nešifrované komunikace – používejte SSL/TLS
- Pomůže navýšení mezilehlých uzlů vyšší bezpečnosti?
- Analýza spojení, časování, kontrola velkého poměru uzlů, . . .

Tor – bezpečnostní rizika

- Provoz *exit relay* může být rizikový – je to proxy – „všechno zlo páchá exit relay“
  - Abuse požadavky, policie, . . . jde za exit relay
  - Náročné na konektivitu, systémové zdroje
- Relativně snadná blokace exit relay – seznam je veřejný
- Důvěra v exit node – probíhá distribuované hlasování
  - Může nahlížet do nešifrované komunikace – používejte SSL/TLS
- Pomůže navýšení mezilehlých uzlů vyšší bezpečnosti?
- Analýza spojení, časování, kontrola velkého poměru uzlů, . . .
- Některé protokoly/aplikace mohou vyzradit IP – např. JavaScript v prohlížečích

Doporučená četba

- McClure S., Scambray J., Kurtz G.: Hacking Exposed 7: Network Security Secrets and Solutions (7th. edition). CompuMcGraw Hill, 2012. ISBN 978-0071780285
  - Kapitola 8 – Wireless hacking
- Dostálek L. a kolektiv. Velký průvodce protokoly TCP/IP: Bezpečnost (2. aktualizované vydání). Computer Press, 2003. ISBN 807226849X
  - IPsec
- WireGuard Whitepaper
- Odkazovaná RFC