Bezpečnost v IT

5. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

19. 4. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- Bezpečnost síťových technologií
- Bezpečnost bezdrátových technologií
- VPN
- IPSsec
- WireGuard
- Tor

Aktuální (kyber)bezpečnostní situace

- Eskalace práv v Linuxovém jádře
  - Na první pohled zní děsivě
  - Vždy důležité, jaké jsou podmínky – GSM modul, XEN
- Spectre v2 BHI má novou variantu „native BHI“
  - Linux + CPU intel
  - Čtení libovolné paměti rychlosti $\approx 3.5 kB/s$
- Politický boj o technologie stále trvá – Čína se chce zbavit závislosti
  - Státní firmy a úřady omezit „cizí“ procesory do roku 2027
  - Loni generoval čínský trh 27 % zisku Intelu
- Oblíbený SSH klient Putty měl 7 let zranitelnost
  - Chybná implementace podpisu pomocí *eliptických křivek*
  - Naštěstí postižena jen varianta `ecdsa-sha2-nistp521`

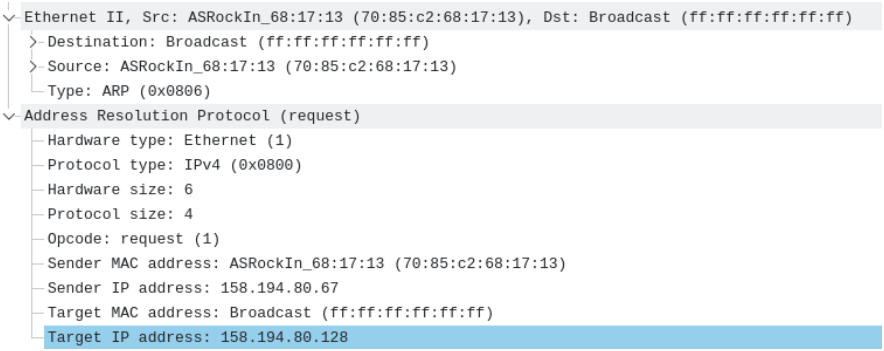
Ethernet

- Protokol určený pro komunikace mezi sousedními uzly
  - Zařízení přijímá rámce určené jemu (MAC adresa)
  - Všesměrové a skupinové rámce
  - Karty mohou podporovat *promiskuitní režim* – přijímají všechny rámce
- Nepřepínaný ethernet – uzly spojené rozbočovačem(hub), nebo jedna linka
  - $\Rightarrow$ sdílené médium $\Rightarrow$ „všichni mohou vidět všechno“
  - (naštěstí) se už nepoužívá
- Přepínaný ethernet
  - Uzly připojeny do *switche*, který vytváří virtuální segment
  - Switch izoluje komunikaci mezi uzly
- Rámce „vybaveny“ kontrolním součtem
  - Pouze odhalení technických chyb
  - Inteligentní útočník může změnit data a přepočítat

IPv4 a Ethernet

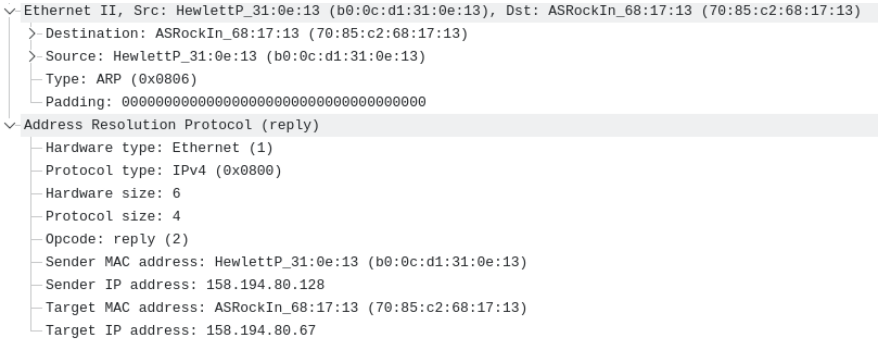
- Pro IP komunikaci potřebujeme znát, kterou IP adresu „obsluhuje“ jaká síťová karta
- ⇒ protokol ARP
  - Využívá všesměrové ethernetové rámce typu: „Kdo má adresu X.Y.Z“
  - Stroj s touto adresou odpoví a prozradí svou MAC adresu
- Uzly si udržují vazby v *ARP cache* (výpis příkazem `arp`)
- Není-li vazba v cache ⇒ `arping`
- Snadné odhalení uzlů v síti `nmap -sn -PR 158.194.80.0/24` pod rootem
- Problém – neprobíhá párování dotazu s odpovědí
  - ARP odpověď je považována za legitimní i když se nikdo neptal
  - Z toho „těží“ několik útoků

ARPing – ukázka



Obrázek: Dotaz na držitele IP adresy

ARPing – ukázka



Obrázek: Odpověď na dotaz

ARP spoofing (ARP cache poisoning)

- Podvržení adresy MAC adresy routeru(výchozí brány) v ARP cache oběti
  - A naopak – podvržení MAC adresy oběti v ARP cache routeru
  - $\Rightarrow$ MITM (obrázek)
- Vytvoření falešné odpovědi(bez žádosti) s IP routeru a oběti a s naší MAC adresou
  - Router si nastaví: „IP oběti najdu na MAC adrese útočníka“
  - Oběť si nastaví: „výchozí bránu najdu na MAC adrese útočníka“
- Komunikace poté „poteče“ přes útočníka, přečte, pozmění a odešle na správné MAC adresy
- Obrana – Statická ARP cache (vs. DHCP)
  - Filtrace ARP odpovědí bez dotazu na managovatelných switchích (např. Cisco Dynamic ARP Inspection)
  - Kontrola MAC a IP adres všech paketů – Dynamic IP Lockdown
  - Nutná spolupráce s DHCP(*DHCP snooping*)
- Snadná realizace pomocí programu `ettercap` (GUI)

MAC flooding

- Switche/routery si udržují vazbu: MAC adresa a fyzický port v *CAM(Content Addressable Memory) tabulce*
- Útočník generuje „záplavu“ paketů s náhodnými zdrojovými a cílovými MAC adresami
- Dojde k přeplnění CAM tabulky falešnými daty, správná data jsou zahozena
- Nemá-li router záznam s cílovou MAC adresou v CAM tabulce odešle data na všechny porty
- Problém: Každý router/switch reaguje odlišně $\Rightarrow$ nepředvídatelnost
- Obrana: Detekce (sledování IP provozu). statické nastavení managovatelného switche

Port stealing

- CAM tabulka je aktualizována vždy, když přijde nějaký paket
- Simulace přepojení oběti do jiného (fyzického) portu:
  - Zdrojová IP adresa: adresa oběti
  - Cílová IP adresa: adresa útočníka
- Router/switch si bude myslet, že se oběť přepojila do jiného portu
- $\Rightarrow$ upravení CAM tabulky $\Rightarrow$ data pro oběť poputují útočníkovi
- Pro MITM musíme znovu upravit CAM tabulku routeru
- Problém: Každá komunikace od oběti útok naruší
  - Musíme neustále posílat upravené pakety (snadnější detekce)
- Obrana: Jak rozlišit oběť od útočníka? Statické nastavení CAM. Aktivní obrana obětí

Další útoky (stručně)

- ICMP redirect
  - Generování falešných ICMP zpráv s údaji o „kratší cestě“
  - Brána si může iniciovat pozměnění routovací tabulky oběti
  - Malá úspěšnost (filtrace, složitější pravidla na tvar „zprávy o kratší cestě“
- DHCP spoofing
  - Vytvoření falešného DHCP serveru v síti, podvržení brány
  - Odchozí data přes útočníka, příchozí nikoliv
  - Získání volných IP adres z pravého DHCP (monitoring, `dhcpx`, . . .)
- DNS spoofing
  - Podvržení IP adresy v odpovědi na DNS dotaz
  - Musí být rychlejší odpověď než skutečný DNS server
  - Musíme se o dotazu dozvědět (kombinace s DHCP spoofing, ARP spoofing)

Protokoly PPP/PPTP

- *Point to Point Protocol* a *Point to Point Tunneling Protocol*
- Použití: Připojení k internetu přes telefonní linku
  - Používáno i dnes (xDSL, optika)
  - Tunelování přes Internet do intranetu (VPN, „zastaralé, ale používá se“)
  - Možná varianta PPPoE (over Ethenet), neplést s PoE
- Zabezpečení – autentizace, šifrování (obojí volitelné)
  - Zpětné volání na uložené číslo (musí být v DB, po autentizaci) – „druhý zámek“
- Zavedené autentizační mechanismy se uplatňují i v bezdrátových sítích

PPP – autentizační protokoly

- *Password Authentication Protocol(PAP)* – zaslání jména a hesla v packetu PAP – RFC 1334
  - „PAP is not a strong authentication method. Passwords are sent over the circuit ”in the clear”, and there is no protection from playback or repeated trial and error attacks. The peer is in control of the frequency and timing of the attempts.“
  - Každý *silnější* protokol musí umět „downgrade“ na PAP
- *Challenge Handshake Auth. Protocol(CHAP)* – strany mají sdílené tajemství v otevřeném tvaru
  - Výzva (challenge) obsahuje náhodný řetězec
  - Klient spojí řetězec a sdílené tajemství a zahashuje
  - Server udělá totéž a porovná hashe
  - Varianty MS CHAPv1 (RFC 2433) (tajemství hashováno MD-4)
  - MS CHAPv2 (RFC 2759) – oboustranná autentizace, různé klíče pro šifrování
- *Extensible Auth. Protocol(EAP)*

Extensible Auth. Protocol(EAP)

- Předchozí protokoly byly provedeny při navazování spojení
- Při EAP dojde pouze k dohodě „autentizujeme se pomoci EAP později“ – RFC 2284
- Konkrétní autentizační metoda(prakticky libovolná) se vyjednává samotným EAP protokolem
  - Nejdříve dohoda na autentizačním schématu
  - Poté samotné provedení
- EAP-MD5 – obdoba CHAP
- EAP-TLS – Na základě certifikátů
- EAP-PSK – *preshared key* RFC 4764
- ...

Bezpečnost bezdrátových technologií – Úvod

- Vzduch jako sdílené médium $\Rightarrow$ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- Standardy IEEE 802.11
  - Dvě pásma(bands) – 2.4GHz, 5GHz
  - Pásmo rozděleno na kanály (konkrétní frekvence, národní regulace)
  - Více verzí 802.11a, 802.11b,g,n,ac,ax, ...
  - Různé rychlosti, šířky kanálů
- Původně bez zabezpečení, později *Wired Equivalent Privacy(WEP)* (nedostatečné)
- Architektury sítí
  - Ad-hoc sítě – bezdrátové sítě mezi uzly(PtP), obtížná autentizace, dohoda na klíčích (Diffie-Hellman)
  - Infrastrukturní – „Vysílač-přijímač“ – AP – klient

Asociace

- AP (může) vysílat identifikátor sítě – SSID (MAC adresa nebo až 32B řetězec)
- Klient zjistí AP skenováním frekvencí a posílá požadavek na asociaci
- Pro asociaci musíme znát SSID
- Většina bezdrátových síťových karet neumožňuje odchytávat pakety bez asociace
- *Monitor mode* bezdrátových síťových karet
  - Umožňuje pasivní odchytávání paketů bez nutnosti asociace k AP
  - Málo výrobců chipsetů/karet podporuje
  - Potřeba specializovaných driverů
    `https://aircrack-ng.org/doku.php?id=compatible_cards`
- Specializovaná HW zařízení. Např.: Pineapple Tetra

Základní bezpečnostní mechanismy

- Poměrně snadné obejít – „security by obscurity“
- Filtrování MAC adres – AP mají k dispozici seznam povolených MAC adres
  - Můžeme odposlechnout běžící komunikaci a poté přenastavit naši MAC adresu
- Pravidelné pakety od AP (*beacons*) nemusí obsahovat SSID
  - Kdo nezná SSID AP, tak se nedokáže asociovat
  - Můžeme odeslat falešný požadavek na *deasociaci* aktivního klienta
  - Rámec s odpovědí obsahuj SSID
- Klienti při skenování odesílají všesměrový paket bez SSID
  - AP mohou mít zakázané odpovídat na tyto pakety
  - Klienti musí mít síť předkonfigurovanou ručně

Wired Equivalent Privacy(WEP)

- Součástí 802.11a/b/g – z roku 1999
- Integrita data kontrolována pomocí CRC-32 (ochrana před technickými chybami)
- Jednostranná autentizace (klient vůči síti)
  - Autentizuje se klient, nikoliv uživatel
  - Sdílený klíč(40b nebo 104b), princip výzva-odpověď
- Šifrování symetrickou proudovou šifrou RC4
  - Generování klíčového proudu ze sdíleného klíče a iniciačního vektoru(24b)
  - Vektor posílán otevřeně (lze odposlechnout)
  - Šifra RC4 je poměrně slabá, při odposlechu většího množství dat lze prolomit

Wi-Fi Protected Access(WPA)

- Z roku 2002 – Dočasná nástupce WEP (podpora tehdejšího HW)
- Rozšířena podpora autentizace (EAP, WPA Enterprise – 802.1x – přemostění na RADIUS server)
- Šifrování stejně slabé jako u WEP, vylepšeno přidán proměnlivý klíč
- Integrita dat chráněna proti „inteligentnímu útočníkovi“
  - 64b kód za daty
  - Klient i AP mají svůj klíč – obdoba digitálního podpisu
  - Při narušení dojde k deasociaci
- WPA-PSK (Pre-Shared Key) – šifrovací klíče generovány(4096 hashů) z předsdíleného klíče a SSID
  - Při znalosti hesla a odchycení úvodního „handshake“ lze snadno dopočítat
- Šifrování pomocí Temporal Key Integrity Protocol(TKIP)
  - RC4 šifra – klíč 128b – dvojí hash tajného klíče (104b), pořadového čísla rámce (32b) a MAC
  - Dále hash s iniciálním vektorem

802.11i/WPA2

- 2004 – plnohodnotná náhrada WEP a WPA
- Silné šifrování s proměnlivým klíčem (802.1x) případně i stálý klíč (PSK)
- Možná předběžná autentizace s jinému AP skrze stávající
  - Pro rychlejší roaming při pohybu klienta
- Klíče v cache (není nutné EAP při reasociaci)
  - Teoretická možnost krádeže
- Umožněna bezpečná deautentizace (odhlášení) a deasociace
  - Zabránění MITM útoku
- Šifrování – Cipher Block Chaining – šifrované bloky závisí na předešlých
  - Šifra AES, 128b klíč, nemění se pro každý paket

Skenování sítí

- Aktivní skenování – klienti odesílají všesměrové *probe request*
  - Zapamatují si AP, které jim odpověděly
  - Již se moc nepoužívá, řada AP neodpovídá
- Pasivní skenování – klient odposlouchává kanály
  - Ze zachycených dat získá MAC adresu AP
  - Podaří-li se zachytit požadavek pro připojení jiného klienta, získáme i SSID
- Nástroje pro zjišťování sítí
  - Kismet – komplexní nástroj pro skenování a odposlech WiFi
  - airodump-ng – aircrack-ng obsahuje sadu nástrojů pro útoky, součástí je skener
- Obrana: Prakticky žádná – potřebujeme, aby AP klienti viděli
  - Snížení síly signálu na „rozumné minimum“

Odposlech sítí

- V nešifrovaných sítích je odposlech(a přečtení) snadný
  - Proč vůbec existují?
  - Veřejná místa (distribuce klíčů)
  - Lenost/neznalost správců
- Právní otázky – je legální odposlouchávat cizí komunikaci?
  - Např. V USA je to nelegální
  - V ČR také: Porušení tajemství dopravovaných zpráv
- Obrana: WPA2/3. Pokud není možné šifrování vyšší vrstvy (IPSec, SSH tunel, SSL/TLS, . . .)
- Odposlech šifrovaných dat je možný, těžší je rozšifrovat

Denial of Service(DOS) – přerušení služby

- Protokoly z rodiny 802.11 mají možnost odpojit „nepořádného“ klienta
  - Špatné klíče
  - Přetěžování síťe
- Fyzické rušení – můžeme na stejných frekvencích provádět komunikaci
  - Zarušení pásma – snížení rychlostí pro ostatní klienty a AP
- De-authentication Attack – podvrhování deautentizačních paketů z AP či z klienta
  - Funguje téměř vždy
  - Je potřeba posílat pakety často (klient se pokouší ihned připojit)
  - Opět je potřeba mít kartu s monitor módem
  - `aireplay-ng --deauth počet -a MAC_AP -C MAC_klient`

Prolomení WEP klíče

- Iniciační vektor(IV) pro proudovou šifru je generován pro každý paket
- Je obsažen v jeho hlavičce, délka 24b – velmi málo
- Je velká šance, že se bude IV opakovat $\Rightarrow$ možné uhádnout klíčový proud
- Případně jde odhadnout z velké množství krátkých paketů (ARP), kde se dá „domyslet“ chybějící informace
- Pro prolomení WEP klíče je potřeba kolem 60 000 IV

WPA3

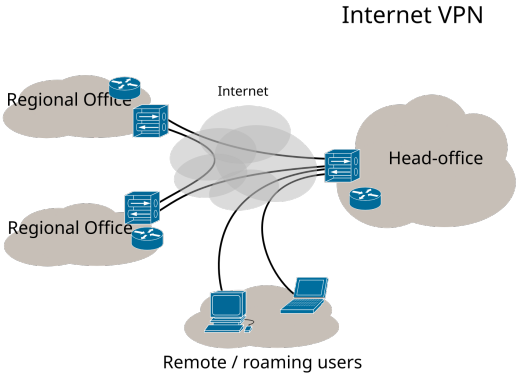
- Nový standard zabezpečení od Wi-Fi Alliance z roku 2018
- WPA3-Personal – AES-128 šifrování s *counter with cipher block chaining message authentication code*
- WPA3-Enterprise – AES-192 s *Galois/Counter Mode* a SHA-384 pro *hash-based message authentication code*
- Pre-shared key nahrazen Dragonfly Hanshake
  - Odolný proti offline slovníkovým útokům
- Zatím není dobrá HW podpora (jak AP, tak klientů)

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



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)

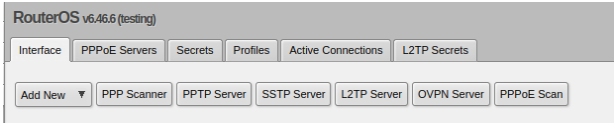
- Publikován $\approx$ 1999 v RFC-2637
- Podílelo se více společností (3Com, Microsoft – součástí Windows)
- Šifrování a autentizace není součástí standardu
  - Přenecháno na konkrétní implementace a vrstvu PPP
- Původní paket obalen PPP hlavičkou, ta následně GRE hlavičkou
  - Takto obalený paket putuje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

- 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