Bezpečnost počítačových systémů

8. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

4. 4. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- Bezpečnost síťových technologií
- Bezpečnost bezdrátových technologií

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?
- Odhalen *backdoor* v knihovně `xz-utils`
  - Příprava několik let, obfuskace, skrývání skutečné funkcionality
  - Dostal se do repozitářů velkých distribucí (Fedora, Debian testing, . . .)
    - `[ebuild  UD] app-arch/xz-utils-5.4.2 [5.6.1]`

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Odhalen *backdoor* v knihovně `xz-utils`
  - Příprava několik let, obfuskace, skrývání skutečné funkcionality
  - Dostal se do repozitářů velkých distribucí (Fedora, Debian testing, . . .)
    - `[ebuild  UD] app-arch/xz-utils-5.4.2 [5.6.1]`
- Open Web Application Security Project oznámil únik dat
  - Osobní údaje členů z let 2006 - 2014
  - Špatně nakonfigurovaný (starý) webový server s Wiki

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Odhalen *backdoor* v knihovně `xz-utils`
  - Příprava několik let, obfuskace, skrývání skutečné funkcionality
  - Dostal se do repozitářů velkých distribucí (Fedora, Debian testing, . . .)
    - `[ebuild  UD] app-arch/xz-utils-5.4.2 [5.6.1]`
- Open Web Application Security Project oznámil únik dat
  - Osobní údaje členů z let 2006 - 2014
  - Špatně nakonfigurovaný (starý) webový server s Wiki
- Bankovní trojský kůň Mispadu(URSA) začíná více cílit na Evropu
  - Šíření SPAMem s PDF a v příloze je škodlivý kód (využívá chybu Windows)

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Odhalen *backdoor* v knihovně `xz-utils`
  - Příprava několik let, obfuskace, skrývání skutečné funkcionality
  - Dostal se do repozitářů velkých distribucí (Fedora, Debian testing, . . .)
    - `[ebuild  UD] app-arch/xz-utils-5.4.2 [5.6.1]`
- Open Web Application Security Project oznámil únik dat
  - Osobní údaje členů z let 2006 - 2014
  - Špatně nakonfigurovaný (starý) webový server s Wiki
- Bankovní trojský kůň Mispadu(URSA) začíná více cílit na Evropu
  - Šíření SPAMem s PDF a v příloze je škodlivý kód (využívá chybu Windows)
- Další chyba v populárních pluginech WordPress

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

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

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
- $\Rightarrow$ protokol ARP
  - Využívá všesměrové ethernetové rámce typu: „Kdo má adresu X.Y.Z“
  - Stroj s touto adresou odpoví a prozradí svou MAC adresu

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`

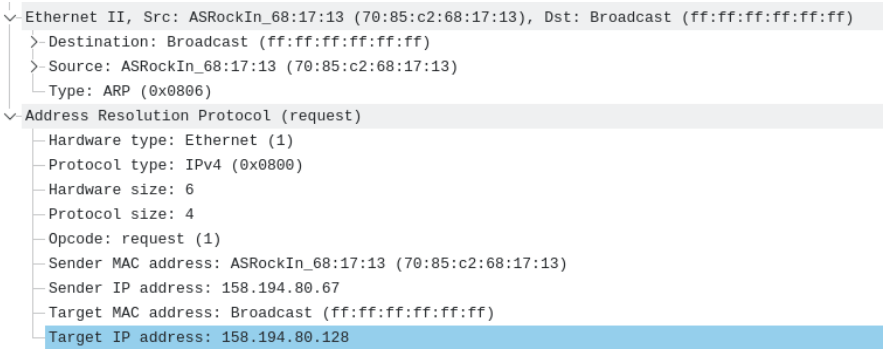
IPv4 a Ethernet

- 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

IPv4 a Ethernet

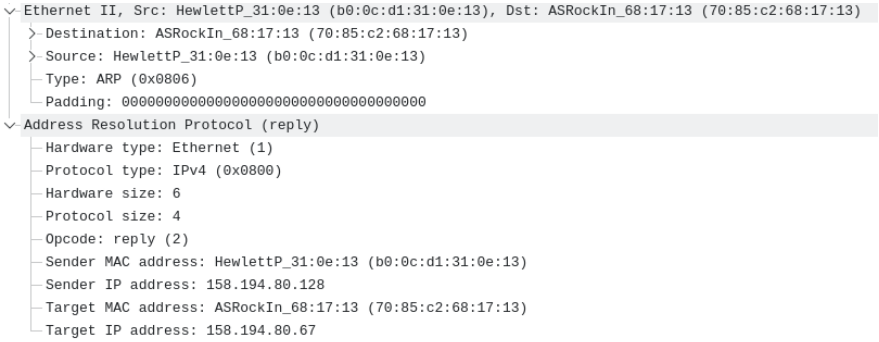
- Pro IP komunikaci potřebujeme znát, kterou IP adresu „obsluhuje“ jaká síťová karta
- ⇒ protokol ARP
  - Využívá všesměrové ethernetové rámce typu: „Kdo má adresu X.Y.Z“
  - Stroj s touto adresou odpoví a prozradí svou MAC adresu
- Uzly si udržují vazby v *ARP cache* (výpis příkazem `arp`)
- Není-li 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)

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“

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

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*)

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*

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

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

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

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

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)

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“

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`, . . .)

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

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“

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

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

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

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

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

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)

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)

Asociace

- AP (může) vysílat identifikátor sítě – SSID (MAC adresa nebo až 32B řetězec)
- Klient zjistí AP skenováním frekvencí a posílá požadavek na asociaci

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

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`

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

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

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)

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

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

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

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

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)

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

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

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

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

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

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

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?

Odposlech sítí

- V nešifrovaných sítích je odposlech(a přečtení) snadný
  - Proč vůbec existují?
  - Veřejná místa (distribuce klíčů)
  - Lenost/neznalost správců

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

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 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

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

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)

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