Počítačové sítě 2

7. Cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

27. 3. 2024

Co bylo na přednášce?

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium $\Rightarrow$ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium $\Rightarrow$ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- AP (může) vysílat identifikátor sítě – SSID (MAC adresa nebo až 32B řetězec)

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium $\Rightarrow$ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- AP (může) vysílat identifikátor sítě – SSID (MAC adresa nebo až 32B řetězec)
- Klient zjistí AP skenováním frekvencí a posílá požadavek na asociaci

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium $\Rightarrow$ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- 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

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium ⇒ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- 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`

Zabezpečení Wi-Fi – Úvod, asociace

- Vzduch jako sdílené médium ⇒ těžko se omezuje dosah
  - Velice snadný odposlech
  - Měli bychom přistupovat jako k nedůvěryhodným sítím
- 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

Prolomení WEP

- Přepneme síťovou kartu do `monitor mode`

  ```
  airmon-ng start wlan1
  ```

  - Nebo pomocí skriptu z ovladačů

- Nyní můžeme zachytávat komunikaci bez asociace k AP (omezení na MAC)

  ```
  airodump-ng --channel 1 --bssid C4:AD:34:25:79:B1 --write wep
                          --output-format pcap wlan1mon
  ```

- Jakmile budeme mít *dostatek* dat můžeme zkusit prolomit klíč

  ```
  aircrack-ng  -b C4:AD:34:25:79:B1 soubor1 soubor2 soubor3
  ```

- Pokud máme dostatek dat, je prolomení otázkou chvilky

Úkol 1 – Promiskuitní režim

- Prozkoumejte možnosti vašeho HW a zjistěte, zda vaše karta podporuje promiskuitní režim

Úkol 2 – odchycení nešifrované komunikace

- V maximálně tříčlenných týmech nakonfigurujte router tak, aby neměl šifrovanou wifi
- Nemáte-li v týmu promiskuitní WiFi kartu, půjčím vám
  - Zprovozněte drivery podporující `monitor mode`
  - Pro Archer T2UPlus `https://github.com/morrownr/8821au-20210708?tab=readme-ov-file`
  - Skript pro monitor mode `https://github.com/morrownr/Monitor_Mode`
- Odchytněte komunikaci z jiného zařízení
  - HTTP Basic Auth (např. na úkol z BEZIT)
  - Nějaká data z nešifrovaného HTTP (odeslání formuláře)

Úkol 3 – Prolomení WEP klíče

- Ve stejných týmech zapněte WEP (heslo si nechte zadat někým jiným, ať jej neznáte)
- Odchytněte dostatek komunikace a zjistěte WEP heslo