63. BEZPEČNOST BEZDRÁTOVÝCH SÍTÍ A ÚTOKY

bezpečnostní cíle – důvěrnost
- integrita
- dostupnost (spolehlivost)

+ třeba také autentizace a nepopiratelnost

- v nezabezpečené síti používat raději VPN
- používat HTTPS a SCP ....

WEP (Wired Equivalent Privacy) – všichni účastníci komunikace používají jeden sdílený klíč :(→ nemění se – málo :(!
- způsob zabezpečení bezdrátových sítí – zastaralé (1997)
- cílem je mít stejně dobré zabezpečení bezdrátových sítí jako drátových
- zajišťoval důvěrnost, integritu a dostupnost
- využívá RC4 šifrování – šifruje přenášené zprávy pro lepší ochranu
  - vygenerují se pseudonáhodný klíč (stream) a s ním se data XORují
  - dešifrování je zase XORování ale inverzně
  - vezme se plaintext a udělá se jeho CRC a to se připojí k plaintextu a z klíče se vygeneruje ten pseudonáhodný stream a tím se to celé XORuje
  - u dešifrování se kontroluje i CRC
- ten klíč je dán klíčem a spojením s IV
- autentizace
  - WEP Open System – bez autentizace – stanice se identifikuje MAC adresou
    ⇒ zabezpečení: MAC filtering – hrozí MAC spoofing
  - WEP Shared Key – používá pro autentizaci 4-way hand shake – 2. strana lístečku
- nedostatky
  - používá CRC pro hashování – slabé – útočník může změnit zprávu a přepočítat CRC
  - klíče (key-stream) se používají opakovaně – útočník zná plaintext tak zjistí i key-stream → known plaintext attack
    → používá se 24bit IV ale po 5000 zprávách se začne opakovat – narozeninový paradox
    ↳ inicializační vektor

    $\underbrace{PT}_{\text{plain-text}} \overset{\text{xor}}{\otimes} \underbrace{C}_{\text{šifra}} = \underbrace{K}_{\text{klíč}}$
  - pokud se IV nemění pro každý paket tak útočník použije IV a generuje vlastní pakety – může udělat DoS
  - útočník může uhádnout klíč – útok hrubou silou
  - caffe latte attack – klienti se připojují automaticky k známé síti
    - útočník vytvoří falešný AP a zjistí klíč od klienta

  ↳ nejhorší je asi to že se ty klíče používají opakovaně

WPA (Wifi Protected Access)
- v reakci na velké nedostatky WEP bylo jako dočasné řešení implementováno WPA (implementovalo část nadcházejícího standardu IEEE 802.11i)
- pro rychlé překlenutí nedostatků WEP byl použit algoritmus TKIP
- prolomeno – je to v podstatě WEP s algoritmem TKIP a tak to bylo prolomeno kvůli dalším nedostatkům WEP
- TKIP – klíč je pro každý paket nový
  - vytvořen ze základního klíče + MAC adresa přijímací stanice + pořadové číslo paketu
    ↳ když se připojí klient k přístupovému bodu tak se vytvoří pomocí hashování
    ↳ nad číslem relace a IV – ten vytváří spolu AP a klient
    ↳ díky tomu se zabrání replay attack !

WPA2
- je úplná implementace standardu 802.11i – ne jen částečná jak WPA
- používá CCMP – založeno na blokové šifře AES
- autentizace WPA/WPA2
  - PSK (Pre-Shared Key) Autentizace – sdílený klíč – není bezpečné – pro domácnosti jen
  - Enterprise Autentizace – podporuje per-user nebo per-system autentizaci

Klíče pro unicast a multicast

UNICAST

- vytváří se PTK klíč pro unicast
  - vezme se PMK nebo PSK + MAC adresa klienta a AP + náhodné číslo
    ⇒ vygeneruje se PTK
- PTK se rozdělí na tři části ⟋ KEY CONFIRMATION KEY
  - EAPOL-Key KCK - pro integritu EAPOL rámců
  - EAPOL-Key KEK - pro šifrování EAPOL
    └ KEY ENCRYPTION KEY
  - TK - zbytek
    - pro šifrování běžné unicast komunikace

BROADCAST A MULTICAST

- AP náhodně vygeneruje GMK
- GMK se používá jako vstup pro generování GTK - tím se šifrují multicast a broadcast
- mění se vždy po připojení nového klienta do skupiny nebo po odhlášení stávajícího ze skupiny

EAPOL rámce

- vytvoření bezpečné komunikace - distribuce klíčů
- Chráněné jinými klíči ~~od~~ než TK ← KCK, KEK
- EAP protokol pro autentizaci a distribuci klíčů využívá EAPOL rámce
  └ umožňuje přenášení klíčů pro následné šifrování komunikace
  └ není to přímo síťový protokol, jen definuje formát zpráv
- EAP-MD5, EAP-TTLS, EAP-TLS, ..., LEAP, ... PEAP, ...
  ↳ je potřeba vybrat správné EAP

CCMP

- protokol pro šifrování dat
- využívá AES a používá 128 bitový klíč a 128 bitovou délku bloku
- zná čísla paketů a unikátní čísla rámců
- standardní šifrovací alg. ve WPA2 - mnohem lepší než šifrování ve WEP a ve WPA/TKIP
  ↳ tam jen XOR
- používá AES Cipher Block Chaining i AES Counter Mode

WPA2 Enterprise

- autentizace na síťové vrstvě (TLS - transport layer security)
- EAP pro autentizaci
- AP dělá šifrování → CCMP
- EAP-MD5 - dělá se autentizace typu Challenge - response - 4WHS
  - response = MD5(id uživatele + heslo + challenge request)
  - je možné odchytit komunikaci a prolomit MD5
- LEAP - Lightweight EAP od CISCO
  - pouze challenge request - response
  - lze snadno odchytit a prolomit challenge-response token

} nepotřebují certifikáty :)

- PEAP, TTLS - využívají TLS pro ochranu autentizačního protokolu
  (protected EAP
  - EAP byl původně drátový
  - je potřeba certifikát pro ověření RADIUS serveru
    ↳ server pro vzdálenou autentizaci
  - autentizační přenos chráněn před odposlechem TLS
  - ověřuje se certifikát serveru pomocí TLS protože SSID může být podvrhnuté a až je certifikát ověřený tak se vůči tomu serveru klient autentizuje
    ↳ server je RADIUS server
  - při použití PEAP se často vypíná to ověření certifikátu serveru (RADIUS) a PEAP potom věří každému RADIUS serveru

Útoky / hrozby:

- Man in the middle
  - útočník odposlouchává z komunikačního kanálu mezi dvěma komunikujícími uzly
  - buď se napojí a pasivně odposlouchává nebo může dělat aktivního prostředníka mezi nimi
  - přijímá zprávy od A a čte je a třeba i modifikuje a přeposílá na B
  - řešením mohou být veřejné a soukromé klíče, ale MITM může zachytit výměnu klíčů a ~~[illegible]~~ oběma (A i B) dát svůj veřejný klíč – oni si myslí že šifrují veřejným klíčem druhé strany a že si to přečte jen druhá strana tak že to dešifruje soukromým kl. ale přitom šifrují veřejným klíčem MITM
- Rogue AP
  - neautorizovaný AP který může odposlouchávat a nebo měnit data ⇒ nepodporovat dynamické AP v síti je řešení

  AP zjistí klíč od klienta ⇒ Coffee Latte Attack
- ARP cache poisoning – třeba nástroj jak udělat MITM nebo DoS
  - využívá se ARP a špatně a chceme získat cizí data
  - přijde na switch cílová adresa a on se podívá na jakém portu je má a tam pošle data
  - podvrhne se ARP cache tak že se řekne bráně že útočníkovo zařízení je nějaký konkrétní uživatel a brána mu bude posílat pakety určené pro tohoto uživatele a uživatelskému zařízení se řekne že útočníkovo zařízení je brána a on mu bude posílat pakety co mají jít ven ze sítě → útočník data pohltí a pošle na správné uzly
  - to že jim to "řekneme" znamená že jim pošleme takový paket
  - tím jim obnovujeme ARP cache – záznamy v cache se časem zneplatňují tak to musíme opakovat – třeba co 10s
  - switch pak zasílá data co přijdou bránou tomu klientovi na útočníka ~~a útočník~~

Jak zabezpečit bezdrátovou síť?

- nepoužívat WEP ale WPA2
- použít CCMP
- pro autentizaci použít PEAP/TTLS – TLS
- nepoužívat PSK – vše sdílené je nebezpečné
- používat firewall pro filtrování paketů
- vyhnout se nebezpečným formám EAP tedy třeba EAP-MD5
- nasadit Wireless IDS – detekce útoků, DoS, Rogue AP, nedělá prevenci ale detekci
- používat dobrá a silná hesla
- u PEAP používat tu validaci certifikátu RADIUS serveru pro autentizaci – nevypínat to

VÝCUC

- cíl
- úlohy/hrozby

ÚTOKY
DDOS
MITM
ARP FLOODING
ARP CACHE POISONING

:(

- WEP
  - RC4 :(+ CRC :(⇒ integrita + důvěrnost
    PROUDOVÁ ŠIFRA
    ↳ proudová šifra (XOR)
  - autentizace
    - WEP open system - bez - jen MAC
    - Shared Key - jak prokáže klient že má Key? ⇒ 4W HS
      ↳ challenge - response
  - opakující se klíče
- WPA - 802.11i jen část
  - WEP + TKIP - každý paket nový klíč
- WPA2 - 802.11i celé už
  - šifrování CCMP - AES šifrování - bloková šifra - 128b bloky i 128 b klíč
    BLOKOVÁ ŠIFRA
  - autentizace
    - PSK (Pre-Shared Key) :(- pouze sdílený :(
      ↳ challenge-response
    - WPA2 Enterprise
  - PMK $\xrightarrow{\text{z něj}}$ PTK - 3 části
    ↳ vygeneruje se
    - EAPOL KCK - integrita
    - EAPOL KEK - šifrování
      } autentizačních rámců v Enterprise
    - TK - šifrování provozu
    ⇒ UNICAST
  - GMK $\xrightarrow{\text{z něj}}$ GTK - šifruje multicast a broadcast
    ↳ vygeneruje se
    ↳ nutná změna při odhlášení/přihlášení do/ze skupiny

  HIERARCHIE KLÍČŮ

  - WPA 2 Enterprise autentizace
    - použití EAP protokolu pro autentizaci
    - rámce EAPOL a šifrování KCK a KEK
    - EAP-MD5 - lze odchytit a crackovat MD5 :(
      - pouze challenge - response
    - LEAP (Leightweight EAP) - CISCO
      - lze odchytit a crackovat token pro autentizaci
      - pouze challenge - response
    - PEAP - vyžaduje RADIUS server - nutné ověřovat certifikáty - často se vypíná
      (Protected EAP)
      - zabezpečeno pomocí TLS

- Jak zlepšit bezpečnost bezdrátových sítí? Co používat? co ne?

TLS - transport layer security
- kryptografický síťový protokol poskytující zabezpečenou komunikaci
- buď jednostranná autentizace (jen server - u serveru musíme zjistit kdo to je) a nebo oboustranná
- využívá algoritmy (SHA-3^{17}, MD5, AES, DES, 3DES, IDEA, RC4, RSA, DSA, ...)

Bezpečnostní cíle bezdr. sítí — důvěrnost
- integrita
- dostupnost
- autentizace a identifikace
- nepopiratelnost

⇒ podrobné schéma → na 2. straně 4WHS

— řeší se vždy — jak bude šifrováno?
- jak bude autentizováno?

WEP

- šifrování jen XORováním :(⇒ používá RC4 — šifruje přenášené rámce / proudová šifra
- integrita pomocí CRC :(
- autentizace — WEP Open System — bez aut., jen MAC adresy
  - PSK — sdílený klíč
    - 4WHS — klient žádost na AP
      - AP pošle challenge
      - klient to zašifruje a pošle zpět (svým klíčem)
      - AP to dešifruje svým klíčem a porovná jestli se to rovná

  ↳ ten PSK se používá i pro RC4 pak

- nedostatky — CRC
  - jen XOR
  - znovupoužívání klíče — 24bit IV tak se po 5000 klíčích začne opakovat
  - z plaintextu se zjistí klíč (a z ciphertextu)

WPA

- napravuje WEP — jen dočasný
- algoritmus TKIP — pro generování klíče

WPA 2

- šifrování CCMP — protokol pro šifrování dat — AES bloková šifra — 128b klíč i blok
- autentizace — Raze PSK
  - WPA 2 Enterprise — využívání EAP
- klíče PTK generovaný z PMK pro unicast
  a GTK generovaný z GMK pro multicast a broadcast
- PTK rozložený na 3 — EAPOL KCK → integrita EAP
  - EAPOL KEK → šifrování EAP
  - TK → šifrování provozu

↳ EAP

- protokol pro autentizaci
- využívá EPOL rámce — šifrované KCK a KSK když jejich než samotný provoz
- EAP-MD5 — challenge-response
- LEAP — — " —
  - CISCO
- PEAP a TTLS — TLS šifrování/zabezpečený — chráněno TLS
  - autentizace vůči RADIUS serveru
  - certifikace RADIUS serveru a ověření certifik.

Útoky: MITM, Replay att., Rogue AP, ARP cache poisoning...

4WHS

(1.) Klient pošle žádost o autentizaci na AP.
(request)

(2.) AP pošle klientovi výzvu jako plaintext!
(challenge)

(3.) Klient výzvu zašifruje svým WEP klíčem
a pošle zpět.
(response)

(4.) AP dešifruje svým klíčem a porovná
s tím plaintextem a pokud se rovná
tak vrátí pozitivní odpověď. Ověřuje i to ID
a heslo třeba.

⟹ autentizováno

Request – Challenge – Response

4 way hand-shake

– v challenge je třeba napsáno:
"Zadejte ID a heslo."

– v response je challenge + to id a
to heslo uživatele (aby se autentizoval)
a celé je to zašifrované

!