

- Radio band 2,4 GHz
  - 802.11 (1997) - 2 Mb/s
  - 802.11b (1999) - 11 Mb/s (DSSS)
  - 802.11g (2003) - 54 Mb/s (OFDM)
- Radio band 5GHz
  - 802.11a (1999) - 54 Mb/s (OFDM)
- 802.11n
  - 2,4 GHz, 5 GHz, 600 Mb/s (MIMO)
- 802.11ac
  - 5 GHz, 1.69 Gbit/s (MIMO 2+2)

3

## IEEE 802.11 - štandard

- IEEE 802.11 - The original 2 Mbit/s, 2.4 GHz standard
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11ac – Enhancements for very high throughput (2013)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11d - International (country-to-country) roaming extensions
- IEEE 802.11e - Enhancements: QoS, including packet bursting
- IEEE 802.11f - Inter-Access Point Protocol (IAPP)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- (TPC) for European compatibility
- IEEE 802.11i - Enhanced security (ratified 24 June 2004)
- IEEE 802.11j - Extensions for Japan: 4.9 GHz - 5 GHz Operation
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11n - Higher throughput improvements: 100+ Mbit/s, based on multiple-input, multiple-output (mimo)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as passenger cars)
- IEEE 802.11r - Fast Roaming/Fast BSS Transition, makes it easier to use wireless VoIP and other real-time interactive applications
- IEEE 802.11s - ESS Mesh Networking, extends WLAN range by allowing data to pass through wireless nodes bringing coverage beyond the typical WLAN connectivity limit
- IEEE 802.11t - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames

4

## Bezpečnosť WiFi sietí

Ing. Matej Kačic  
BIS



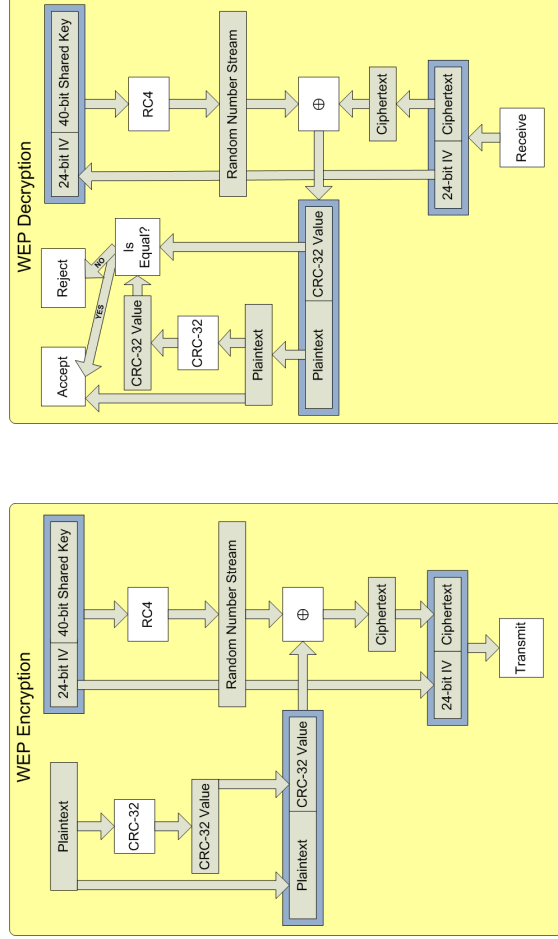
Vysoké učení technické v Brně, Fakulta informačních technologií v Brně  
Božetěchova 2, 612 66 Brno  
ikačic@fit.vutbr.cz

21.11.2013

## Bezpečnostné ciele

- Autentifikácia
  - Musíme overovať identitu
- Dôvernosť
  - Autentifikovaní ľudia sú schopní interpretovať obsah rámcov
  - Je to dostatočne bezpečné?
- Integrita
  - Zaisťiť, aby prenášané dáta boli chránené pred akoukoľvek modifikáciou
- Spoľahlivosť / Dostupnosť

2



## Autentifikácia WEP – Open system

- Open system
  - Bez autentifikácie, po pripojení je komunikácia šifrovaná
  - Stanica sa identifikuje 48bit MAC adresou
- Používané techniky „zabezpečenia“:
  - MAC filtering
  - SSID hiding
- Potreba použiť vyššiu formu zabezpečenia! – Ipsec, SSP, VPN

## WEP

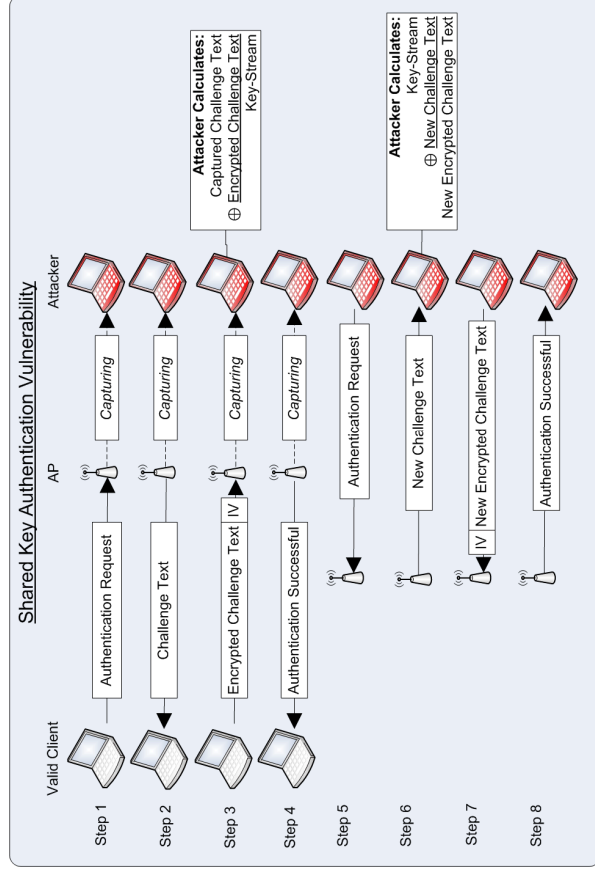
- Wired Equivalent Privacy
- založené na RC4 stream cipher (bez šifrovania, 40-bit kľúč, 128-bit kľúč)
- stream cipher: data sú xorovaná pseudonáhodným streamom
- **znovupoužití** stejného pseudonáhodného streamu
- Zaisťuje (**zaistoval**) Dôvernosť, Integritu a dostupnosť

- Je použitý WEP pre autentifikáciu
- 4-way handshake
  1. Klient posíla AP žiadosť o autentifikáciu (48bit MAC adresu a transaction sequence number of 1)
  2. AP posíla späť (transaction sequence number of 2, challenge text)
  3. Klient posíla
    - transaction sequence number of 3
    - IV pre WEP
    - challenge text zašifrovaný IV a zdieľaným kľúčom WEP
    - ICV (integrity check value) – generované a zašifrované WEPom
  4. AP dešifruje a porovná s výzvou, ktorú poslal, a kontroluje ICV.
    - transaction sequence number of 4
    - Výsledok autentifikácie – úspech/úspech
  5. Klient používa WEP k šifrovaniu rámcov

- Autentifikácia na základe MAC adresy
- Náročná administrácia – každý klient musí byť pridaný do systému
- MAC adresa je prenášaná ako cleartext
- Útočník dokáže zachytiť paket s MAC adresou a nastaviť svojej wifi kartu túto adresu

1024 13: 962919	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Authentication, SN=220, FN=0, Flags=...
1026 13: 964166	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Authentication, SN=220, FN=0, Flags=...
1137 17: 368374	Cisco-LI 4c:7d:61	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2026, FN=0, Flags=...
1138 17: 368374	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2026, FN=0, Flags=...
1143 17: 368446	Cisco-LI 4c:7d:61	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2030, FN=0, Flags=...
1147 17: 368446	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Probe Response, SN=243, FN=0, Flags=...
1152 17: 416049	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Probe Response, SN=795, FN=0, Flags=...
1152 17: 416049	Cisco-LI 53:35:3d	Apple 12:2e:b8	IEEE 802 Probe Response, SN=795, FN=0, Flags=...
1154 17: 428072	Cisco-LI 53:35:3d	Apple 12:2e:b8	IEEE 802 Probe Response, SN=795, FN=0, Flags=...
1156 17: 431759	Cisco-LI 53:35:3d	Apple 12:2e:b8	IEEE 802 Probe Response, SN=795, FN=0, Flags=...
1158 17: 434207	Cisco-LI 4c:7d:61	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2831, FN=0, Flags=...
1163 17: 469261	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2831, FN=0, Flags=...
1165 17: 478377	Cisco-LI 4c:7d:61	Apple 12:2e:b8	IEEE 802 Probe Response, SN=2033, FN=0, Flags=...
1169 17: 520100	Cisco-LI 98:9f:13	Apple 12:2e:b8	IEEE 802 Probe Response, SN=247, FN=0, Flags=...

Destination address: Apple 12:2e:b8 (08:23:37:12:2e:b8)  
Source address: Cisco-LI 98:9f:13 (08:1c:16:98:9f:13)  
BSS Id: Cisco-LI 98:9f:13 (08:1c:16:98:9f:13)  
Fragment number: 0  
Sequence number: 229  
IEEE 802.11 Wireless LAN management frame



- AP nevysiela SSID siete v beacon rámcoch v snahe skryť svoju sieť
- Sieť sa neukazuje len v zozname dostupných sietí
- Je možné ho zistiť odchytením komunikácie na sieti
  - PROBE request/response, ASSOCIATION request...
- Neefektívna forma ochrany

1966 28: 836678	Apple 12:2e:b8	Broadcast	IEEE 802 Probe Request, SN=550, FN=0, Flags=..., SSID="HiddenSecret"
1961 28: 848702	Apple d9:9c:75	Broadcast	IEEE 802 Probe Request, SN=2107, FN=0, Flags=..., SSID="UNLV"
1962 28: 871038	Apple d9:9c:75	Broadcast	IEEE 802 Probe Request, SN=2109, FN=0, Flags=..., SSID="UNLV"
1963 28: 876995	Apple 99:9e:33	Broadcast	IEEE 802 Beacon frame, SN=494, FN=0, Flags=..., BI=100, SSID="Taylor Rile"
1964 28: 879717	Apple d9:9c:75	Broadcast	IEEE 802 Probe Request, SN=2110, FN=0, Flags=..., SSID="UNLV"
1965 28: 890650	Apple 12:2e:b8	Broadcast	IEEE 802 Probe Request, SN=551, FN=0, Flags=..., SSID="HiddenSecret"
1966 28: 890650	Cisco-LI 4c:7d:61	Broadcast	IEEE 802 Beacon frame, SN=43, FN=0, Flags=..., BI=100, SSID="Samurai"
1967 28: 935161	Cisco-LI 13:35:3d	Broadcast	IEEE 802 Beacon frame, SN=1461, FN=0, Flags=..., BI=100, SSID="Bullet Pro"
1968 28: 938337	Cisco 26:3e:81	Broadcast	IEEE 802 Beacon frame, SN=3148, FN=0, Flags=..., BI=100, SSID="UNLV-Guest"
1969 28: 943453	D-Link 2c:84:ba	Broadcast	IEEE 802 Beacon frame, SN=2292, FN=0, Flags=..., BI=100, SSID="Radar"

Destination address: Apple 12:2e:b8 (08:23:37:12:2e:b8)  
Source address: Cisco-LI 98:9f:13 (08:1c:16:98:9f:13)  
BSS Id: Cisco-LI 98:9f:13 (08:1c:16:98:9f:13)  
Fragment number: 0  
Sequence number: 229  
IEEE 802.11 Wireless LAN management frame

Tagged parameters (41 bytes)  
Tag Number: 0 (SSID parameter set)  
Tag length: 12  
Tag interpretation: "HiddenSecret"

Supported Rates: 1.0 2.0 5.5 11.0  
The Number 9 (Protected Rates)



- Shared key recovery
  - Publikovaných niekoľko možných útokov (2001 - 2007)
  - Najlepší útok (2007), redukuje uhádnutie 104bit kľúča na 60 sekúnd.
  - 95% úspešnosť pri 85 000 rámcoch
  - Princíp štatistického ohodnotenia všetkých možných kľúčov -> veľké množstvo dát
  - Kľúč získava „hlas“ ak produkuje rovnaký čiastočný key-stream v zachytených rámcoch

15

- Caffé Latte attack
  - Využíva slabosť klientov pripojovať sa automaticky na známe sieť
  - Útočník sleduje probe žiadosti od klienta a vytvára falošný AP
  - Klient sa automaticky snaží autentifikovať do tohoto AP
  - Kľúč dokáže odhaliť behom 20 min.

Postup:

1. Klient posíla auth. Žiadosť
2. Útočník odpovedá challenge textom
3. Klient vracia IV a zašifrovaný challenge text
4. Útočník zisťuje key-stream pre IV a posíla info o úspešnej autentifikácii

16

- Slabý ICV – používa CRC-32 ako hašovací alg
  - CRC – je kryptograficky slabý alg. (lineárna funkcia)
  - Útočník dokáže zmeniť ktorýkoľvek bit v šifrovanom texte a správne nastaviť šifrovaný haš
  - $C' = C \oplus (\Delta, c(\Delta))$
- Key-stream discovery
  - RC4 sa stáva zraniteľným, ak 2 správy sú šifrované rovnakým key-streamom
  - IEEE implementovalo 24bit IV
  - Ale IV sa začne opakovať po približne 5000 správach – narodeninový paradox
  - Ak nastane kolízia, útočník dokáže použiť rovnicu  $C1 \oplus C2 = P1 \oplus P2$  a získava xor plaintextov
  - Ak útočník odhalil plaintext dokáže najst key-stream  $C \oplus P = K \rightarrow$  vie dešifrovať všetky pakety s rovnakým IV
  - Pre dešifrovanie všetkých paketov, útočník potrebuje najmenej  $2 \cdot 2^{24} \text{ IV} = 33,5 \text{ mil. framov}$

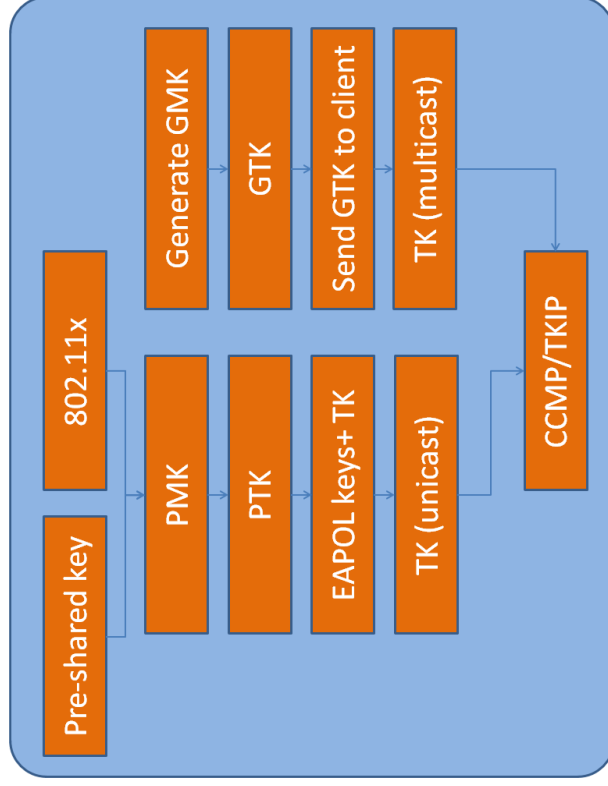
13

- Frame injection
    - Útok sa spolieha na to, že štandard nepožaduje, aby sa IV menil pre každý paket
1. Útočník dokáže znovu použiť IV a key-stream a generuje nekonečno validných paketov
  2. Útočník zachytáva rámce od validných klientov a posíla ich do siete neobmedzený počet krát - DoS

14

- PMK – Pairwise Master key
- PTK – Pairwise Transient Key
- EAPOL key -
  - KCK – Key confirmation key
  - KEK – Key Encryption key
- TK – Temporal key
- GMK – Group Master key
- GTK- Group Transient Key
- MSK – Master session key

22



## WiFi Protected Access

- Implementuje časť štandardu 802.11i
- Dočasné riešenie (dokončenie štandardu, kompatibilita)
- Data šifruje pomocou RC4 (128b key, 48b IV)
- TKIP – Temporal Key Integrity Protocol
  - Key Mixing – kombinuje tajný root kľúč + IV pred vstupom do RC4
  - Sequence counter – pakety menšie ako aktuálne číslo sú zahodené (replay attack)
  - MIC – Message integrity check – 64bit
  - Slabina algoritmu Michael – TKIP blokuje prevádzku po dobu 1 min v prípade detekcie 2 rámcov, ktoré neprešli testom integrity, sieť sa rešartuje a generujú sa nové kľúče a znovu prebehne autentifikácia

19

- Plná implementácia štandardu 802.11i
- Používa CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
  - Založený na blokovej šifre AES
- Autentifikácia v WPA/WPA2
  - Pre-Shared Key (PSK) Authentication
    - Navrhnuté pre domácnosť a malé firmy
    - Všetko čo používa zdieľané heslo bezpečné nie je!!
  - Enterprise Authentication
    - Používa 802.1x
    - Poskytuje per-user or per-system authentication
- **Považujeme ho za bezpečný, ale..**

21

- Vytvorenie bezpečnej komunikácie, distribúcia kľúčov
- Sú chránené kľúčom iným od TK
  - 128-bit key confirmation key(KCK)
  - 128-bit key encryption key(KEK)
- Komunikácia prebieha pomocou skupiny bezpečnostných protokolov – distribúcia kľúčov nezávisle k normálnej komunikácii
- Útočník dokáže získať dostatok dátových rámcov a objaveniu TK, ale nedokáže čítať EAPOl rámce
- Útočník začína od začiatku

- PTK kľúč (384bit alebo 512bit) je odvodený pomocou generátora pseudonáhodných čísiel so vstupom:
  1. PMK
    1. = PSK
    2. Prvých 256bit MSK z 802.1x
  2. MAC adresa klienta a AP
  3. Náhodné číslo generované klientom a druhé AP
- PTK je rozdelený do troch kľúčov:
  - EAPOl-Key KCK – prvých 128bit, používa sa pre integritu eapol rámcov
  - EAPOl-Key KEK - druhých 128 bits, používa sa pre šifrovanie eapol...
  - TK – ostávajúce bity (CCMP 128, TKIP 256), šifrovanie bežnej komunikácie

	TKIP TK	CCMP TK	KCK	KEK	Total Bits Required
TKIP PTK	256		128	128	512
CCMP PTK		128	128	128	384
TKIP GTK	256				256
CCMP GTK		128			128

- AP náhodne generuje GMK
- GMK je vstupom pre generovanie GTK
- GTK sa mení vždy pri každom prihlásení a odhlásení klienta



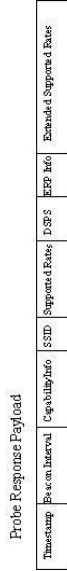
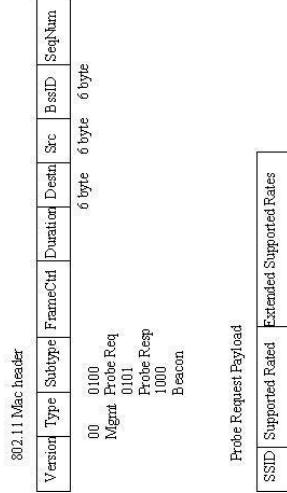
1. Control Frame:

- RTS, CTS, ACK

2. Data Frame

3. Management Frame:

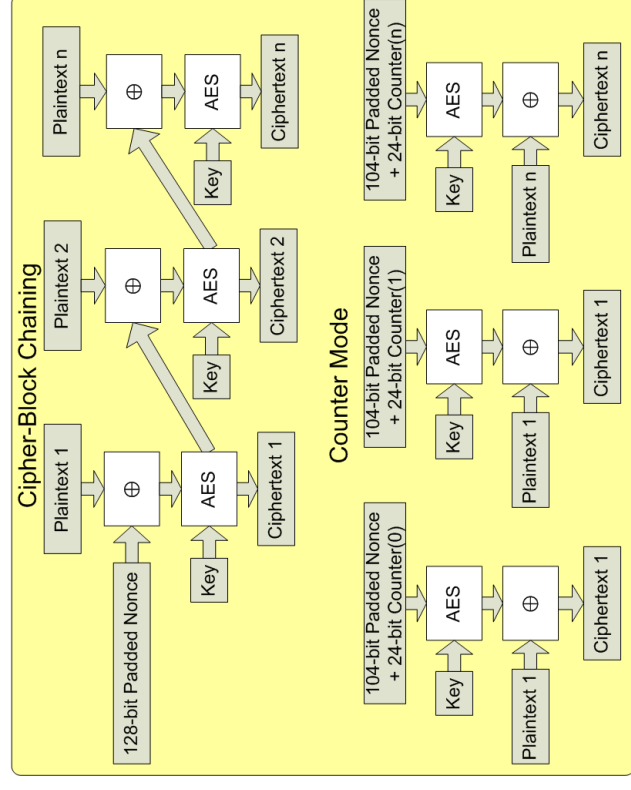
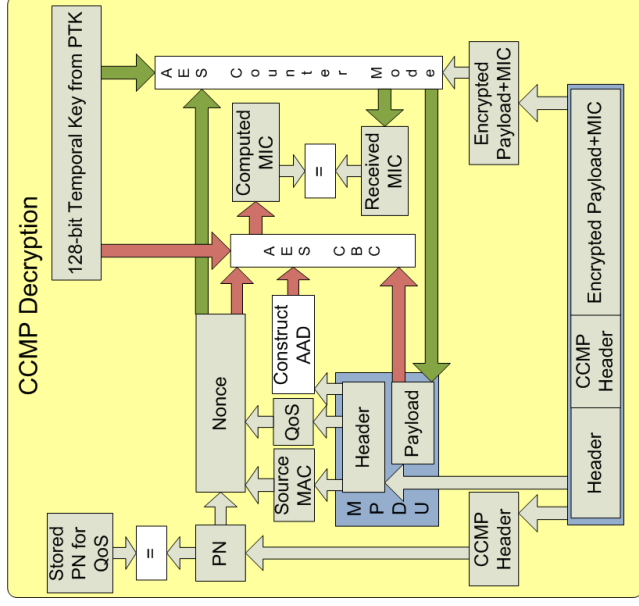
- Beacon
- Probe Req, Probe Resp
- Assoc Req, Assoc Resp
- Reassoc Req, Reassoc Resp
- Disassociation
- Authentication
- Deauthentication



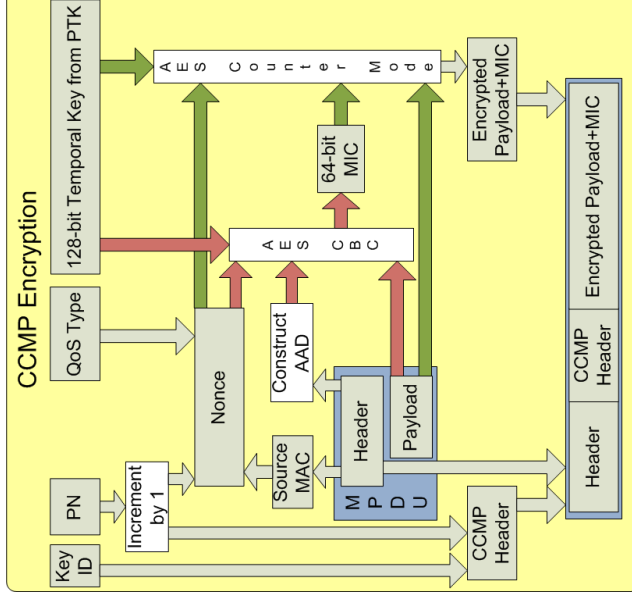
- PN – číslo paketu
- Nonce – unikátne číslo každého rámca
- MIC – Message Integrity Code
- AAD - additional authentication data

- ToDS=1, rámec je určený pre distribučný systém
- FromDS=1, rámec pochádza z distribučného systému
- ToDS=1, FromDS=1, komunikácia medzi dvoma AP distribučného systému
- ToDS=0, FromDS=0, komunikácia v Ad-Hoc sieti posíla len prístupový bod klientom.

Frame Path	Address 1	Address 2	Address 3	Address 4
Frame between two wireless clients	Destination MAC	Source MAC	BSSID	N/A
Frame from network through AP to Client	Destination MAC	AP's MAC	Source MAC	N/A
Frame from client to network through AP	BSSID	Source MAC	Destination MAC	N/A
Frame traveling between two APs in a WDS	Receiving AP's MAC	Transmitting AP's MAC	Destination MAC	Source MAC



- Poskytuje autentifikáciu na sieťovej vrstve
  - EAP zabezpečuje autentifikáciu
  - Access point zabezpečuje šifrovanie (TKIP/CCMP)
- Pozostáva z:
  - Supplicant (Client)
  - Authenticator (AP)
  - Authentication Server (RADIUS or IAS server)
- Extensible Authentication Protocol (EAP)
  - 802.1X používa niekoľko typov EAP pre autentifikáciu klientov
  - Typy EAP: PEAP, LEAP, EAP-MD5, EAP-TLS, EAP-TTLS
  - Správny výber typu EAP má veľký vplyv na bezpečnosť siete





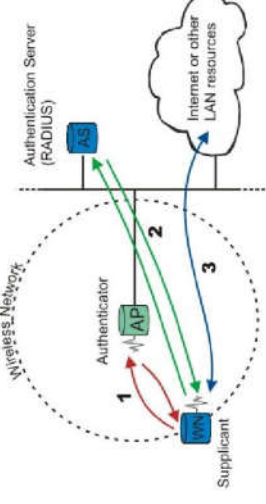
- CISCO proprietárny protokol
- Nepoužíva certifikáty
- Challenge-response autentizace
- Postup útoku:
  - Odchytenie komunikácie
  - crack challenge-response tokenu
  - asleap

38

- EAP pôvodne navrhnutý pre drôtové siete - pre odpočúvanie bol nutný fyzický prístup
- Protected EAP (PEAP) and Tunnelled Transport Layer Security (TTLS) používajú TLS k ochrane autentifikačných protokolov v bezdrôtovom prostredí
- Nutnosť certifikátu pre overenie RADIUS servera
- PEAP podporuje MS-CHAPv2 ako vnútornú autentifikačnú metódu.
- TTLS podporuje MS-CHAPv2, CHAP, PAP, ...

39

- 802.1X + RADIUS



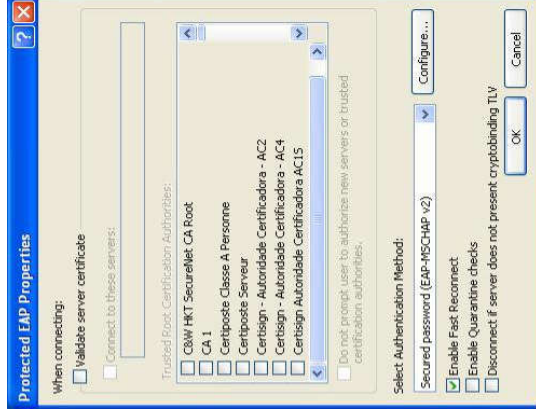
No.	Time	Source	Destination	Protocol	Length	Info
2	2011-00:4f:62:26:f3:df	IntelCor_73:0d:f4	00:4f:62:26:f3:df	EAP	73	Request, Identity [RFC3748]
3	2011-00:4f:62:26:f3:df	IntelCor_73:0d:f4	00:4f:62:26:f3:df	EAP	78	Response, Identity [RFC3748]
4	2011-00:4f:62:26:f3:df	IntelCor_73:0d:f4	00:4f:62:26:f3:df	EAP	88	Request, MD5-Challenge [RFC3748]
5	2011-00:4f:62:26:f3:df	IntelCor_73:0d:f4	00:4f:62:26:f3:df	EAP	88	Response, MD5-Challenge [RFC3748]
6	2011-00:4f:62:26:f3:df	IntelCor_73:0d:f4	00:4f:62:26:f3:df	EAP	71	Success

36

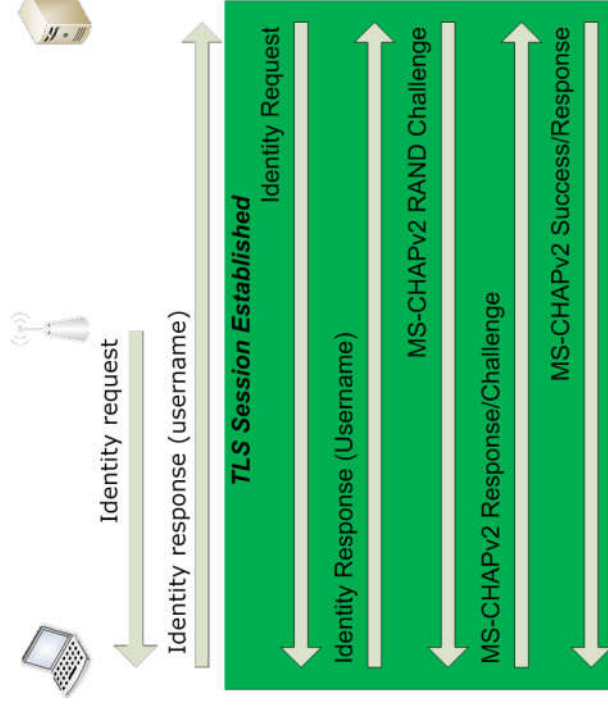
- Pôvodne iba pre LAN
- Autentizácia typu challenge-response
  - response = md5(user\_id+password+challenge\_request)
- Postup útoku:
  - Odchytenie komunikácie
  - “crack” md5 hashe
    - eapmd5pass
    - eapmd5crack.py
    - cca 350tis k/s (WPA-PSK cca 1500 k/s)

37

- Mnoho nasadení vypína validáciu certifikátom
- PEAP následne dôveruje každému RADIUS serveru

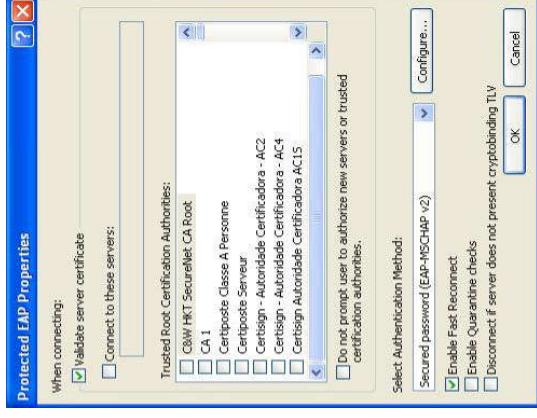


- PEAPv0 with EAP-MSCHAPv2
- Autentizácia serveru voči klientovi (certifikát)
- Postup útoku:
  - Rogue AP (hostapd)
  - Vlastný radius server (freeradius-wpe)
  - Deautentizácia klienta (airdrop-ng)
  - Crack challenge (asleep)

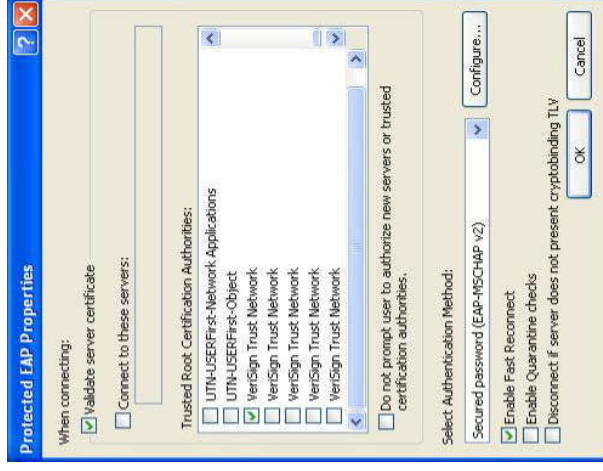


- SSID môže byť ľahko podvrhnuté
- TLS poskytuje metódu pre validáciu access point (Authenticator) resp. siete
- Až keď je certifikát overený, klient poslela autentifikačné informácie
- Autentifikačný prenos je chránený pred odposluchom TLS tunelom

- Validácia certifikátu servera je povolená
- Štandardné nastavenie Wireless Zero Configuration (WZC)
- Užívateľ potvrdzuje validitu certifikátu
- Minimum informácií v dialog boxe
- Útok rovnaký ako predtým, ale nutnosť potvrdiť certifikát

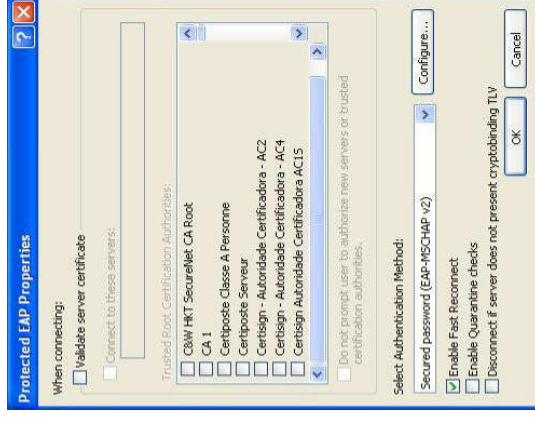


- Validácia certifikátu servera je povolená
- Dôveryhodná koreňová certifikačná autorita je vybraná
- **Nevaliduje sa CN!**
- Útok:
  - Odchytanie platného loginu a zistenie CA TLS certifikátu
  - Kúpa certifikátu od dôveryhodnej CA
  - Každé CN môže byť použité
  - Nastavenie RADIUS k použitiu tohto certifikátu

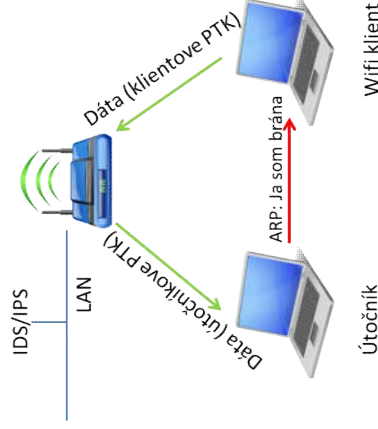
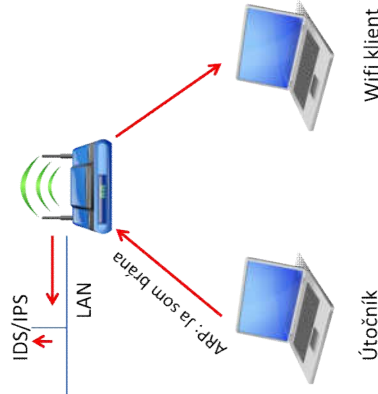
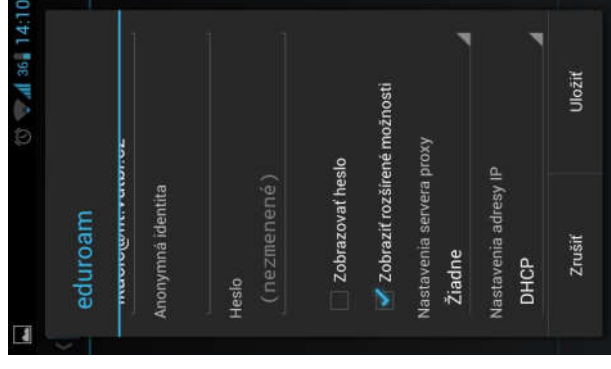
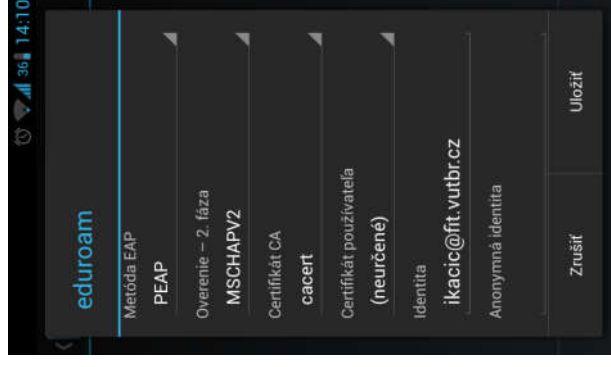
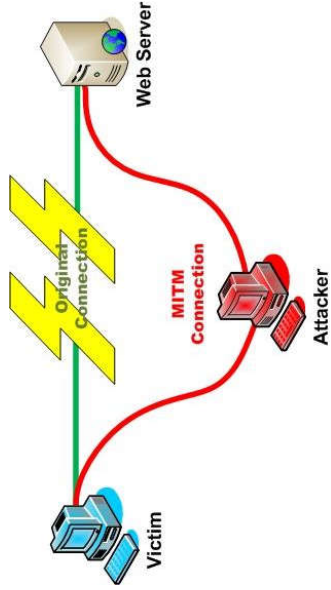


- Wireless Pwnage Edition (WPE) patch pre FreeRADIUS 2.0.2
  - Returns success for any authentication requests
  - Logs all authentication credentials
    - Challenge/response
    - Password
    - Username
- Performs credential logging on PEAP, TTLS, LEAP, EAP-MD5, EAP-MSCHAPv2, PAP, CHAP, and others

- Mnoho nasadení vypína validáciu certifikátom
- PEAP následne dôveruje každému RADIUS serveru







- Používa GTK kľúč
  - Rovnaký pre AP aj všetkých pripojených klientov
  - Posiela upravené rámce klientom
  - Klienti tieto rámce považujú za validné rámce poslané prístupovým bodom
- **Stealth** ARP poisoning, DoS attack, ...
- Náročná detekcia, obzvlášť na mobilných zariadeniach

## • “Harden and patch” infraštruktúry :

- Access points
- Wireless controllers
- Authentication servers
- Nepoužívať skryté AP
- Vypnúť nebezpečné typu EAPu (md5)
- Zabrániť nezabezpečeným klientom používať bezdrôtovú sieť
- Použiť Firewall a izolovať bezdrôtovú sieť od vnútornej siete

54

- Zväziť nasadenie Wireless IDS
- Detekuje:
  - De-auth attacks
  - RTS and CTS denial of service attacks
  - Rogue APs
- IDS je iba detekcia a nie prevencia
- POZOR na wireless IPS

55

- Neautorizovaný prístupový bod - Rogue AP
  - Inštalovaný zamestnancom
  - Inštalovaný útočníkom
    - Pripojený do LAN siete – backdoor
    - Mimo LAN siete -
  - Ako detekovať rogue AP?

52

- Použiť CCMP pre šifrovanie
  - Migrovať z TKIP
  - Nikdy nepoužívať WEP
- Použiť PEAP, TTLS, TLS pre autentifikáciu
  - TLS vyžaduje PKI
  - Vyhnúť sa použitiu Pre-Shared Keys (PSK)
    - Všetko čo je zdieľané nie je bezpečné
    - Ak musíte použiť PSK, zvoľte unikátne SSID and použite komplexný kľúč o dĺžke viac ako 14 znakov

53

Wi-Fi Fish Finder  
Security Assessment Tool for WiFi Clients  
(c)2009 Md Sohail Ahmad, Prabhakar Dhyani, Airtight Networks

CH 6 [ Elapsed: 5 mins ] [ 2009-07-30 11:47 ]

STATION	AUTH	ENC	Security-Posture	MODE	Probed SSID
00:1C:BF:01:E8:99	WPA2-802.1x	CCMP	Vuln	Infra	Test-PEAP-Vulnerable
---	WPA2-802.1x	CCMP	Secure	Infra	Test-WPA2-1X-AES
---	WPA2-802.1x	TKIP	Secure	Infra	Test-WPA2-1X-TKIP
---	WPA2-PSK	CCMP	Secure	Infra	Test-WPA2-PSK-AES
---	WPA2-PSK	TKIP	Secure	Infra	Test-WPA2-PSK-TKIP
---	WPA1-802.1x	CCMP	Secure	Infra	Test-WPA1-1X-AES
---	WPA1-802.1x	TKIP	Secure	Infra	Test-WPA1-1X-TKIP
---	WPA1-PSK	CCMP	Secure	Infra	Test-WPA1-PSK-AES
---	WPA1-PSK	TKIP	Secure	Infra	Test-WPA1-PSK-TKIP
---	WEP -Open	WEP	Vuln (WEP Cracking)	Infra	Test-WEP-Open
---	-Open	OPEN	Vuln (Unencrypted)	Infra	Test-Open
---	WEP -SKA	WEP	Vuln (WEP Cracking)	Infra	WEP_Shared

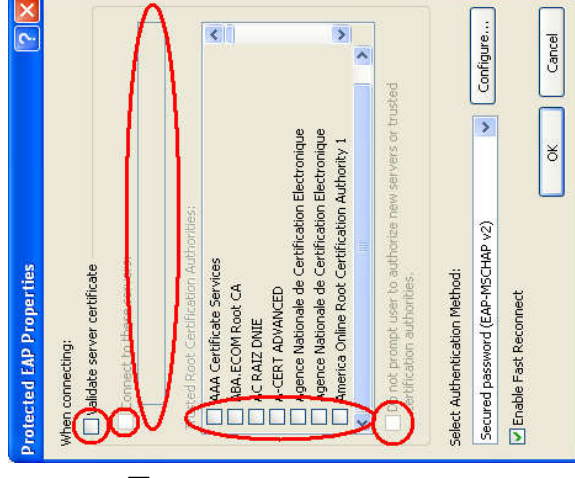
## Nástroje pre audit wifi sietí – aircrack-ng

- <http://www.aircrack-ng.org/>
- [airbase-ng](#) -- Multi-purpose tool aimed at attacking clients as opposed to the AP itself.
- [aircrack-ng](#) -- 802.11 WEP and WPA/WPA2-PSK key cracking program.
- [airdecap-ng](#) -- Decrypt WEP/WPA/WPA2 capture files.
- [airdecloak-ng](#) -- Remove WEP Cloaking™ from a packet capture file.
- [airdriver-ng](#) -- Script providing information and allowing installation of wireless drivers.
- [airdrop-ng](#) -- A rule based wireless deauthentication tool.
- [aireplay-ng](#) -- Inject and replay wireless frames.
- [airgraph-ng](#) -- Graph wireless networks.
- [airmon-ng](#) -- Enable and disable monitor mode on wireless interfaces.
- [airodump-ng](#) -- Capture raw 802.11 frames.
- [airolib-ng](#) -- Precompute WPA/WPA2 passphrases in a database to use it later with aircrack-ng.
- [airserv-ng](#) -- Wireless card TCP/IP server which allows multiple application to use a wireless card.
- [airtun-ng](#) -- Virtual tunnel interface creator.
- [easyside-ng](#) -- Auto-magic tool which allows you to communicate to an WEP AP without knowing the key.
- [packetforge-ng](#) -- Create various type of encrypted packets that can be used for injection.
- [tkiptun-ng](#) -- Proof-of-concept implementation the WPA/TKIP attack: inject a few frames into a WPA TKIP network with QoS
- [wesside-ng](#) -- Auto-magic tool which incorporates a number of techniques to seamlessly obtain a WEP key in minutes.

- Používanie dlhých a zložitých hesiel
- Aplikovanie všetkých aktualizácií rýchlo
  - Vrátane aktualizácie firmwaru pre wireless karty
- Posilnenie bezpečnosti systému (hardening)
- Zakázať ad-hoc siete
- Zabrániť premosteniu siete
- Zaistiť, že klient je správne nakonfigurovaný

## Zabezpečenie PEAP konfigurácie

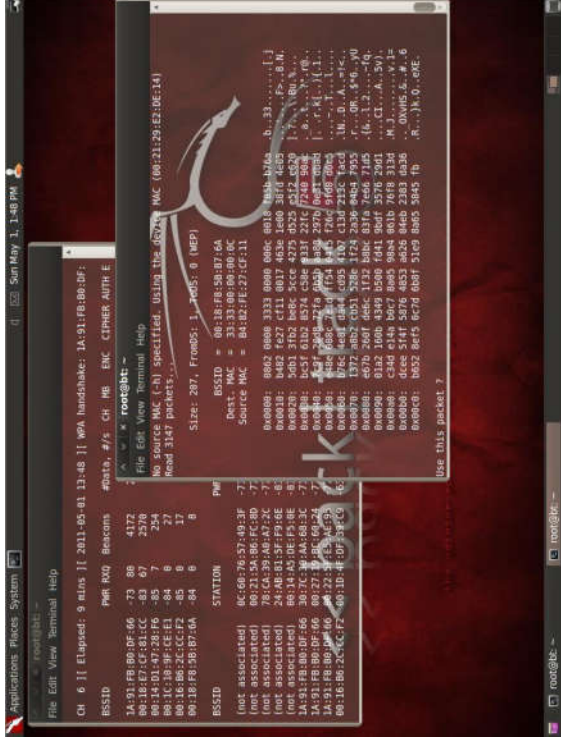
- Zaistiť:
  - “Validate server certificate”
  - “Connect to these servers” and specify the CN of the RADIUS server
  - “Trusted Root Certificate Authorities” – Povoľiť len CA, ktorá odpovedá certifikátu servera
  - “Do not prompt user to authorize new servers authorize new servers
  - Vynútiť pomocou zásad politiky systému





## Ďakujem za pozornosť

- <http://www.backtrack-linux.org/>



## Záver

- Používať
  - WPA2 v režime AES/CCMP
  - Silné a dostatočne dlhé heslá
  - Certifikáty
  - „Správnu konfiguráciu“
- V prípade nezabepečenej siete použiť vpn, ipsec,...
- Nespoliehať sa slepo na mechanizmy nižších vrstiev
  - Používať https, scp a podobne
- Zväziť použitie Wireless IDS/IPS