Мрежова сигурност I

http://training.iseca.org/

Wi-Fi 1/2

2010-10-26

Boyan Krosnov

Acknowledgements

Some materials are based on work by

- Wikipedia users
  - MarkWarren, Zedh, Geocachernemesis, Stannered, Adamantios, Mark0

Преговор и план на курса

- Увод в мрежовата сигурност
- Криптография
- Увод в мрежите
- Ethernet

→ Wi-Fi

- IP
- UDP, DHCP, ARP, IP routing protocols
- IPv6
- TCP
- Тест – средата-края на Ноември
- Демо
- ...

План

- Слоевете
- История на Wi-Fi
- Стандарти
- Физическа среда
- Ad-hoc mode
- Infrastructure mode
- Mesh
- Authentication and Encryption

- Инструменти и атаки

Слоевете

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, DNS, NTP, DHCP
4/5. TCP, UDP, RTP, SCTP
3. IP / IPv6
2. Ethernet, Wi-Fi, etc.
1. physical media, modulation and coding

История

- 1985 - ISM bands
  - 5% of spectrum
- 1991 - Pre-standard
  - WaveLAN - NCR -> Lucent -> Proxim
- 802.11-1997 - 1Mbps, 2Mbps
- 1999
  - 802.11a – 6-54Mbps @5GHz
  - 802.11b – 5.5Mbps, 11Mbps
  - Wi-Fi Alliance formed
- 2003 - 802.11g – 6-54Mbps @2.4GHz
- 2009 – 802.11n – up to 600 Mbps @2.4GHz & 5GHz

Стандарти

- IEEE
  - Standards
  - http://standards.ieee.org/getieee802/802.11.html
- Wi-Fi Alliance
  - Certification, Interop and Early Standards
  - http://www.wi-fi.org/

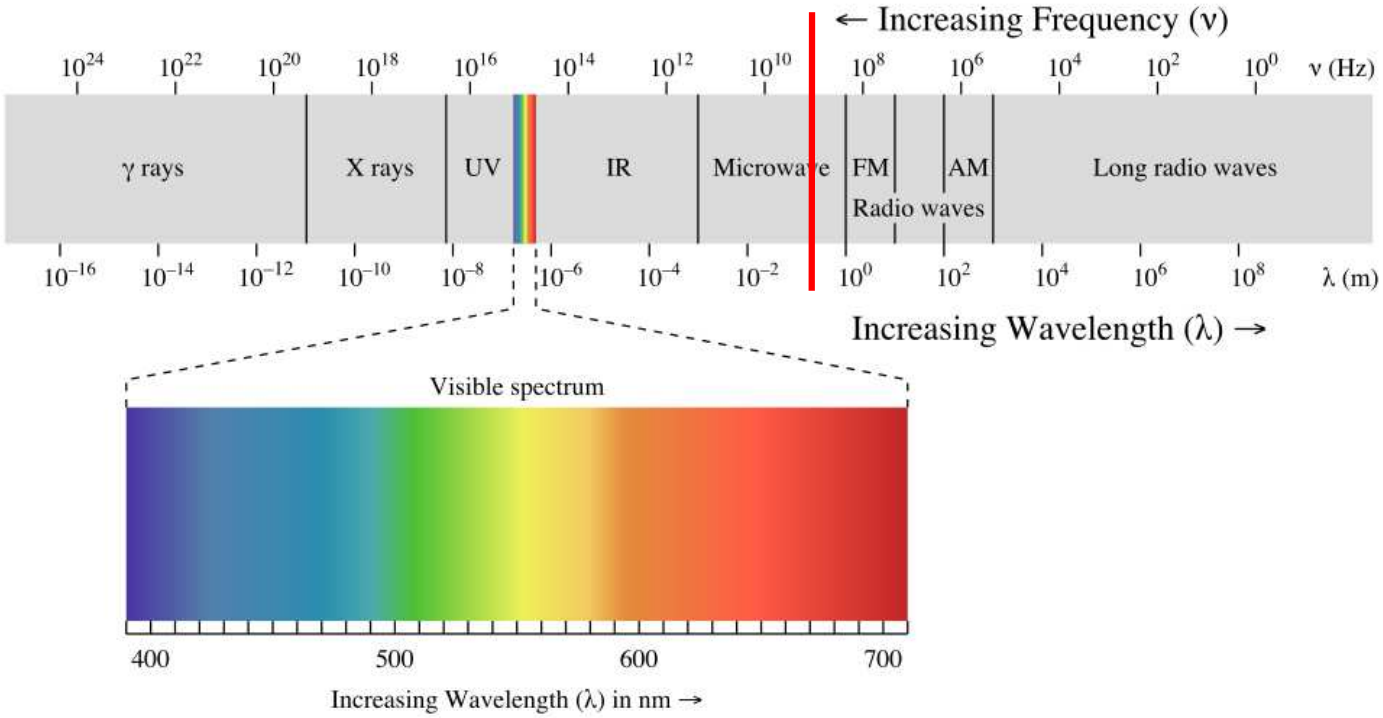
Стандарти

- 802.11-2007, 802.11-2011
- 802.11 a,b,g,n
- 802.11i – WPA2
- 802.11w – Protected management frames

- WPA – replaced by WPA2
- WPS

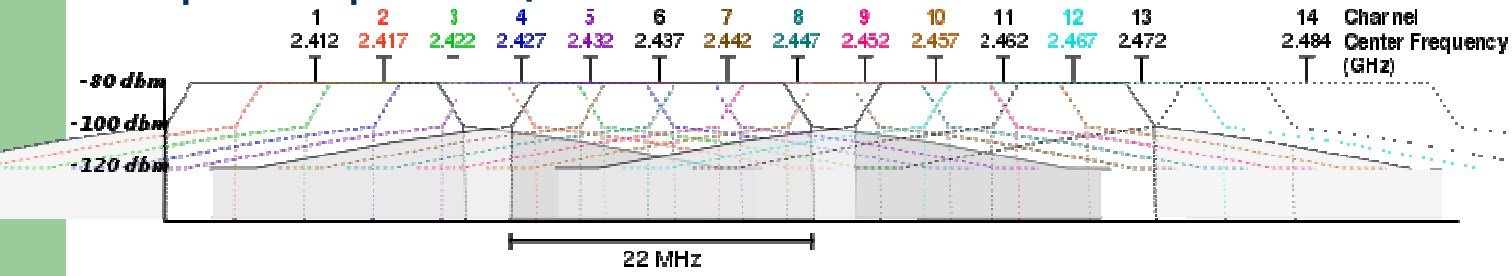
- Drafts
  - Draft 802.11s – Mesh networking
  - Draft 802.11u – Interworking with external networks

Физическата среда



Физическата среда

- Припокриващи се канали



- Други технологии на същите честоти

Физическата среда

- Ефир
- Дизайн на физическата среда
- Параметри
  - Прозрачност
  - Мощност на сигнала
  - Разпространение на сигнала

Ad-hoc mode

- a.k.a. IBSS (Independent Basic Service Set)

- Мрежа без централно управление
- Станциите комуникират директно една с друга

- Няма пълна свързаност, комуникацията не е гарантирана

Infrastructure mode

- Access point
  - Basic Service Set (BSS)
  - Authentication & Encryption
  - BSSID (BSS identifier)
- Multi-AP networks
  - Mobility & Hand-over
  - SSID (ESS/IBSS identifier)
- Bridge към Ethernet

Фрейма

- Data фреймове

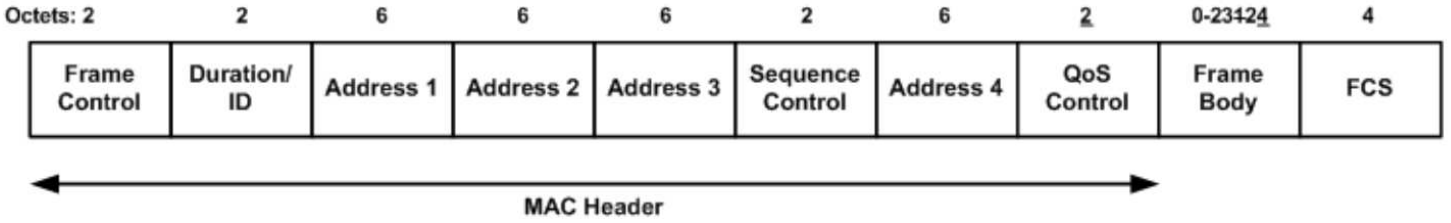


Figure 7-1—MAC frame format

- Контролни фреймове – различен формат

Mesh

- WDS
- MANET
- Само-конфигурираща се мрежа
- Автоматичен relay на трафик между станциите

Въпроси

Authentication and Encryption

- 802.1X, EAP

- WEP
- WPA
  - TKIP/RC4
  - Съвместимост със стар хардуер
- 2004 - 802.11i - WPA2
  - CCMP/AES
  - “Robust Security Network”

EAP

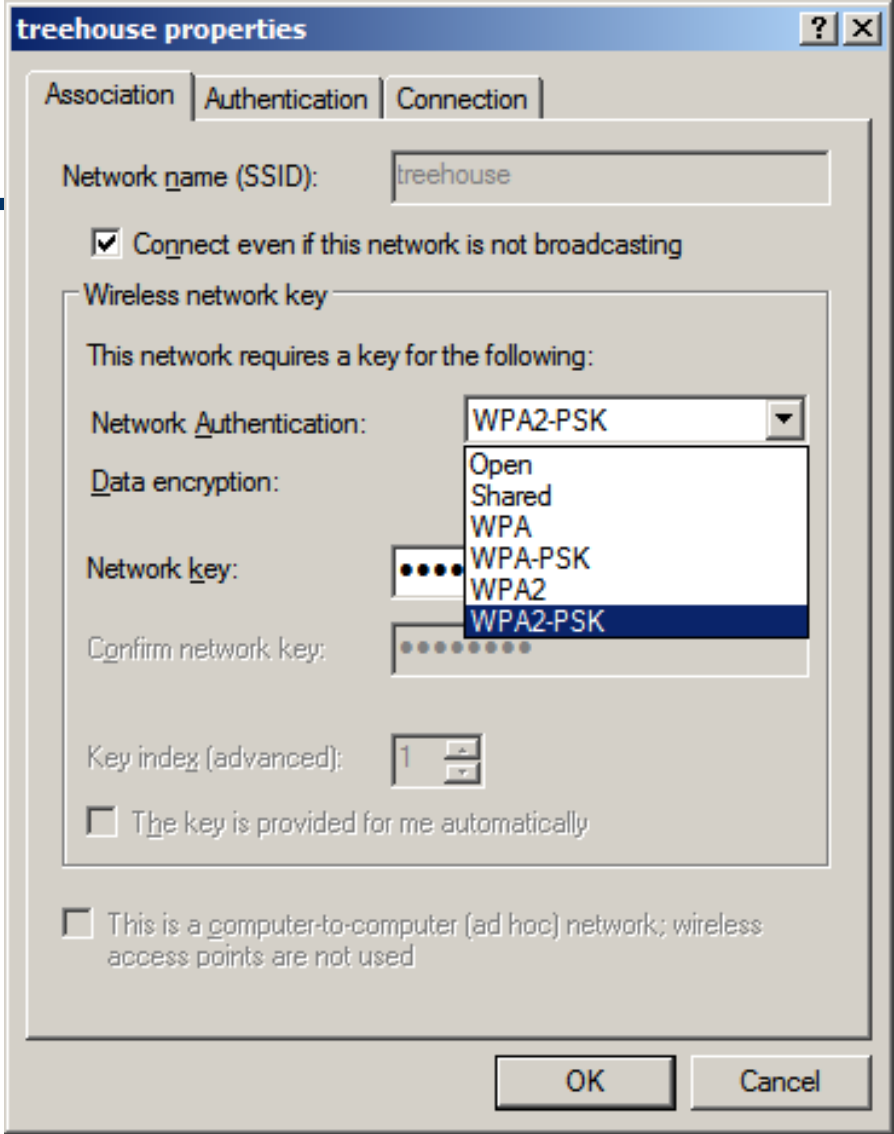
- IETF standard
  - 1998 – RFC 2284 – PPP EAP (obsoleted)
  - 2004 – RFC 3748 – EAP (proposed standard)
    - 2008 – RFC 5247 – EAP Key Management framework
- Everything over EAP
  - TLS (certificates)
  - EAP-MD5, EAP-PSK
- EAP over everything
  - EAP over GSM
  - EAP over 802.1X
  - EAP over PPP
  - EAP over RADIUS

Optional crypto

- Използването на WEP/WPA/WPA2 е по избор
- ... и изключено по подразбиране

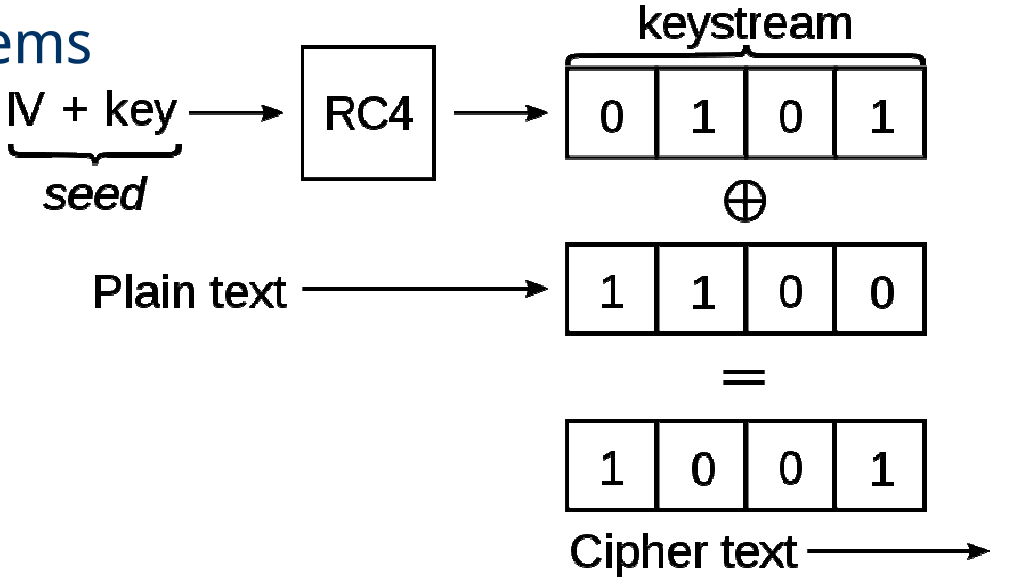
Options

- Open, Shared
  - WEP
- WPA / WPA2
  - “Enterprise”
  - PMK derived through EAP
- WPA-PSK / WPA2-PSK
  - PMK= f(PSK)



WEP

- Stream cipher – RC4
- Short IV – 24 bits
  - birthday paradox
  - related key attack
- Other problems



Authentication and Encryption (WPA/WPA2)

1. Association

2.A. 802.1X / EAP Authentication

or

2.B. Use PMK derived from PSK

3. Establish PTK

- PSK = Pre-shared key
- PMK = Pairwise master key
- PTK = Pairwise transient key
- GTK = Group transient key

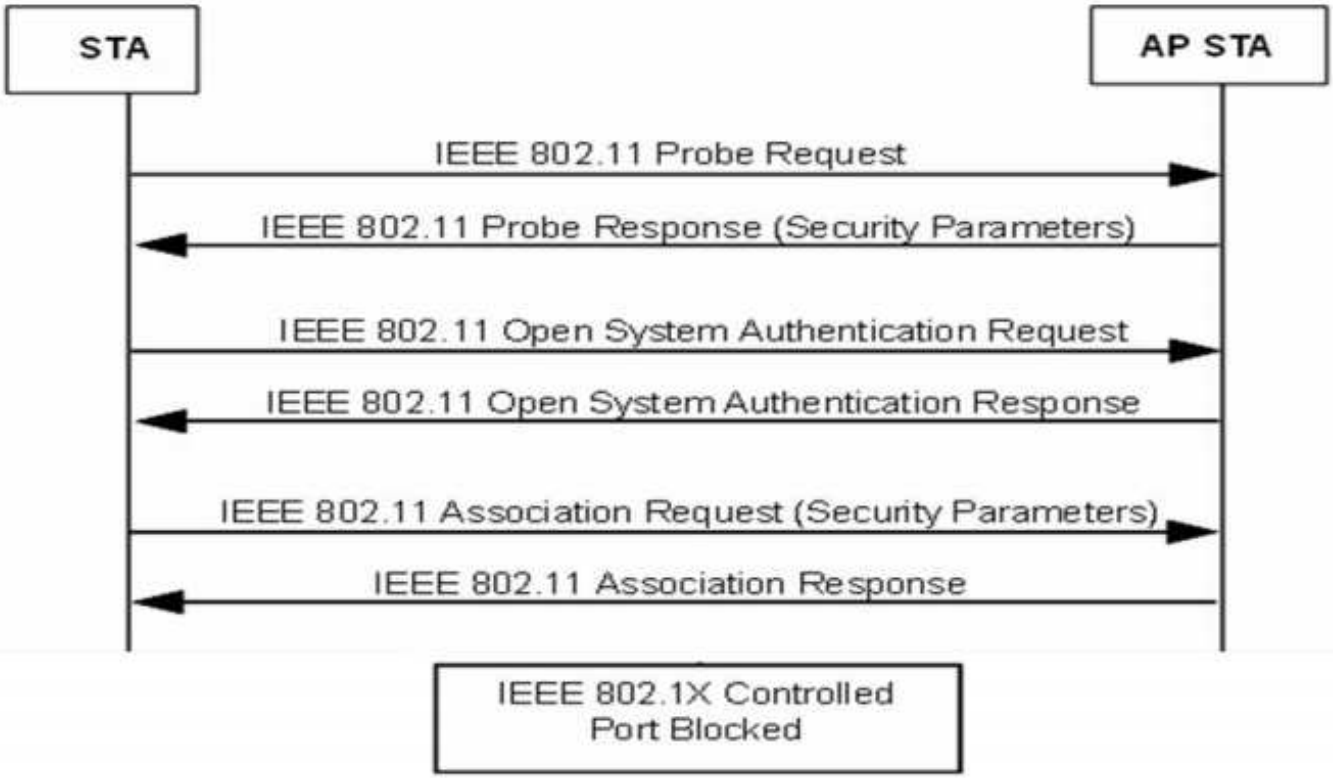


Figure 5-11—Establishing the IEEE 802.11 association

2.A. Authentication (WPA/WPA2)

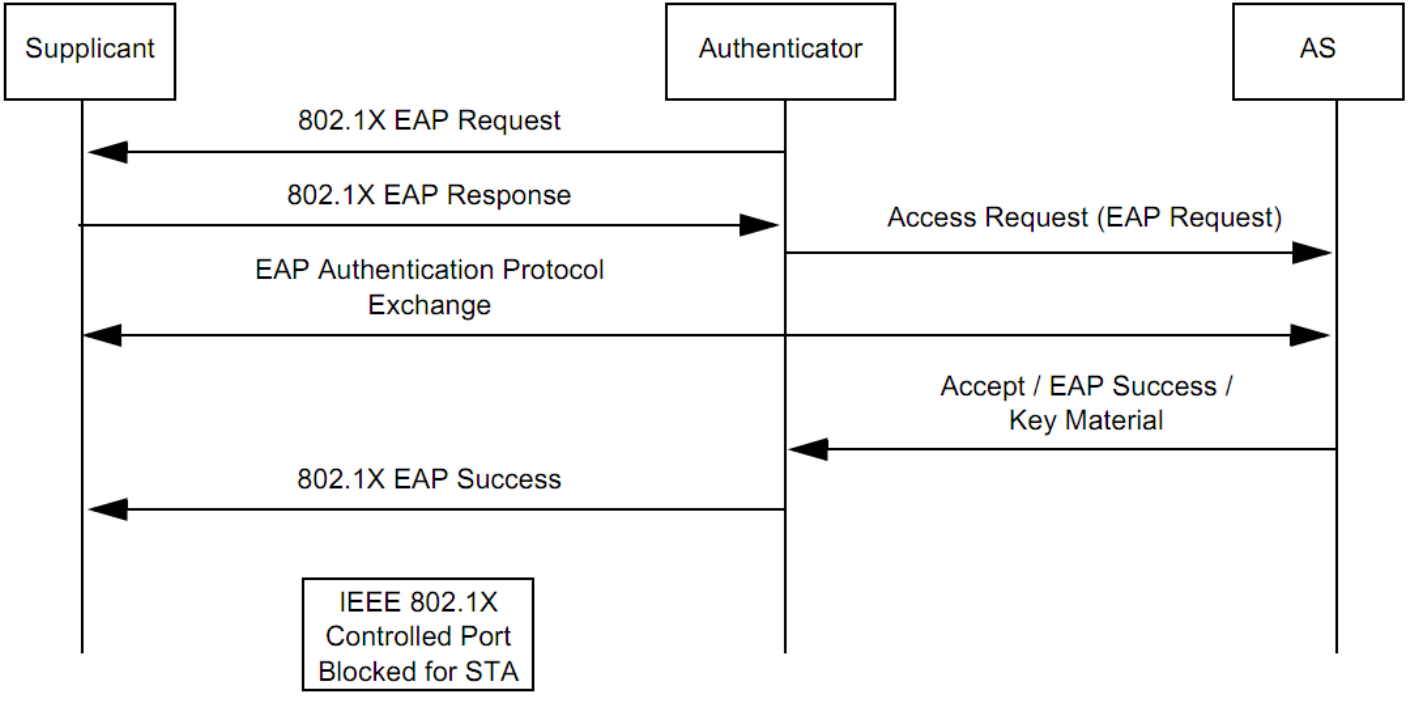


Figure 5-12—IEEE 802.1X EAP authentication

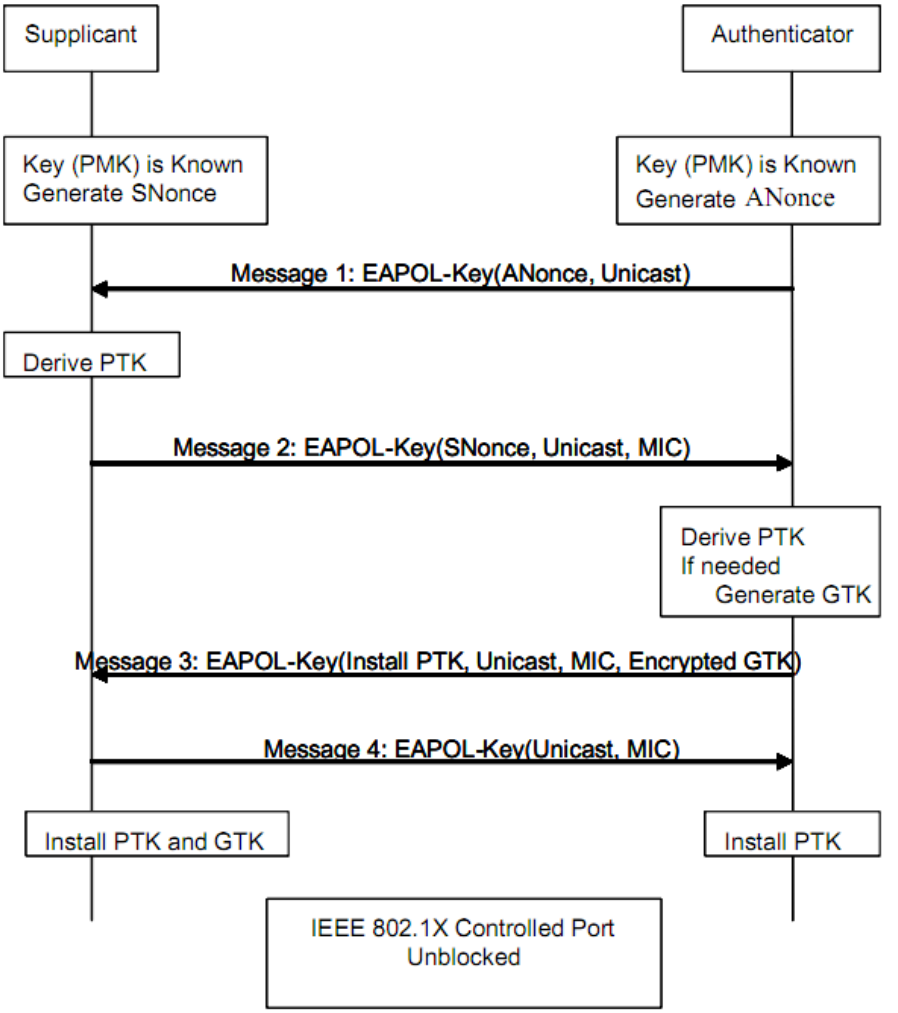


Figure 5-13—Establishing pairwise and group keys

Въпроси

Мрежова сигурност I

http://training.iseca.org/

Wi-Fi 2/2

2010-10-26

Boyan Krosnov

План

- Преговор
- История на Wi-Fi
- Стандарти
- Физическа среда
- Ad-hoc mode
- Infrastructure mode, roaming
- Mesh
- Authentication and Encryption

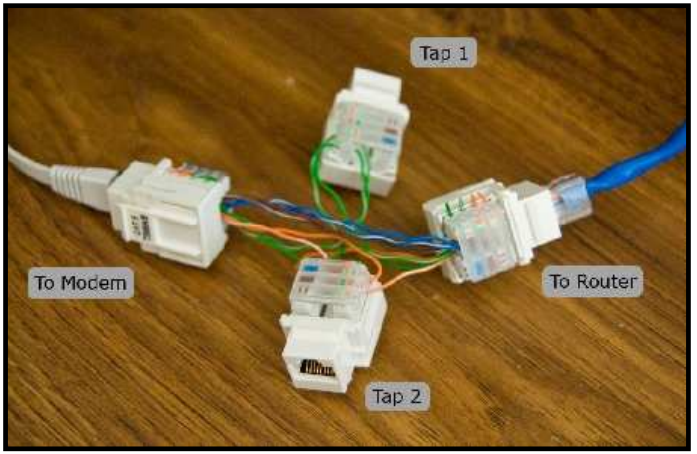
→Инструменти и атаки

Класове проблеми

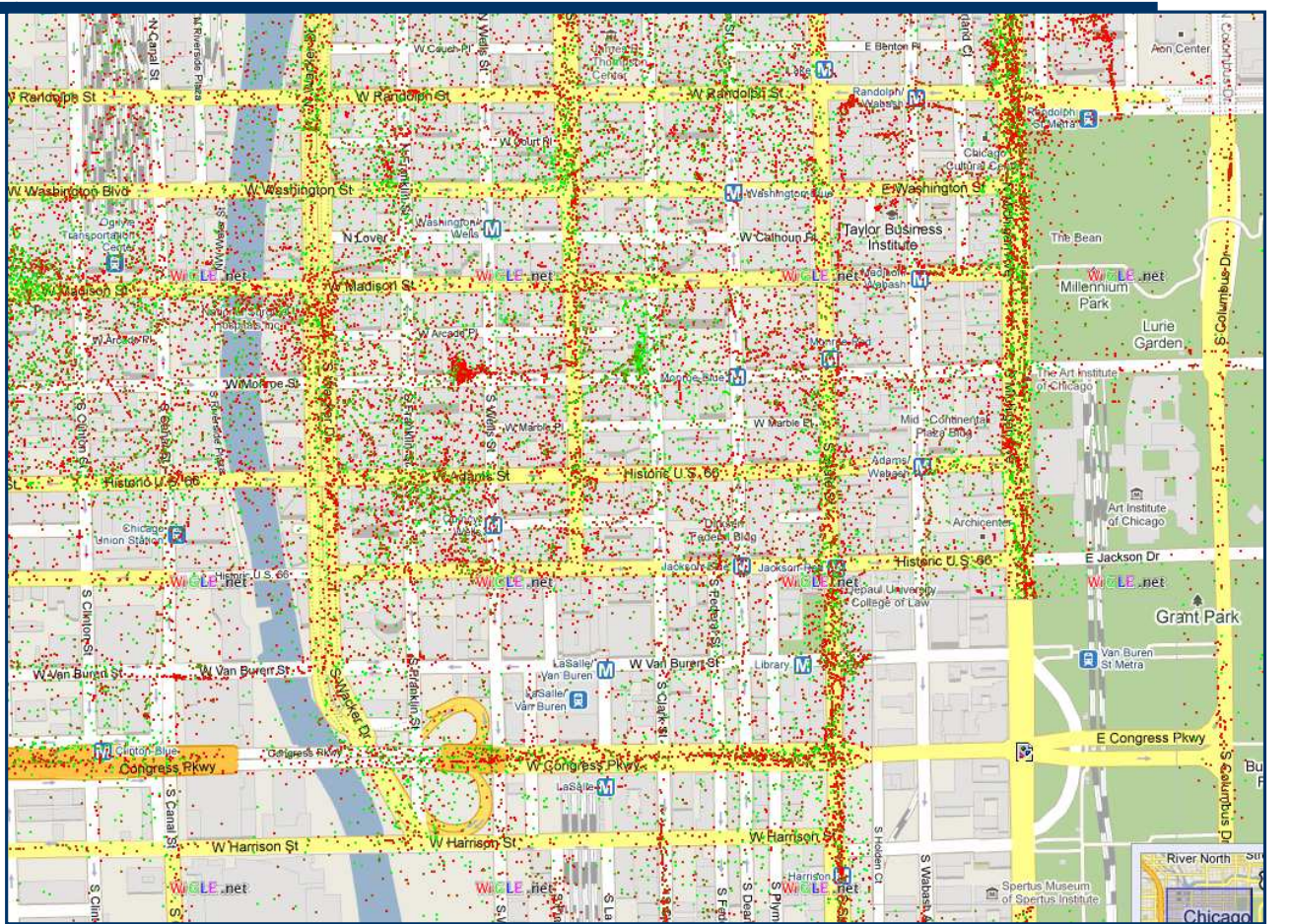
- Подслушване
- AP impersonation, Endpoint impersonation
- Physical DoS
- Logical DoS
  - disassociation
- WEP слабости
- TKIP/RC4 слабости
- CCMP/AES слабости
- Password (PSK/PMK) brute force
- Бъгове в драйвери

Ethernet - Физически слой - атаки

- DoS на споделената среда
- Пасивно подслушване - 10/100
- MITM



Wardriving


W Randolph St
W Washington Blvd
W Madison St
W Monroe St
W Adams St
Historic U.S. 66
W Van Buren St
W Congress Pkwy
W Harrison St
E Washington St
E Jackson Dr
E Congress Pkwy
Millennium Park
Lurie Garden
The Bean
Grant Park
Art Institute of Chicago
Taylor Business Institute
Aon Center
Chicago Union Station
Ogilvie Transportation Center
River North
Chicago
WiGLE.net

Impersonalization

- SSID/BSSID spoofing
- MAC spoofing
  - MAC filter brute force

Physical DoS

- Заглушаване
  - Continuous wave transmitter
  - Микровълнова печка (800 W магнетрон)
- Фарадеев кафез
  - Anti-wifi боя

Логически DoS

- Disassociation / deauthentication

5.8.2.3 Disassociation

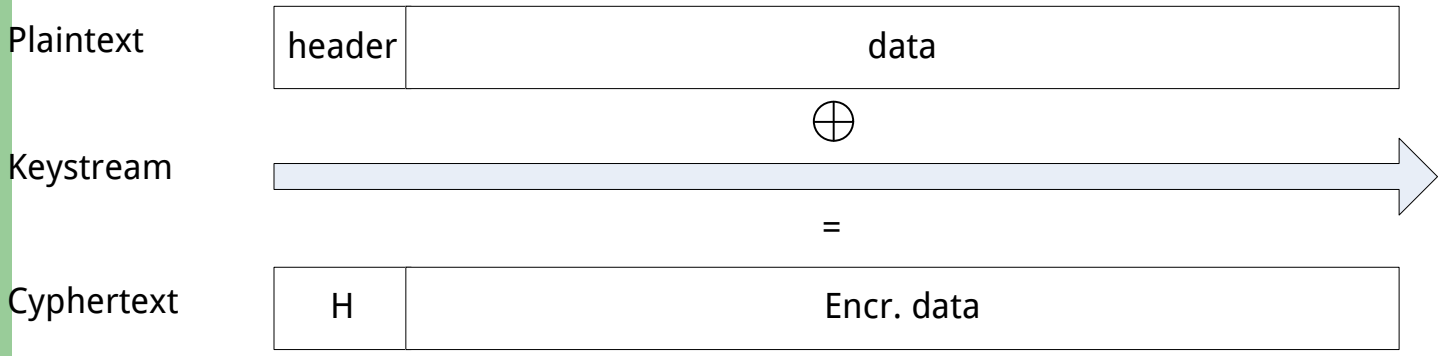
Disassociation initiated by either STA in an RSNA causes the deletion of the PTKSA at both ends and the deletion of the GTKSA in a non-AP STA. The controlled and uncontrolled ports created for this association will also be deleted.

- Frame fuzzing

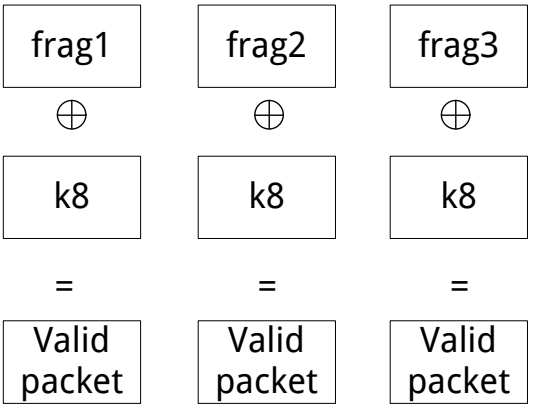
WEP

- Weak crypto
- Fragmentation attack
  - Obtain key material from traffic
- Chop-Chop
  - get packet
  - chop one byte off
  - try 256 different check-sums by asking AP
- Café Latte attack
  - Pretend to be AP (optional)
  - Client associates. Get ARP packet from client. Send crafted ARP. Client responds

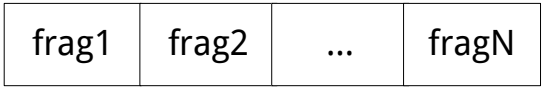
WEP Fragmentation attack



H⊕ header = 8 bytes of Keystream (K8)



"BAD" packet



TKIP/RC4 слабости

- 2008 - Beck-Tews attack
  - chop-chop revisited
  - “Practical attacks against WEP and WPA”
- 2009 - Ohigashi-Morii attack
  - “A Practical Message Falsification Attack on WPA”

CCMP/AES слабости

- 2006 “Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol”
  - TMTO - Effective key strength – 85 bits
- 2010 Hole 196

- Най-големия проблем е все още brute force на паролата

Hole 196

8.5.1 Key hierarchy

RSNA defines two key hierarchies:

a) Pairwise key hierarchy, to protect unicast traffic

b) GTK, a hierarchy consisting of a single key to protect multicast and broadcast traffic

NOTE—Pairwise key support with TKIP or CCMP allows a receiving STA to detect MAC address spoofing and data forgery. The RSNA architecture binds the transmit and receive addresses to the pairwise key. If an attacker creates an MPDU with the spoofed TA, then the decapsulation procedure at the receiver will generate an error. GTKs do not have this property.

196

Проблеми в драйверите

- madwifi bug
- Apple bug

- Fuzzing

Въпроси

Tools

- BackTrack Linux

- aircrack-ng
- pyrit – WPA/WPA2-PSK PMK pre-computation
- mdk3 – attack toolbox
- Kismet
- Wireshark
- openwrt

Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

In fact, Aircrack-ng is a set of tools for auditing wireless networks.

pyrit

Pyrit allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. Exploiting the computational power of Many-Core- and other platforms through ATI-Stream, Nvidia CUDA, OpenCL and VIA Padlock, it is currently by far the most powerful attack against one of the world's most used security-protocols.

mdk3

- **Features:**
- Bruteforce MAC Filters
- Bruteforce hidden SSIDs (some small SSID wordlists included)
- Probe networks to check if they can hear you intelligent Authentication-DoS to freeze APs (with success checks)
- FakeAP - Beacon Flooding with channel hopping (can crash NetStumbler and some buggy drivers)
- Disconnect everything (aka *AMOK-MODE*) with Deauthentication and Disassociation packets
- WPA TKIP Denial-of-Service
- WDS Confusion - Shuts down large scale multi-AP installations

Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins which allow sniffing other media such as DECT.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and infering the presence of nonbeaconing networks via data traffic.

Допълнителни материали

Ще публикуваме на сайта на курса

Въпроси