Advanced Security Issues in Wireless Networks

Seminar aus Netzwerke und Sicherheit
Security Considerations in Interconnected Networks

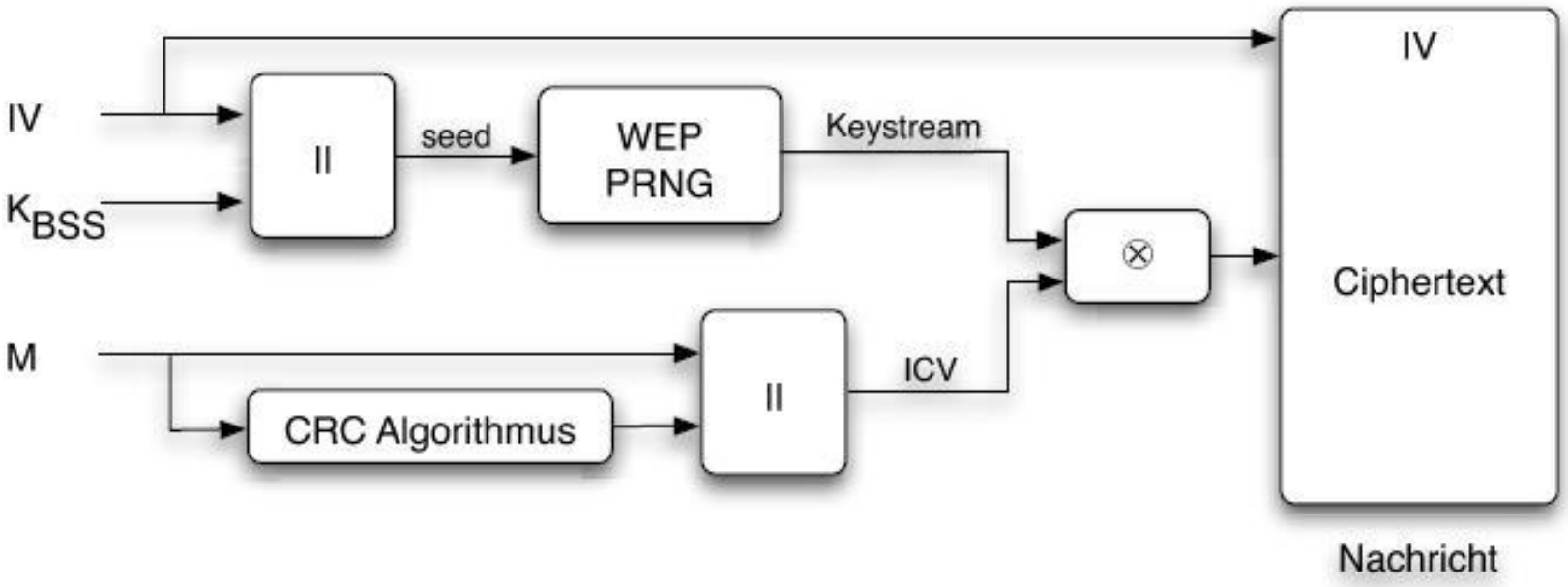
Alexander Krenhuber
Andreas Niederschick

9. Januar 2009

Short Overview of WEP

- Wired Equivalent Privacy (WEP)
- Uses RC4 stream cypher
- Pseudo Random Number Generator (PRNG) gets Key and Initialisation Vector (IV) as input
- Key Scheduling Algorithm (KSA) generates a keystream
- Every station in the Basic Service Set knows the key
- New IV for every message
- An integrity check value is concatenated to every message
- The message is XORed with the Keystream (permuation of numbers 0-255)

WEP Encryption



Attacks on WEP

- Early attack from Fluhrer, Shamir, Mantin $\Rightarrow$ FSM-Attack
- Encryption methodology is commonly known
- The first few bytes of a packet are easy to predict (e.g. TCP-Header)
- IV is transmitted unencrypted and therefore known as well
- KSA can be simulated for these known bytes

Attacks on WEP

- If a few conditions hold, the next byte can be guessed (probability: ≈5%)
- 4.000.000 to 6.000.000 needed packets to recover the key at a 50% chance.
- Better attacks use more condititions
- KoreK attack needs about 70.000 packets
- PTW attack needs about 35.000 to 40.000 packets
- Key can be recovered in less than 1 minute

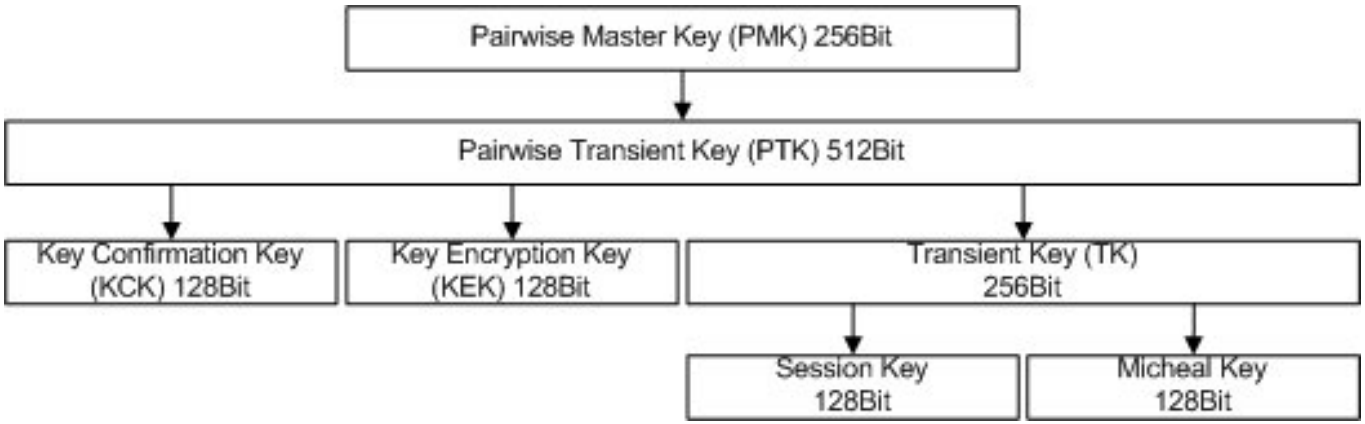
Short Overview of WPA

- Wi-Fi Protected Access (WPA)
- New Security Standard IEEE 802.11i was delayed
- Wi-Fi Alliance originally named WECA (Wireless Ethernet Compatibility Alliance) approved on 31. Oktober 2002 WPA as subset of IEEE 802.11i
- Certified April 2003

Goals of WPA:

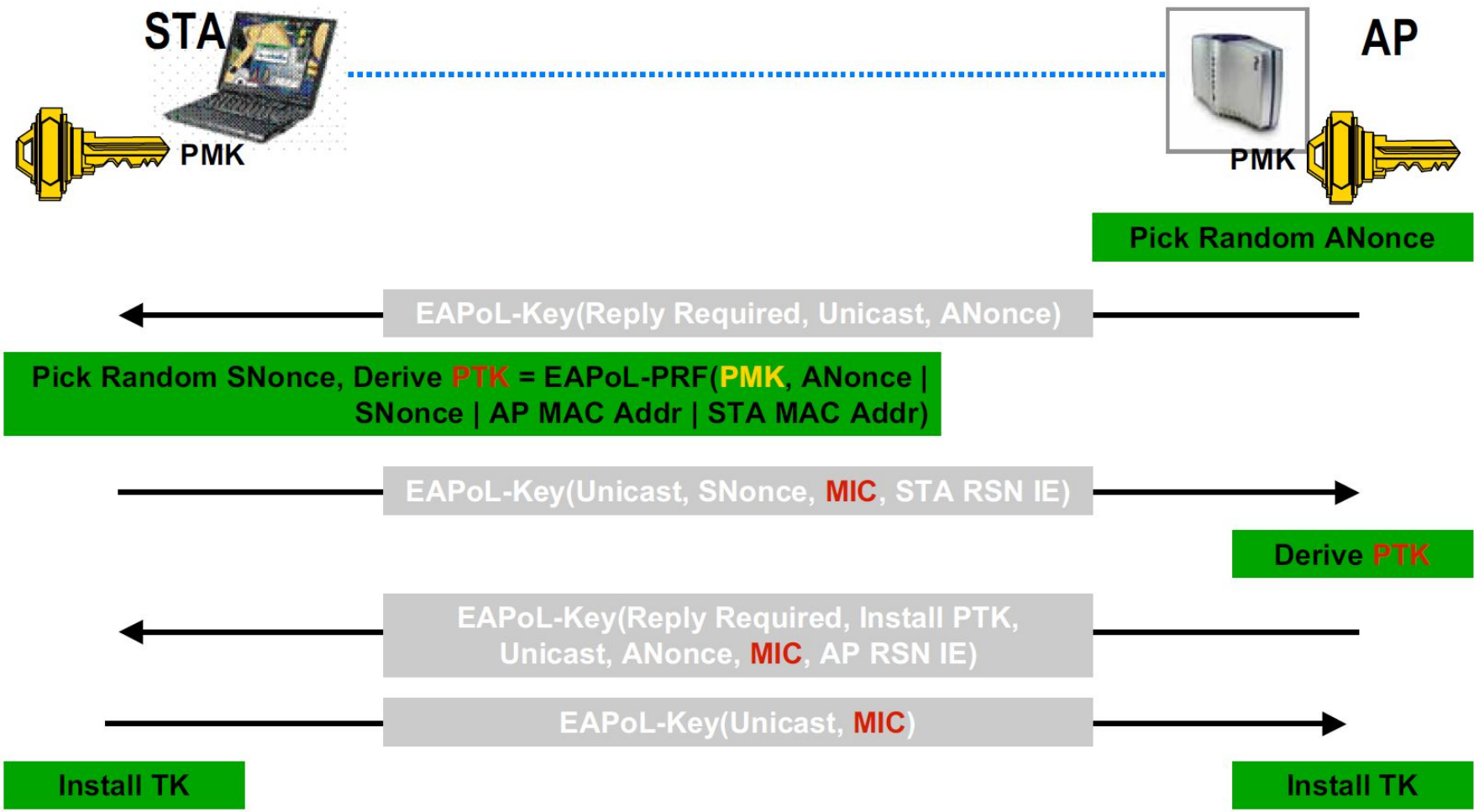
- Downwards compatibility (RC4 stream cipher)
- Dynamic keys through Temporal Key Integrity Protocol (TKIP)
- Data integrity by using a Message Integrity Check (MIC)
- Authentication via Pre-Shared Keys (PSK) or Extensible Authentication Protocol (EAP)

Key Types



- **Pre-Shared Key (PSK):** `8-63 printable ASCII Zeichen (95 verschiedene)`
- **Pairwise Master Key (PMK):**
  `PMK = PBKDF2(PSK, SSID, SSID_Len, 4096, 256)`
- **Pairwise Transient Key (PTK):** `PTK = sha1_prf(PMK, PKM_Len, Pairwise key expansion, data, sizeof(data))`
- **Key Confirmation Key (KCK):** `bind PMK to AP and client`
- **Key Encryption Key (KEK):** `encryption of group keys`
- **Session Key:** `key that encrypts the actual data`
- **Michael Key:** `encryption of the Message Integrity Check (MIC)`

Authentication mechanism - PSK



aus Verbesserte WLAN Sicherheit mit WPA, EAP und 802.11i von Maximilian Riegel

Weakness

1. **Generate PMK:** `PMK = PBKDF2(PSK, SSID, SSID_Len, 4096, 256)`
2. **Generate PTK:** `PTK = sha1_prf(PMK, PKM_Len, Pairwise key expansion, data, sizeof(data))`
   where data is composed of: LowerMac, HigherMac, LowerNonce, HigherNonce
   - MAC of client and AP (packet 3)
   - AP nonce (packet 3)
   - Client nonce (packet 2)
3. **Generate the MIC:**
   TKIP: MIC = hmac_md5(key, 16, data);
   AES: MIC = hmac_sha1(key, 16, data);
4. **Compare computed MIC with captured MIC from packet 4**

Brute Force

- Generating the MIC value is an exhaustive computing process
- Brute force attack are realy time consuming
- Only a dictionary attack make sense
- Around 100 keys/s

Rainbow Tables:

- First described in 1980 by Martin Hellman
- Use precalculated data stored in memory to reduce time consuming crypto process
- Once generated a lookup is very performant
- Already effective used against MD5, LM, NTLM Hashes
- But WPA uses the SSID as salt, therefor for every existing SSID a rainbow table must be generated
- Fortunately many equal SSIDs http://www.wigle.net/gps/gps/main/ssidstats
- Around 20.000 keys/s

Distributed Cracking

- Published in October 2008 by Russian security company Elcomsoft
- Password cracking suite called Distributed Password Recovery
  - use the power of Cuda enabled NVIDIA GFX Cards
  - up to 10.000 computing nodes with 64 cores / 4 GPUs
- A month before a similar program was posted in the Nvidia Cuda forum
- Pyrit - http://code.google.com/p/pyrit/
- Around 2000 lines of code
- Both programs offer similar performance
- GeForce 8800GTS up to 7500Keys/s
  GeForce GTX 280 up to 11500Keys/s

Distributed Cracking

- Using one 8800GTS

days	Numeric (10)	Alpha (26)	Alpha Numeric single (36)	Alpha Numeric case (62)	Printable ASCII (96)
8	0.077	161	2176	168472	5566277
9	0.77	4189	2144989	-	-

- Using 10.000 8800GTS

days	Numeric (10)	Alpha (26)	Alpha Numeric single (36)	Alpha Numeric case (62)	Printable ASCII (96)
8	0	0.02	0.2	17	556
9	0	0.42	7.8	1044	53436
10	0	11	282	64760	5129881
11	0.007	283	10156	4015166	-

- Very popular 16 numeric symbols computing time is around 2 years
- 14+ Alpha Numeric case sense symbols can be considered as safe for a while

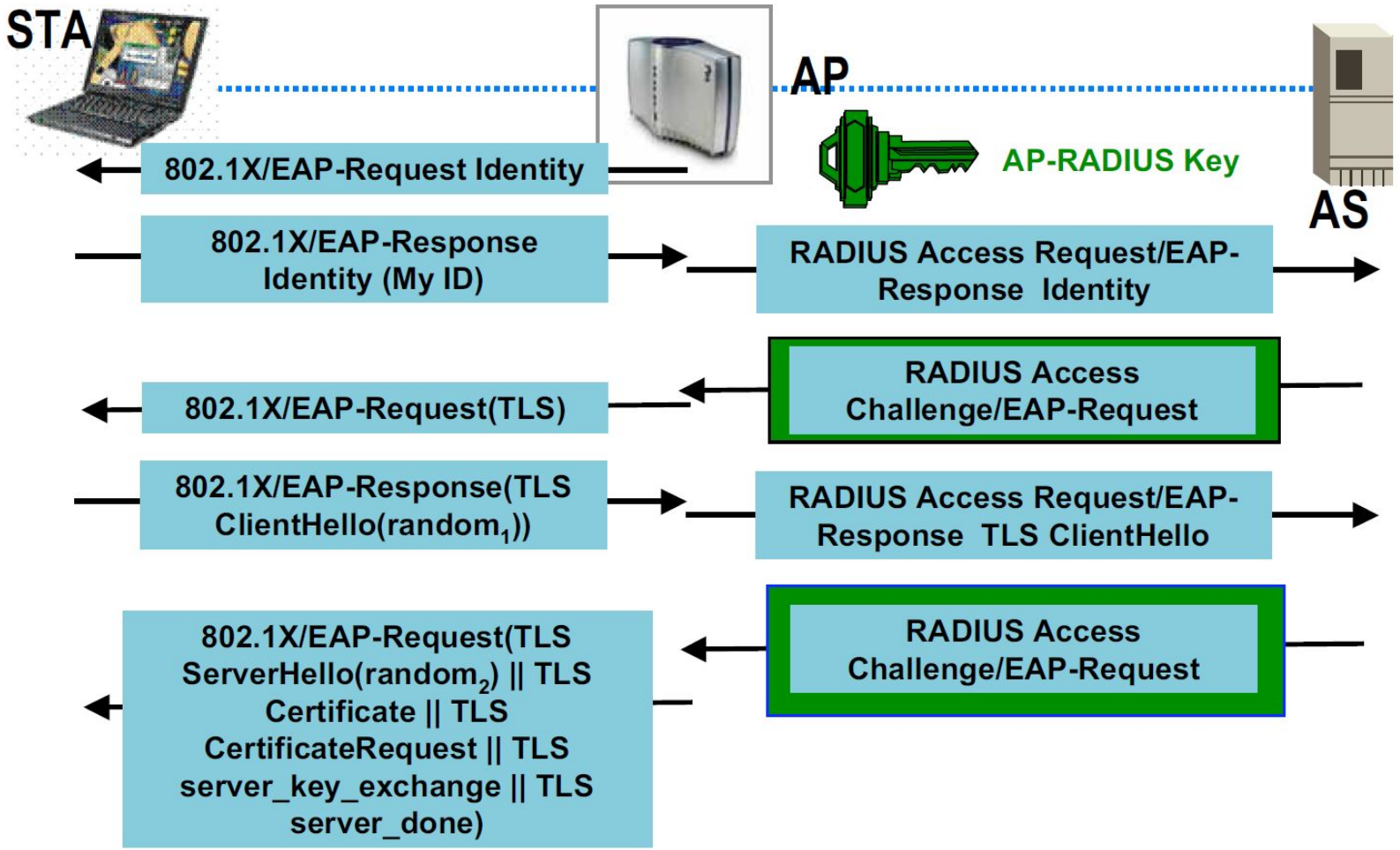
Key Exporting

- Brute force can be really time consuming
- Why not export the PSK from a connected client
- Easy target and much less effort to hack
  - Buffer Overflows
  - Spyware
  - Trojan
  - Rainbow tables :)
- Key is stored in known places:
  - Vista: `C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces`
  - XP: `HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces`
  - 2000: `HKLM\SYSTEM\CurContSet\Control\Class\Adapter_ID_Number`
  - Linux: `in some wpa_supplicant config file`

WPA Enterprise

- **All WPA features but...**
- **Central Authentication management**
- **EAP**
  - General protocol for host or user identification
  - Only defines message formats
  - In 802.1X the encapsulation is called EAPOL, EAP over LANs
  - Different types:
    - EAP-TLS
    - EAP-TTLS/MSCHAPv2
    - PEAP
    - ...
- **Authentication**
  - Authenticator: by Certificate
  - Supplicant: by Certificate (EAP-TLS)
    by Username and Password (EAP-TTLS, PEAP)

Authentication mechanism - Enterprise



aus Verbesserte WLAN Sicherheit mit WPA, EAP und 802.11i von Maximilian Riegel

Other Attacks

- Man in the Middle
- chopchop on WPA TKIP
- Denial of Service
- Domain Login Cracking
- 802.1X EAP Replay
- 802.1X RADIUS Replay
- 802.1X LEAP Cracking

Rogue Access Points

- Hardware is getting cheaper
- APs are easy to operate
- Therefore the chance of illegal access to wireless networks increases
- Rogue Access Points (RAPs) have to be kept in mind

Categories of RAP

- `Open APs`
- Officially used APs which are poorly configured and therefore might be exploited by attackers
- `Backdoor APs`
- Installed by an employee or an attacker
- Can be very harmfull because backdoor APs are connected to the wired network of an organisation

Categories of RAP

- `Fake APs`
- Installed by an attacker
- Can be used to retrieve data like passwords or set up a man-in-the-middle attack
- Can be located inside or outside an organisation
- Fake APs often use the same security configurations like official APs to complicate detection

Detecting RAP

- Staff equiped with an antenna and software like Netstumbler walks through an organisation
- Takes much time and RAPs can be deactivated while the scanning takes place
- Placing sensors in the organisations area
- Can be administered from a central point
- Both methods need hardware to listen on different frequencies due to the possible usage of different standards

Detecting RAP

- Querie Routers and Switches for allowed MAC-adresses
- Only known computers are allowed to communicate
- MAC-adresses can be spoofed easily
- Differences of temporal traffic characteristics
- Assumption: wired and wireless communication has divergent spreading of packets
- Therefore wireless APs can be detected in wired networks

Performance Influence

- How do secure methods influence data transmission performance?
- Test setup:
  - Lenovo T61 as Client
  - Linksys WRT54GS running OpenWRT as AP
  - Intel 4965AGN, Nec Aterm WL54AG, Netgear WG511
  - Distance: 5 meters including one brick wall
  - Performance measured using iperf with 100MBit/s Ethernet client

	Intel 4965AGN	Nec WL54AG	Netgear WG511
Open	27206	21004	21213
WEP 128Bit	25093	20617	20178
WPA TKIP	22975	18209	19532
WPA AES	26886	20442	21293
WPA2 AES	26623	na	na

Tips

- Do use WPA/ WPA2 AES
- If possible do use Enterprise Mode
- If PSK is your choice do use random 63 character passwords
- Passwords should not be derived from a known word
- Sentences might seem safe because of their length, but are likely to be weak
- Secure your clients and APs

Q & A