

WEP – Probleme und Risiken



Alexander C. Nägele
Benjamin B. Bratkus
Tobias D. Walter

Technische Funktion

- **Kommunikationsarten:**
 - AdHoc – direkte Kommunikation
 - Infrastructure – Kommunikation über Access Points
- **Zellstruktur**
 - jeder Access Point bedient eine Zelle
- **SSID**
 - benennt das Netzwerk
 - dient der Unterscheidung versch. Netze

Standards

Standard	Frequenzband	Max. Datenrate	NOC	Max. Reichweite
802,11	2,4 Ghz	2 Mbit/s	3	100 / 300 Meter
802.11a	5 Ghz	54 Mbit/s	4	20 / 1500 Meter
802.11b	2,4 Ghz	11 Mbit/s	3	50 / 300 Meter
802.11g	2,4 Ghz	54 Mbit/s	3	50 / 300 Meter

- NOC = Non Overlapping Channels
- Datenrate in der Regel nur 50%

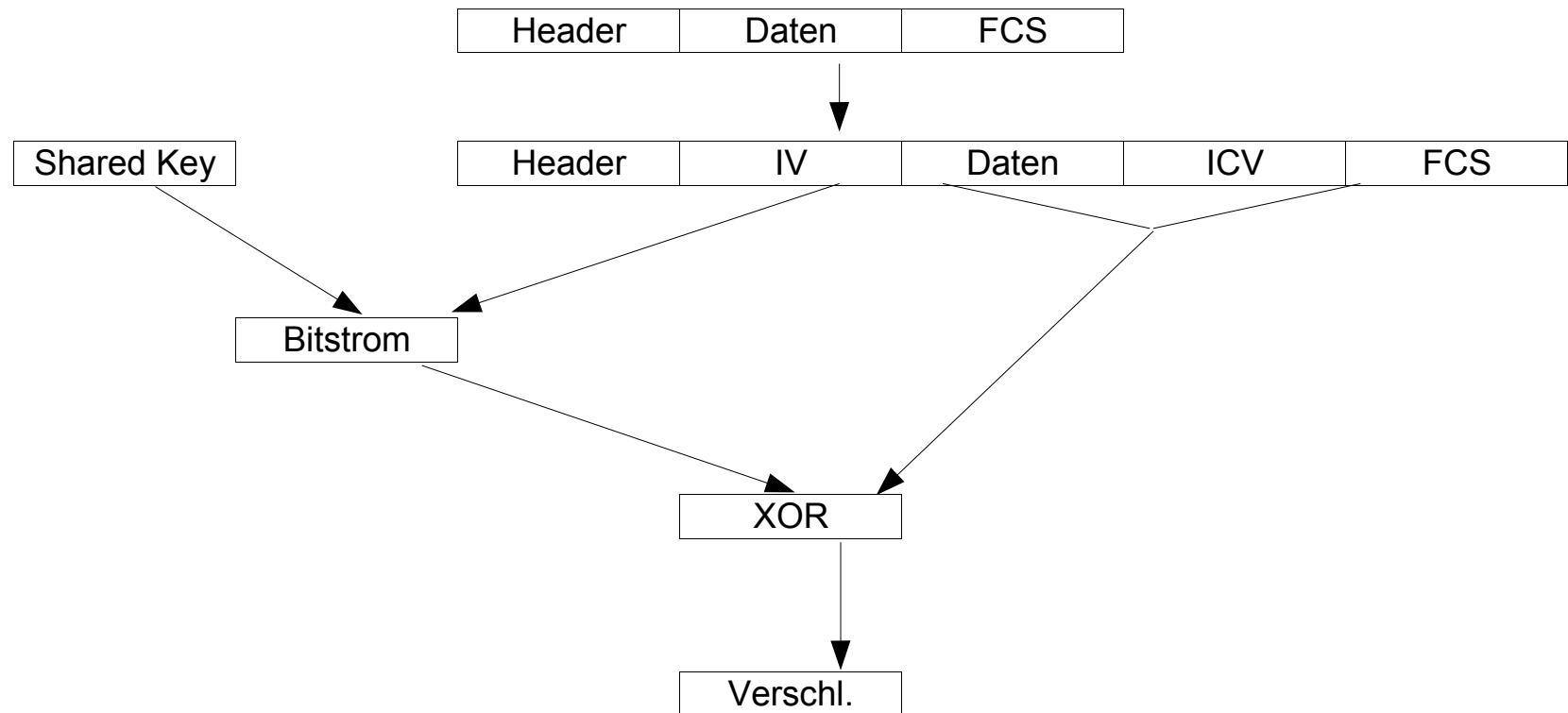
Frameformat von 802.11

- Format:
 - MAC-Header (30 Byte)
 - Body (0 – 2312 Byte)
 - Checksum (4 Byte)

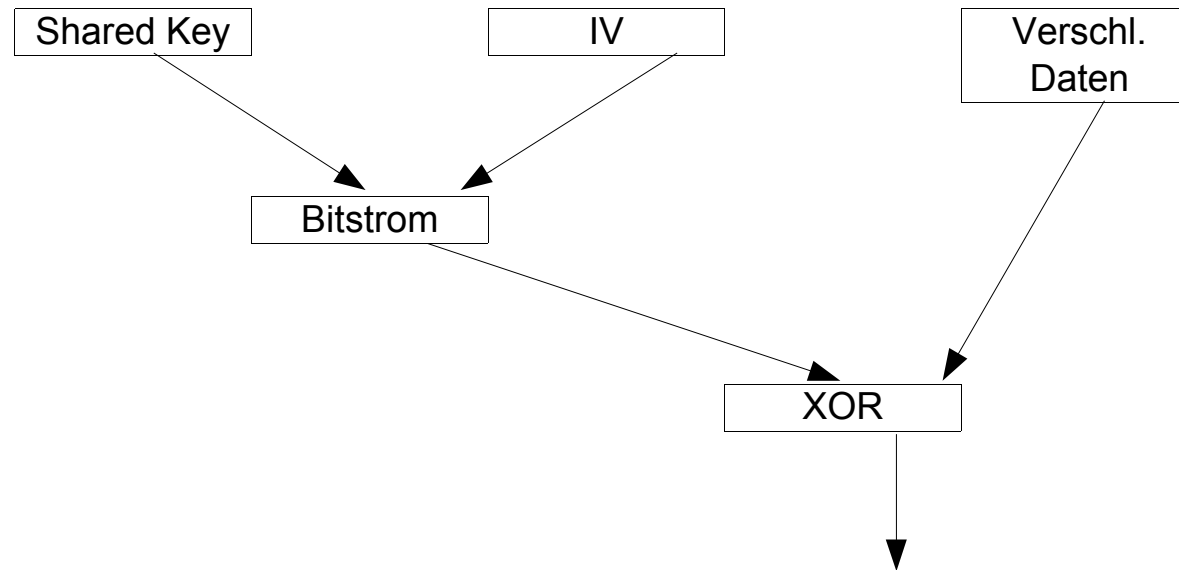
Frame Control	Duration / ID	Address I	Address II	Address III	Sequence Control	Address IV	Frame Body	Frame Checksum	
2	2	6	6	6	2	6	0 – 2312	4	Byte

Protoc. Version	Type	Sub-type	To DS	From DS	MF	Retry	Power Manag.	More Data	WEP	Order	
2	2	4	1	1	1	1	1	1	1	1	Bit

WEP – Wie wird verschlüsselt



WEP – Wie wird verschlüsselt



Warum WEP scheiße ist

- Schwäche im RC4-Algorithmus
- Wiederverwendung des Initialisierungsvektors
- Keine Methode, Schlüssel automatisch auszutauschen
- Erste Implementierung nur mit 40 Bit Schlüssel
- Simple Passphrasen

Möglichkeiten, WEP zu knacken

- FMS-Attacke
- Ausnutzen der RC4-Schwachstelle
- Brute Force Attacke
- Dictionary Attacke

FMS-Attacke

- Von Fluhrer, Martin und Shamir
- Nutzt Schwachstelle im Key-Scheduling-Algorithmus aus
- Schwache Initialisierungsvektoren lassen Rückschlüsse auf den Schlüssel zu
- ca. 5 bis 10 Millionen Pakete bzw. 100 bis 1000 MB Netzverkehr werden benötigt

RC4-Schwachstelle

- Anhand einer verschlüsselten Nachricht und deren Klartext kann man den Bitstrom errechnen (XOR)

Nachricht	01101011
Bitstrom	10111001
Verschlüsselte Nachricht	11010010

Nachricht	01101011
Verschlüsselte Nachricht	11010010
Bitstrom	10111001

RC4-Schwachstelle

- Alle Nachrichten, deren verschlüsselter Bitstrom mit diesem IV erzeugt wurden, können entschlüsselt werden
- Authentisierung am Access Point möglich
- Beliebige Pakete können ins Netz gesendet werden

RC4-Schwachstelle

- Möglichkeiten, um an die benötigten Daten zu gelangen
 - Abhören einer Shared-Key-Auth.
 - Einschleusen von Paketen

Brute Force und Dictionary Attack

- Brute Force
 - durchprobieren möglicher Keys
 - grosser Rechenaufwand
- Dictionary Attack
 - basiert auf der Annahme einfacher Passphrasen
 - Wörterbuch mit möglichen Passphrasen

Wie macht man WLAN sicherer

- Verschlüsseltes Tunneling
 - IPSec
 - VPN
- Access Points vor der Firewall
- WPA (Weiterentwicklung von WEP)

Referenzen

- zum Nachlesen:

- WLAN-Standard

<http://grouper.ieee.org/groups/802/11/>

- Weakness in the key scheduling algorithm of RC4
von Fluhrer, Martin und Shamir

<http://downloads.securityfocus.com/library/>

- comp.security.misc
- comp.os.linux.networking
- comp.security.firewalls

- Tools:

- Aircrack-ng - aircrack-ng.org
- WepCrack - sourceforge.net/projects/wepcrack

Vielen Dank für die Aufmerksamkeit...