Contents

1 Mobilfunk

1.1 Global System for Mobile Communications (GSM)

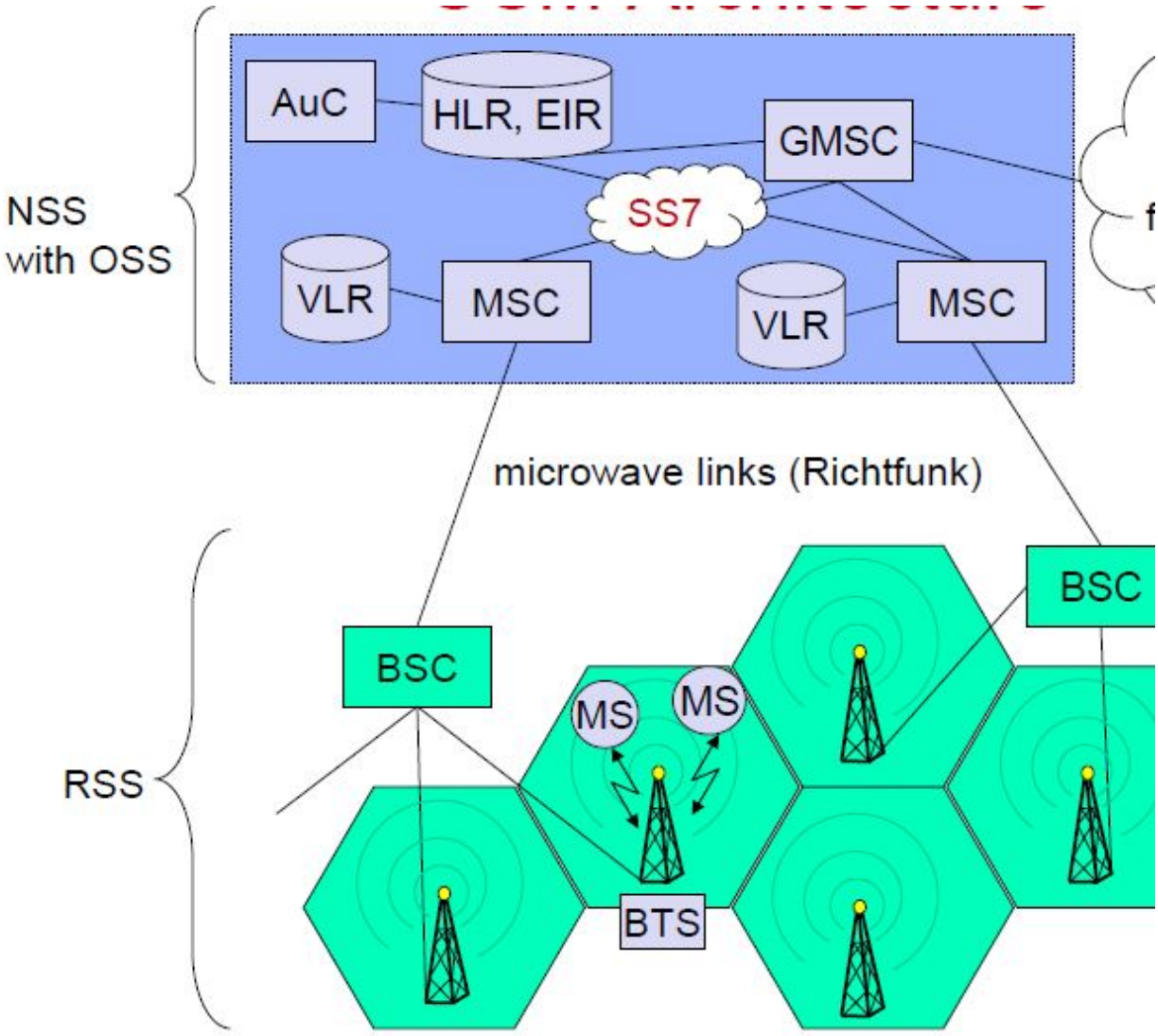

Figure 1: GSM-Overview

- MSG: Mobile Switching Center, verwaltet andere BSCs
- VLR: Visitor Location Register, kennt über HLR alle darunter verbundenen Nutzer/Geräte
- HLR: Home Location Register
  - kennt aktuelle MSC/BSCs jedes Nutzers
  - EIR: Equipped Identity Register, enthält IMEIS aller registrierten Nuter
  - AuC: Authentication Center, enthält dei symetrischen Schlüssel jeder SIM-Karte
- BTS: Base Transciever Station
- NSS: Network and Switching Subsystem
- OSS: Operation Subsystem

1.1.1 Ablauf eines Anrufs (Handy zu Handy)

1. Verbindung mit aktueller Basisstatino und Senden der gewünschten Telefonnummer
2. System schaut in Home File des Angerufenen nach, identifiziert Zellregion
3. Alle Basisstationen der Zellregion machen Broadcast nach dem angerufenen Handy
4. Handy antwortet
5. Anruf wird über die Basistation mit der besten Verbindung abgewickelt

1.1.2 GSM - Authentifizierung und Verschlüsselung

  - Identifier:
  - IMEI: Gerätespezifische ID, einzigartig für jedes Handy (International Mobile Equipment Identifier)
  - IMSI: Kunden-ID pro SIM-Karte (International Mobile Subscriber Identifier)
  - TMSI: Temporäre IMSI, wird regelmäßig geupdatet

- Authentifizierung: mittels A3 und A8 Algorithmus + 128bit Pre-Shared-Key K_{SIM} der SIM-Karte
- Verschlüsselung: mittels A5 Algorithmus + 64/54bit Session Key K_C, neu pro Verbindung

1.1.3 GSM - Ablauf Authentifizierung und Verschlüsselung

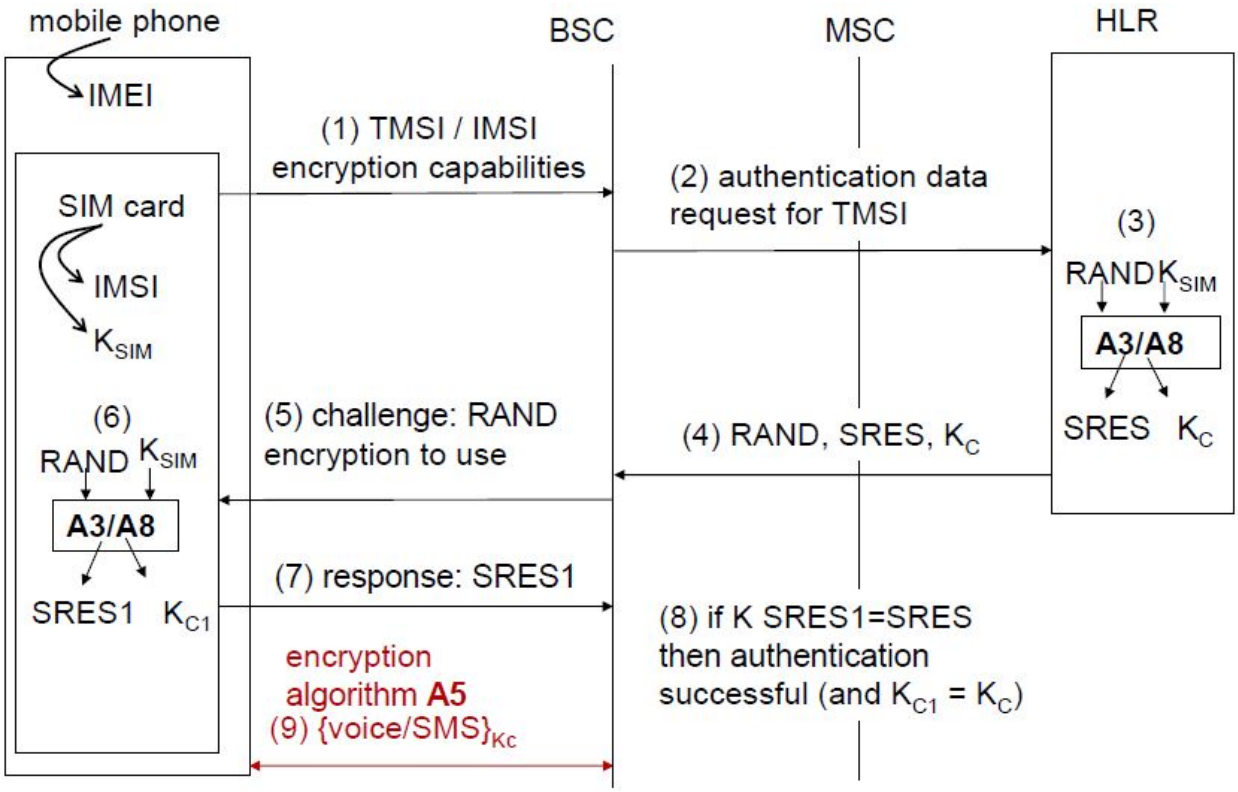

Figure 2: GSM - Ablauf Authentifizierung und Verschlüsselung

Zu **1**:

- Falls TMSI nicht der Verwaltung bekannt, soll das Handy die IMSI schicken → Robustheit

- Verschlüsselungsmöglichkeiten:
  - A5/0: keine Verschlüsselung
  - A5/1: 64bit Key
  - A5/2: 54bit Key

1.1.4 GSM - Gratisanrufe

1. Ross Anderson Hack
   - Nutze IMSI des Opfergeräts/SIM-Karte
   - HLR schickt 5x (RAND,SRES)-Paare an MSC/BSC
   - Höre die Paare ab, da BSC-MSC Verbindung unverschlüsselter Funk
   - Schicke schnell genug S_{Res} an BSC
   - $\Rightarrow$ BSC aktzeptiert S_{Res}, K_C ist bekannt und wird für den Anruf verwendet
   - $\Rightarrow$ SIM mit genutzter IMSI muss zahlen
2. SIM-Karten klonen (Extrahiere K_{SIM}
   - Physische Extraction: Versuche den Schlüssel aus der SIM-Karte zu holen. Schwierig, da SIM-Karten das extra verhindern sollen
   - Over-The-Air-Cloning: Analysieren mehrerer RAND-S_{Res} Paare, und versuche, den A3/A8 Algorithmus damit zu brechen und K_{SIM} zu erfahren
   - $\rightarrow$ A3/A8 ziemlich schlecht, war daher möglich
   - $\rightarrow$ A3/A8 mussten teuer ersetzt werden

1.1.5 GSM - Abhören

1. Abhören der BSC-MSC Verbindung für K_C
   - unverschlüsselter Funk
   - K_C wird zum verschlüsseln der Kommunikation genutzt
2. IMSI-Catcher
   - Handys verbinden sich immer mit der Basisstation mit der stärksten Verbindung
   - BS_{Evil} kann Handy auffordern, IMSI statt TMSI zu senden
   - manchmal Abhören möglich; vor allem aber fürs Tracking
   - $\rightarrow$ beim Festlegen der Verschlüsselung: fordere unverschlüsselte Kommunikation

1.2 Universal Mobile Telecommunication System (UMTS)

- Verbesserungen gegenüber GSM/bleibende + neue Probleme
- Positiv:
  - gegenseitige Authentifizierung von Handy und Netzwerk
  - neue Versionen A5/3 und A5/4 zur Verschlüsselung: 64bit bzw. 128bit Schlüssel
  - $\rightarrow$ akademisch, aber kaum praktisch gebrochen
- Negativ:
  - Abwärtskompatibilität mit GSM $\rightarrow$ MITM-Angriff via Downgrading

– Verbindung zwischen RSS und NSS immer noch ungeschützt

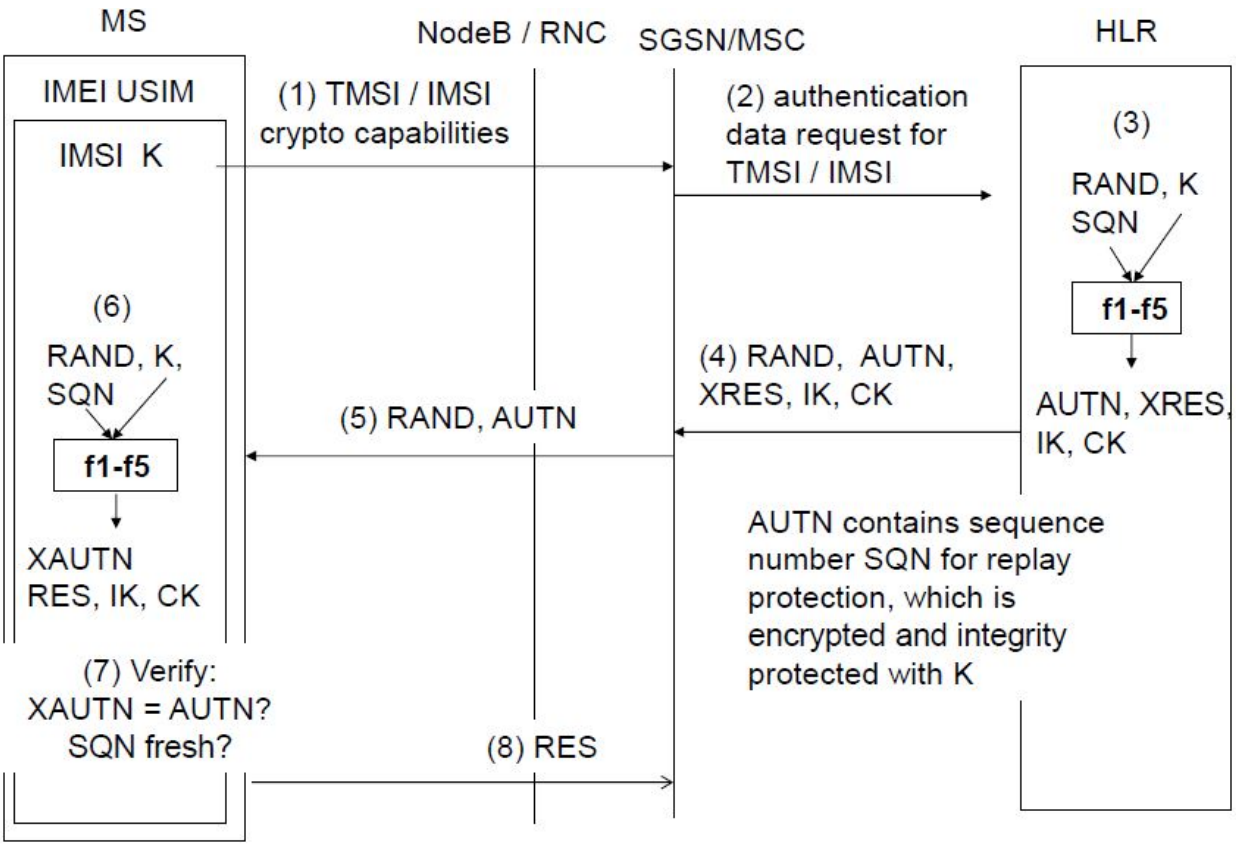

Figure 3: UMTS - Ablauf Authentifizierung und Verschlüsselung

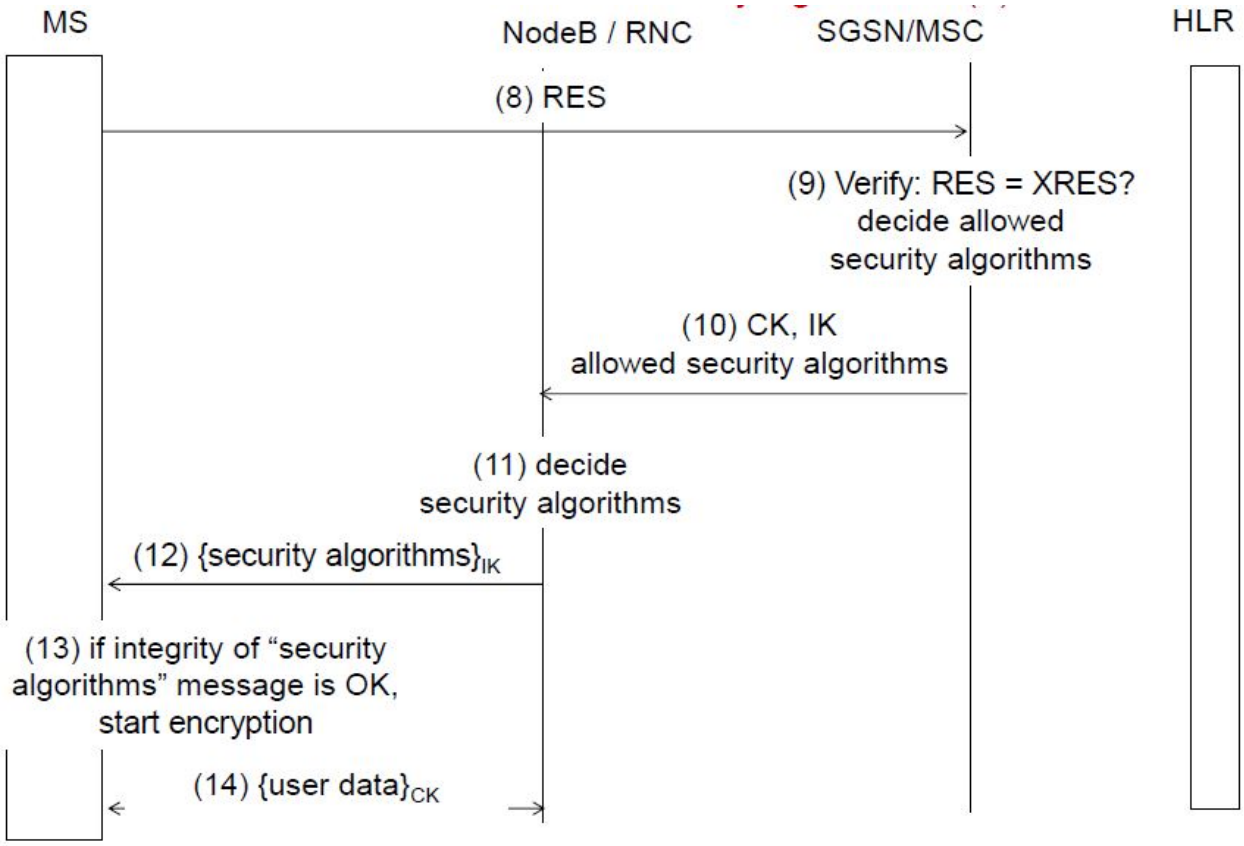

Figure 4: UMTS - Ablauf Authentifizierung und Verschlüsselung

1.2.1 GSM-UMTS Degradation Angriff (MITM)

1. Annahme: Handy kann sowohl UMTS als auch GSM
2. ISMI-Catcher ahmt Handy in UMTS für Basisstation nach
3. Basisstation schickt IMSI-Catcher frisches AUTN
4. IMSI-Catcher bricht Verbindung ab
5. IMSI-Catcher authentifiziert sich gegenüber dem Handy mittels AUTN
6. Festlegung der Verschlüsselung: Angreifer wählt A5/0 bzw. A5/1 (GSM)
7. Ergebnis:
   - Handy telefoniert (unverschlüsselt) mir dem Angreifer
   - Angreifer baut normalen UMTS Anruf mit seiner eigenen Nummer/SIM auf, ahmt den Anruf des Handys damit nach
   - → Angerufener sieht andere Nummer
   - Angreifer muss für den Anruf zahlen

1.3 Signaling System 7 (SS7)

- Gedacht für die Kommunikation zwischen Telekommunikationsbetreibern und innerhalb ihrer Netzwerke
- Vertrauensbasis: Jedem wird vertraut, deshalb keine Authentizitäts- und Plausibilitätschecks

- Aktuell: Genutzt für GSM und UMTS
- Jeder kann sich einen SS7-Zugang für unter 1000 Dollar kaufen

1.3.1 Lokalisierung und Tracking

- Frage HLR: Was ist die IMSI dieser Telefonnummer? Bei welcher MSC befindet sich diese IMSI?
- Frage MSC: An welcher Basisstation befindet sich die IMSI?

1.3.2 Abhören

- "Diese IMSI ist in meinem Netzwerk, schicke mir die Authentifizierung und die Schlüssel" → Ja, so einfach
- Funktioniert sogar, wenn der Nutzer gerade mit einem anderen Netzwerk verbunden ist

1.3.3 Manipulation/Anrufweiterleitung

- "Diese IMSI will, dass Anrufe und SMS zu meinem Netzwerk weitergeleitet werden"

1.4 Long Term Evolution (LTE)

- Netzarchitektur: BSC als Zwischenstufe zwischen Basisstation udn MSC(MME) entfernt
- LTE Sicherheit: basiert hauptsächlich auf UMTS Sicherheitskonzepten
- Authentifizierung:
  - MSCs/MMEs Verantwortlichkeit
  - AES wird sowohl für Verschlüsselung als auch Authentifizierung verwendet
- IPSec: Zuvor SS7 im Netzwerk, jetzt ersetzt durch sichere IPSec Kommunikation (Optional)

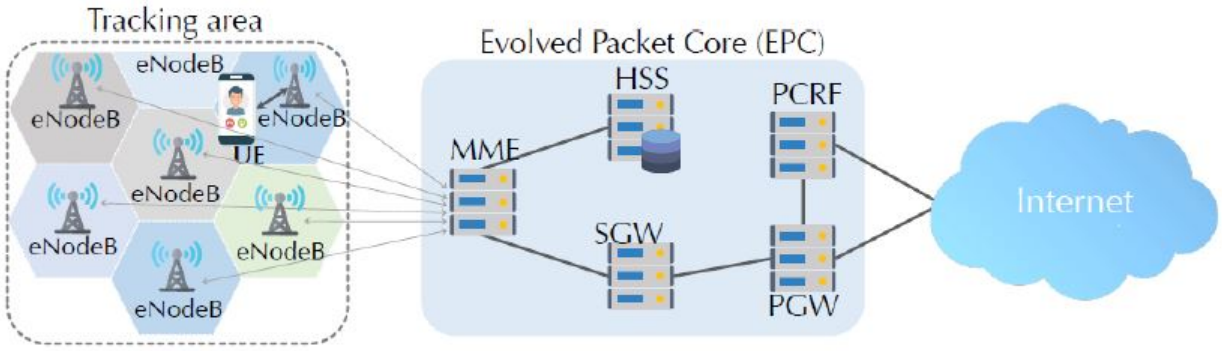

Figure 5: LTE - Netzarchitektur

1.4.1 LTE - Basisstation Imitation

- Nachrichten des Typs "Service X nicht erlaubt" der Basisstation sind nicht Integritätsgeschützt
- → "LTE nicht erlaubt" kann benutzt werden für:
  - Degradation Attack zu 2G(GSM) und 3G(UMTS)
  - Permanenter DoS, hält bis Handyneustart an

1.4.2 LTE - Angriff auf Integrität des Netzverkehrs

- User Traffic aus Performancegründen nur verschlüsselt, nicht Integritätsgeschützt
- → Verändern der verschlüsselten Daten, z.B. zu Müll

1.4.3 LTE - Privatssphäre

- GUTI (= TMSI) analog zur TMSI nur selten geändert (aus Performancegründen)
- Ortung durch Imitation einer Basisstation (eNodeB)
  - → Handy kann unauthentifiziert aufgefordert werden, die Signalstärke aller hörbaren Basisstationen zu senden

1.5 Sicherheit und Privatssphäre - Lessons Learned

1. Keine Security by Obscurity in der Kryptographie
2. Fordere gegenseitige Authentifizierung
3. Schütze C+I in jedem Systempart
4. Kryptoalgorithmen müssen austauschbar sein
5. Beachte zukünftige Technologieentwicklungen und starke Angreifer bei der Bedrohungsanalyse
6. Der Entwicklungsprozess muss transparent sein
7. Abwärtskompatibilität öffnet alte Sicherheitslücken
8. Zwingende Standards für Pseudonymmanagment
9. Verfügbarkeit, Zuverlässigkeit und Robustheit reduzieren oft die Sicherheit

2 WLAN/WIFI

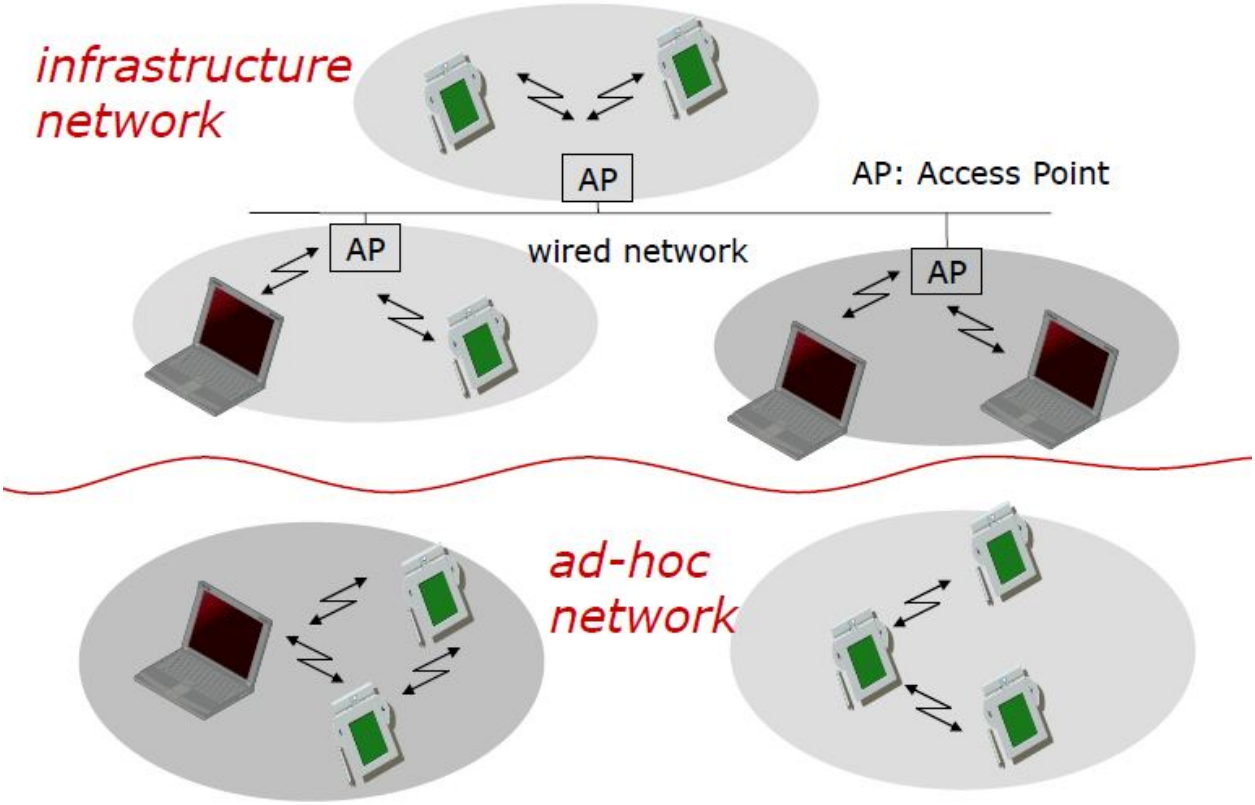

Figure 6: WiFi - 2 Network Types

- Netzwerkverbindung: Aktiv vs. Passiv
  - Aktiv: Gerät fragt aktiv und wartet auf Antwort vom Netzwerk
  - Passiv: Gerät lauscht nach "Beacon" Signalen (gesendet von Access Point)
- Netzwerkauthentifizierung: Offenes System vs. gemeinsamer Schlüssels vs. WPA3
  - Offenes System: keine Kryptographie, Gerät schickt Anfrage, AP schickt Antwort
  - Gemeinsamer Schlüssel: Challenge-Response Protokoll, je nach Version (WEP/WPA/WPA2)
  - WPA3: über öffentliche Schlüssel

2.1 Open Networtk Protection

- Unerlaubte Geräte werden durch "versteckte" ESSID an Verbindung gehindert
  - APs schicken keine "Beacons", warten stattdessen auf direkte Anfrage nach ESSID
- → Sicherheitslücken:
  1. lauschen nach "erlaubten" Geräten bzw. dessen Verbindungsaufbau
  2. ESSID jetzt bekannt, verbinde dich mit dem Netzwerk
- → Privacy Issues:

  - Geräte suchen aktiv nach versteckten Netzwerken, verraten so bisher besuchte Netzwerke/Orte an Dritte

- → MAC-Adressen Whitelisting:
  - kann durch Sniffen und Imitieren einer erlaubten Adresse umgangen werden

2.2 Rogue Access Point (Evil Twin Attack

1. Angreifer kreiert Access Point, ahmt legitimen AP nach, indem Beacon Signal mit passender ESSID (Netzwerkname) gesendet werden → "Evil Twin"
2. Gerät verbindet sich mit dem AP mit dem stärksten Signal
3. Durch passende Positionierung → Gerät verbindet sich mit Evil Twin

→ Folgen/Gefahren:

- Fake Hotspot Login
  - Name, PW, Kreditkarte
- Man in the Middle
  - klauen von Klartextdaten
- Phishing
  - Mittels DNS-Spoofing Umleiten

Abwehr:

- VPN
- SSL/TLS

2.3 Wired Equivalent Privacy (WEP)

- Ziel: Erreichen derselben Sicherheit wie bei einer Kabelverbindung
- Ein gemeinsamer, dauerhafter, Master Key für alle Netzwerkmitglieder

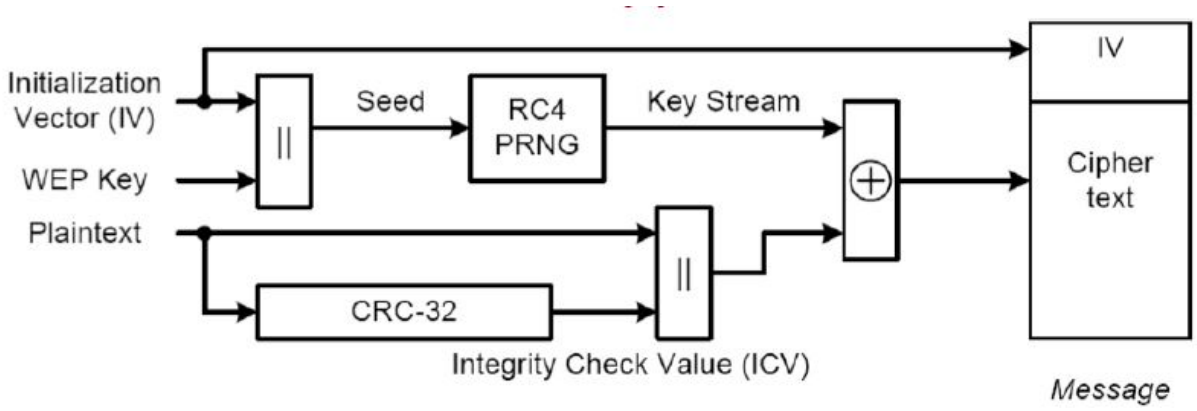

Figure 7: WEP - Verschlüsselung

2.3.1 WEP - Entschlüsselung:

1. Lesen des Initialen Vector, Konkatenation mit Schlüssel, um Seed zu erzeugen
2. XOR des Key-Streams mit verschlüsselter Nachricht
3. Integritätscheck der Nachricht

2.3.2 WEP - Sicherheitslücken:

- Kryptographische Attacken: Schwachstellen in RC4-Algorithmus, Echtzeit-Knacken möglich
- Non-Krypto Attacken: IV wird teils nach Geräteneustart auf 0 zurückgesetzt
  - "Two-Time-Pad" Attacke → Entschlüsselung möglich

2.3.3 Two-Times-Pad Attacke

1. $m_1 \oplus k = c_1$; $m_2 \oplus k = c_2$
2. $c_1 \oplus c_2 = m_1 \oplus m_2$ //k fällt weg, da doppeles XOR
3. "Crib Dragging"
   - Annahme, dass Wort w in m_1 an Position p vorkommt
   - XOR w zu ($m_1 \oplus m_2$ an Position p
     - Angenommen Zeichen für m_2 erkennbar
   - Falls m_2 als Klartext sinn macht → Treffer

2.3.4 CRC-basierte Attacke auf Nachrichtenintegrität

1. $(a||x) \oplus (b||y) = (a \oplus b)||(x \oplus y)$, falls jeweils gleich lang
2. $CRC(a \oplus b) = CRC(a) \oplus CRC(b)$
3. Abgefangene Nachricht $C = \text{keystream} \oplus (M||\text{CRC}(M))$
4. Neue Nachricht $M' = M \oplus d$:
   - $C' = \text{keystream} \oplus (M'||CRC(M'))$
   - $= \text{keystream} \oplus (M'||CRC(M \oplus d))$
   - $= \text{keystream} \oplus [(M \oplus d)||CRC(M) \oplus CRC(d))]$
   - $= \text{keystream} \oplus [(M||CRC(M)) \oplus (d||CRC(d))]$
   - $= [\text{keystream} \oplus (M||CRC(M))] \oplus (d||CRC(d))$
   - $= C \oplus (d||CRC(d))$

2.3.5 Attacke auf Zugangskontrolle mittels Replay

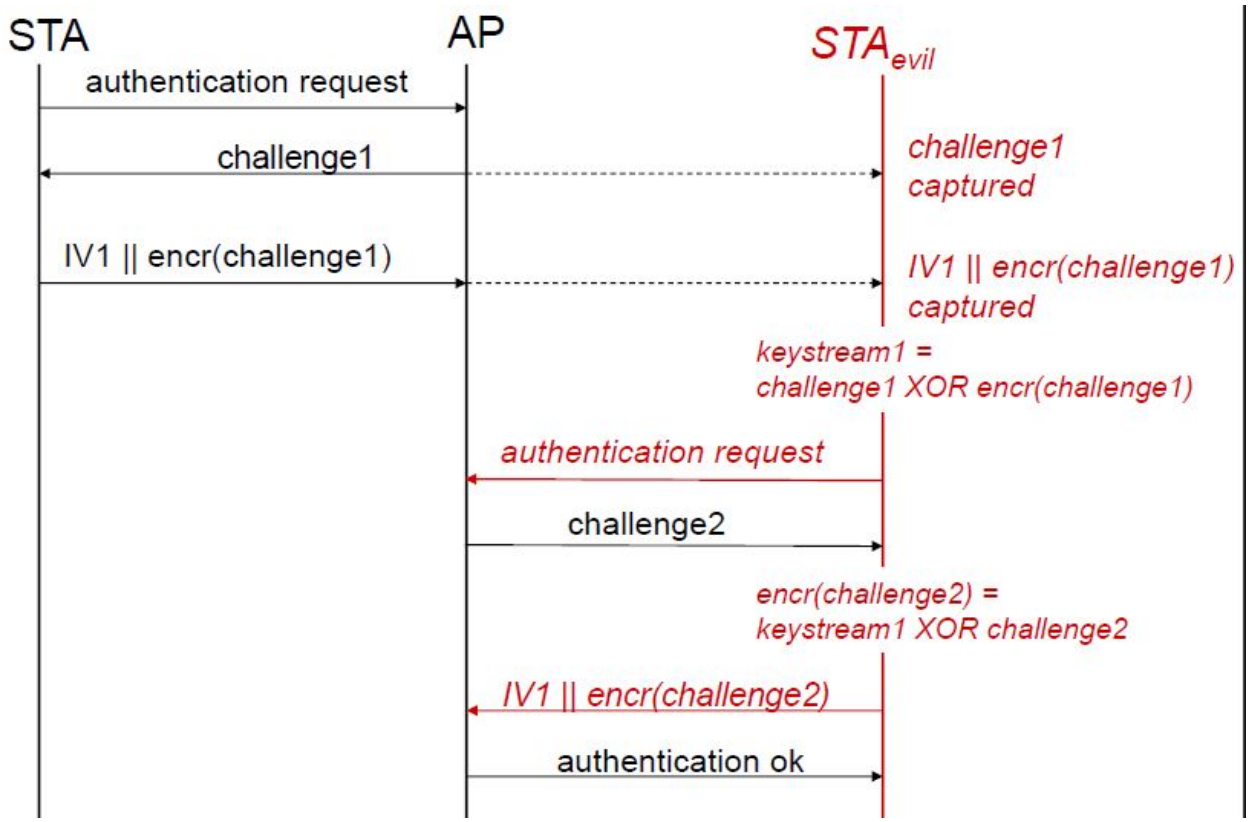

Figure 8: WEP - Replay

2.3.6 Attacken

- Zugangskontrolle
  - WEP Schlüssel knacken
  - Replay-Attacke für Zugangskontrolle
- Vertraulichkeit
  - WEP Schlüssel knacken
  - IV Wiederverwendung
    - → Two Times Pad
  - Insider Attacken (geleakter Schlüssel)
- Integrität
  - WEP Schlüssel knacken
  - CRC basiert Attack
  - Insider Attacke (geleakter Schlüssel)
  - IV-Wiederverwendung:
    - Ein Paar (IV,keystream) reicht aus um beliebige Nachrichten zu schicken (XOR mir keystream)
- Verfügbarkeit

  - Verbindungsabbruch verläuft unauthentifiziert
- Key Managment Problems
  - Geteilter Schüssel Jahrelang auf allen Geräten
    - → Kompromittierung
  - keine Mechanismen für Schlüsselauswechseln
    - kompromittierte Schlüssel werden meistens ignoriert

2.4 Wireless Protected Access (WPA)

- WEP als Grundlage, aber mit mehreren Designverbesserungen
  1. 128bit Schlüssel statt (128-24) bzw. (64-24)bit Schlüsseln (IV bei WEP Key mit drin)
  2. 48bit Initialisierungsverktoren statt 24bit IVs
  3. Temporäre Schlüssel, abgeleitet vom Master Key
  4. Kryptographisch sichere Integritätsprüfung von Nachrichten (im Vergleich zu CRC-basierten Attacken)
  5. Authentifizierung und Schlüsselmanagment mittels 4-Wege-Handshake

2.5 Wireless Protected Access 2 (WPA2)

2.5.1 WPA2 Key Hierarchy

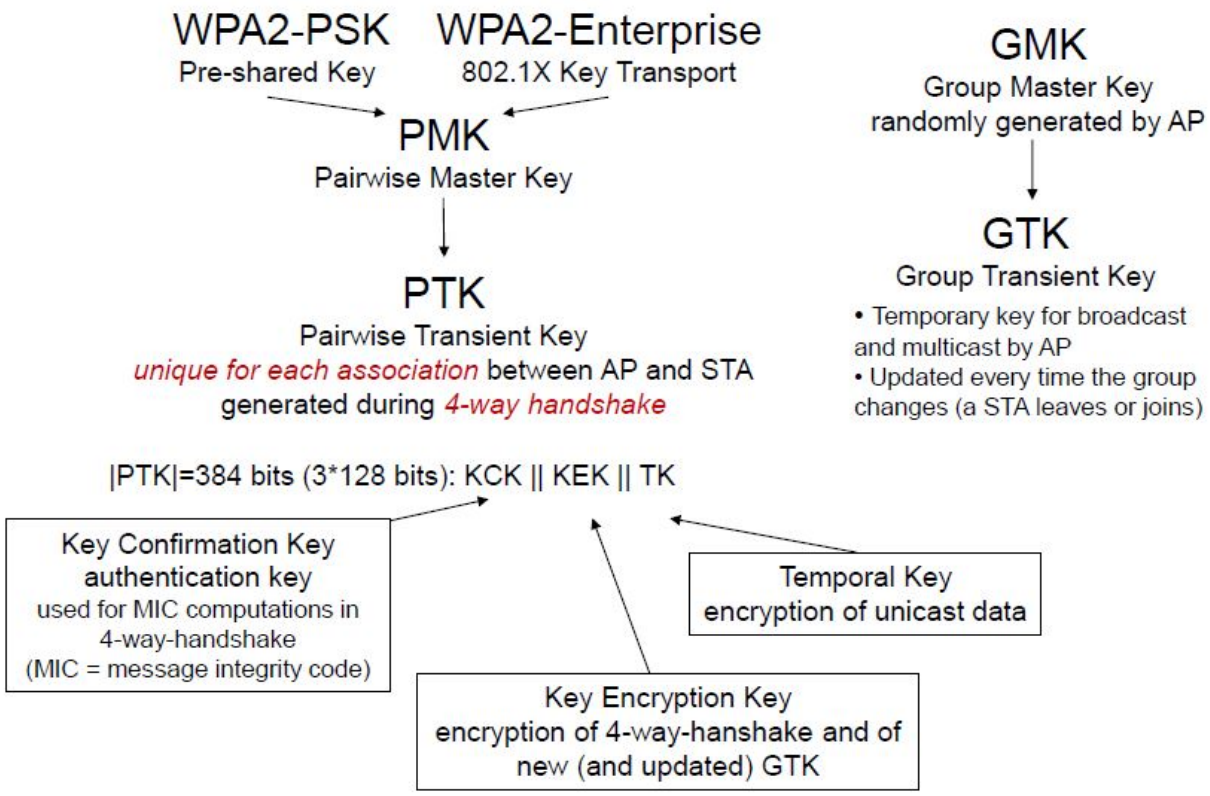

Figure 9: WPA2 - Key Hierarchy

2.5.2 Pre Shared Key

- PMK basiert auf Passwort (8-63 Zeichen)

- PBKDF2: Password Based Key Derivation Function 2
  - kryptographisch sichere Passwortgenerierung
  - PMK = PBKDF2 (passwort,salt)
  - salt = ESSID (Netzwerkname)

2.5.3 WPA2 Enterprise

- PMK generiert während 802.1x Authentifizierung (über AP)
  - → Individueller Schlüssel für jedes Gerät und Sitzung

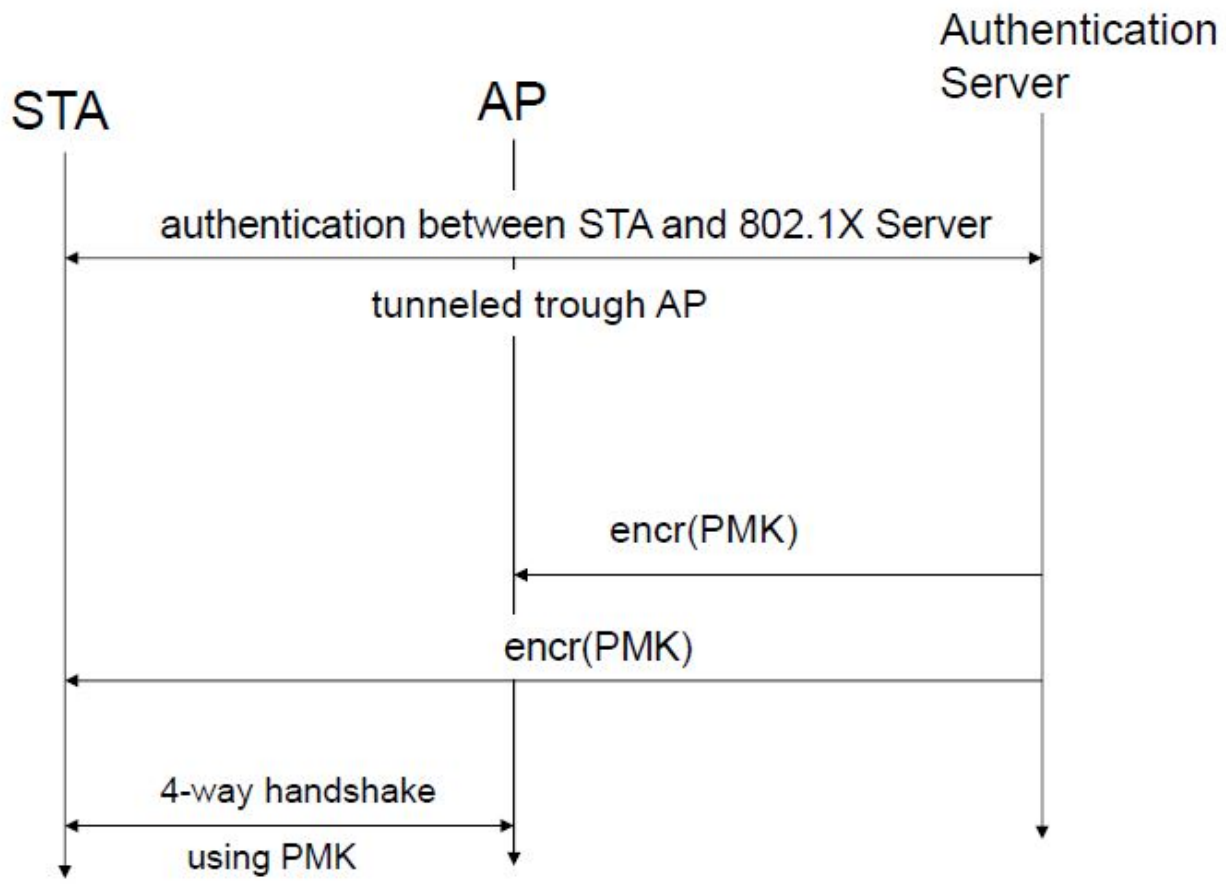

Figure 10: WPA2 Enterprise

2.5.4 4-Wege-Handshake

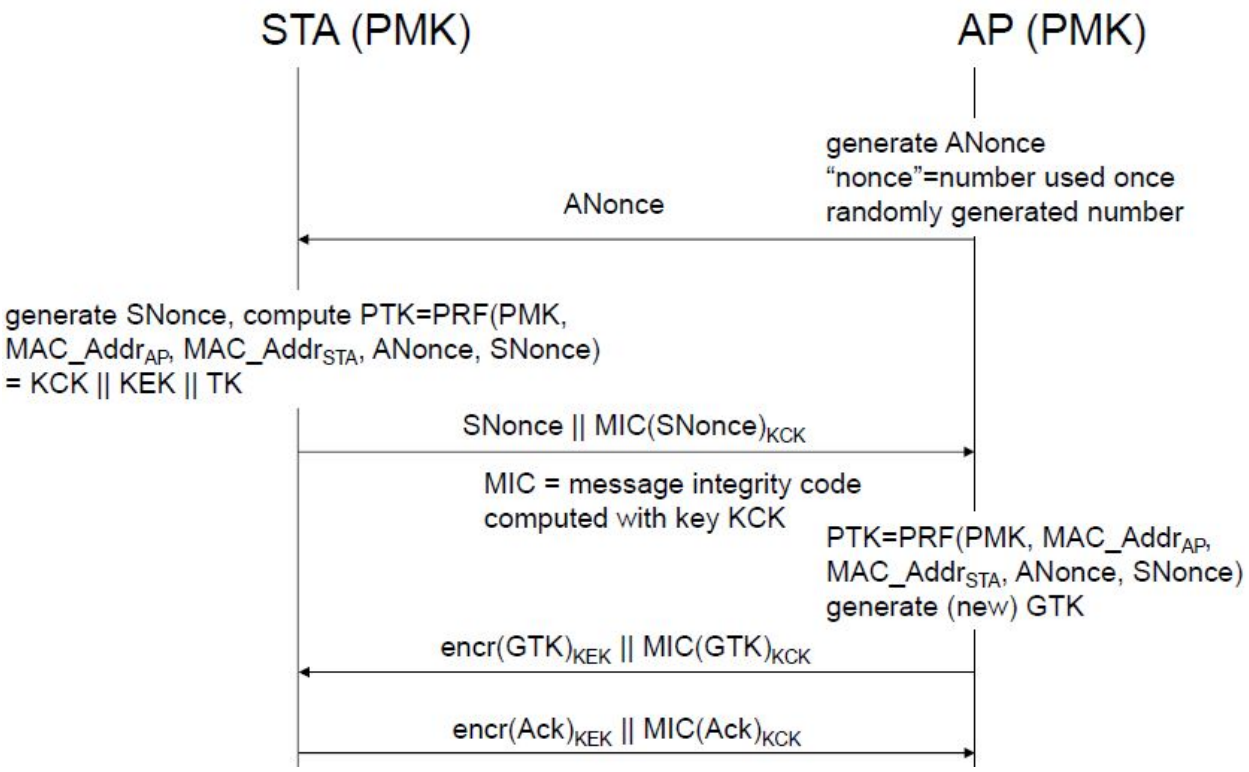

Figure 11: 4-Wege-Handshake

- ANonce, SNonce: Zufallszahl
- $PTK = PRF(PMK, MAC - ADDR_{AP}, MAC - ADDRSTA, ANonce, SNonce)$
- $= KCK||KEK||TK$

2.5.5 WPA2-PSK Key Cracking

- PMK=PBKDF2(password,Netzwerkname) (Netzwerkname ist einsehbar)
  - Höre 4-Wege-Handshake ab:
    - Names, Mac-Adressen bekannt
    - Rate Passowrt, erzeuge PMK
    - Berechne PTK
    - Prüfe PTK, z.B. mit $MIC(SNonce)_{KCK}$
- Gegenmaßnahmen: Nutze einzigartige Netzwerknamen (gegen Rainbowtables) sowie einzigartige, starke Passwörter

2.5.6 Insider Angriff auf WPA2-PSK

- Alle STAs nutzen denselben PMK als Basis für ihre Schlüssel
  - Höre ANonce und SNonce ab → MAC-Adressen bekannt, berechne PTK

2.5.7 Hole 196

- Individuelle PTKs bei WPA2, aber ein GTK für AP-Broadcasts, bekannt für alle

1. STA_{Evil} imitiert AP (nutzt dessen MAC-Adresse)
2. STA_{Evil} sendet ARP Update: Meine MAC-Adresse ist jetzt das Internet Gateway
3. Andere STAs senden Internetverkehr gerichtet an STA_{Evil}
4. AP entschlüsselt den Internetverkehr, und verschlüsselt ihn nue für STA_{Evil}, da ja an STA_{Evil} gerichtet
    - $\rightarrow$ STA_{Evil} ist Man-In-The-Middle für den Internetzugang

- Gegenmaßnahme Hole 196
    - Statistische ARP-Tabellen

2.5.8 Key Reinstallation Attack

1. Falls AP nicht Nachricht 4 des 4-Wege-Handshake erhält (ACK), wird die Nachricht 3 vom AP erneut gesendet (GTK)
2. Wenn STA zum zweiten Mal Nachricht 3 des 4-Wege-Handshake erhält, wird der PTK erneut installiert, d.h. der Initialisierungsvektor wird zurückgesetzt
3. Nach der Neuinstallation des PTK werden Nachrichten mit bereit gesetzten Intialisierungsvektor verschlüsselt
    - $\rightarrow$ Two-Time-Pad

2.6 Wireless Protected Access 3 (WPA 3)

- entwickelt um Cracking Attacken gegen WPA2-PSK Passwörter zu verhindern
- nutzt dazu Simultaneous Authentication of Equals (SAE)
    - ausgeführt vor dem 4-Wege-Handshake
    - verwendet Public Key Cryptography
    - für jede Session wird ein neuer PMK mit hoher Entropie aus dem Passwort generiert

2.6.1 Dragonblood Angriff gegen WPA3-SAE

- Bösartiger AP vermittelt STA, dass nur WPA2 möglich ist
- STA startet WPA2-4-Wege-Handshake mit $AP_{Böse}$
- Side WPA2-PSK-Angriff: Nach Austausch der Nonces, MICs etc. hat der Angreifer alles, um offline das Passwort zu ermitteln

Gegenmaßnahmen:

- Trust on first Usage: STA merkt sich, dass das Netzwerk WPA3 kann
    - aktzeptiert kein WPA2
- Verschiedene Passwörter für WPA2 und WPA3

3 Bluetooth

3.1 Piconet

3.1.1 Struktur

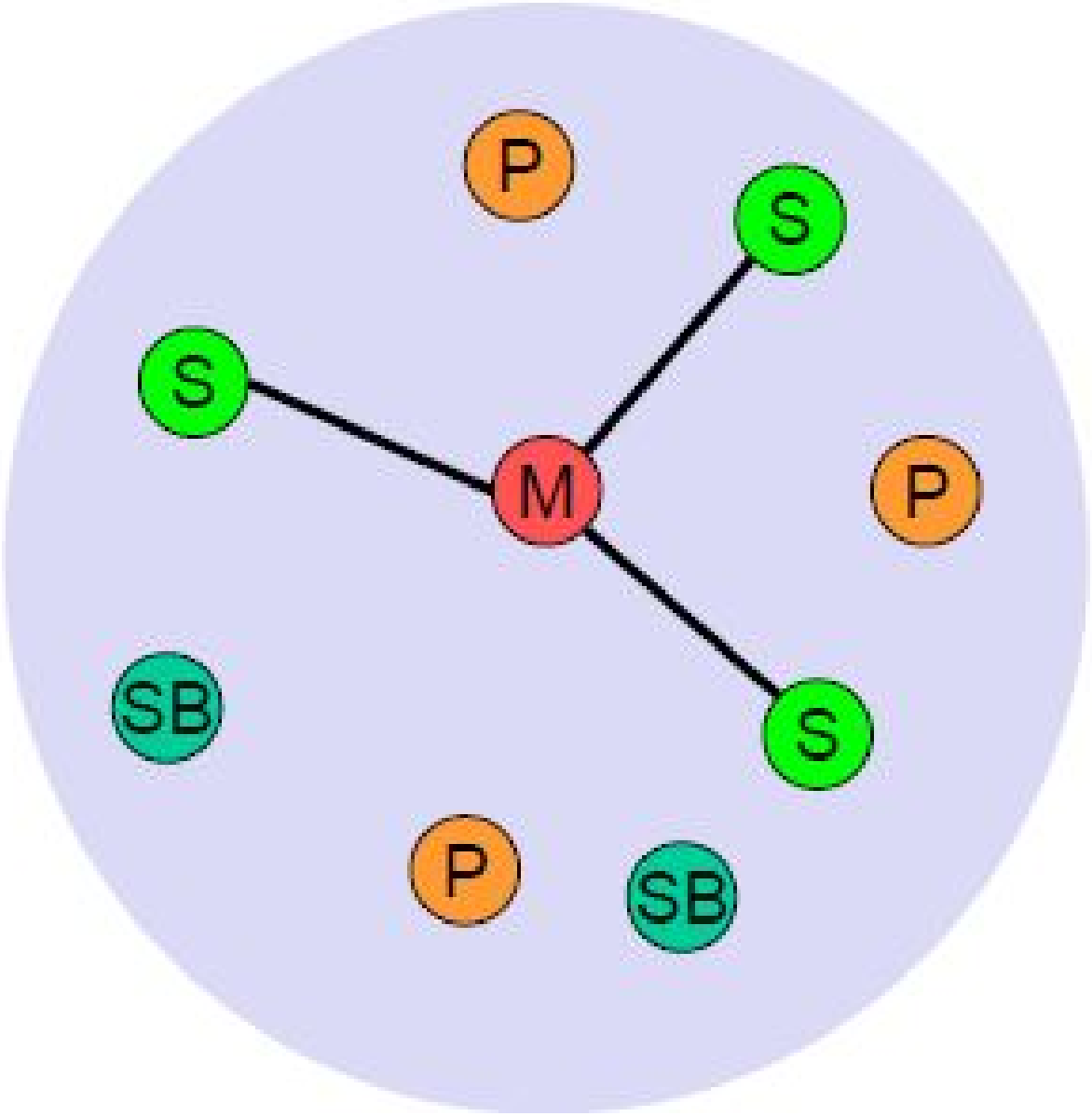

Figure 12: Piconet Struktur

- M = Master
- S = Slave
- P = Parked; bleibt synchronisiert; lauscht mit
- SB = Stand By; nicht im Piconet; könnte sich verbinden

- Mehrere Geräte verbunden in Ad-Hoc Netzwerk (d.h. z.B. kein zentraler AP, siehe WIFI)
- Ein Gerät ist Master für die Lebensdauer des Piconets, Slaves müssen sich synchronisieren
- Frequency Hopping: 800 Sprünge pro Sekunde, einzigartiges Sprungmuster hängt dabei von der Bluetooth Adresse des Masters ab (48Bit unique)
- Teilnahme an Piconetz heißt, sicht mit den Frequenzsprüngen zu synchronisieren Pro Piconetz 1 Master max 7 Slaves gleichzeitig, $>$ 200 Parked möglich

3.1.2 Zweck und Anwendung

- 1990: Aufkommen von Personal Short Range Devices
  - Universelle Funkschnittstelle für Ad-Hoc kabellose Verbindungen
  - Ersatz für Infrarotübertragungen
- Anwendungen in:
  - kabellose Telefonie
  - FAX
  - Dateitransfer

3.1.3 Sicherheitslogik

- Ziel: Äquivalenz zu komplett überschaubaren, kurzen Kabelverbindungen
  - Authentizität der Kommunikationspartner
  - Zugangskontrolle
  - Vertraulichkeit
  - Integrität
  - Integrität
  - Verfügbarkeit
- Im Vergleich zu WAN/WLAN: keine vordefinierte, zentralisierte Infrastruktur; spontane Netzwerkbildung zwischen (gleichwertigen) Geräten

3.2 Bluetooth 1.0-2.0

3.2.1 Security Design

- Symmetrische Verschlüsselung, 128bit Schlüssel
- Schlüsselerzeugung durch SAFER+ Algorithmen E_1, E_{21}, E_{22}, E_3
  - Ausgeschieden vor AES-Halbfinale, Attacke bekannt
- Eigentlich Verschlüsselung: E_0, viele theoretische Attacken, echte "geheime, zufällige" Schlüssellänge 60bit statt 128bit

3.2.2 Schlüsselhierachie

1. Initialisierungschlüssel durch PIN
   - temporär für die Durchführung des Link Key Protocol
   - genutzt bei ersten Treffen beider Geräte, oder falls der Link Key "verloren" wurde
2. Link Key
   - Auf beiden Geräten generiert aus Initialisierungsschlüssel
   - Bei erneuten Treffen beweisen sich beide Geräte gegenseitig, dass sie den Link Key besitzen
3. Encryption Key
   - für eigentliche Datenverschlüsselung, generiert aus Link Key

3.2.3 Erzeugung des Initialisierungsvektors

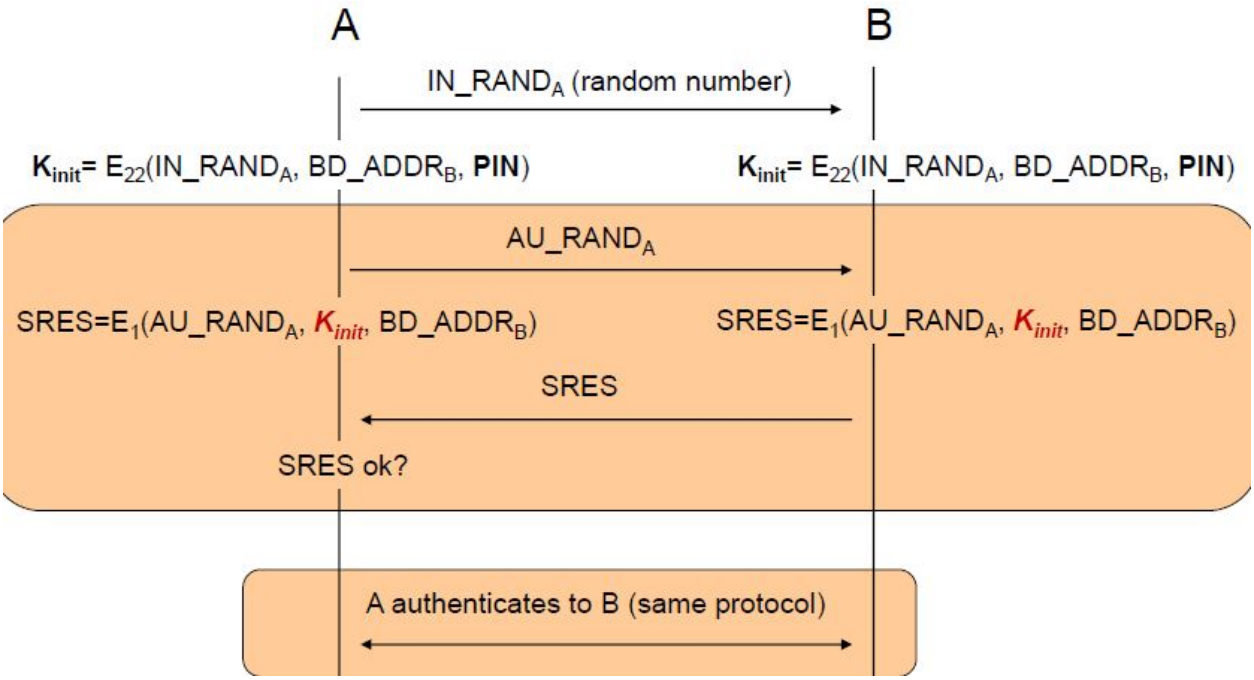

Figure 13: Erzeugung des Initialisierungsvektors

3.2.4 Link Key Generation

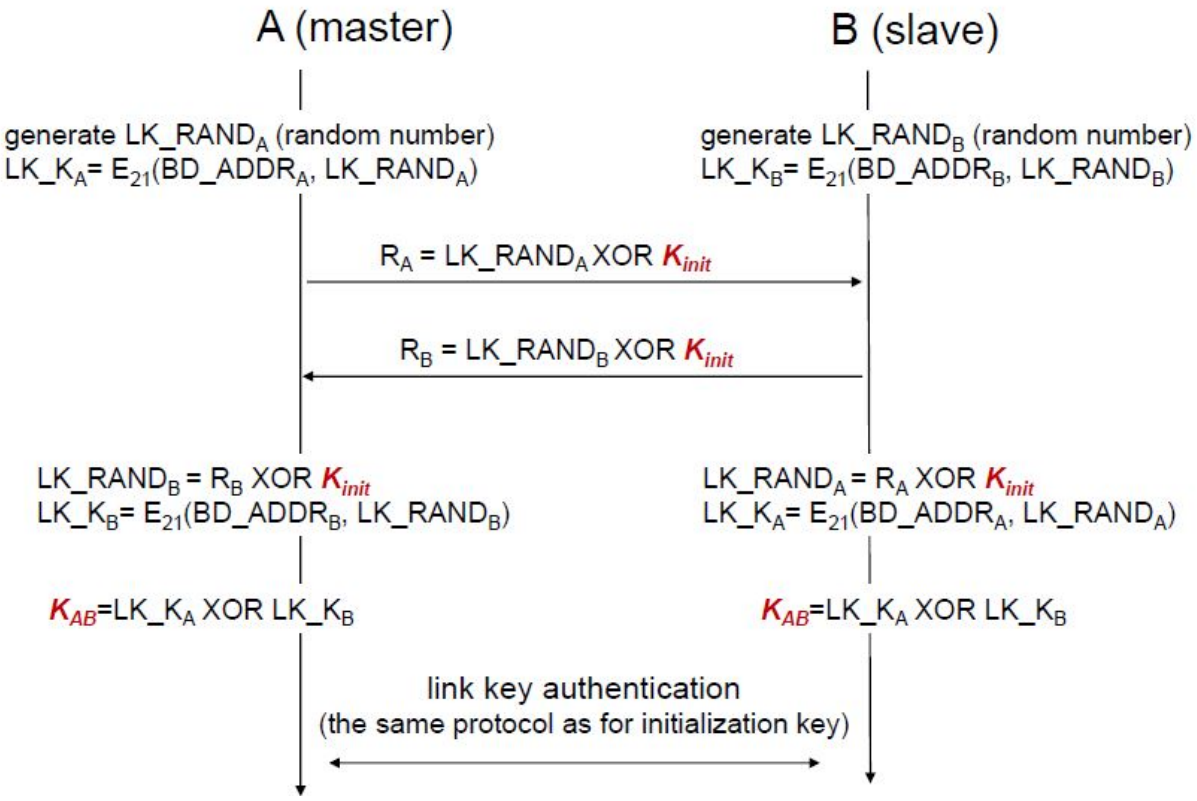

Figure 14: Link Key Generation

- Updaten des Link Keys:
  - Selbes Protokoll wie für die Link Key Generierung
  - ABER: vorherheriger K_{AB} statt K_{init}

3.2.5 Encryption Key

- Gemeinsamer Schlüssel zwischen Master A und Slave B
  1. $A \rightarrow B$: EN_RAND$_A$
  2. A und B: $K_C = E_5(\text{EN\_RAND}_A, K_{Link}$

3.2.6 Attacken

- Passives PIN Cracking
  - $K_{init} = E_{22}(\text{IN\_RAND}_A, \text{BD\_ADDR}_B, \text{PIN})$
  - $S_{RES} = E_1(\text{AU\_RAND}_A, K_{init}, \text{BD\_ADDR}_B)$
- PIN ist der einzige Wert, der nicht in Klartext übertragen übermittelt wurde
  - Lausche nach IN_RAND$_A$, AU_RAND$_A$ und S_{RES}
  - Probiere PINs durch:
    - berechne K_{init_Test}

        * berechne S_{RES_Test}
        * $S_{RES} == S_{RES\_Test}$?
- Aktives PIN Cracking
    - Variante 1: Nutzt die zunächst einseitige Authentifizierung bei der Generierung des Initialisierungsschlüssels aus
        * Wähle beliebige PIN_X, berechne $K_{init,x}$
        * Schicke $\text{AU\_RAND}_{Angreifer}$ an B, B schickt S_{RES} mit korrekter PIN
    - Variante 2; Zwingt A und B zum erneuten Pairing
        * Spoofing eines der Geräte: "Ich habe den Link Key vergessen"
        * "Forgot Key" Nachrichten logischerweise unverschlüsselt
        * Abhören des erneuten Pairings → Profit

3.2.7 Sicherheitslücken

- Encryption Key basiert auf Pin → wird durch PIN geleaked
    - PINs oft zu kurz/zu enfach/feste teils kompromittierte Stadartwerte
    - PIN Crackig möglich, sowohl offline als auch online
- Bluetooth Geräte nehmen oft Verbindungen zu beliebigen Geräten an und senden ihre BD_ADDR
    - teilweise ohne das Wissen des Benutzers
    - teilweise können Nutzers manipuliert werden, bösartige Verbindungen zu aktzeptieren
- Schwache/kompromittierte Kryptographie → Bluetooth 4.0+ nutzt AES
- Encryption IV reuse: IV hängt von Systemuhr und Adresse des Masters ab
    - wiederholt sich nach 23.3 Stunden laufender Verbindung → Two-Times-Pad
- keine Integritätschecks bei Verschlüsselung
- keine Ende-zu-Ende Verschlüsselung; $A \rightarrow C \rightarrow B$; C liest mit
- Degradierung des Sicherheitsniveaus möglich

3.3 Secure Simple Pairing (ab Bluetooth 2.1)

- unauthentisierter bzw, authentisierter asymetrischer Schlüsselaustausch mittels Diffie-Hellmann
    - sicher gegen passives lauschen; authentisiertes DH zusäzlich sicher gegen Man-In-The-Middle und Evi-Twin Attacken

3.3.1 Diffie Hellmann Schlüsselaustausch

- Öffentlich: p, große Primzahl + g (1<g<p-1), Generator der multiplikativen Gruppe n mod p
    - $g^x \mod p$ erzeugt alle $n = \{1; 2; ...; p-1\}$

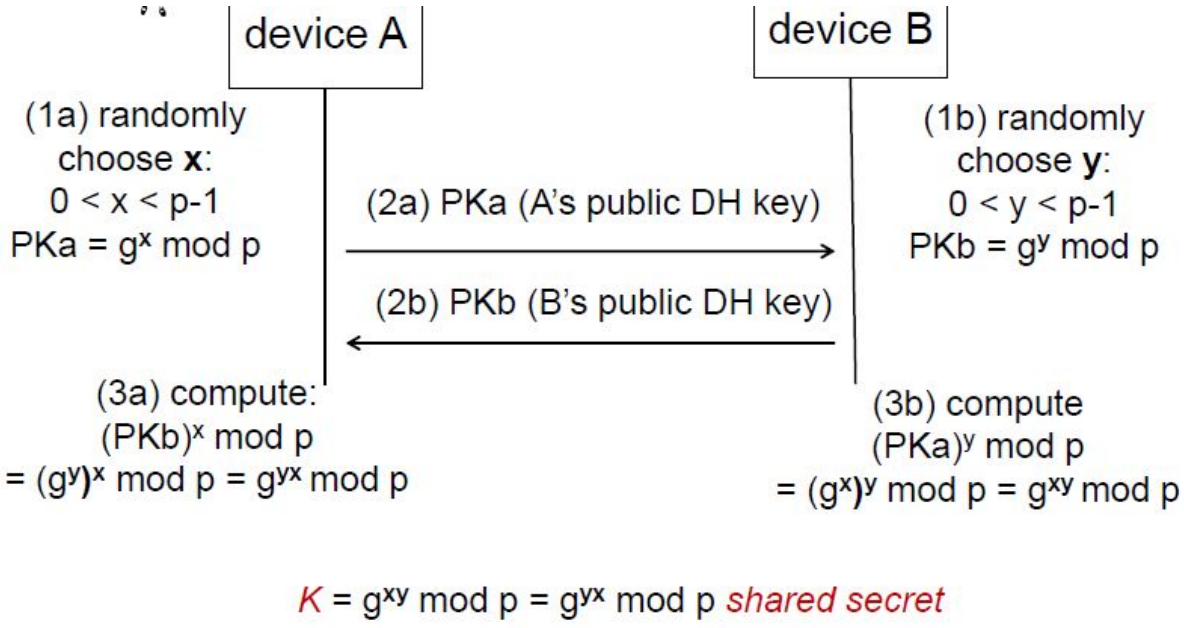

Figure 15: DH Key Exchange Protocol

- Man-In-The-Middle Angriff möglich
  - $A \rightleftharpoons$ Evil $\rightleftharpoons B$
  - Evil leitet Schlüsselaustasuch mit A und B ein, liest und leitet Daten weiter

3.3.2 Authentisierter Diffie-Hellmann

- Verifiziere getauschte Schlüssel nochmal über externen Out-Of-Band Kanal
  - Verhindert MITM-Angriffe, da dann die Schlüssel nicht passen (A und B haben verschiedene Schlüssel PKA und PKB
- 2 Varianten: Integritätscheck vs. extra gemeinsames Geheimnis
  - Integrity
    - Numerischer Vergleich:
      - 6-Ziffer-Hash des DH-Schlüssels
      - muss gleich sein, sonst MITM
      - Nuter vergleicht, gibt das OK
    - NFC: Nutzt NFC als OOB-Kanal um Integrität zu vergleichen
      - NFC hat nur kurze Reichweite, Angreifer müsste direkt daneben sein
- Shared Secret:
  - extra Passwort: Gerät A nennt N, Eingabe in B, Authentifizierung des DH Schlüssels über N
    - nur Sicher, falls N echt zufällig und einmalig genutzt
- Ausnahme: Just Works
  - unathentisierter DH Austausch
  - nur eingeplant falls alles andere nicht möglich, z.B. ein Display + Eingabe bei einem Gerät
    - → Degradierungsattacke zu "Just Works" möglich

3.3.3 Basic Numeric Comparison

- h() cryptographische Hashfunktion, f() 6-Stellige Hashfunktion
- A und B haben PKA+PKB ausgetauscht

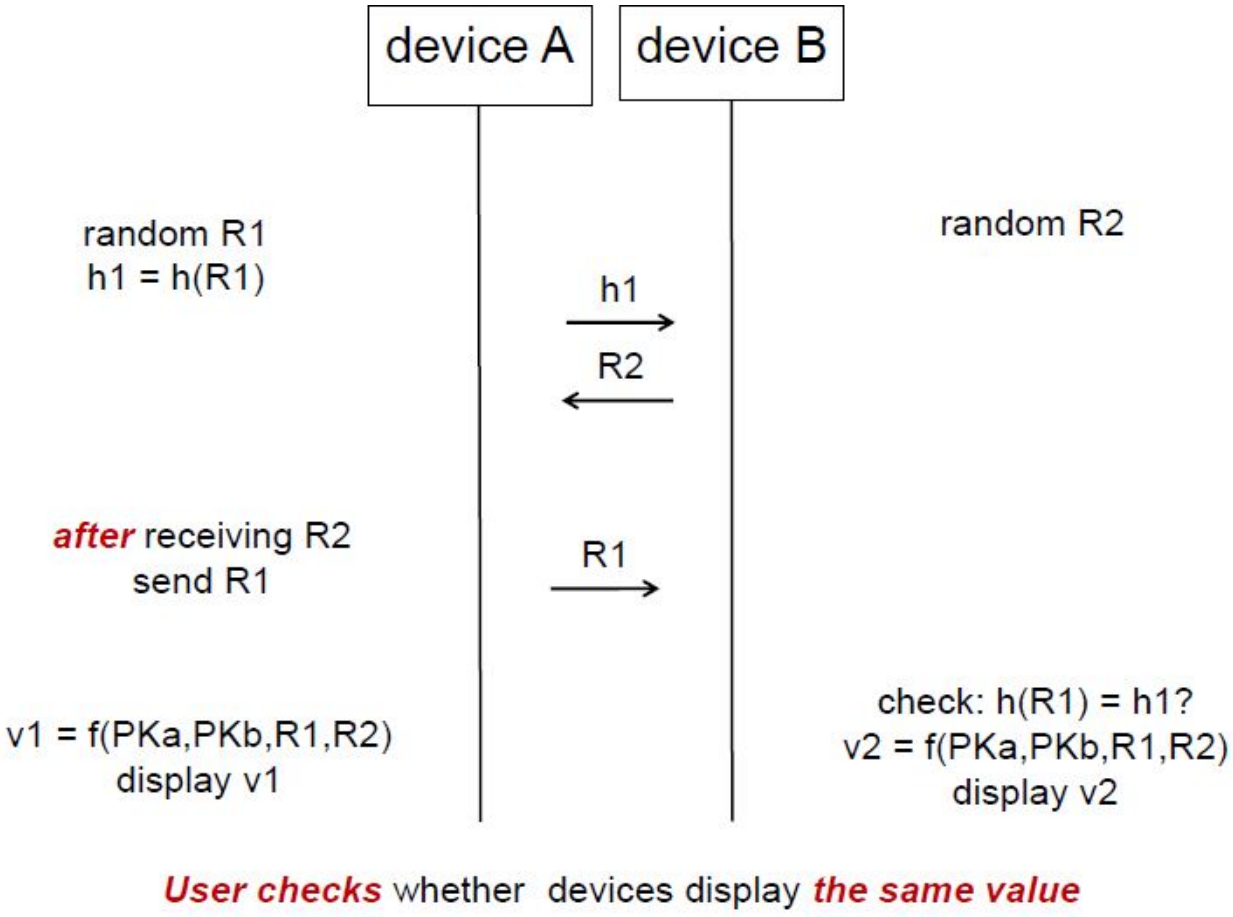

Figure 16: Basic Numeric Comparison

3.3.4 Basic Passkey Authentication Protocol

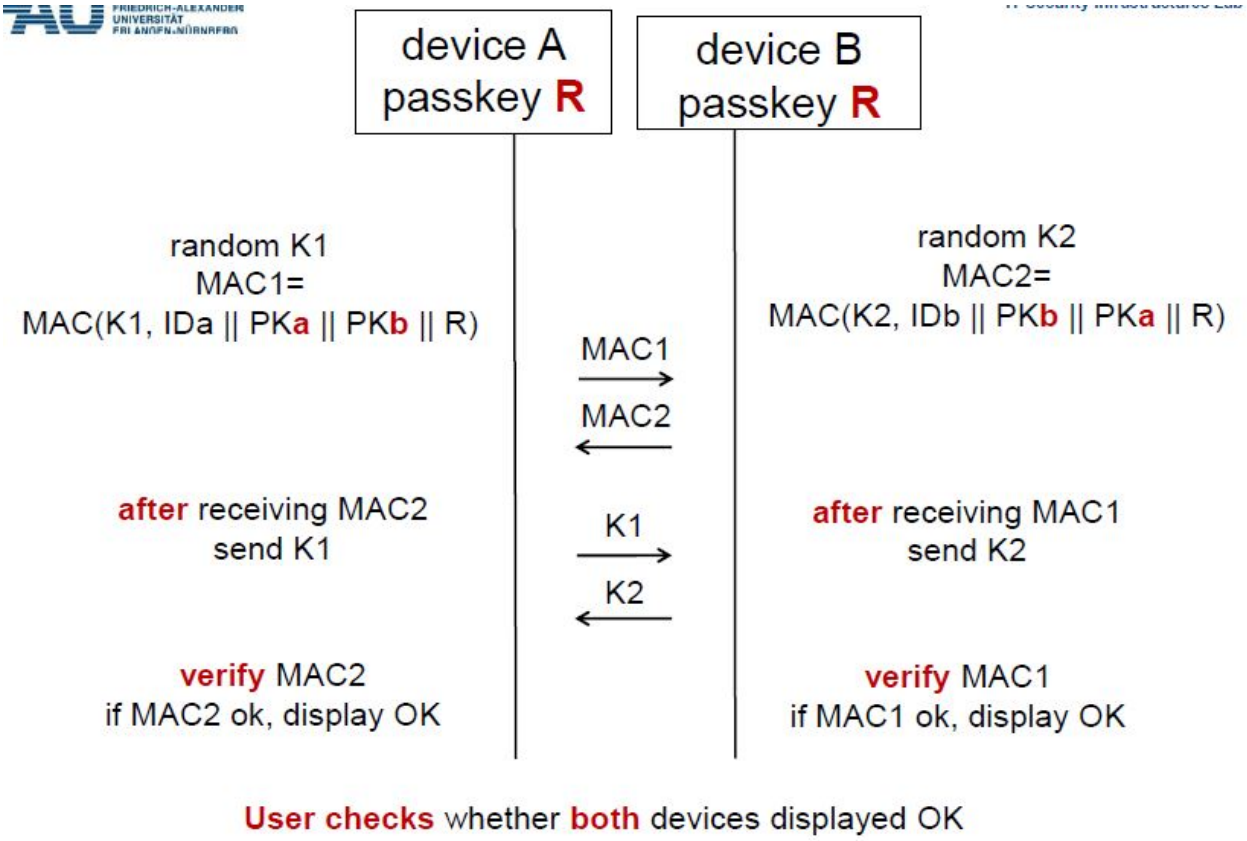

Figure 17: Basic Passkey Authentication Protocol

4 Device Pairing

- Festlegung von gemeinsamen Geheimnissen zwischen zwei Geräten
- Sicherheitsziel: sicherer Kanal mit C+/+A

4.1 Out-Of-Band Kanal (OOB)

- andersartig als primärer Kanal
- Geräte bauen über den primären Kanal eine sichere Verbindung auf, z.B. mittels Diffie-Hellmann
- OOB-Kanal ist dafür da, um MITM-Angriffe auf Initiatoren auszuschließen
- Beispiele für OOB-Kanäle:
  - Physisch (USB)
  - menschliche Aktion (PIN eingeben)
  - sekundäre Übertragungsart (Infrarot,NFC)
  - Audio (Piepsen)
  - Objekte (siehe WANDA)
  - Visuell (QR-Code Scannen)

4.2 Resurrecting Duckling

- regel die Zugangskontrolle zu Geräten einer Person oder Organisation
- Geräte sollen nur Kommandos ihrer eigentlichen Benutzer aktzeptieren
- Gerät soll aber kontrolliert übertragbar (Verkauf) und abschaltbar (kaputt) sein
- Prinzip:
  1. "Duckling"-Gerät hat zwei Zustände, imprintable und imprinted
  2. Die "Mother Duck" sende den Imprinting Key über einen physischen Kanal
  3. "Duckling" wechselt dann von imprintable zu imprinted
  4. Umkehr von imprinted zu imprintable
     - Auf Befehl der Mother Duck
     - Nach bestimmten Zeitintervall
     - Nach bestimmter Transaktion

4.3 Shake Well Before Use

1. Ziel: Spontane Verbindung zwischen zwei Geräten mit Bewegungssensor, z.B. Handy und Controller
2. Schüttle beide Geräte gleichzeitig
3. Nutze die Sensordaten, um einen gemeinsamen Schlüssel zu berechnen

4.4 Network-In-A-Box

1. Ziel: Beitritt in sicheres WLAN, normalerweise (kompliziertes) Zertifikatverfahren
2. AP hat Root-Zertifikat (Public-Private-Key Paar)
3. STA generiert public-private-Key Paar
4. OOB: Tausch Hashes der öffentlichen Schlüssel über Infrarot Kanal aus

4.5 Seeing Is Believing

1. Ziel: Authentifizierter Austausch von öffentlichen Schlüsseln
2. Tausch öffentliche Schlüssel aus
3. Gerät A erzeugt einen Strichcode, der den Hash seines öffentlichen Schlüssels repräsentiert
4. Gerät B scannt den Barcode visuell per Kamera, prüft den erhaltenen Schlüssel

4.6 WANDA

1. Ziel: Übergebe einen Schlüssel sicher an ein Zielgerät
2. Nutze "Zauberstab":
   - Hat vorne und hinten jeweils eine Antenne
   - Zielgeröt kann auf kurze Distanz mittels Signalstärke ermitteln, welche Antenne gerade sendet
   - Antenne A steht für eine gesendete 0, die andere (Antenne B) für eine 1
   - Zauberstab schickt Geheimnis als Binrstring
   - $\rightarrow$ Zielgerät kann auf nahe Distanz den Schlüssel lesen

4.7 WiFi Protected Setup (WPS)

- Ziel: Sicheres Pairing zwischen AP und STA
- 3 Varianten:
  - Knopfdruck: Gleichzeitiges Knofdrücken sowohl bei STA als auch AP aktiviert unathentifiziertes Diffie-Hellmannn $\rightarrow$ Problem: gleichzeitiger Angreifer
  - PIN: Nutze PIN, um Diffie-Hellmann Schlüssel einseitig zu überprüfen. Gib dazu die PIN des AP (meist auf der Rückseite) in STA ein (seltener: umgekehrt)
  - NFC: Bring STA nahe an AP, damit STA den Schlüssel von APs RFID-Tag lesen kann

5 Zigbee

5.1 ISO/OSI Einordnung

- Zigbee
  - Öffentliche Spezifikation, Geräte weit verbreitet
  - Standards definiert von ZigBee-Alliance
  - ZigBee Clusters → Profil
- IEEE 802.15.4
  - Für Netzwerke aus Sensoren und Actuatoren
  - Design: größere Reichweite als Bluetooth; monate-/jahrelange Batterielebensdauer; nur Sensordaen und Kontrollbefehle, keine Sprache/Multimedia

5.2 Zigbee Personal Area Network (PAN)

- jeder ZigBee-Einsatz besteht aus mindestens einem PAN
- PANs sind logisch getrennt → normalerweise 1 PAN pro smarten Haushalt
- MESH network topology
  - Nachrichten können von beliebigen Quellen zu beliebigen Zielen geroutet werden
  - mehrere Geräte als Router für Nachbarn möglich
  - Hohe Zuverlässigkeit durch mehrere Pfasdmöglichkeiten

5.3 Netzwerk

- Coordinator (C); Begründet, koordiniert das Netzwerk, maximal 1 pro Netzwerk
- Router (R): permanent an Stromversorgung
- Endgerät (E):
  - Duty-Cycling falls Batteriebetrieben
  - oft inaktiv um Energie zu sparen
  - führt kein Routing aus
  - benötigt R oder C als Elternknoten um an Netzwerk teilzunehmen

5.4 Sicherheit

- ZigBee definiert keine Sicherheitsziele, nur Sicherheitsannahmen:
  - Sicherheit beruht auf dem sicheren Verwahren symmetrischer Schlüssel sowie der sicheren Initialisierung, Installation und Verarbeitung
  - Während des Ttransports des initialen Schlüssels kann ein well-known key zur Verschlüsselung verwendet werden → kurzer moment der Verwundbarkeit
  - Alternative Verwendung eines zuvor geteilten (über OOB-Kanal) individuellen Schlüssel zum Schutz des transporierten Schlüssels
  - keine garantierte sichere Hardware → physischer Zugang könnte Zugang zu Schlüssel ermöglichen

5.5 Commisioning

- PAN nutzt gemeinsamen, symmetrischen Schlüssel (AES-CCM) zur Kommunikation im Netzwerk
- Commisioning: Gründung eines neuen Netzwerkes bzw. hinzufügen eines neuen Knotens
  - beinhaltet Transfer des Netzwerkschlüssels zum neuen Gerät
  - Sicheres Commisioning fundamental für ZigBee Netzwerksicherheit

5.5.1 EZ-Mode Commsioning

- verpflichtend zu implementieren in Geräten
- gestartet durch Nutzer

1. IoT-Gerät scannt nach offenen Netzwerken auf verschiedenen Kanälen
2. Falls Netzwerk neue Knoten zulässt; Antwort mit Netzwerkinformationen
3. IoT-Gerät entscheidet ob es Netzwerk beitritt
4. Der verschlüsselte Netzwerkschlüssel wir an IoT-Gerät geschickt
   - NDA-geschützter globaler link key
   - ODER vorkonfigurierter, IoT-Gerät spezifischer Schlüssel

5.5.2 Touchlink Commissioning

- kann optional Implementiert werden

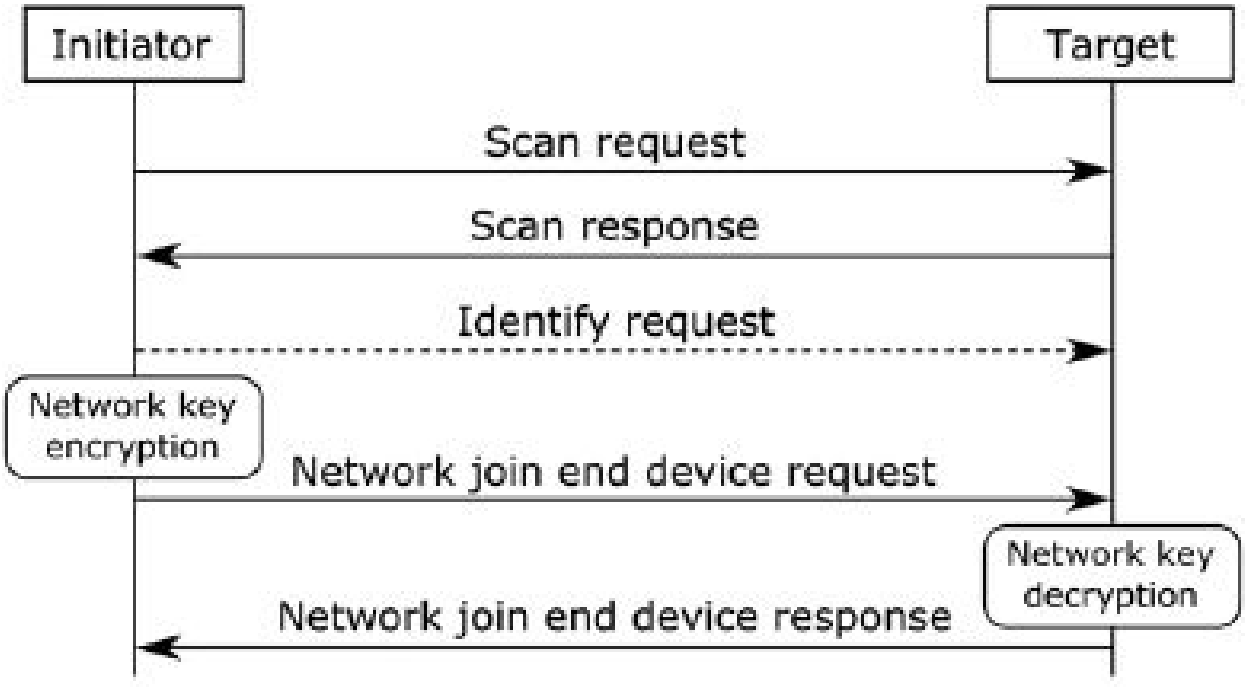

Figure 18: Touchlink Commissioning

5.6 Attacken ohne jegliche Schlüsselkenntnis

- Inter-PAN Frames:
  - Meschanismus, wodurch ZigBee-Geräte unischeren Informationenaustausch mit Geräten in der Umgebung durchführen, OHNE zweingend im selben PAN zu sein
  - Übertragung von Touchlink befehlen

5.7 Aktiver Scan nach Geräten

- an sich keine Attacke, aber eine Vorraussezung für alle anderen Attacken
- Scann nach touchlink-fähigen Geräten in drahtloser Reichweite
- nutzt "Scan-Request" + "Scan-Response" (siehe Touchlink Commissioning)

5.8 Identify Action Attack

- Löse mittels "Identify Request" die Identifizierungsaktion des Zielgeräts aus
  - z.B. Blinken Piepsen
- Nachricht beinhaltet Feld um Dauer zu spezifizieren: 16bit → 65000+ Sekunden
  - meistens nicht von Hersteller begrenzt
- Wiederhertellung; manuell das Gerät von der Stromversorgung trennen

5.9 Reset to Factory-New Attack

- Setzt das Zielgerät auf den Werkszustand zurück
- einfach mittels "Reset to factory new request" Touchlink Befehl
- könnte beispielsweise eine Smart-Doorlock entriegeln
- Wiederherstellung: Neues Commissioning des betroffenen Geräts

5.10 Permanent Disconnect Attack

- Zwei Angriffsmöglichkeiten:
  - Ändere den drahtlosen Kanal des Geräts
  - Ziel neu verbinden mit "Nullnetzwerk"
- Mittels "Network Update Request" Touchlink-Befehl
- Denial of Service oder Ransom möglich
- Wiederherstellung: phsysischer Reset; Angreifer einfach mit erneuter "Attacke"

5.11 Attacken mit Kenntnis des globalen Master Keys

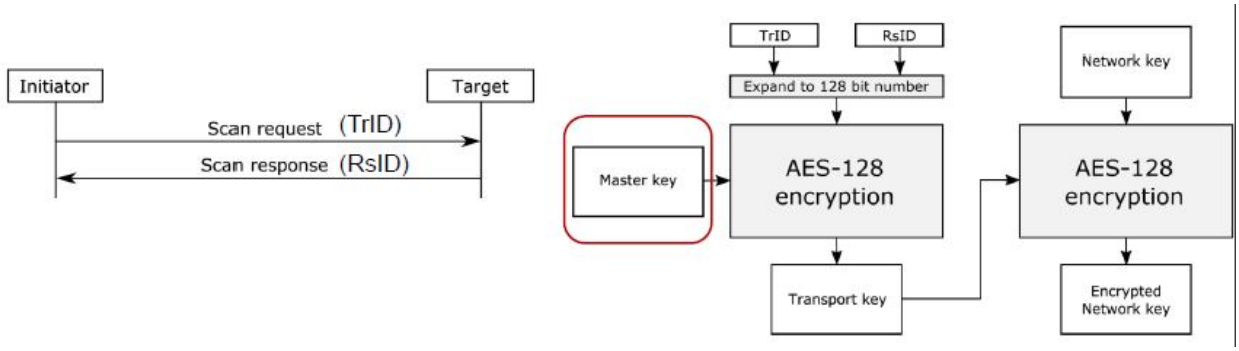

Figure 19: Master Key Attack

- → ZLL Master Key wurde 2015 geknackt

5.11.1 Hijack Attack

- Aktiver Angriff: benötigte Interaktion
- Verbindet Geräte mit den Netzwerken des Angreifers
- Schicke Befehl (An-/Abschalten, öffnen, schließen)

5.11.2 Network Key Extraction

- Passiver Angriff: Höre ein Touchlink-Commissioning ab
  - Zwinge Nutzer zum Commisioning durch Reset-to-factory-new angriff
- Offline-Cracking des Netzwerkschlüssels, da alles benötigte vorliegt

5.11.3 Enternungsprüfung um Touchlink-Befehle zu aktzeptieren

- Zielgerät misst Signalstärke des "Scan-Request" Befehls
  - falls Signalstärke > festgelegter Tresholder → schicke "Scan-Response"
- → Durch stärksten Sender auf Seiten des Angreifers kann die "legitime" Distanz überschritten werden

6 RFID

6.1 Radio Frequency Identification Definiton

- Identification und Tracking mittels Radiowellen
- Keine Batterie in passiven RFID-Tags
- Ausbau aus
  - Integrierter Schaltkreis: Speichern + Verarbeiten von Daten, (De-) Modulation des Radiosignals
  - Antenne: Erhalte induktiven Strom zum Betrieben, transferieren der ID

6.2 Passives RFID

- Ablauf
  1. RFID Lesegerät nutzt Induktion um das passive RFID Tag mit Strom zu versorgen
  2. Passives Tag emmitiert Trägersignal, mit den Daten darauf moduliert
  3. RFID Lesegerät demoduliert das eingehende Signal und prüft die erhaltenen Daten
- Tamper-Proof: Veränderung in der Umgebung können ein zusätzliches Bit im Tag setzen
- Anwendung:
  1. Überwach physische Integrität kritischer Behälter: Chemische Substanz setzt z.b. ein Bit, wenn eine bestimmte Temperatur überschritten wird
  2. Tamper Detection: z.B. wenn Kabelschleife getrennt wird, wird ein Bit gesetzt
  3. Zugangkontrolle: ID-Karte fürr Gebäude
  4. Tacking: Kleidung im Laden, teurer Wein
  5. Elektronische Zahlung: elektronische Tickets, Mautstation

6.3 RFID Standards

- ISO Vicinity Cards and RFID $\rightarrow$ 1-1,5m Distanz
- ISO Proximity Cards and RFID $\rightarrow <$ 1m Distanz
  - darauf basierend: NFC Form $\rightarrow$ 20cm Distanz
- EPC globals: Barcodesatz in Versorgungs und Lieferketten

6.4 Electronic Product Code (EPC)

6.4.1 EPC Generation 2 - Klassen

1. Passiv: Speichert EPC ID, Passwort, mit Kill Switch
2. Passiv erweitert: += Seicher, authentifizierte Zugangskontrolle
3. Semi-Passiv: Tag benötigt Batterien/Sensoren
4. Aktiv: Batterie, Tag-To-Tag Kommunikation, ad-hoc Nerzwerkbildung

6.4.2 EPC global Tag Format

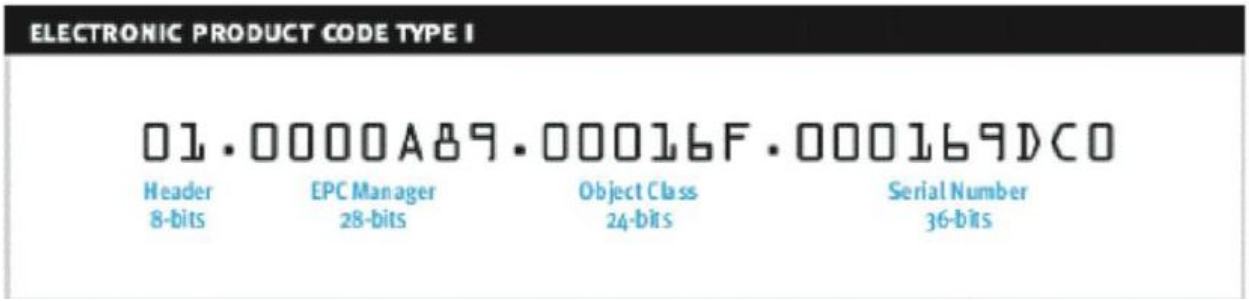

Figure 20: EPC global Tag Format

- Verwendung
  - genaueres Inventar
  - Diebstahlabschreckung
  - Lokalisierung und Tracking
    - im falschen Regal
    - wird genommen, aber wieder zurückgelegt → Ware kaputt/schlecht?

6.4.3 Sicherheitsprobleme

- Firmen: Unathorisiert bespähen, könnten Lieferketten der Konkurrenz analyisieren
- DoS der Konkurrenz: Jamming-Angriffe können das Geschäft lahmlegen
- Unerlaubte Markforschung beim Konkurrenten
  - Unauthorisierte Lesegeräte können leicht Statistiken über das Konsumentenverhalten aufstellen
- Malware: Bösartige RFID-Tag-Ids verwenden, SQL Injection

6.4.4 Privatsphäreprobleme

- Handlungen: Überwache die Interaktion von Personen mit dem gelagerten Produkten
- Zuordnung: Verknüpfe Person mit dessen einzigartigen RFID Tags
- Vorlieben: Erfahren Kundenvorlieben
- Transaktionen: Zwei Personen mit identifizierten Tags tauschen Tag aus

6.5 RFID Bill of Rights

1. Das Recht zu wissen, ob ein Produkt ein RFID-Tag enthält
2. Das Recht eingbettete RFID-Tags zu entfernen, deaktiveren oder zuerstören
3. Das Recht auf Nicht-RFID-Alternativen, ohne Nachteile
4. Das Recht zu wissen, welche Informationen ein RFID Tag speichert
5. Das Recht zu wissen, wann, wo und warum ein RFID-Tag gelesen wird

6.6 RFID-basierte Identification: elektronische Dokumente

- Biometrische Pässe/Ausweise
  - geregelt nach ISO Proximity Cards Standard → <1m Lesedistanz
  - Nutzt Public Key Infrastrukturen; Länder signieren ihre Pässe etc.

6.6.1 E-Passport-Zugangskontrolle

- Basic Access Control (BAC)
  - nutzt symmetrische Kryptographie
  - der schlüssel wird dabei aus zyklisch lesbaren Daten gebildet: Geburtsdatum, gültig bis, Dokumentenummer → verhindert, dass Dritte ohne optische Verbindung Daten auslesen können
- Active Authentication/ Extended Access Control (EAC)
  - nutzt asymetrische Kryptographie
  - schützt biometrische Informationen
  - Daten sind digital signiert → integritätsgeschützt
  - Lesegerät authentifiziert sich beim Dokument mit eigenem Zertifikat

6.6.2 Klauen von elektronischen Pässen

1. BAC-Schlüssel: Benötigt physischen bzw. optionalen Zugang zum Pass, um den Schlüssel zu bilden
2. Lese jetzt die Passdaten aus (jetzt ohne Sichtlinie möglich "normales" RFID)
3. Schreibe die Daen auf eine Blanke RFID-Karte
   - Klon überzeugt nur elektronischen Leser, eher keinen menschlichen Kontrolleur

6.6.3 Fingerprint elektronische Pässe

- elektronische Pässe antworten unterschiedlich auf Komandos eines Lesegeräts
- das Lesegerät muss sich dafür nicht authentifiziert haben
  - Nationalität meist genauso übermittelbar

6.6.4 Tracking via Replay Attack

1. Höre einen legitimen BAC Schlüsselaustausch des Zielpaares ab
   - Genauer: Die verschlüsselte Nachricht des Lesegeräts, welche unter anderem die NONCE des Paares enthält
2. Zur Identifikation: Schicke diese Nachricht erneut an den fraglichen Pass, messe die Antwortzeit
   - Pass prüft zuerst die Integrität der Nachricht mit dem eigenen Integritätschlüssel
   - Dann erst wird die NONCE zwecks Replay Schutz geprüft
3. Anderer Pass: Check schlägt bereit bei Integrationscheck fehl; richtiger Pass: Check schlägt erst bei NONCE-Check fehlt
   - Deutlicher Zeitunterschied bezogen auf die Antwortzeit

6.6.5 RFID-basierte Zugangskontrolle und Zahlungsmittel

- Zugangskontrolle bei Autos
  - läuft mittels Digital Signature Transponder (DST)

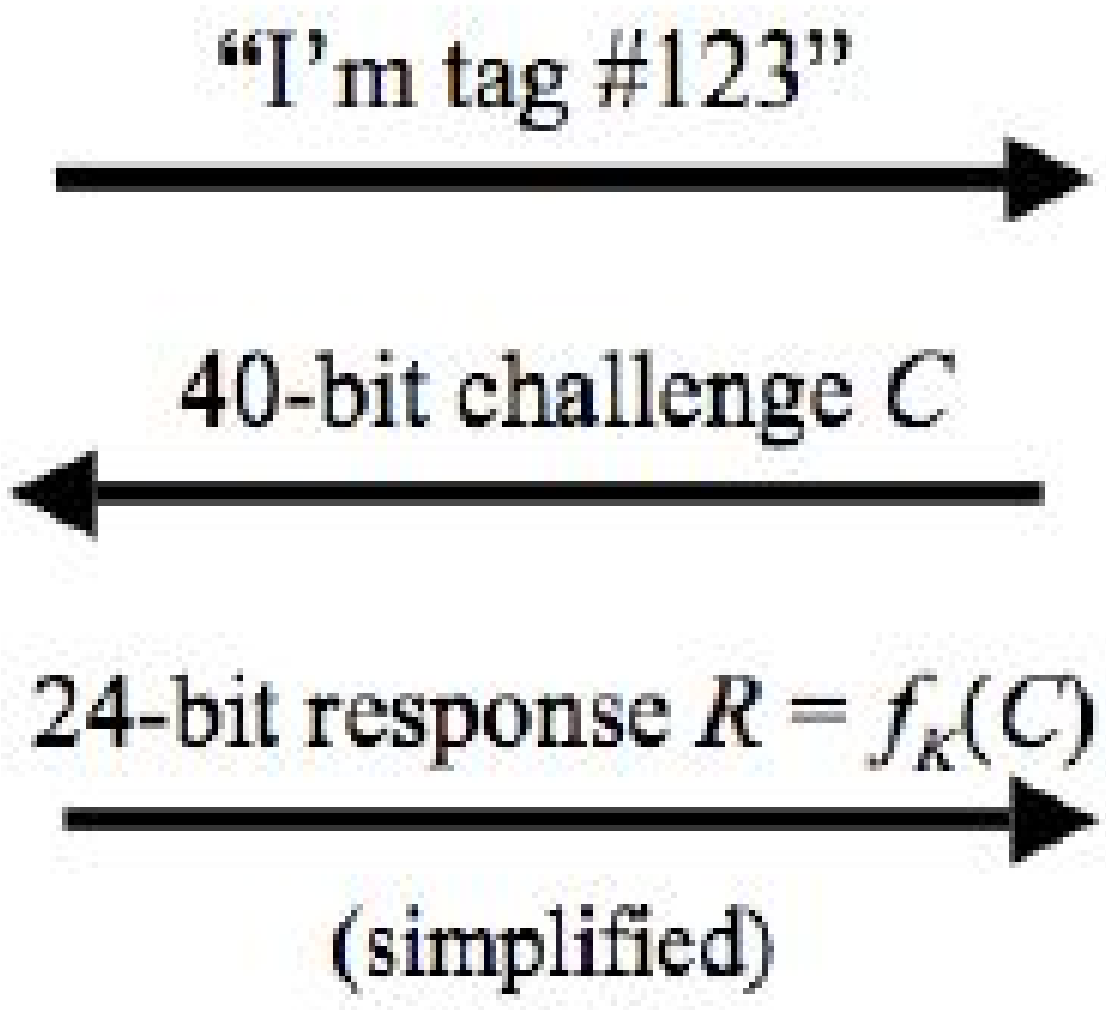

Figure 21: Auto brum brum

- Angriff auf Zugangskontrolle
  1. Schlüssel K nur 40bit, f_k Security by Obscurity
  2. Lausche für zwei Challenge Response Paare $(C, f_k(C))$
  3. Cracke den Schlüssel K
  4. Bei simplen mechanischen Zündschloss, nutze ihn während ein PC die Challenge-Response übernimmt

- Ghost+Leech Angriff auf Zugangskontrolle+Zahlungssysteme

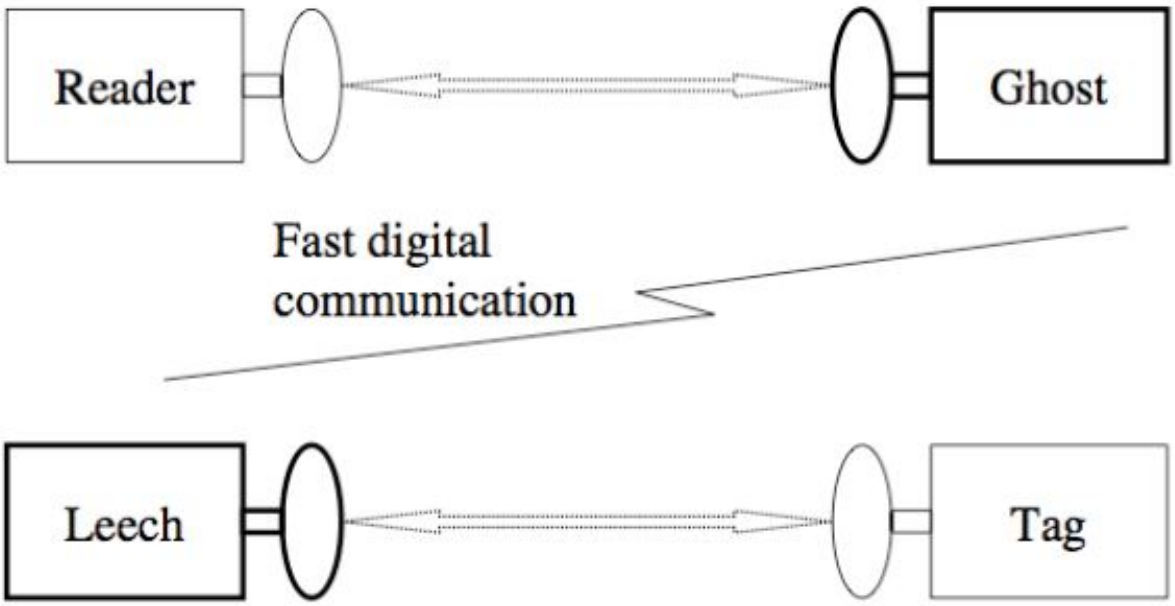

Figure 22: Leech

- Umgeht Challenge Response Authetifizierung
- Gegenmaßnahme: Distance Bounding Protocols
  - Nutze mehrere Challenge Response Runde um mittels der Antwortzeit zu bestätigen dass der Tag tatsächlich innerhalb einer erlaubten Distanz ist
  - → Ghost-Leech Kommunikation müsste dafür extrem schnell sein