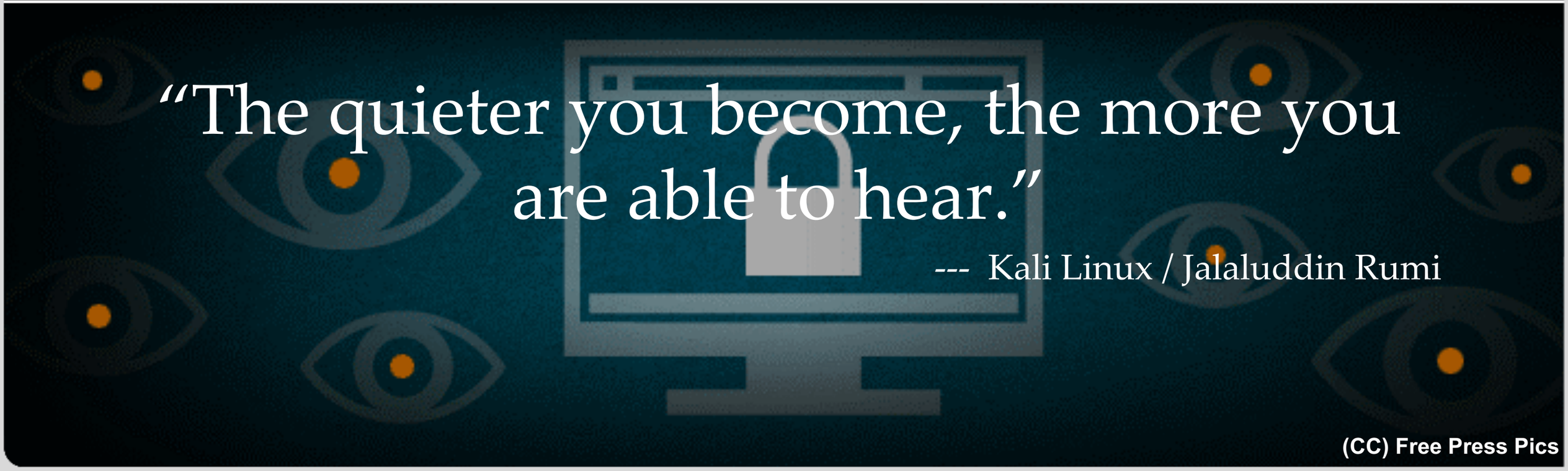
Karlsruher Institut für Technologie

WPA2 Handshake and Half-Handshake Attacks

KASTEL-Praktikum Sicherheit
Benny Görzig (bgoerzig@gmail.com), Florian Loch (me@fdlo.ch)

Betreuer: Erik Krempel, Pascal Birnstill (Fraunhofer IOSB), Daniel Keller (LKA BW)



Agenda

1. Einleitung
2. WPA2-Cracking
3. Handshakes mitschneiden
4. Fazit & Ausblick

1. Einleitung

1. Motivation
2. Zugangsschutz
3. Nutzerverhalten

Motivation

- Drahtlose Funknetzwerke heute wohl verbreitetste Art der Netzwerkanbindung
- Übertragung sensibler Informationen
- Physikalische sehr exponiert, (passiver) Angreifer muss lediglich in Reichweite sein
- Entsprechender Schutz der Verbindung auf OSI-Schicht 2 obligatorisch
  - Vertraulichkeit
  - Integrität
  - (Authentizität)

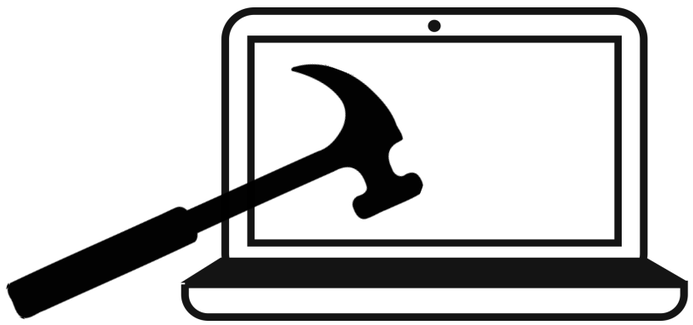
Zugangsschutz: WPA2

- Vollständige Umsetzung von IEEE 802.11i (RSN)
- Unterstützt zwei Authentifizierungsmodi
  - WPA2-PSK: „ Personal“ mit Pre-Shared-Key
  - WPA2-EAP: „Enterprise “ mit 802.1X (EAP over IEEE 802)
- Aushandlung individueller Sitzungsschlüssel (PTK) in 4-Wege-Handshake

- Fokus heute: WPA2-PSK
  - De facto Standard für Heimnetzwerke & kleine Firmennetze

WPA2-PSK: Angriffe möglich?

- Angriffe auf Protokollebene (theoretisch) existent, jedoch ...
  - ... starke Vorannahmen
  - ... oftmals nicht praktikabel
- Rückgriff auf Bruteforce-Angriff, um PSK zu ermitteln



- Interessante Alternative: Social-Engineering-Attacken
  - Mensch oft das schwächste Glied bei Sicherheitsmechanismen
  - Nutzer durch geschickte Manipulation zur Preisgabe des Schlüssels bringen
  - Heute nicht Thema, für Interessierte: WifiPhisher, Fluxion

WPA2-PSK: Bruteforce in Praxis realistisch?

- Beständigkeit von WPA2 gegenüber Bruteforce-Angriffen hängt maßgeblich vom verwendeten PSK ab
  - *“Most users will take the road of least resistance.”* [4]
  - Länge Ø 6 Zeichen (min. 8 für PSK bei WPA2)
  - 80% alphabetisch, nur 13.7% alphanumerisch
  - Menschen tendieren dazu, kurze, in Wörterbüchern gelistete Begriffe (oder Kombination daraus) zu verwenden
- Standardpasswörter sterben nicht aus
  - ISPs und Hardware-Hersteller setzen teils erschreckend schlechte Standardpasswörter

1. Einleitung

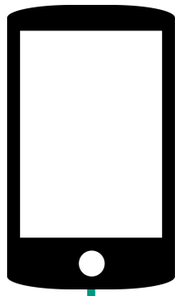
2. WPA2-Cracking

- Der WPA2-Handshake
- Online-Cracking
- Offline-Cracking

3. Handshakes mitschneiden
4. Fazit & Ausblick

Cracking: Viele Wege führen nach Rom...

- Zwei generelle Ansätze für Bruteforce-Angriffe:
  - Online
  - Offline
- Für Bruteforce-Angriffe auf WPA2-PSK gilt immer:
  - Passwortkandidaten finden, mit dem Authentifikation beim Access Point möglich ist (Kollision)



Supplicant/Client

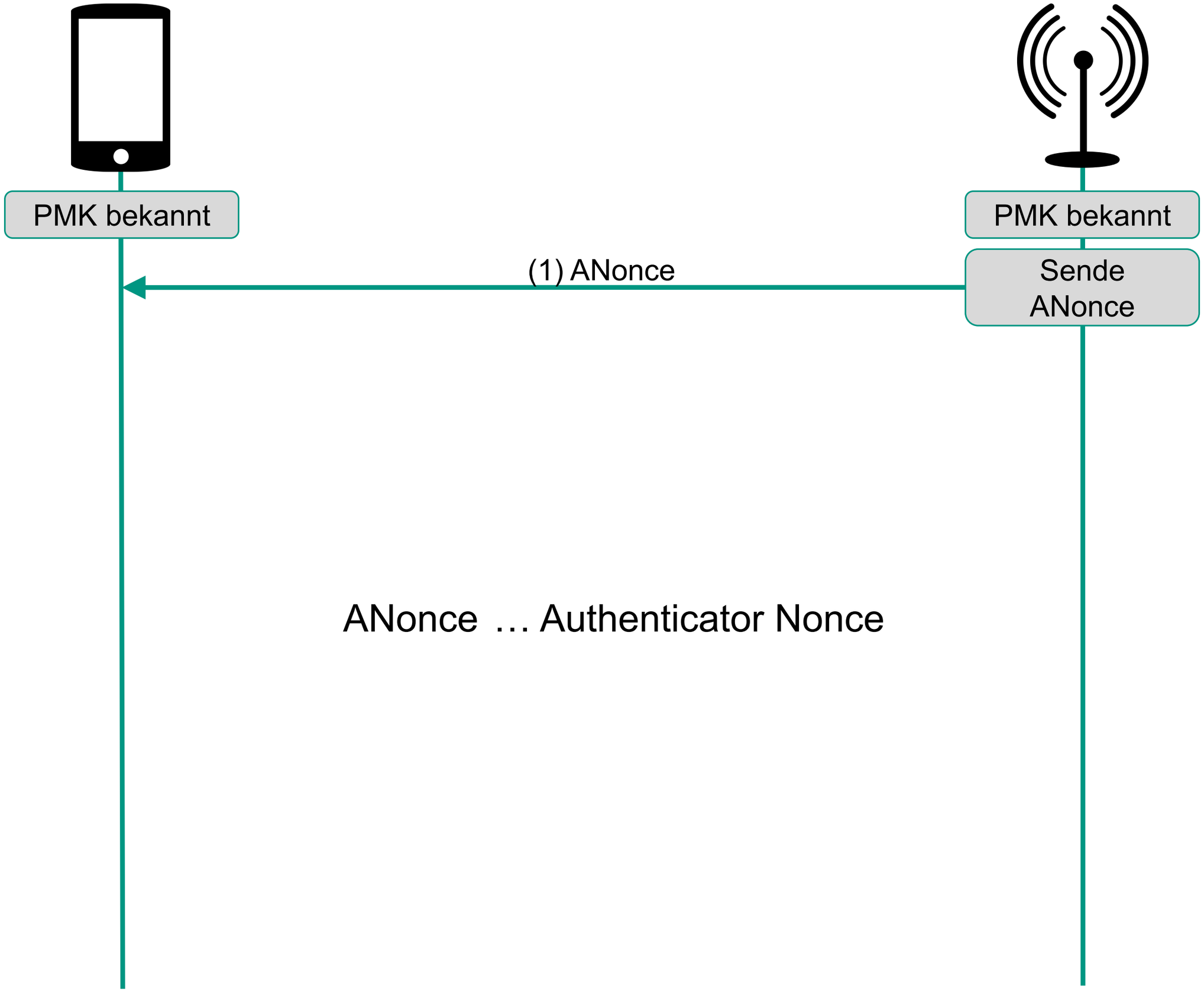
Authenticator/AP

PMK=PBKDF2(PSK, SSID)

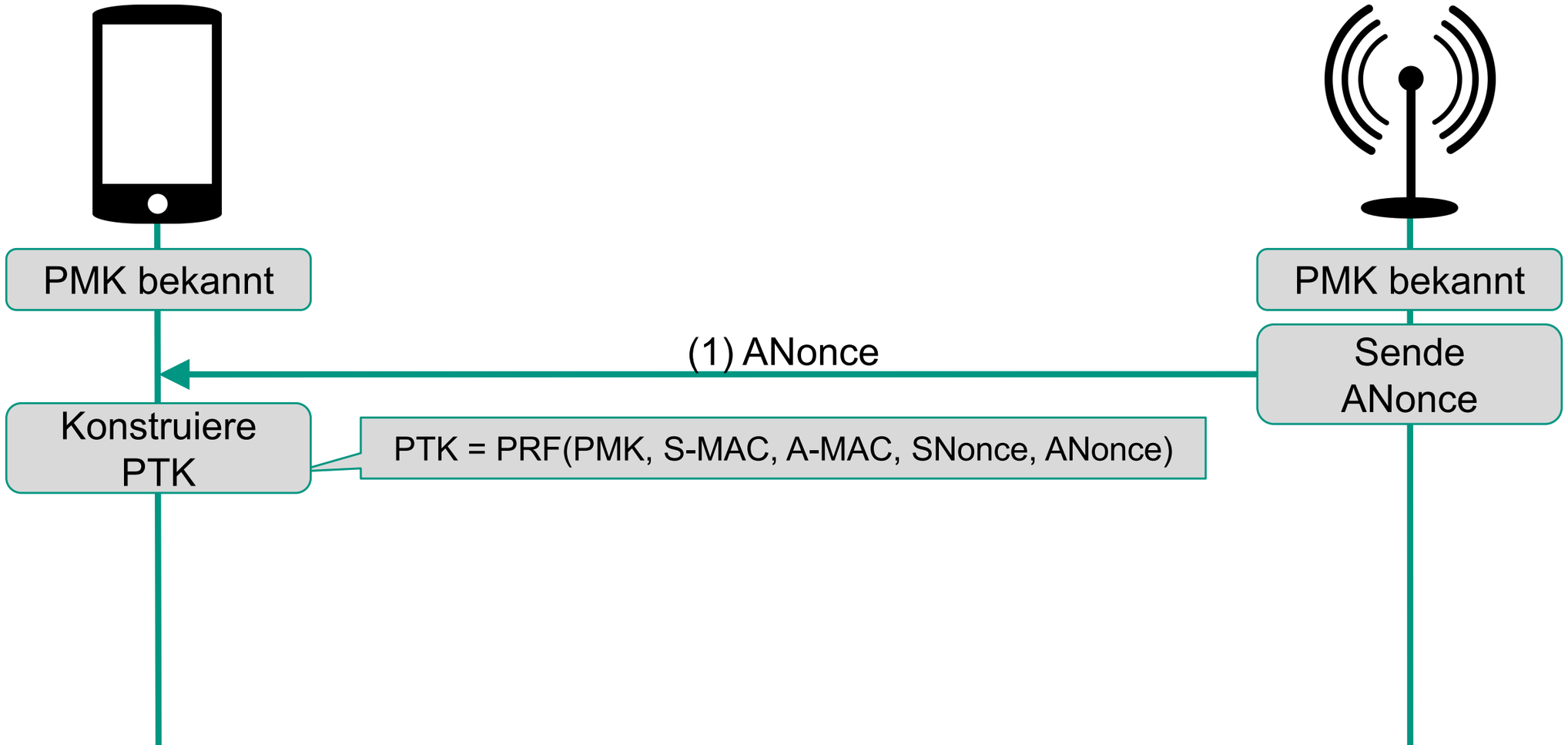
PMK bekannt

PMK bekannt

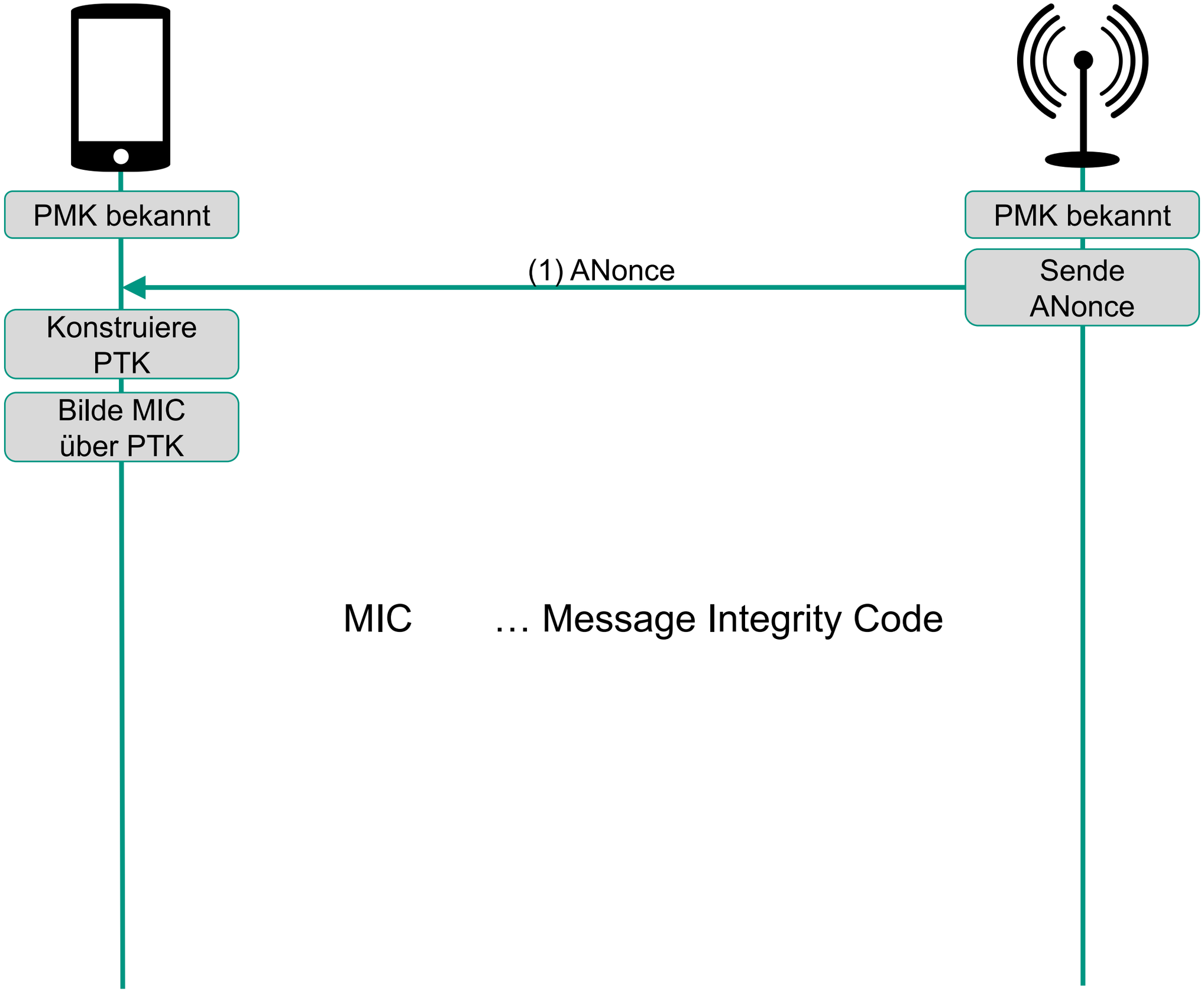
PSK … Pre-Shared Key, Passwort
PMK … Pairwise Master Key
PBKDF2 … Pseudo-Random Function
SSID … Netzwerkname



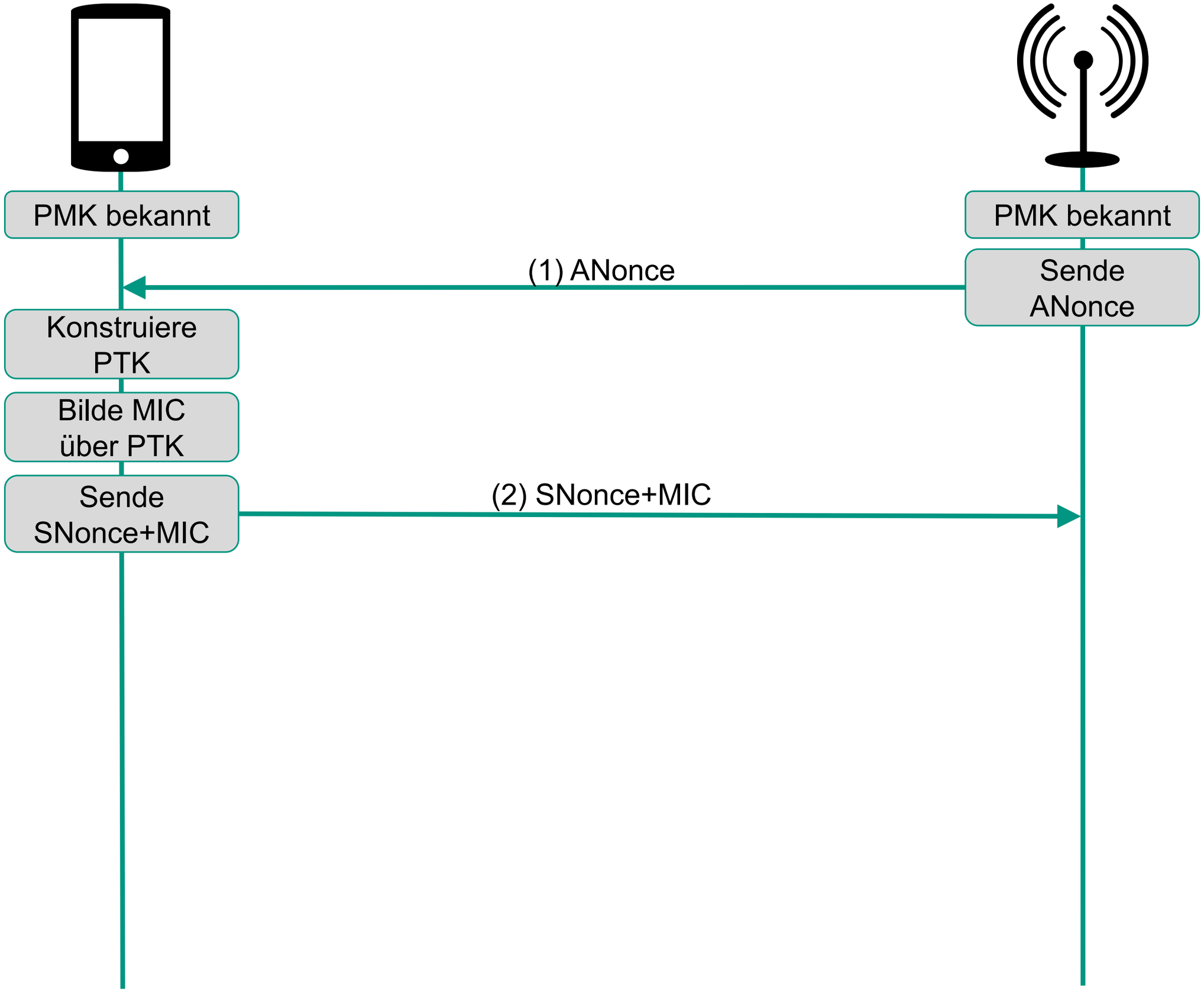
ANonce … Authenticator Nonce

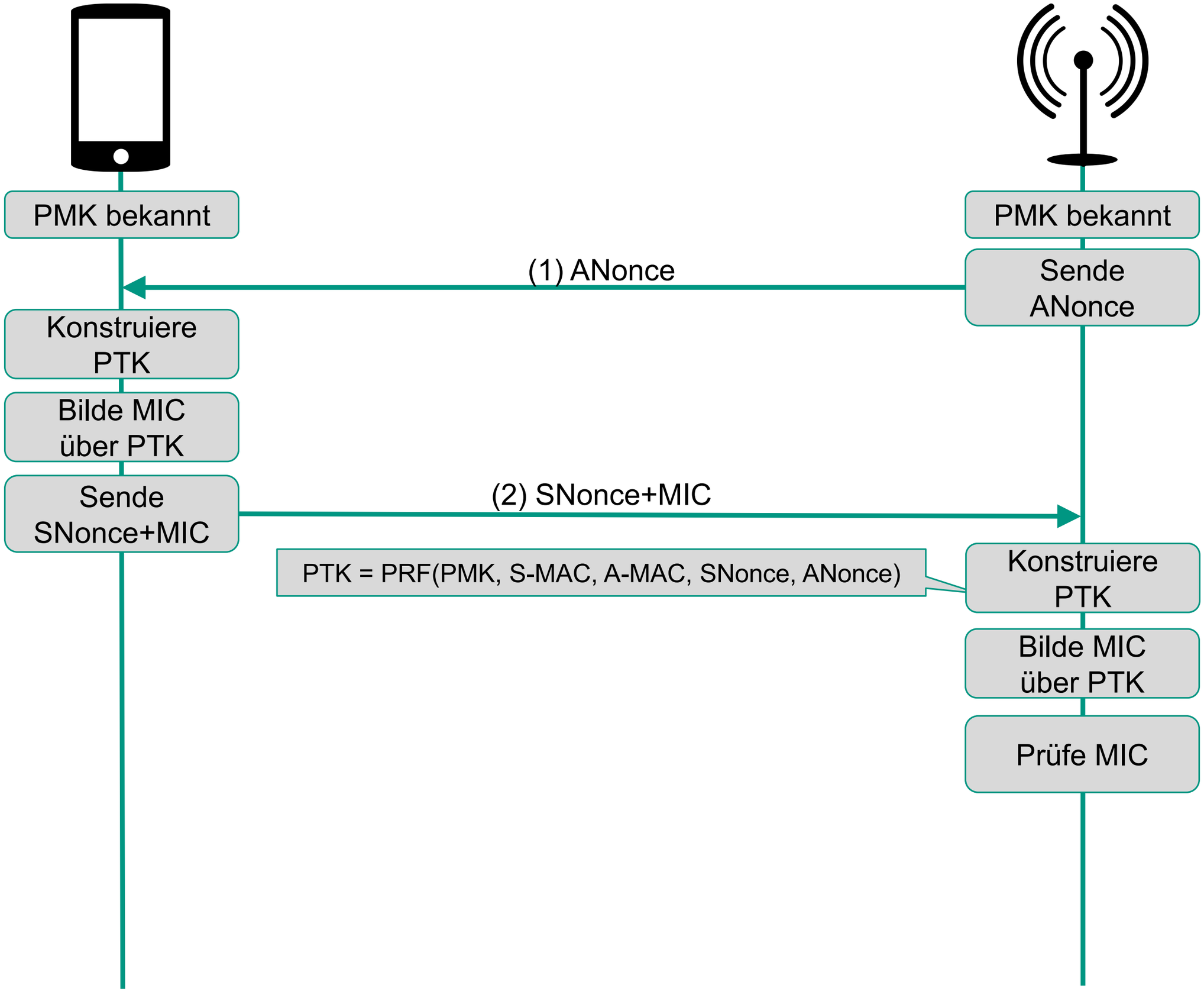


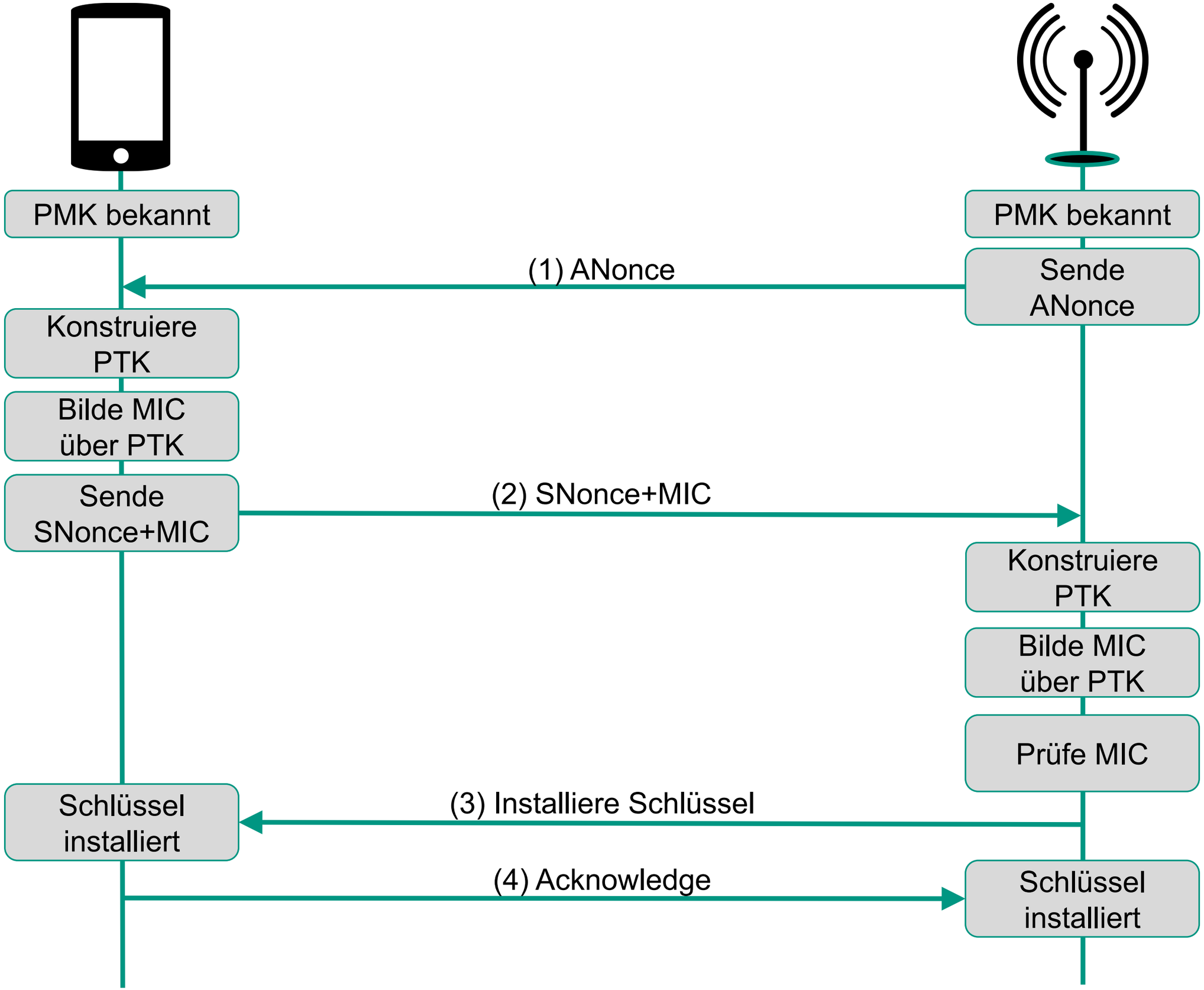
PTK … Pairwise Transient Key
PRF … Pseudo-Random Function
S-MAC … Supplicant MAC
A-MAC … Authenticator MAC
SNonce … Supplicant Nonce



MIC … Message Integrity Code

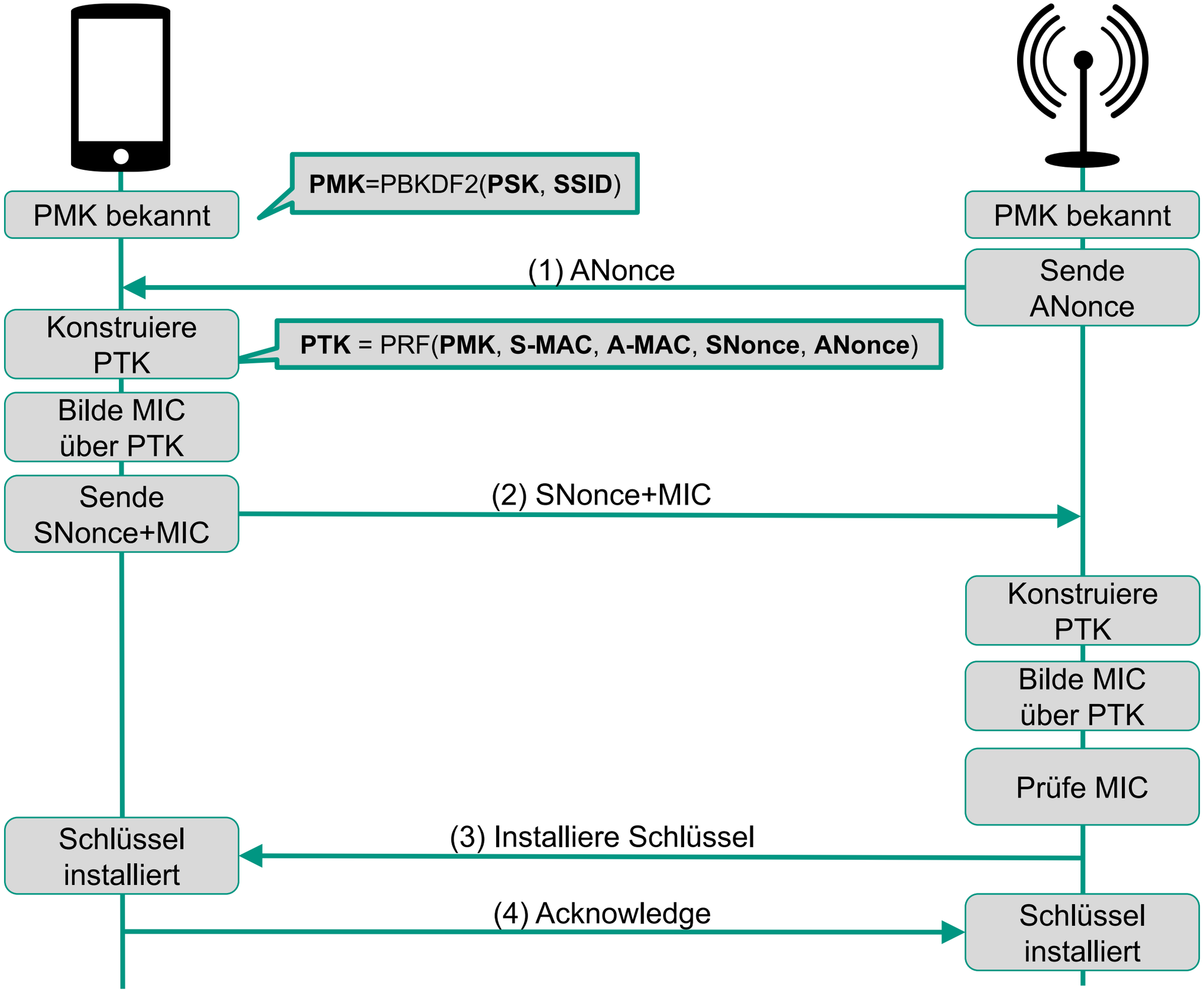

PMK bekannt
(1) ANonce
PMK bekannt
Sende ANonce
Konstruiere PTK
Bilde MIC über PTK
Sende SNonce+MIC
(2) SNonce+MIC

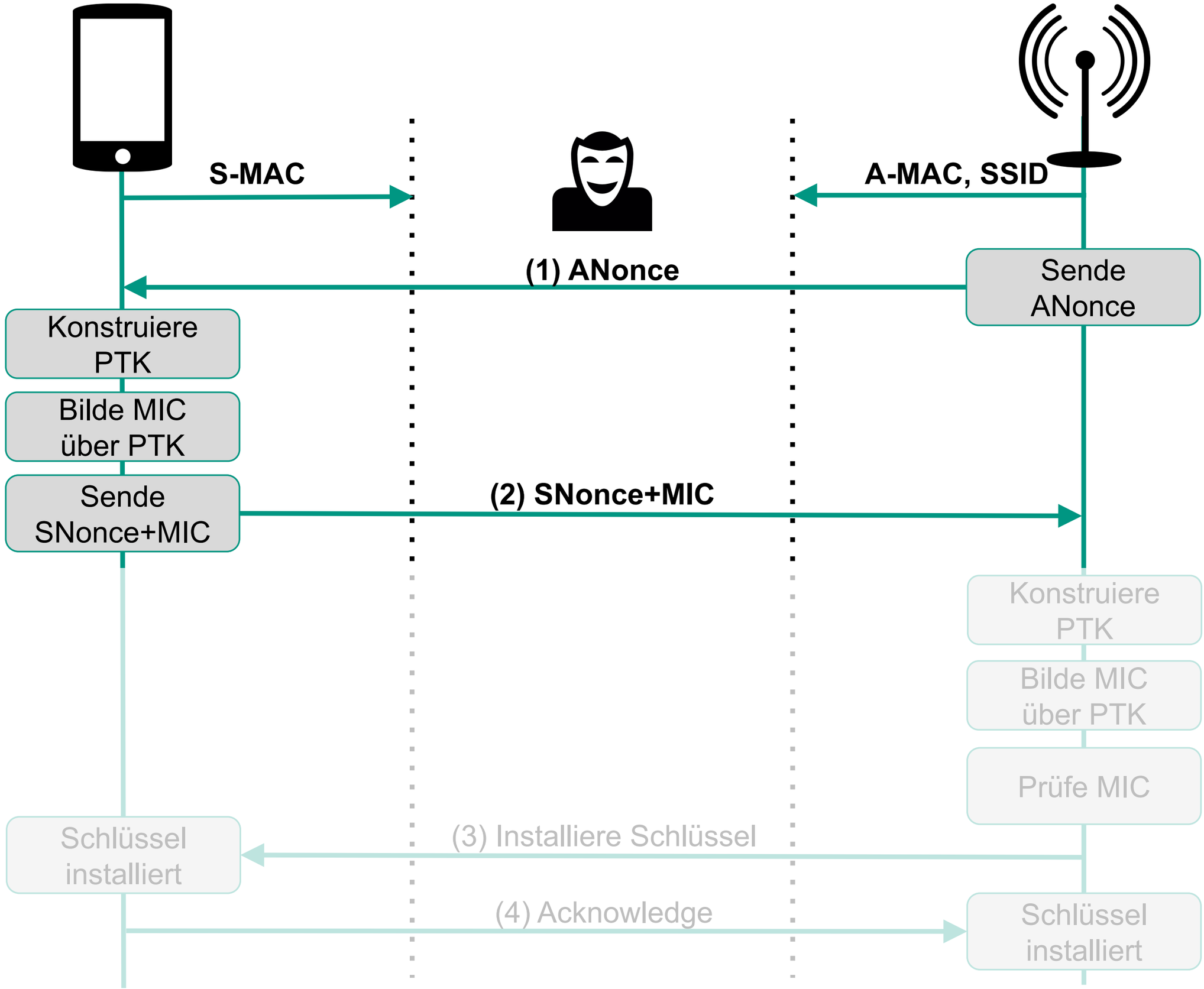

PMK bekannt
(1) ANonce
PMK bekannt
Sende ANonce
Konstruiere PTK
Bilde MIC über PTK
Sende SNonce+MIC
(2) SNonce+MIC
PTK = PRF(PMK, S-MAC, A-MAC, SNonce, ANonce)
Konstruiere PTK
Bilde MIC über PTK
Prüfe MIC

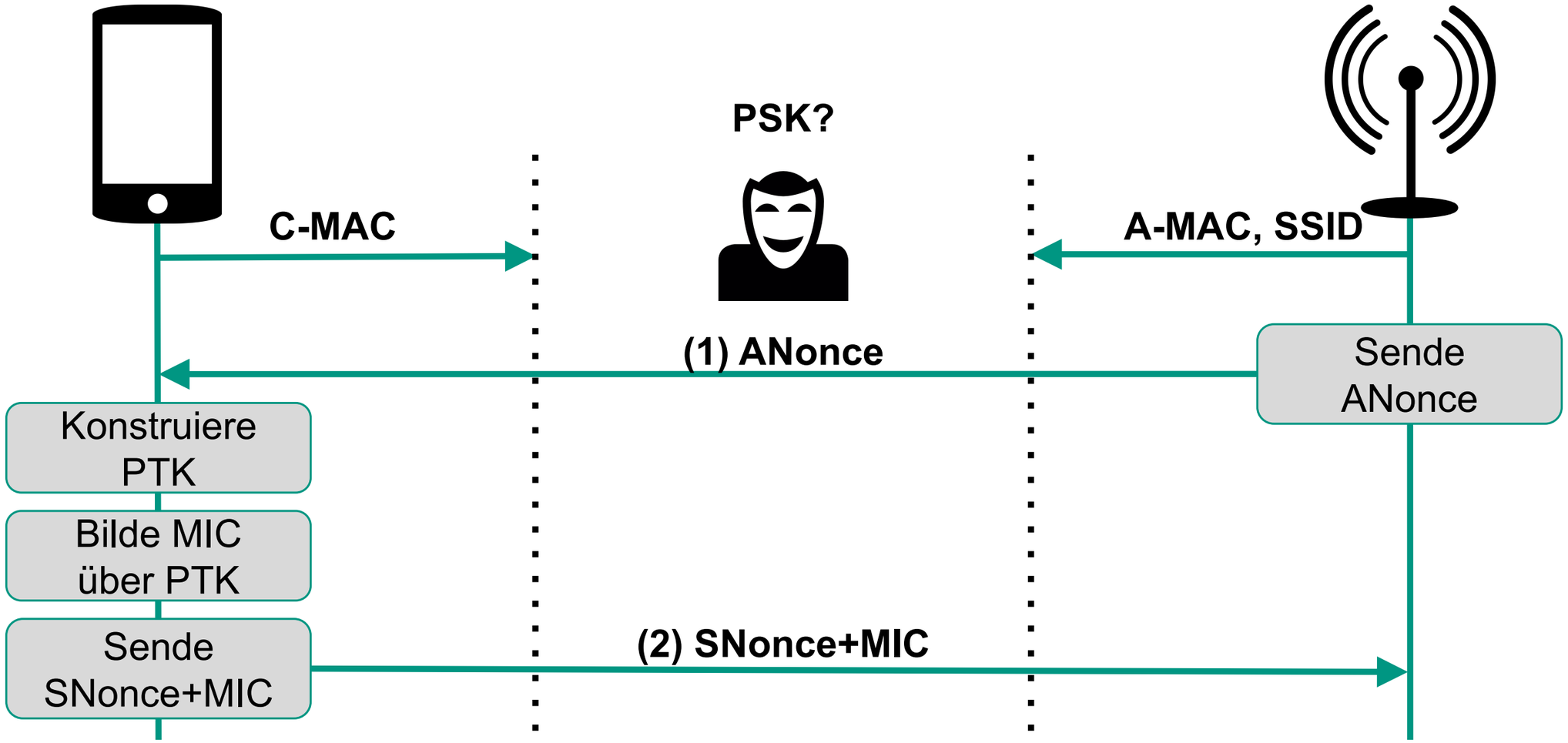

PMK bekannt
PMK bekannt
(1) ANonce
Sende ANonce
Konstruiere PTK
Bilde MIC über PTK
Sende SNonce+MIC
(2) SNonce+MIC
Konstruiere PTK
Bilde MIC über PTK
Prüfe MIC
Schlüssel installiert
(3) Installiere Schlüssel
(4) Acknowledge
Schlüssel installiert

Cracking: Offline

- Idee: Angreifer spielt Rolle des AP beim Handshake (später) lokal nach
  - Es werden allerdings einige Informationen benötigt: SSID, SNonce, ANonce usw.
- Woher diese nehmen? Siehe Handshake!


PMK bekannt
PMK=PBKDF2(PSK, SSID)
PMK bekannt
(1) ANonce
Sende ANonce
Konstruiere PTK
PTK = PRF(PMK, S-MAC, A-MAC, SNonce, ANonce)
Bilde MIC über PTK
Sende SNonce+MIC
(2) SNonce+MIC
Konstruiere PTK
Bilde MIC über PTK
Prüfe MIC
Schlüssel installiert
(3) Installiere Schlüssel
(4) Acknowledge
Schlüssel installiert


S-MAC
A-MAC, SSID
(1) ANonce
Sende ANonce
Konstruiere PTK
Bilde MIC über PTK
Sende SNonce+MIC
(2) SNonce+MIC
Konstruiere PTK
Bilde MIC über PTK
Prüfe MIC
Schlüssel installiert
(3) Installiere Schlüssel
(4) Acknowledge
Schlüssel installiert



- Angreifer spielt Handshake jetzt lokal nach
  - Möglichen Wert für PSK bestimmen
  - PMK für diesen berechnen (4096 Runden PBKDF2)
  - Berechneter MIC == aufgezeichneter MIC? → mögliches Passwort gefunden

Offline-Cracking: Realitätscheck

- Hardware: Verbund aus 8 x Nvidia GTX 1080 + 2 x Intel Xeon E5 2620V3 leistet 3177,6 kHashes/Sekunde (Sagitta Brutalis, ca. 18500 $) [7]

- Passwort aus vorherigem Beispiel voraussichtlich in 9h gebrochen (statt in 165 Jahren!)
- 8 alphanumerische Zeichen benötigen aber immer noch im Mittel 400 Tage
- Problem: Suchraum gigantisch, Laufzeit der erschöpfenden Suche explodiert

- Geht das nicht auch effizienter? $\Rightarrow$ Wörterbuchangriff

Cracking: Offline mit Wörterbuch

- Motivation: Nutzer favorisieren leicht zu merkende Passwörter
  - *“Users may fulfill policy requirements in predictable ways, such as basing their passwords on names, or words”* [5]
  - Häufig: Simple Kombinationen (bspw. <Wort> + <Zahl>) und Permutationen (O -> 0, A -> 4) um Richtlinien zu erfüllen
- Statt raten: Passwörter mit Wörterbuch „zusammenbauen“
- Probleme:
  - Güte und Verfügbarkeit von Wörterbuch entscheidend
  - 4096 Runden PBKDF2 pro PMK sind teuer ; kann nur bedingt vorgeneriert werden da von SSID abhängig

Wörterbuch-Cracking: Realitätscheck

- Hardware: Verbund aus 8 x Nvidia GTX 1080 + 2 x Intel Xeon E5 2620V3 leistet 3177,6 kHashes/Sekunde (Sagitta Brutalis, ca. 18500 $) [7]
- Annahmen:
  - Passwort aus max. 2 oft benutzen Wörtern (Top 10.000)
  - enthält bis zu eine Zahl aus maximal 2 Ziffern
  - Ordnung der Einzelteile beliebig
  - = 10.001 * 10.001 * 111 * 3 = 33.306.660.333
- Circa 3 Stunden für Prüfen des vollständigen Suchraums nötig
- Falls man keine entsprechende Hardware besitzt...
  - ... Kapazitäten bei AWS mieten
  - ... Online Services für WPA2-Cracking (Seriosität fraglich)

1. Einleitung
2. WPA2-Cracking

3. Handshakes mitschneiden

4. Fazit & Ausblick

- On-Site
- Off-Site

Handshakes (effizient) mitschneiden

- Es existieren zwei Familien von Angriffen
  - On-Site
    - Passives Lauschen, „Abwarten-und-Tee-Trinken“
      - Authentifizierungen eher selten, ineffizienter Angriff
    - Deauth-Angriff
  - Off-Site
    - Evil-Twin-Angriff

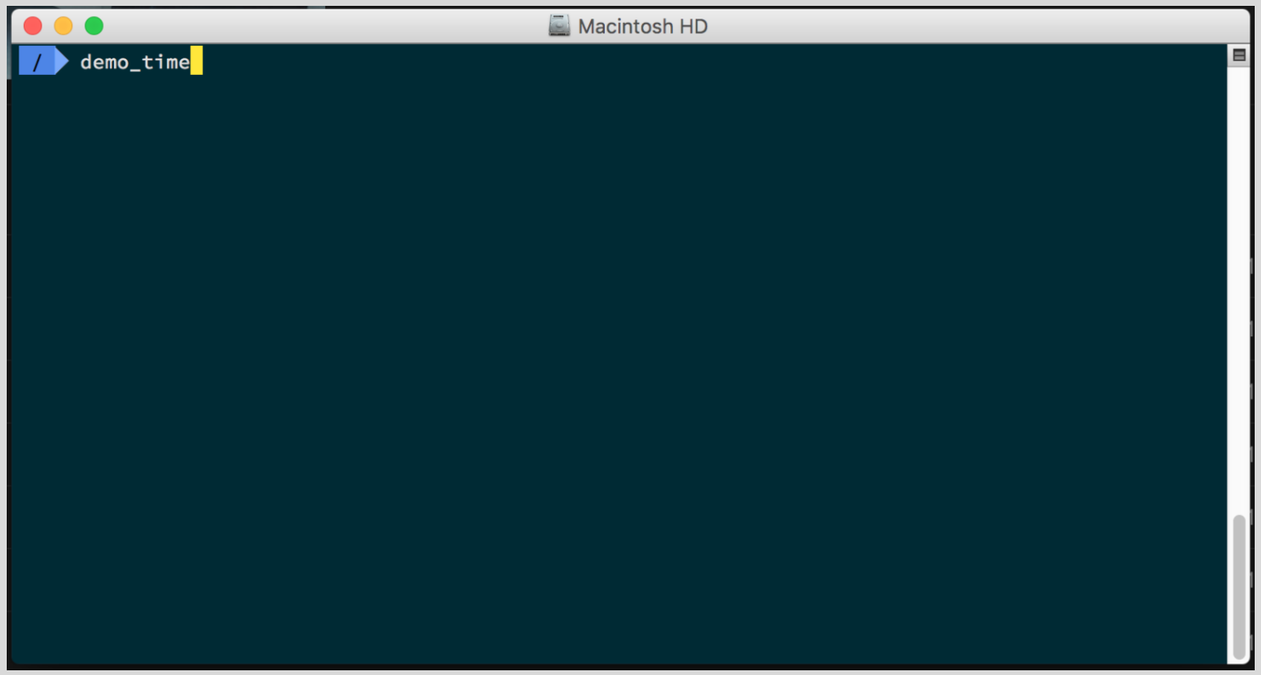
Angreifer provoziert Handshake

- Abstrakt: Schritt 1+2 des Handshakes zwischen Client und AP mitschneiden für späteres Offline-Cracking

Sniffing: On-Site (aktiv), aka “Deauth-Attack“

- Idee: Forciere Neu-Authentifizierung des Clients beim AP
- Ausnutzen von Deauth-Frames
  - Management-Frames unverschlüsselt; ohne Kenntnis von PSK erzeugbar
  - Angreifer sendet Deauth-Frame an Client (und AP)
  - Gespoofter Absender: MAC-Adresse des AP
- Nachteile:
  - Aktives Eingreifen in den Netzwerkverkehr
  - Je nach Szenario „leicht “ detektierbar, für Nutzer jedoch quasi nicht wahrnehmbar

Demo



- Deauth-Angriff:
  - (Ziel auswählen)
  - Deauth-Pakete senden
  - Handshake mitschneiden
  - Handshake mit Wörterbuch brechen

„Deauth-Attack“: Realitätscheck

- Wie leicht zu erkennen?

- Feldversuch 1: WPA2-PSK Heimnetzwerk mit bis zu 8 aktiven Clients
  - Über 24 Stunden kein Deauth-Paket
    - Nur ein AP → keine Clientverwaltung notwendig
    - Keine Schlüsselneuaushandlung benötigt
  - Deauth-Attacke äußerst auffällig durch Spikes

„Deauth-Attack“: Realitätscheck

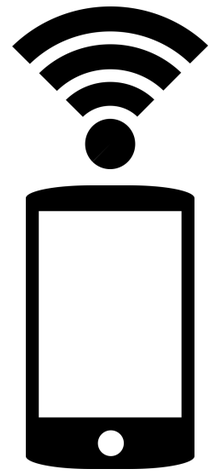
- Feldversuch 2: WPA2-EAP als Firmennetzwerk mit bis zu 30 aktiven Clients
  - Ca. 2 Deauth-Pakete/min, oftmals in Spikes (5-10 Pakete „zeitgleich“)
    - 3 APs in Reichweite → Clientverwaltung notwendig
    - Clients bewegen sich („Reasoncode 8“)
    - Stationäre Systeme benötigen Schlüsselneuaushandlung („Reasoncode 2“)
  - Auch hier: Deauth-Attacke auffällig durch (höhere) Spikes

Sniffing: Off-Site-Angriffe

- Ziel:
  - Angriffe gegen Client über Netzwerke, welche sich nicht in Reichweite befinden
  - Angriffsziele sollen nicht mehr von umgebenden Netzwerken sondern Clients in Reichweite abhängig sein
- Idee: Client zu Authentifizierungsversuch verleiten; Handshake provozieren
- Voraussetzungen:
  - Client muss sich weiterhin in Reichweite befinden
  - Konfiguration (SSID & Sicherheitskonfiguration) des Zielnetzwerkes muss bekannt sein
    - Woher erfährt der Angreifer die SSIDs die dem „Opfer“ bekannt sind ?

Exkurs: Probe-Requests und Probe-Responses

- APs senden in Intervallen sog. „Beacon-Frames“ aus, um Netzwerk und Konfiguration bekannt zu machen
- Client kann Probe-Requests versenden
  - zwingend für Detektion von „versteckten Netzen“
  - enthält SSID
  - AP antwortet mit Probe-Response
- Probe Response enthält u.a.:
  - Unterstützte Datenraten des APs
  - Sicherheitskonfiguration (z.B. OPN, WPA2 PSK)

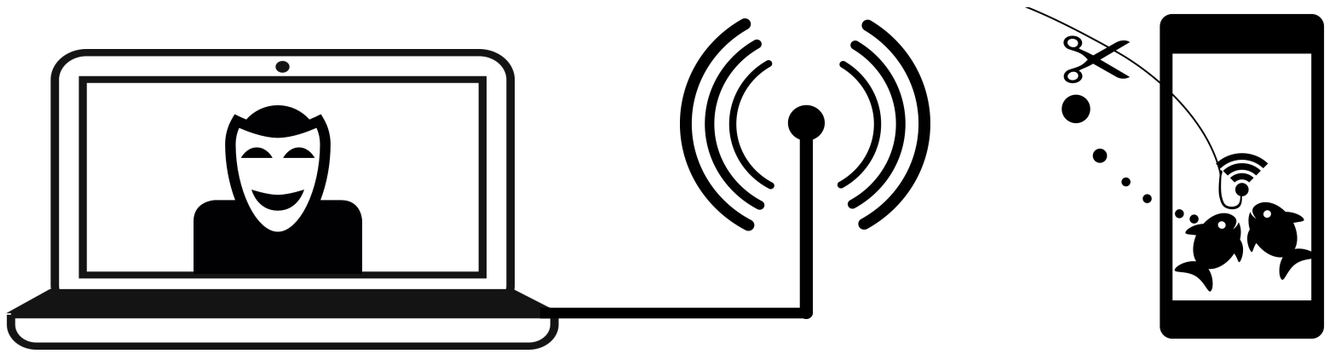


Exkurs: Probe-Requests und Probe-Responses

- Viele Geräte senden fortlaufend Probe-Requests aus...
  - Eigene Analysen:
    - Windows Phone, Windows 10, macOS
    - Android 6 sendet auch wenn verbunden!
  - ... auch für nicht versteckte Netze - unnötig und unsinnig!
- Problem dabei:
  - Öffnet Tracking von Endgeräten Tür und Tor
  - Client verrät ihm bekannte Gegenstellen

Sniffing: Off-Site: „Evil-Twin-Attack“

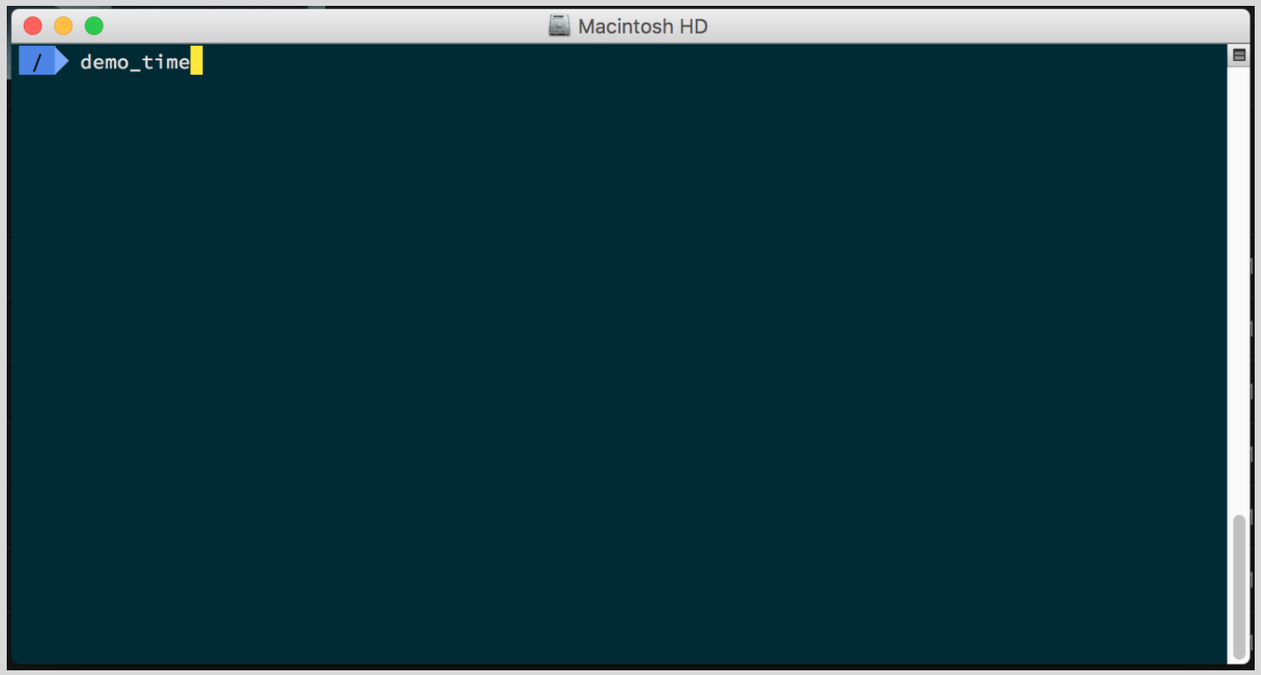
- Erstelle eigenen Mimikry-AP mit SSID aus Probe-Request
  - Sende Beacon-Frames bzw. entsprechende Probe-Response an Client
- Wenn Client „ anbeißt“, dann Handshake bis Schritt 2 durchführen
- Anschließend Verbindungsabbruch
  - Agieren als MITM unmöglich, würde Kenntnis des PSK erfordern



Sniffing: Off-Site: „Evil-Twin-Attack“

- Nachteile:
  - Client muss in Reichweite sein
  - Fake-AP auffällig → aktives Teilnehmen im Netzwerk
- Abhängig vom Endsystem wird Fake-AP “erkannt”
  - Windows-Phone/Windows 10: Erkennt Abweichung des Profils
  - Android 5/6, Windows 8.1: Verbindet automatisch, manche Geräte wechseln sogar bei aktiver Verbindung wenn Signal stärker
- Lösung: Mehrere Konfigurationen auf dem Interface öffnen

Demo



- Evil-Twin-Angriff:
  - (Ziel auswählen)
  - (Probe-Requests auslesen)
  - Evil-Twin aufsetzen
  - Handshake mitschneiden
  - PSK brechen

1. Einleitung
2. WPA2-Cracking
3. Handshakes mitschneiden

4. Fazit & Ausblick

- Fazit
  - WPA2
  - Vorgestellte Angriffe
- Ausblick

Fazit: WPA2-PSK

- Management-Frames sind nicht (implizit) authentifiziert
  - Erweiterung 802.11w erlaubt Authentifizierung einiger Management Frames
- Keine Perfect-Forward-Secrecy
- AP muss sich gegenüber dem Client bei Handshake nicht authentifizieren
- Probe-Requests kritisch bzgl. Tracking von Endgeräten
  - Erkenntnis: Endgeräte zu gesprächig
  - Ø 50 Probe-Requests/Stunde pro Gerät [9]
  - Android sendet mehr Probe-Requests als iOS, Mac OS, Windows 10

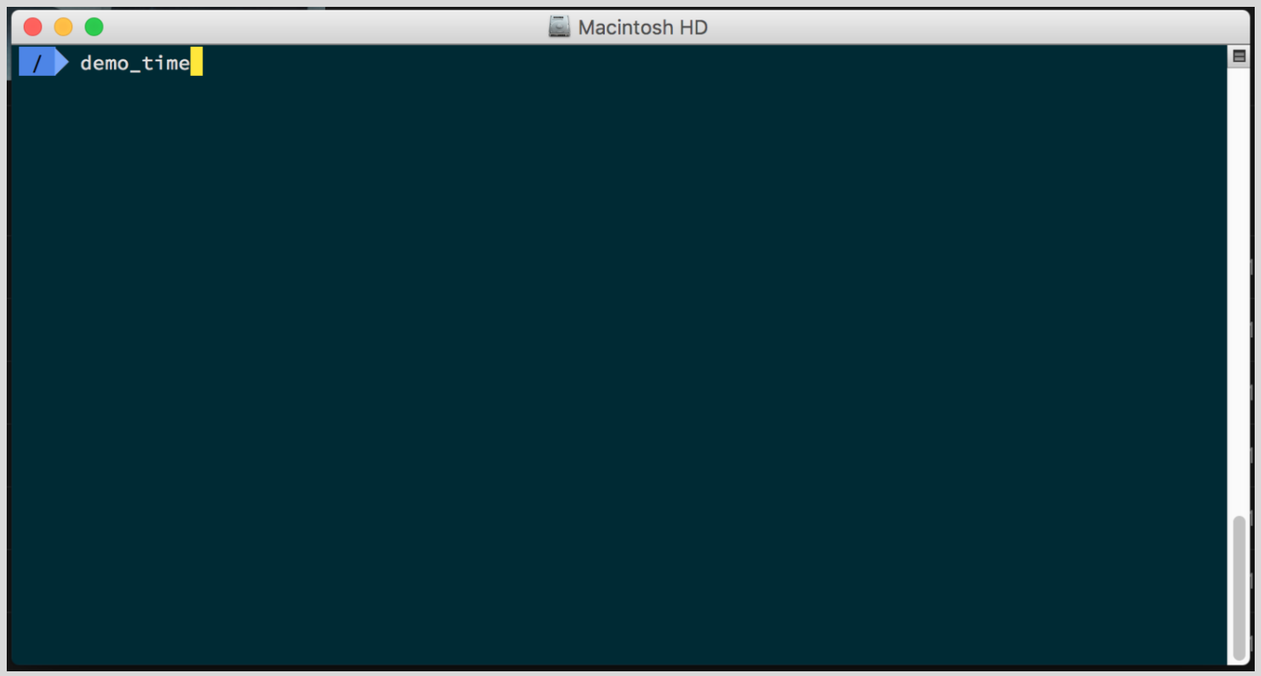
Fazit: Praktikabilität vorgestellter Angriffe

- Komplexität des Schlüssel entscheidet letztlich über Sicherheit von WPA2-Netzen
  - Schwache Schlüssel stellen eine realistische Sicherheitsbedrohung dar
  - Hinreichend komplexe Schlüssel nicht in annehmbarer Zeit zu brechen
- Netze müssen für Angriff auf deren PSK nicht in Reichweite sein
- Vorgestellte On- und Off-Site-Verfahren stellen in Kombination mit Wörterbüchern einen praktikablen Angriff auf den PSK dar

Ausblick

- Ein Verbesserungsansatz: Automatisierung des Evil-Twin-Angriffs
  - Horizontale Skalierung:
    - Für alle Probe-Requests eines Clients falsche APs bereitstellen
    - Viele Handshakes mitschneiden
    - Jeden Handshake lediglich gegen eine effiziente Wortliste prüfen
    - “Jedes Smartphone war einmal mit einem schlecht gesicherten Café-WLAN verbunden”
  - ⇒ Suche nach der “lowest hanging fruit”

Demo



- Vorstellung von „Tool“

Fragen?

Vielen Dank
für
Eure Aufmerksamkeit!

Benny Görzig (bgoerzig@gmail.com) & Florian Loch (me@fdlo.ch)

https://github.com/kastel-wpa2

Literatur & Quellen

[1] Jörg Rech. Wireless LANs : 802.11-WLAN-Technologie und praktische Umsetzung im Detail; 802.11a/h, 802.11b, 802.11g, 802.11i, 802.11n, 802.11d, 802.11e, 802.11f, 802.11s, 802.11ac, 802.11ad.

[2] SANS Institute. IEEE 802.11 Pocket Reference Guide.

[3] IEEE Computer Society: IEEE Std 802.11TM-2012 (Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications). 2012.

[4] Moshe Zviran: Password Security: An Empirical Study. 1999. URL: http://calhoun.nps.edu/bitstream/handle/10945/40319/haga_password_security.pdf?sequence=1

[5] Richard Shay. Correct horse battery staple: Exploring the usability of system-assigned passphrases. 2012. URL: https://cups.cs.cmu.edu/soups/2012/proceedings/a7_Shay.pdf

Literatur & Quellen

[6] J. Bonneau, E. Shutova. Linguistic properties of multi-word passphrases. 2012. URL: http://www.jbonneau.com/doc/BS12-USEC-passphrase_linguistics.pdf

[7] Benchmark von Sagitta Brutalis. URL: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

[8] Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. URL: http://papers.mathyvanhoef.com/asiaccs2016.pdf

[9] Short: How Talkative is your Mobile Device? An Experimental Study of Wi-Fi Probe Requests

https://frdgr.ch/wp-content/uploads/2015/06/Freudiger15.pdf

Bildquellen

https://openclipart.org/detail/3619/hammer Icon made by alst

https://openclipart.org/detail/262305/smartphone Icon made by ciubotaru

http://www.flaticon.com/free-icon/anonymous_14446 Icon made by Picol

https://openclipart.org/detail/17423/wirelesswifi-symbol Icon made by ispyisail

https://openclipart.org/detail/208540/laptop Icon made by jmlrtinez

https://de.wikipedia.org/wiki/Aircrack#/media/File:Aircrack-ng-new-logo.jpg

https://www.kali.org/wp-content/uploads/2015/05/kali-dragon-middle.png

https://de.wikipedia.org/wiki/Heartbleed#/media/File:Heartbleed.svg