

Wifi security

Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.





AI GENERATED

Wat leer je in dit hoofdstuk?

Na dit hoofdstuk kan je:

- ✓ **beveiligingsproblemen** van draadloos vs bedraad uitleggen (+ managementframes en PMF)
- ✓ de **kernfout van WEP** benoemen: dezelfde keystream twee keer gebruiken
- ✓ de evolutie **WEP → WPA1 → WPA2 → WPA3** technisch motiveren
- ✓ de **4-way handshake** kennen en **KRACK** zien als “WEP opnieuw”
- ✓ **WPA3** begrijpen: SAE, forward secrecy, PMF, Enhanced Open
- ✓ **enterprise mode** met **802.1X** en **eduroam**, en de evil-twin-fout

Vrijheid met een prijskaartje

Plots geraak je van overal in het gebouw op het netwerk. En zelfs **erbuiten**.

Een netwerkkabel heeft ingebouwde beveiliging: je hebt **fysieke toegang** nodig.

Met wifi ligt het bedrijfsnetwerk open in een straal van **tientallen meters**.

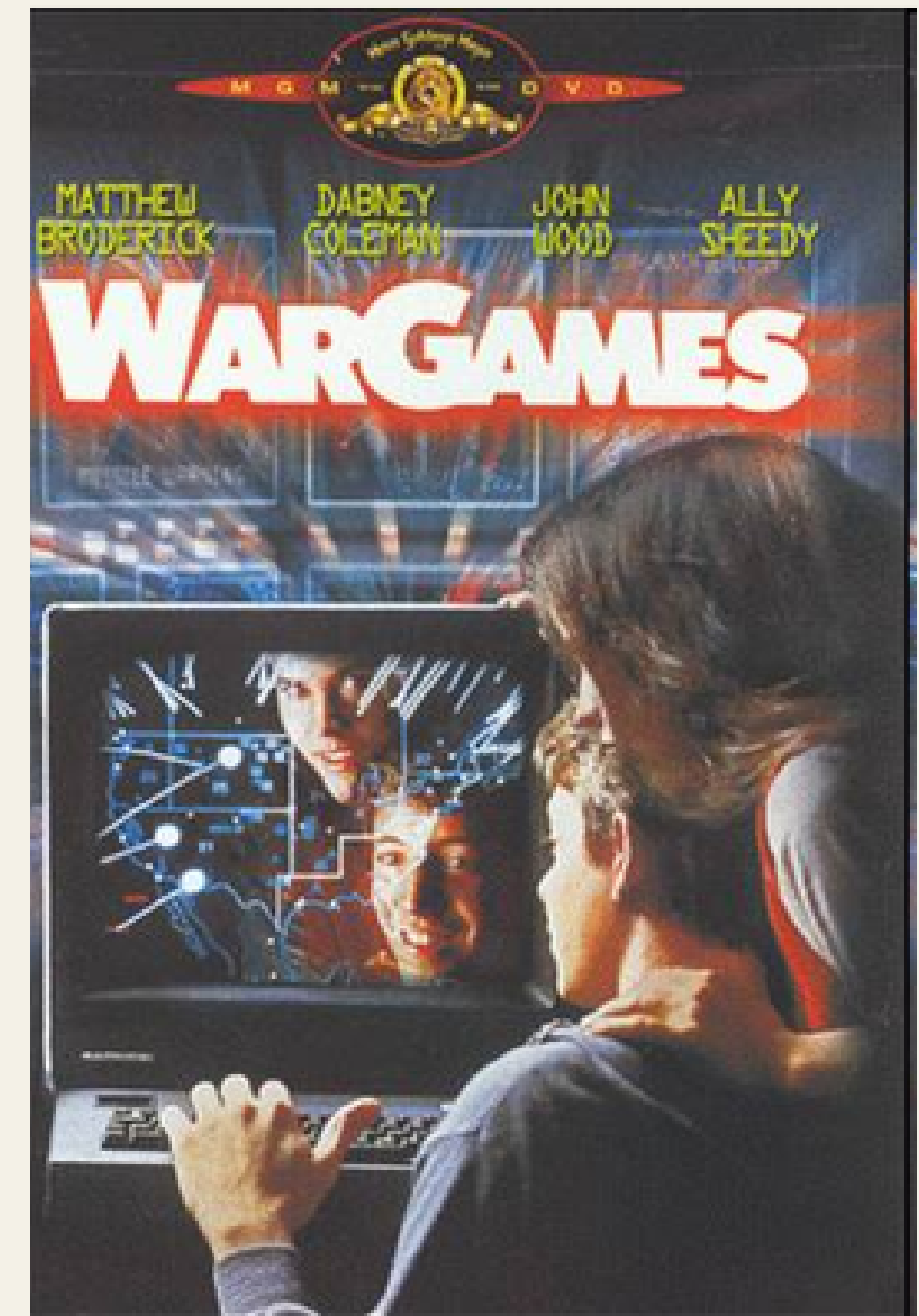


Wardriving

Rondrijden in de stad met een laptop die scant naar **draadloze netwerken**.

Extra aandacht voor netwerken met **geen of zwakke** beveiliging.

De term komt van *wardialing*, uit de cultfilm **Wargames** (1983).



Problemen met wifi



Eavesdropping

Iedereen kan “zien” wat er door de lucht vliegt. Het medium is letterlijk de lucht.



Invasion

Zonder beveiliging verbind je zomaar. Bij een kabel heb je fysieke toegang nodig.

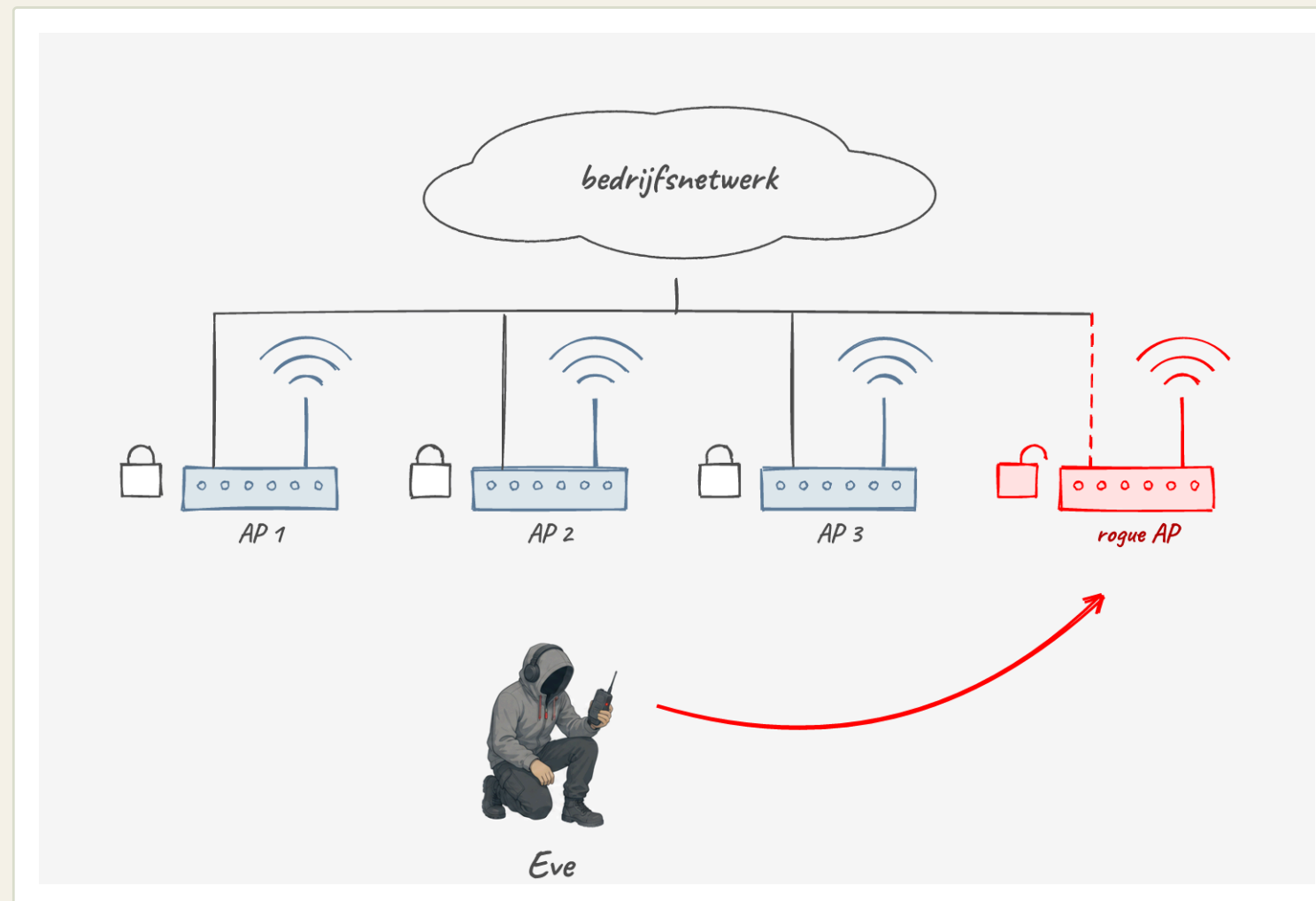


Man-in-the-middle

De aanvaller zet zich tussen jou en het netwerk. Daarover straks meer.

Daarbovenop: **rogue access points** als backdoor en **DoS** op fysiek niveau.

Rogue access points



Een rogue AP: de ideale backdoor voor hackers.

Goedbedoelde werknemers plaatsen zelf een (goedkoop) AP bij om het bereik uit te breiden.

Eén zwak beveiligd AP tussen tientallen goed beveiligde: de aanvaller kiest het **zwakste punt**.

Ruis op de frequentieband



Bedraad werkt met CSMA/**CD** (Collision Detection). Botsingen in de lucht zijn **niet te detecteren**, daarom Collision **Avoidance**.

Op de nieuwe **6 GHz**-band (Wifi 6E/7) is enkel WPA3 of Enhanced Open toegelaten.

MANAGEMENTFRAMES

In de 802.11-standaard zijn managementframes **niet beveiligd**. Geen CIA.

Ze regelen het beheer: `verbinden` `SSID broadcasten` `netwerk verlaten`
`handover`

Overgenomen van bedrade netwerken, waar fysieke beveiliging volstond.

Aanvallen via managementframes



Disassociation flooding

Valse “verlaat het netwerk”-frames → **DoS**.



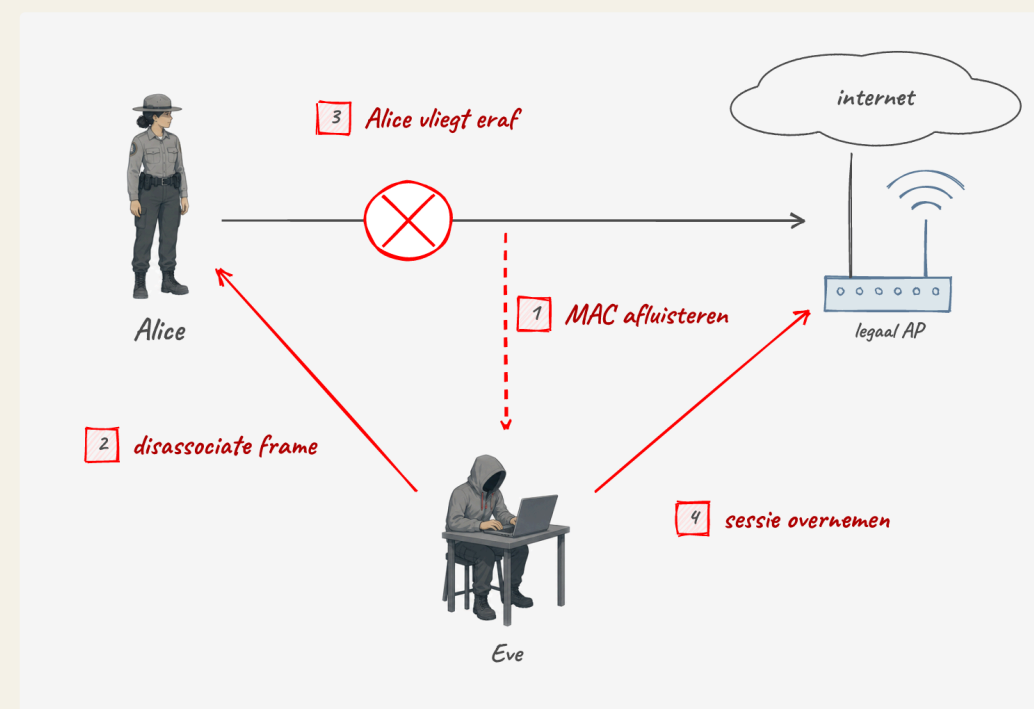
Identity spoofing

MAC-adres spoofen → **sessie overnemen**.



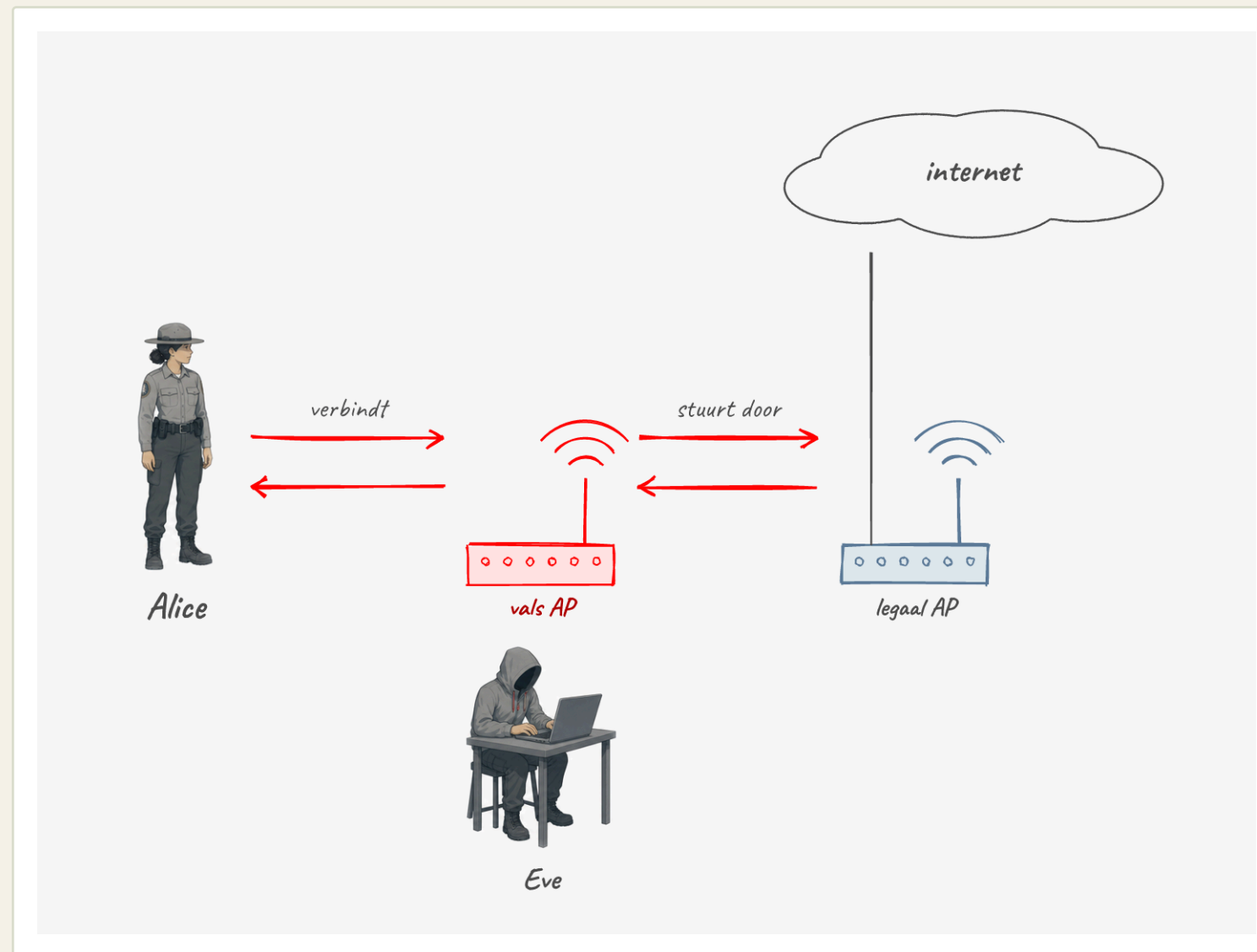
Impersonation

Fake AP opzetten → **MITM-aanval**.



Eve spooft de wifi-sessie van Alice.

Fake access points



Een fake AP voor een MITM-aanval.

Met een **Wifi Pineapple** (Hak5) zet je zo een fake hotspot op.

Klassieker: een fake **Telenet Wi-Free** met een gecloneerde loginpagina. Elke login levert een wachtwoord op. (Wi-Free stopte in 2023, het trucje werkt nog op elke hotspot met loginpagina.)

PROTECTED MANAGEMENT FRAMES

802.11w / PMF beveiligt de belangrijkste managementframes met een integriteitscheck.

Een valse “verlaat het netwerk” wordt genegeerd: de aanvaller kent de sleutel niet.

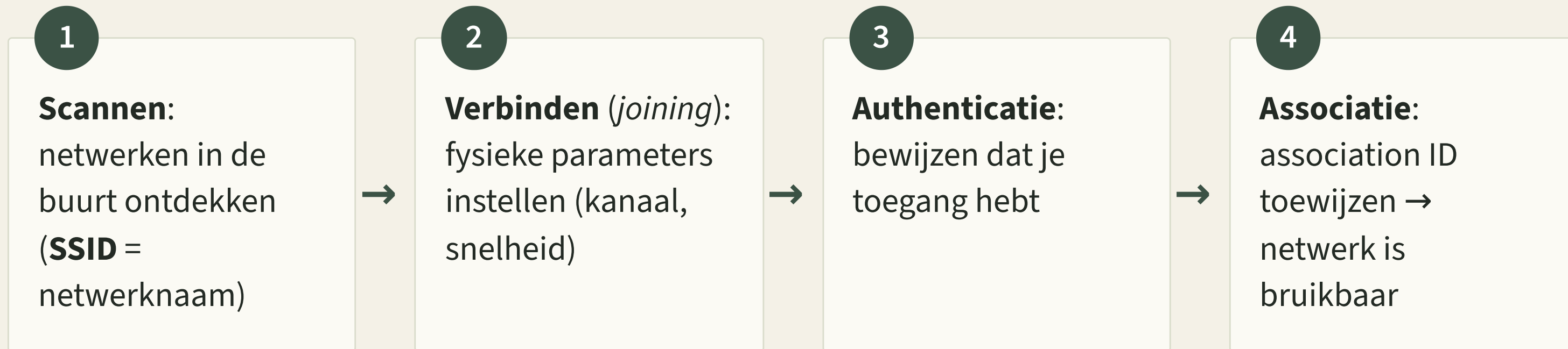
Optioneel sinds 2009, **verplicht in WPA3**. Beacons en probes blijven wel onbeschermd.

802.11 · 1997/1999

De originele standaard

Hoofdstuk 8, *Authentication and privacy*: **10 van de 528** pagina's.

Verbinden met een wifi-netwerk



Dat loopt allemaal via de onbeveiligde managementframes.

SSID VERBERGEN?

SSID-broadcasting uitschakelen is **snake oil**.

Het SSID zit ook in een hoop andere pakketjes. Een wifi-hacker plukt het er zo uit.

Authenticatie in 802.11



Open-system

Geen authenticatie: de client vraagt, het AP zegt “welkom”.



Shared-key

Challenge-response met de **WEP-sleutel**.



MAC-ACL

Whitelist van MAC-adressen.
Niet in de standaard, wel bij veel fabrikanten.

Origineel **geen mutual authentication**: je kan zomaar verbinden met een fake AP.

Shared-key authentication

1

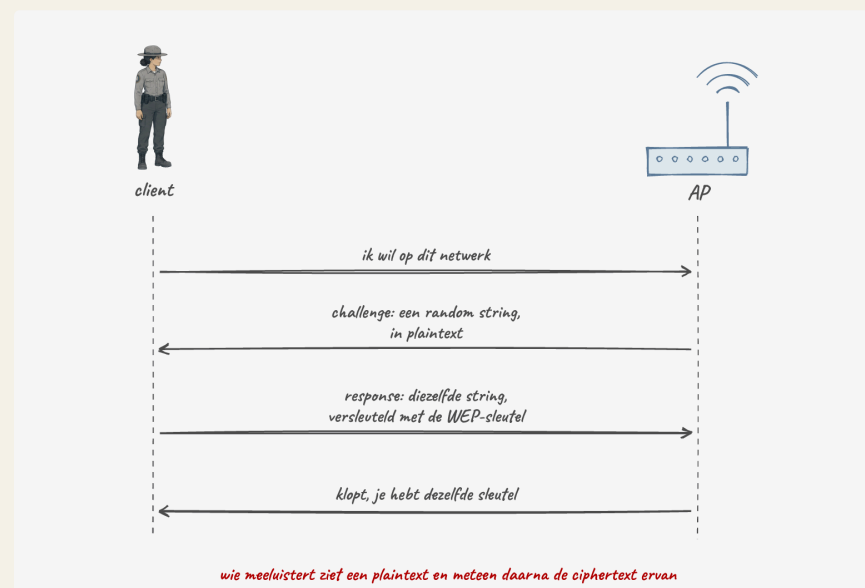
AP stuurt een random **challenge** (plaintext)

2

Client encrypteert met de **WEP-sleutel** en stuurt de **response** terug

3

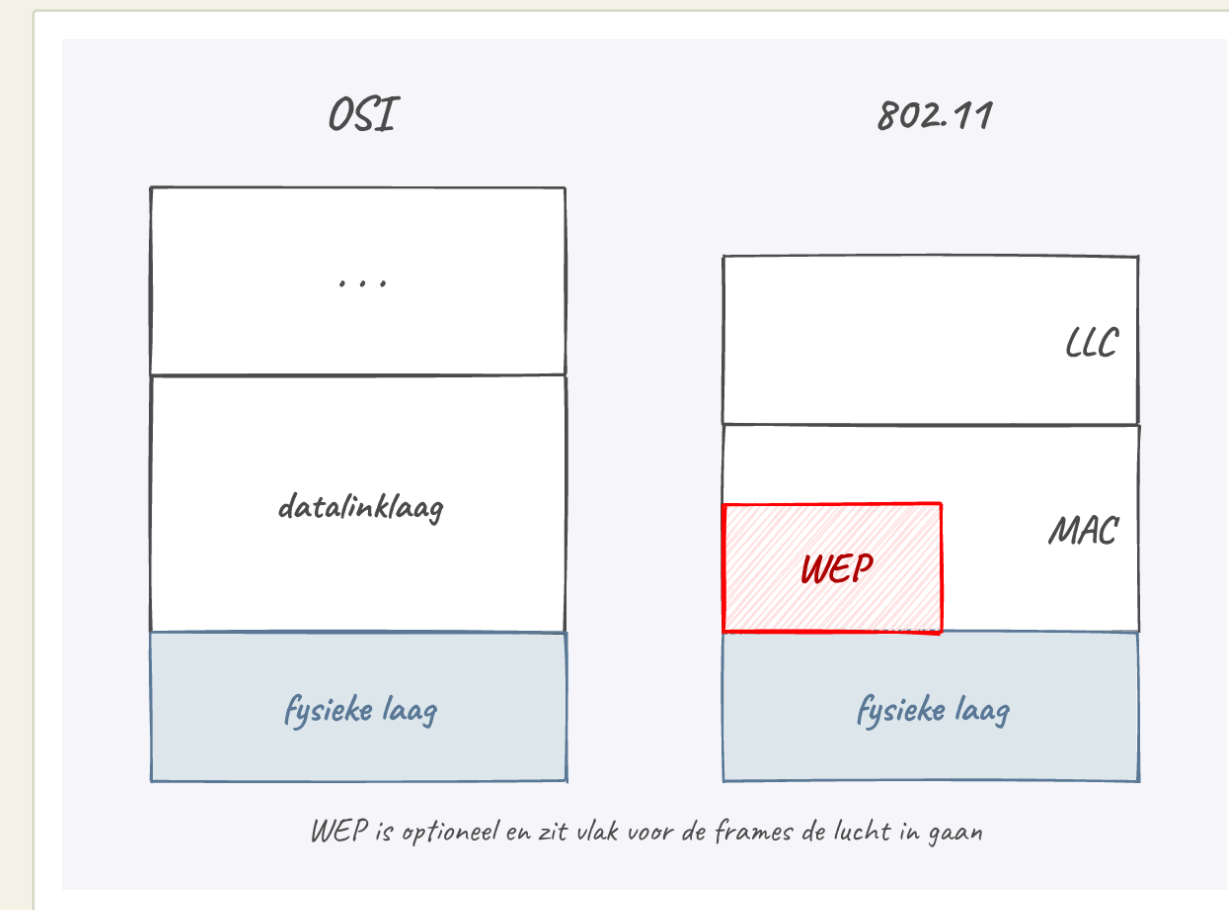
AP decrypteert en vergelijkt:
match = toegang



Wie meesnift, ziet **plaintext én ciphertext**: een gekende-plaintextaanval. Oh ironie: open-system is daardoor **veiliger**.

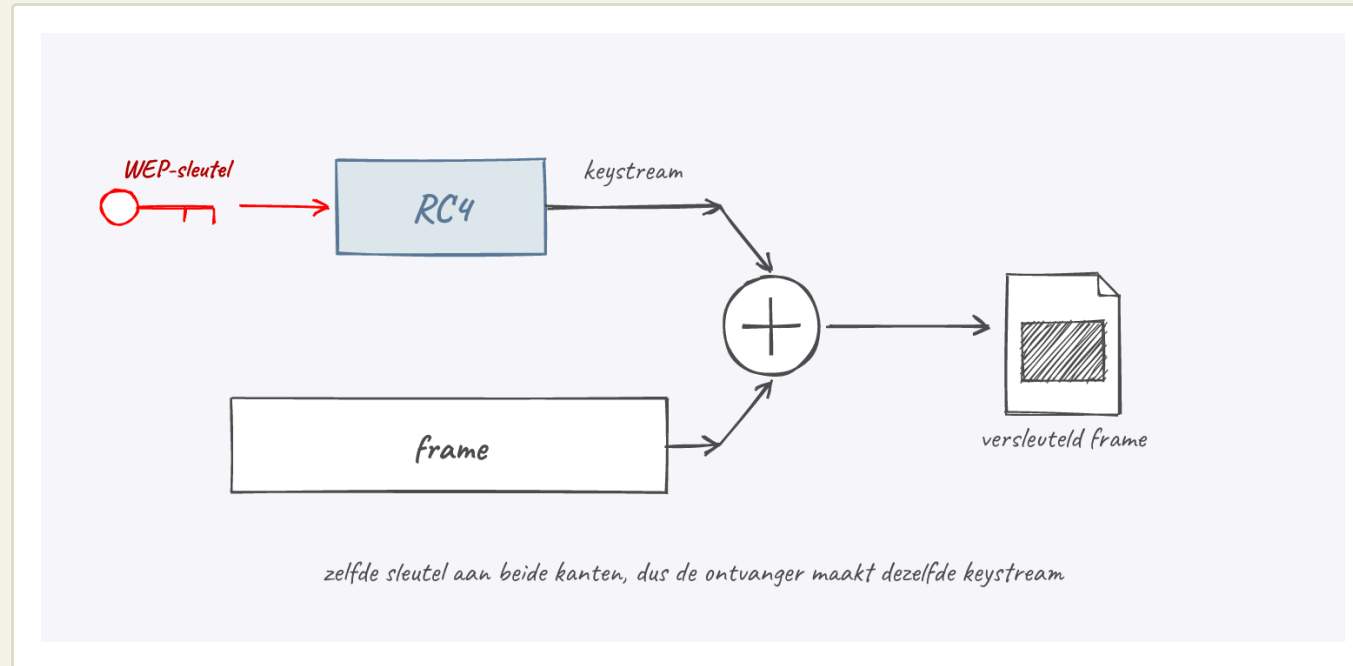
WEP

- Belofte: even veilig als een **bedraad** netwerk
- Hart: de **RC4**-streamcipher
- WEP-sleutel = seed voor de keystream
- Keystream $\oplus$ frame = ciphertext
- **Optioneel**: veel netwerken gebruikten het niet eens



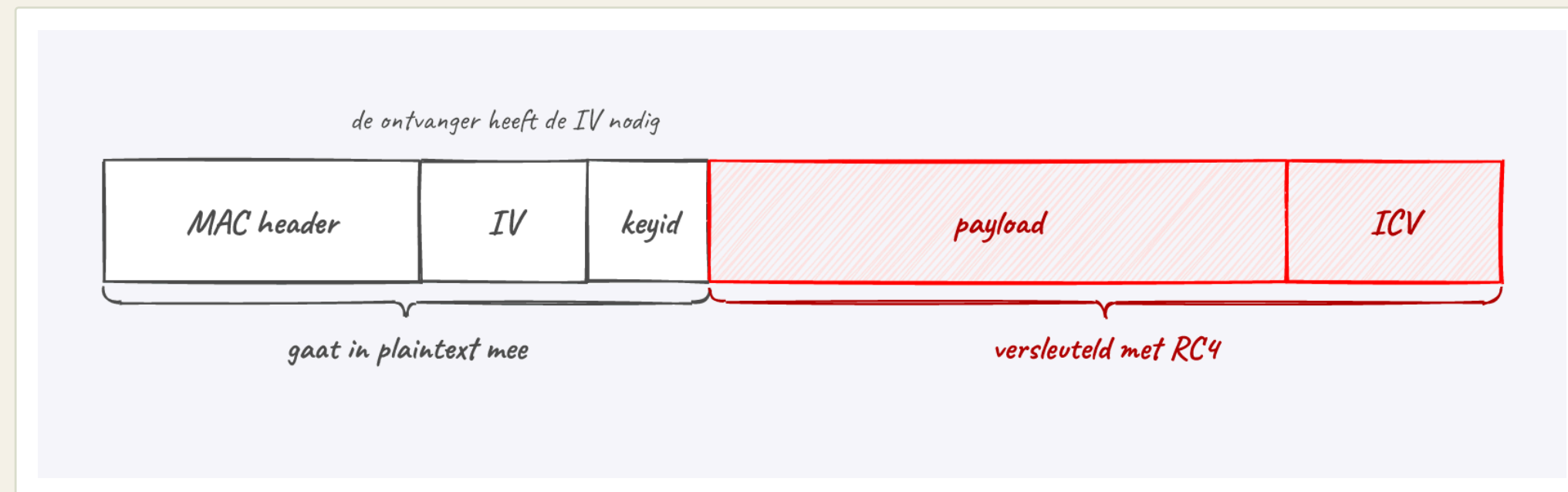
WEP in de 802.11 stack.

WEP: encryptie en integriteit



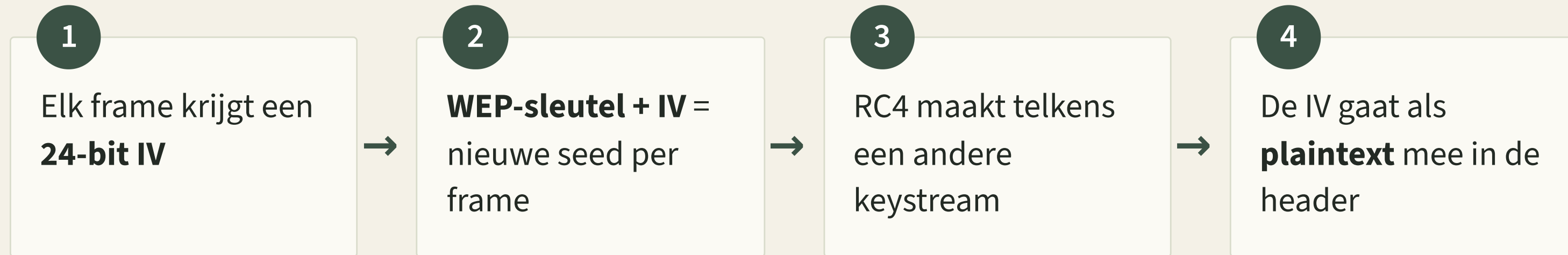
- **CRC-32** genereert een **ICV** (Integrity Check Value)
- De ICV wordt mee geëncrypteerd door RC4
- Frame aanpassen → ICV ongeldig (in theorie...)

WEP encryptie.



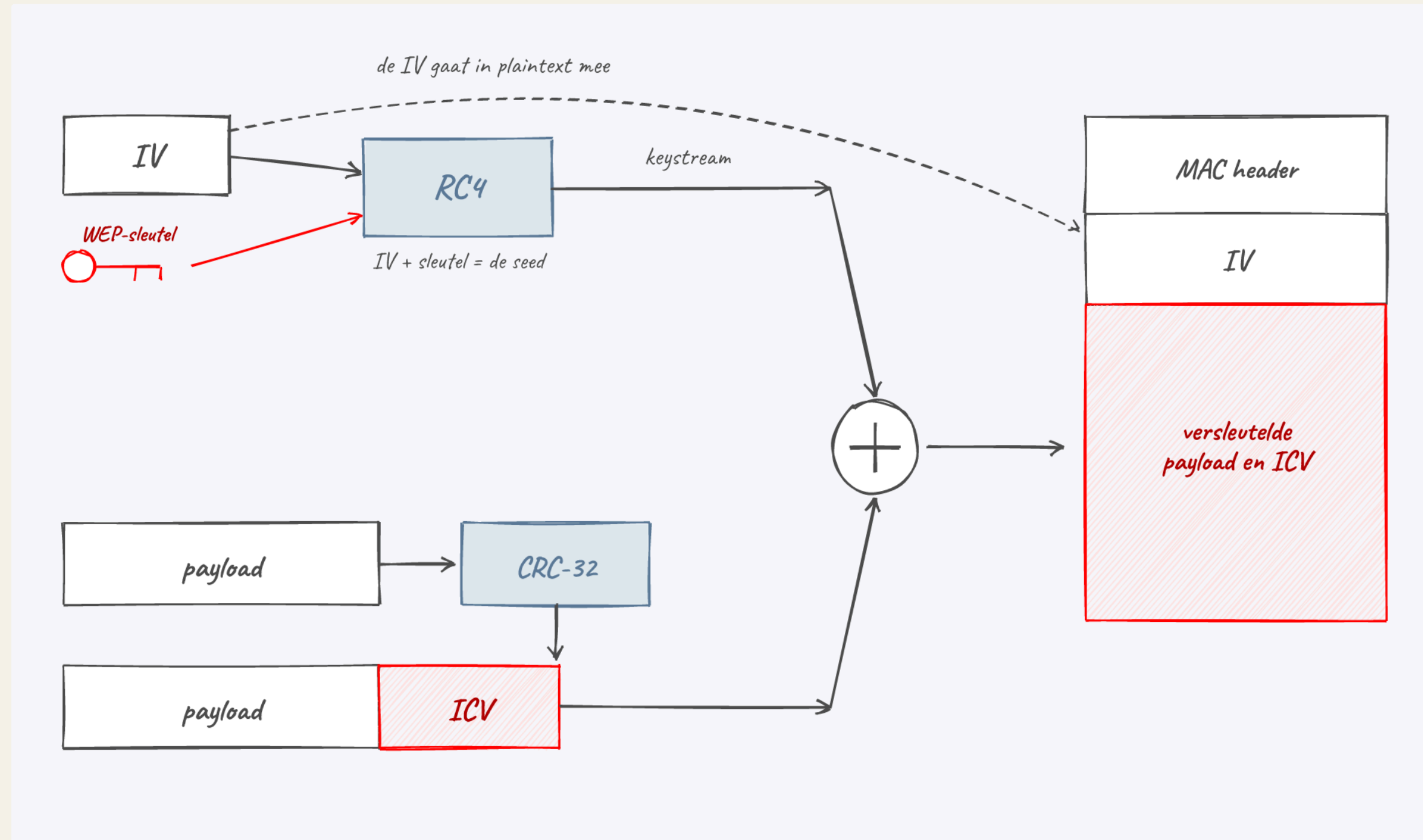
De initialisatievector (IV)

Zelfde sleutel = **zelfde keystream** voor elk frame. Dat kan niet.



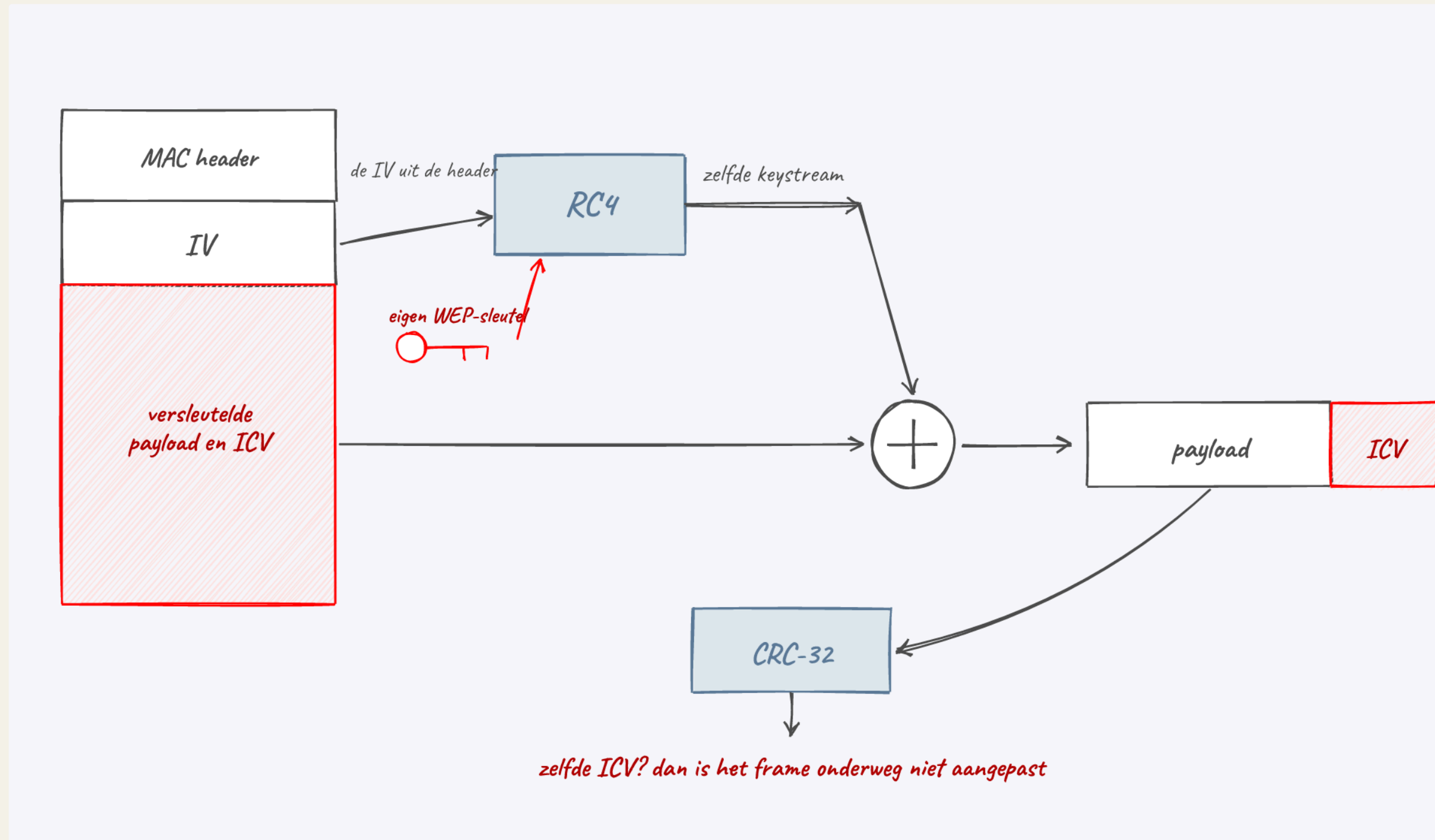
Een sleutel verlengen met een getal heet **salting**. Dat zie je terug in het hoofdstuk over authenticatie.

WEP: encryptie



WEP encryptie.

WEP: decryptie



WEP decryptie.

EEN HORRORVERHAAL

Hoe WEP faalde

Kort na de eeuwwisseling geraakte je in bijna elk wifi-netwerk binnen, enkele jaren later zelfs in **enkele minuten**.

Vier grote problemen



1. RC4

Streamcipher die geen **sleutelhergebruik** verdraagt.



2. IV

Te klein en slecht gespecificeerd: **weak keys** en **collisions**.



3. CRC-32

Lineair: **bitflip-aanvallen** mogelijk.



4. Sleutels

Geen re-keying, geen centraal **sleutelbeheer**.

En een vijfde die alles versterkt: **geen replay protection**. De aanvaller mag pakketjes onbeperkt heruitzenden en gebruikt je netwerk als experimenteertuin.

PROBLEEM 1 · RC4

Dezelfde keystream **twee keer** gebruiken bij een streamcipher is fataal.

$$(p_i \oplus k_i) \oplus (q_i \oplus k_i) = p_i \oplus q_i$$

De **sleutel valt weg**. Ken je één plaintext, dan is de andere triviaal te berekenen. En $k_i = c_i \oplus p_i$ geeft de keystream cadeau. WEP probeert dit op te lossen met de IV... maar ook dat gaat fout.

Weak keys: de FMS-aanval

Fluhrer, Mantin & Shamir (2001): sommige IV's zorgen voor **sleutellekkage** naar de keystream.



Implementaties: Airsnort WEPCrack

Collisions

Twee pakketjes met dezelfde IV = dezelfde keystream.

16,7 mln

mogelijke IV's (2^{24})

916/s

pakketjes bij 11 Mbps en frames
van 1500 bytes

± 5 uur

en alle IV's zijn op: **collisions
gegarandeerd**

$$\frac{16.777.216}{916 \text{ pakketten/s}} \approx 18.302 \text{ s} \approx 5 \text{ uur}$$

IV collisions misbruiken

Passief

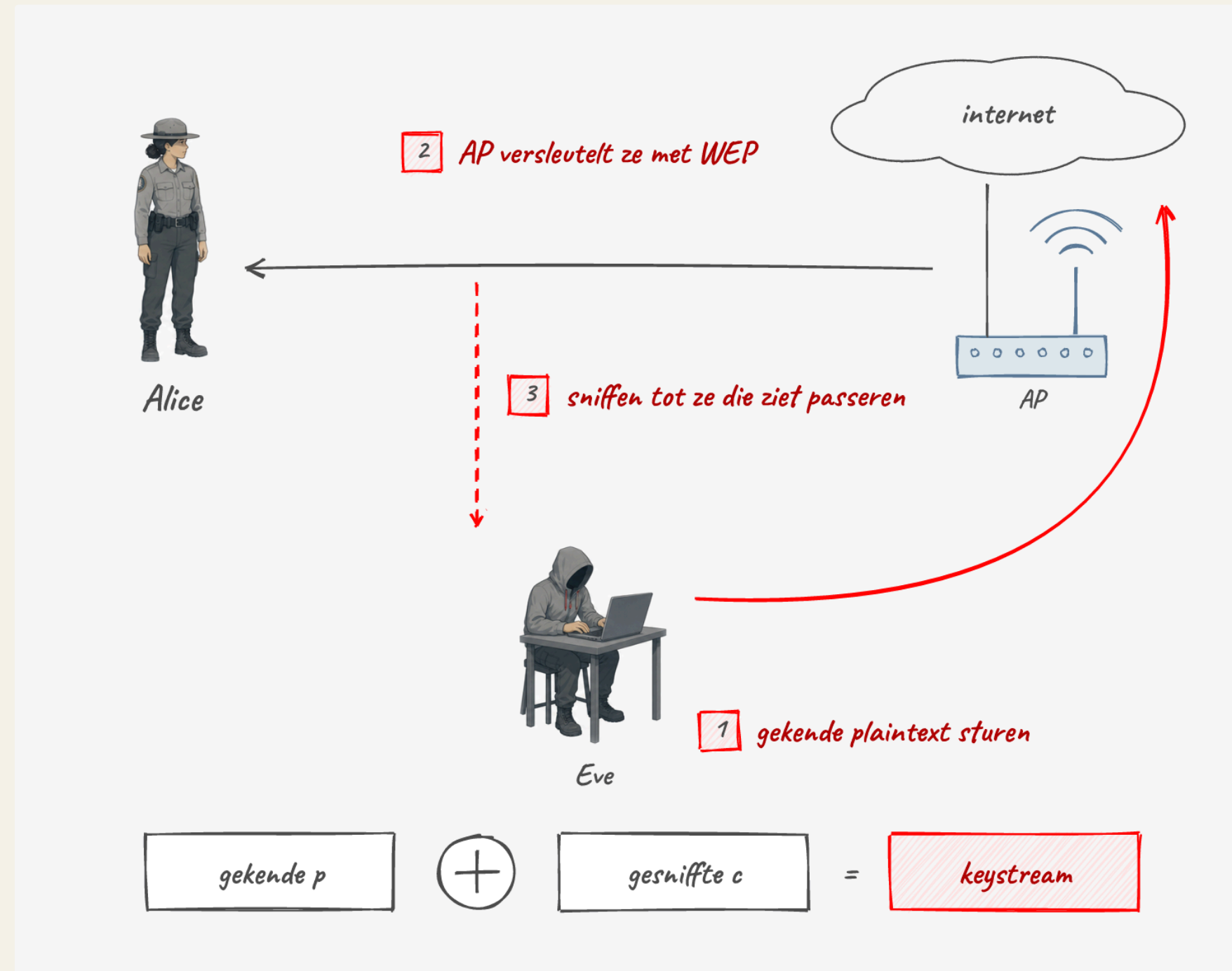
- Meeluisteren tot er een IV collision is
- Twee pakketten met dezelfde IV XOR'n → XOR van beide plaintexts
- IP-trafiek is voorspelbaar → cryptanalyse

vs

Actief

- Gekende plaintext van buitenaf naar het AP sturen (bv. ping)
- Ciphertext sniffen
- $k_i = c_i \oplus p_i \rightarrow \textbf{keystream!}$

Gekende plaintext injecteren

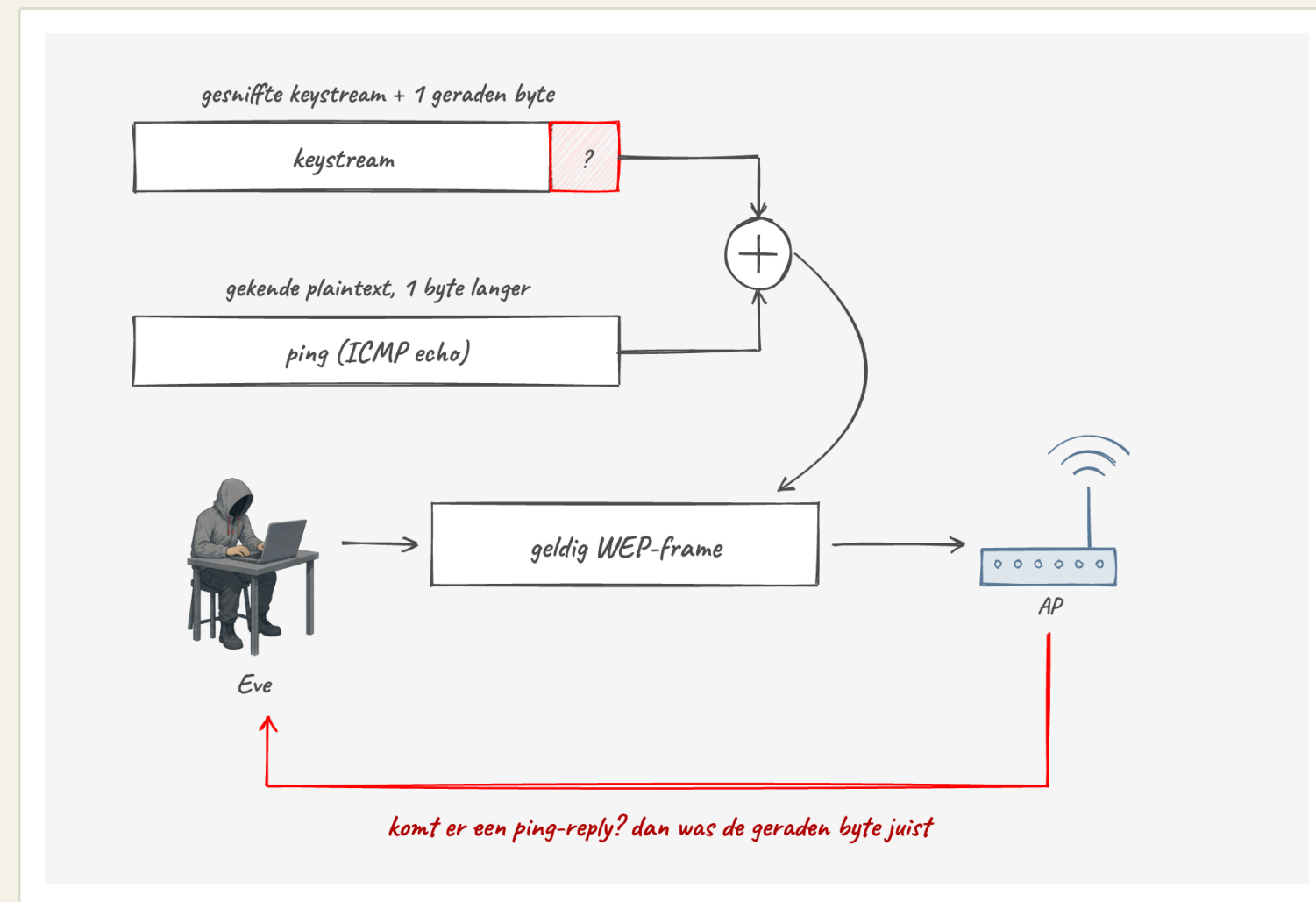


Known plaintext injecteren.

Keystreams laten groeien

Geen replay protection: de aanvaller laat een keystream **byte per byte** groeien.

1. Ping die **1 byte langer** is dan de keystream
2. Willekeurige byte achter de keystream plakken (1 kans op 256)
3. XOR'n en versturen
4. Reactie? **Juiste byte!** Geen reactie? Volgende proberen



Keystreams groeien.

De verjaardagenparadox

23

mensen: dan is er al **meer dan 50%** kans dat twee dezelfde verjaardag hebben

~5000

pakketjes met een willekeurige 24-bit IV: **meer dan 50%** kans op een collision

CRC is geen MAC

Een CRC heeft **geen sleutel**: iedereen kan er een berekenen. Voor integriteit heb je een **MAC** nodig: een *message authentication code*, niet te verwarren met een MAC-adres (daarom zegt men bij wifi **MIC**). En CRC-32 is bovendien lineair:

$$CRC(m_1) \oplus CRC(m_2) = CRC(m_1 \oplus m_2)$$

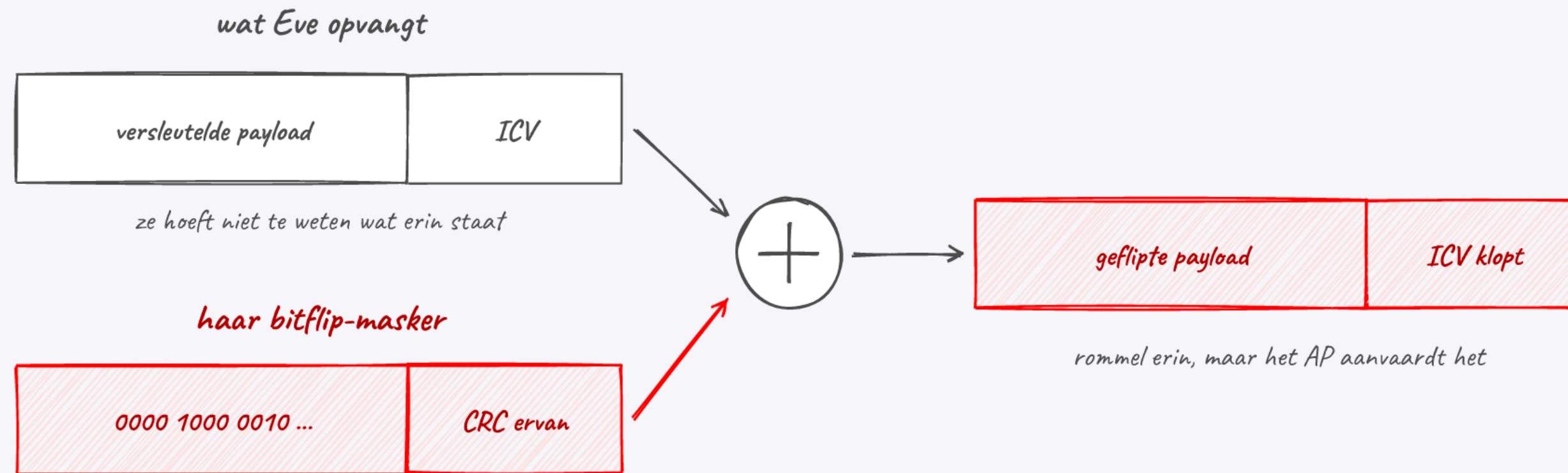
Gevolg: je kan een pakket **gecontroleerd** aanpassen zonder de CRC te breken.

De bitflip-aanval



Het AP aanvaardt het frame omdat de ICV klopt, ook al is de inhoud **rommel**.

Bitflip-aanval: visualisatie

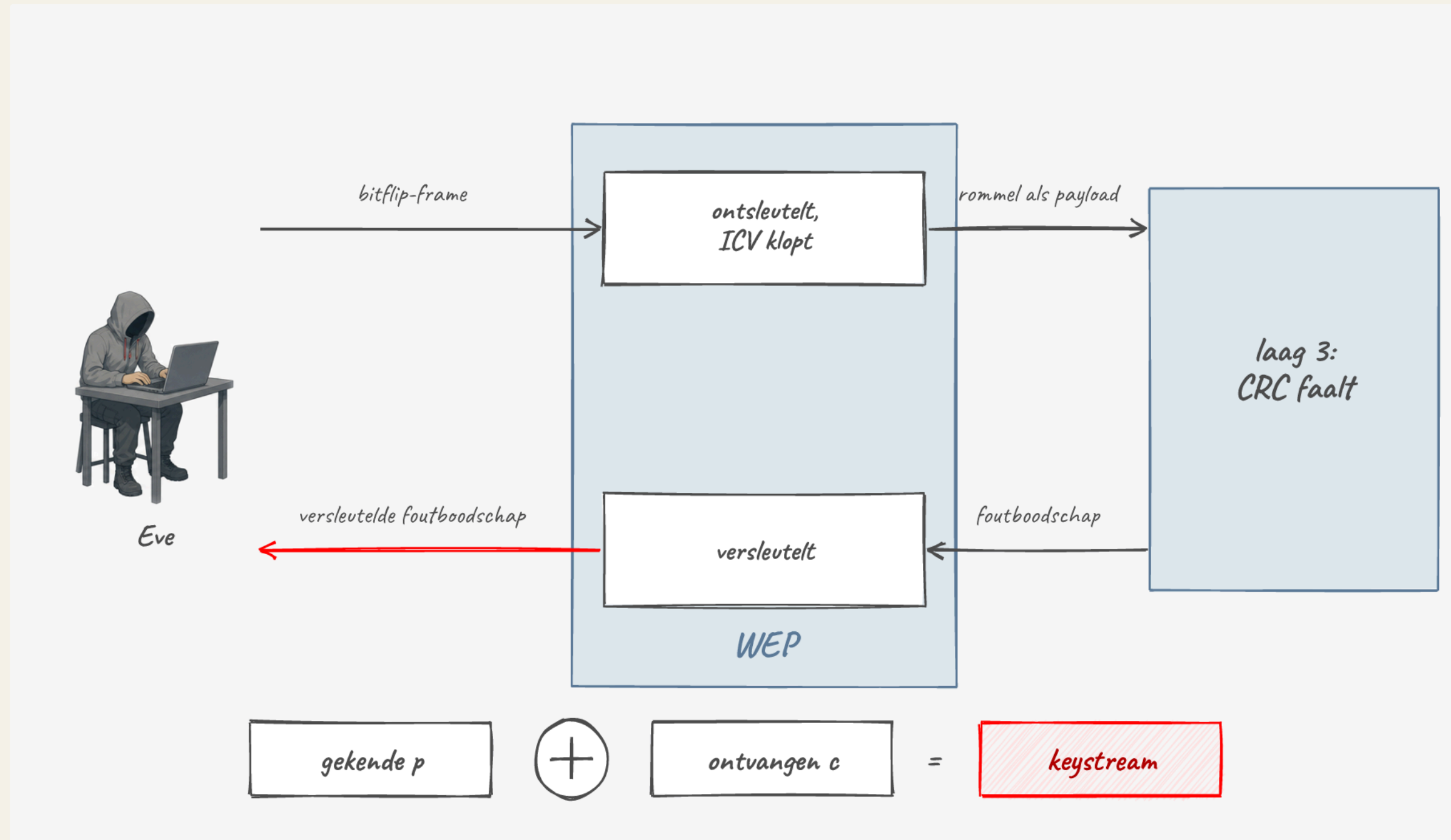


CRC-32 is lineair: $CRC(a) \text{ XOR } CRC(b)$ is hetzelfde als $CRC(a \text{ XOR } b)$

dus flipt de ICV netjes mee en blijft het frame geldig

De bitflip aanval.

Bitflip-aanval: gekende foutboodschappen



Corrupte pakketjes genereren gekende foutboodschappen.

Sleutelmanagement

Maandenlang **dezelfde WEP-sleutel** op alle apparaten. Een ontslagen werknemer is een potentieel lek, en admins vervangen sleutels **manueel**.

- ✗ Geen **geautomatiseerd re-keying**-mechanisme
- ✗ Geen **gecentraliseerd** sleutelbeheer

“

WEP is het perfecte schoolvoorbeeld van wat er fout loopt wanneer je zelf een crypto-algoritme ontwikkelt.

— Bart Preneel, KUL/COSIC

2001

WEP oplossen

Miljoenen WEP-apparaten in gebruik en dringend een oplossing nodig.

Twee pistes



WPA1

Tijdelijke oplossing. Werkt op bestaande hardware via een **firmware-update**.



WPA2

De **ultieme** oplossing. Volledig nieuwe protocollen, **nieuwe hardware** vereist.

WPA is geen IEEE-standaard, maar een **certificering** van de Wifi Alliance (WPA2 = 802.11i).

Personal of enterprise?

Zowel WPA1 als WPA2 bestaan in twee modes.

Personal

- Gedeelde sleutel: **pre-shared key** (PSK)
- Voor thuisgebruik
- Geen 802.1X

vs

Enterprise

- **802.1X**
- Centraal sleutelbeheer
- Voor bedrijven

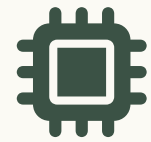
Overzicht: WEP → WPA1 → WPA2 → WPA3

Standaard	Encryptie	Integrity	Auth & sleutelbeheer
WEP	RC4	CRC-32	Geen
WPA1	TKIP (RC4)	Michael	PSK of 802.1X
WPA2	CCMP (AES)	CBC-MAC	PSK of 802.1X
WPA3	CCMP/GCMP (AES)	CBC-MAC of GMAC	SAE of 802.1X + PMF

Personal = pre-shared key (PSK). Enterprise = 802.1X.

WPA1: de beperkingen

WPA1 is een wrapper rond WEP, met drie randvoorwaarden:



Firmware-update

Miljoenen bestaande apparaten moeten via een update mee kunnen.



Minimale overhead

AP's draaiden al op **maximale capaciteit**.



Vast aan WEP

RC4 zit deels **hardwired** in de hardware.

TKIP: de WEP-wrapper van WPA1



Michael (MIC)

Tegen het **CRC-32**-probleem (bitflips).



IV-regels

Tegen **replay**-aanvallen.



Key mixing

Per pakket, tegen **weak keys** in RC4.

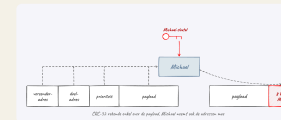


Re-keying

Eigen sessiesleutel per client, **geregeld ververs**t.

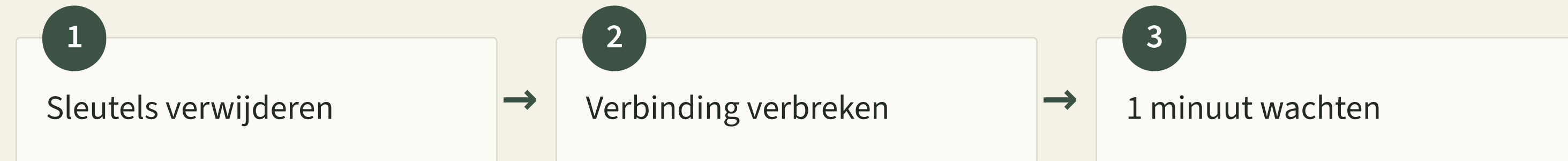
Michael: de MIC

Cryptografisch sterker dan CRC-32: payload + **Michael-sleutel** + adres van verzender en ontvanger.



MIC generatie met Michael.

Twee foute MICs binnen de minuut? **Aanval gedetecteerd!**



Die noodrem is meteen een **DoS**: twee foute pakketjes en niemand geraakt binnen. Samen met de zwakke Michael en de Beck-Tews-aanval (2008) werd TKIP in 2012 **afgevoerd**.

TKIP: een betere IV

24 bit

de IV bij WEP

48 bit

de IV bij TKIP: de *TKIP Sequence Counter* (TSC)

En een **strikte volgorde**: een pakket met een lagere IV dan het vorige wordt geweigerd. Dat houdt replay-aanvallen tegen.

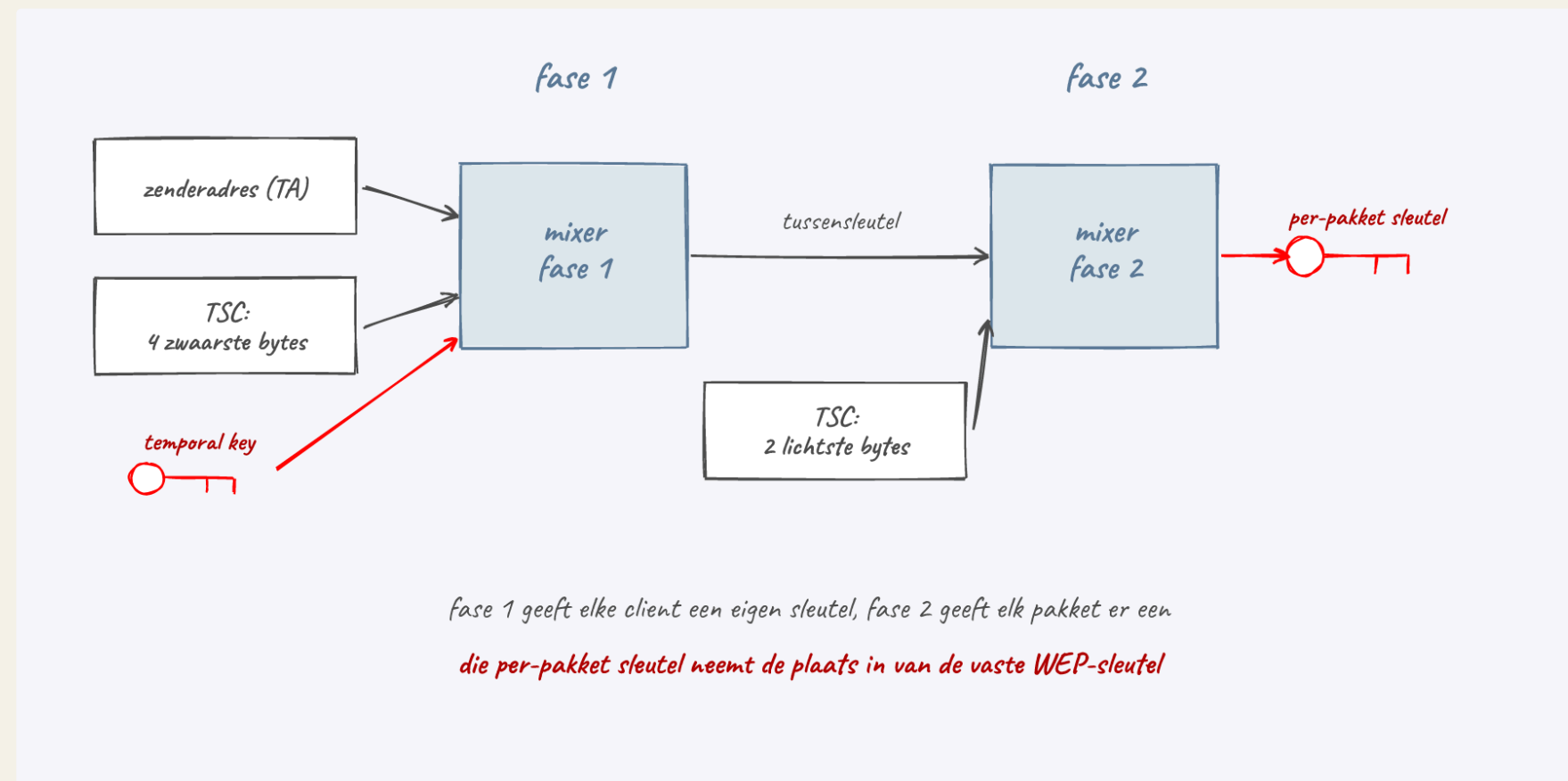
TKIP: key mixing in twee fases

1

Fase 1: sessiesleutel + **MAC-adres van de verzender** + deel van de teller (TSC) → tussensleutel (uniek per client)

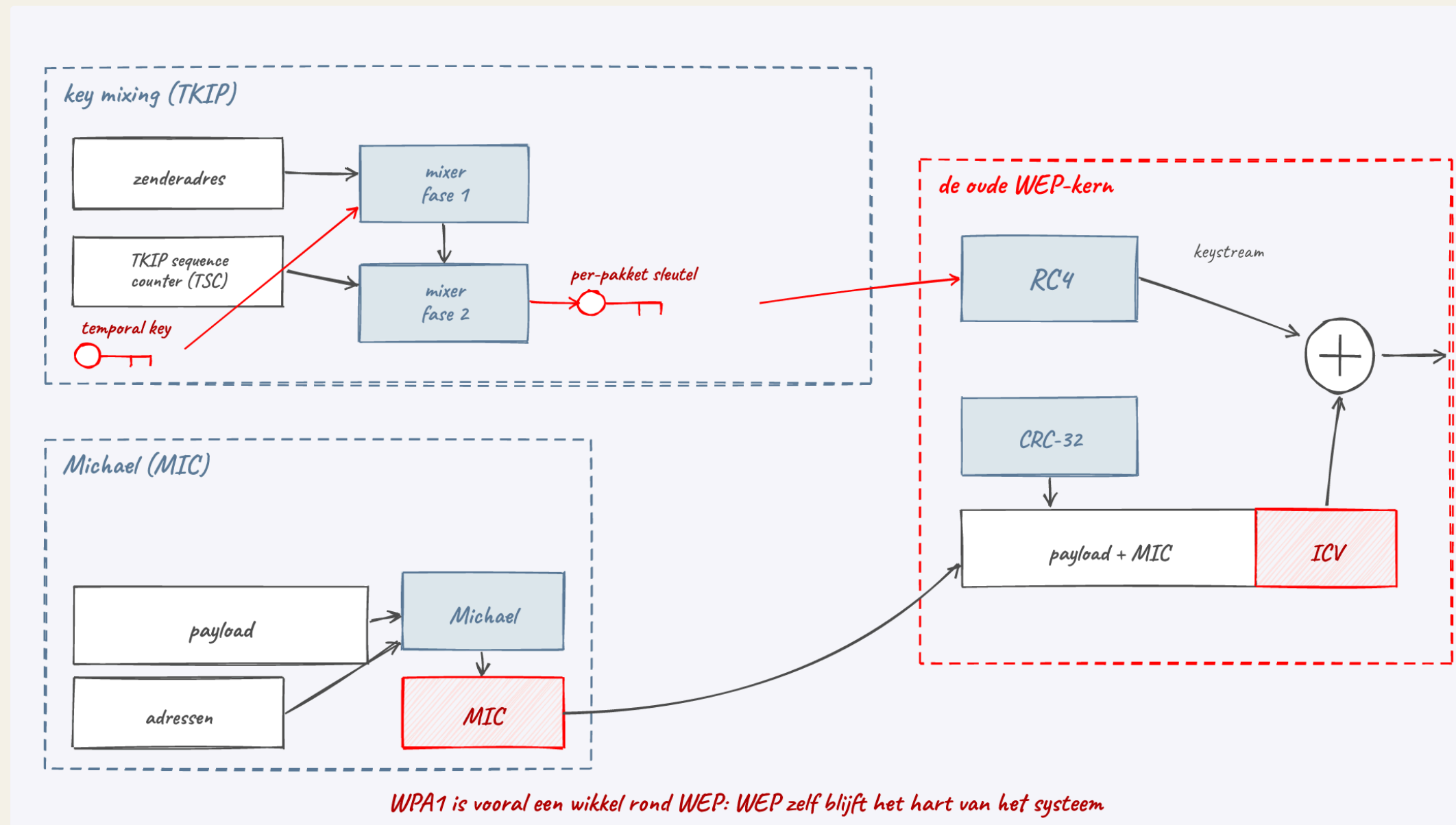
2

Fase 2: tussensleutel + rest van de teller → **per-pakket RC4-sleutel**



Key mixing proces.

WPA1: het totaalplaatje



WPA1 in volle glorie: een wrapper rond WEP.

WPA1-Personal kraken via de handshake: coWPAtty Aircrack

AES ALS HART

WPA2 en WPA3

WPA2: AES vervangt RC4

Eindelijk geen streamcipher meer. WPA2 combineert twee AES-modes:



AES Counter mode

Encryptie: blokken onafhankelijk van elkaar.

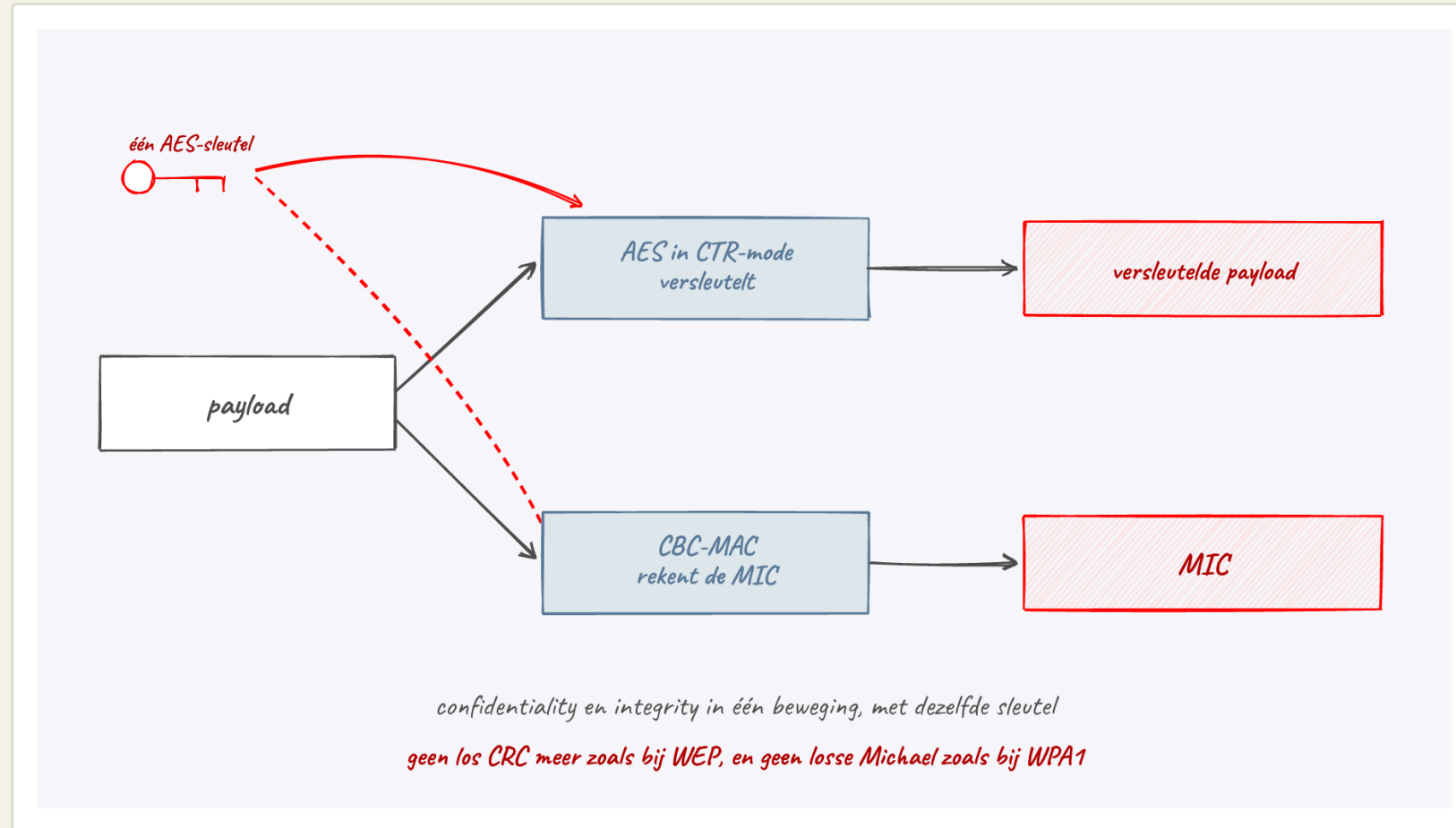


AES CBC-MAC

Integriteit: berekent de MIC.

Samen: **CCMP**, *Counter Mode Cipher Block Chaining Message Authentication Code Protocol*.

CCMP: elegant

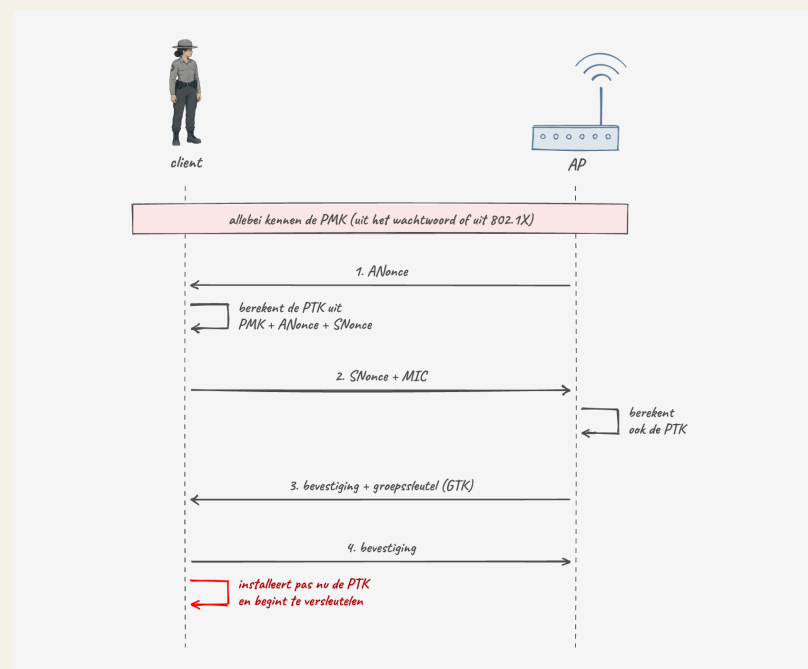


- **CBC-MAC:** keten van encrypties, het finale blok = MIC
- **Counter mode:** blokken onafhankelijk, een payload counter als extra seed
- 48-bit IV (*packet number*)

CCMP: confidentiality en integrity parallel.

De 4-way handshake

Voor er data versleuteld wordt, leiden client en AP een verse sessiesleutel (**PTK**) af uit een gedeelde **PMK**.



Twee nonces = elke sessie een andere sleutel. Onthoud: gaat bericht 4 verloren, dan stuurt het AP **bericht 3 opnieuw** en installeert de client de sleutel nog eens. **Hier ging KRACK spelen.**

PERSONAL MODE

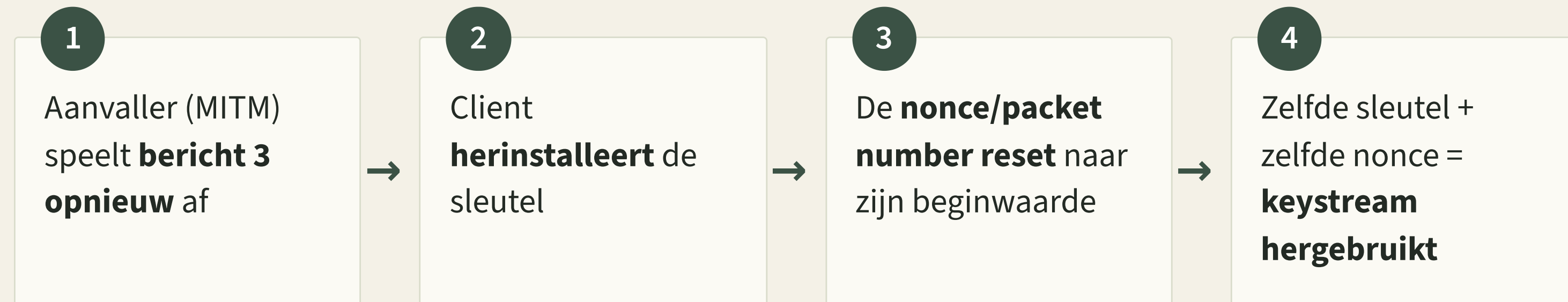
Iedereen met de passphrase (die ook de handshake van een ander opvangt) kan de data van **andere gebruikers** decrypteren.

In **enterprise mode** is dat onmogelijk.

WPA2-Personal is ook **altijd al** te kraken via een **offline dictionary-aanval** op de gesnifte handshake. Sinds 2018 (**PMKID**) zelfs zonder verbonden client. Kies een lang, willekeurig wachtwoord.

KRACK: WEP komt terug spoken

De Belgische onderzoeker **Mathy Vanhoef** vindt een fout in de **4-way handshake** (niet in AES).



Exact de fout van WEP (probleem 1), nu in **AES-CTR**. Patchbaar, dus WPA3 is géén noodreactie.

KRACK: de teller springt terug

normaal



elk pakketje een volgend nummer, dus een andere keystream

na KRACK



*bericht 3 opnieuw afgespeeld:
sleutel herinstalleerd, teller terug op 1*

*zelfde sleutel + zelfde nonce = zelfde keystream,
net als een IV-botsing bij WEP*

KRACK

De les van WEP was nooit “RC4 is slecht”, maar
“**hergebruik nooit een keystream**”.

Twintig jaar later dook diezelfde fout op in WPA2, met een veel beter cipher.
Een sterk algoritme kiezen is niet genoeg: je moet het **correct gebruiken**.

2018

WPA3: state of the art

Verplicht voor elk nieuw Wi-Fi CERTIFIED-toestel sinds juli 2020. **≠ Wifi 6** (dat is snelheid, 802.11ax).



SAE (Dragonfly)

Diffie-Hellman met het wachtwoord: offline dictionary wordt **online**.



Forward secrecy

Oude opgenomen trafiek blijft veilig, ook als het wachtwoord later lekt.



PMF verplicht

Geen deauth-floods meer (802.11w).



Enhanced Open (OWE)

Publieke hotspot, maar iedere client een **eigen sleutel**. Aparte certificering. Authenticeert het AP **niet**: een evil twin blijft mogelijk.

WPA3: 6 GHZ EN TRANSITION MODE

Op de nieuwe **6 GHz**-band (Wifi 6E/7) is enkel **WPA3** (of Enhanced Open) toegelaten.

Elders draait vaak **transition mode** (WPA2 + WPA3 samen). Handig, maar een aanvaller kan een toestel dan naar het zwakkere **WPA2 downgraden**.

Vanhoef na KRACK



Dragonblood (2019)

Side-channel in SAE:
wachtwoord toch te raden.
Downgrade in transition
mode.



FragAttacks (2021)

Fouten in
fragmentatie/aggregatie,
deels al sinds **1997** (WEP
t.e.m. WPA3).



SSID Confusion (2024)

De **netwerknnaam** wordt niet
altijd geauthenticeerd:
verbinden met een ander
netwerk dan getoond.

Vier keer dezelfde Belgische hoek.

ENTERPRISE MODE

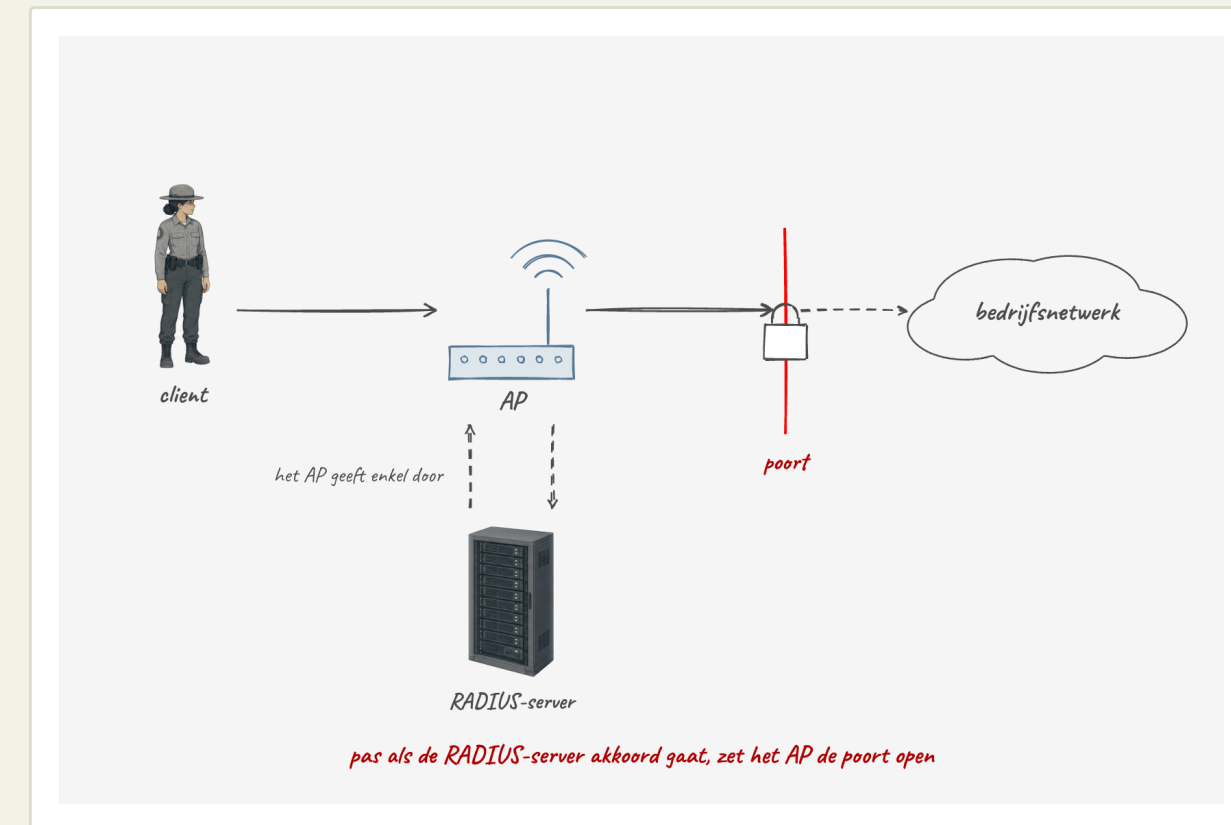
802.1X

Iedere gebruiker een eigen account en eigen sleutels. Je gebruikt het elke dag:
eduroam.

802.1X: een framework

- ✓ (Mutual) **authentication**
- ✓ **Centraal user management** (RADIUS-server: *Remote Authentication Dial-In User Service*)
- ✓ Veilige **sleuteluitwisseling**

Het AP is enkel een **doorgeefluik** naar de RADIUS-server. Je plukt er een **EAP**-methode in.



Port-based authenticatie.

EAP-methoden



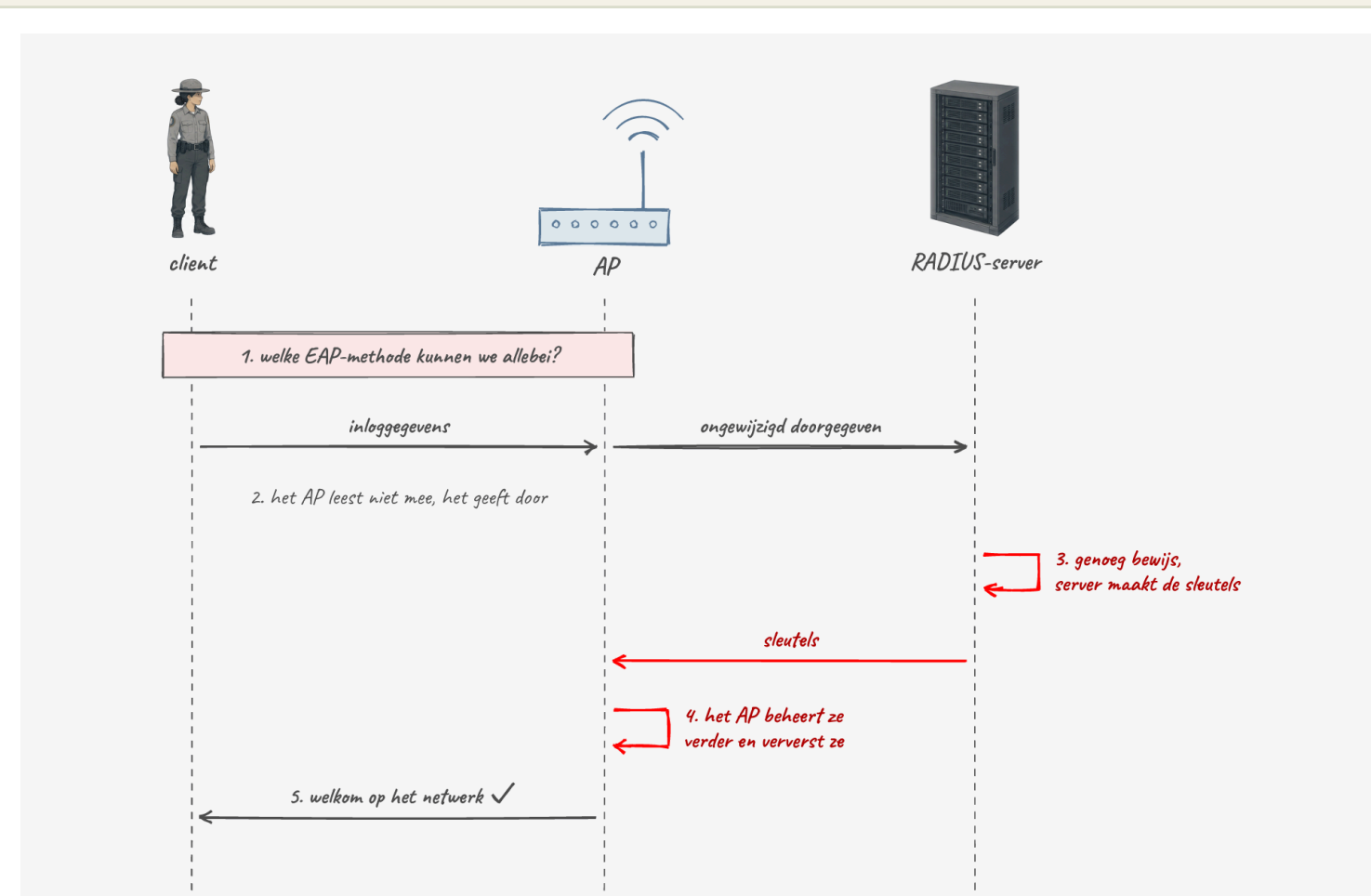
EAP-TLS

TLS-handshake met een **certificaat** aan beide kanten. Veiligst.

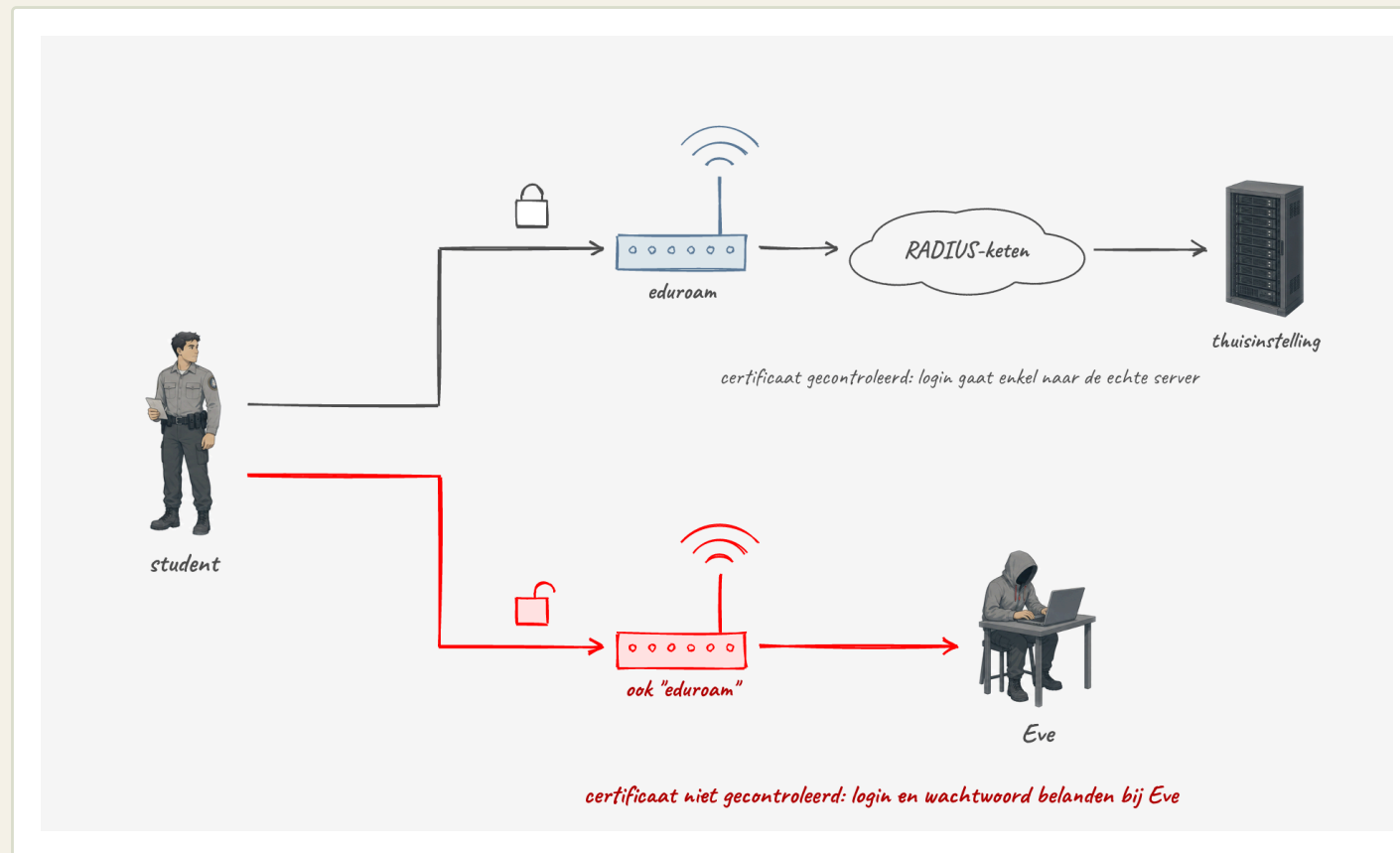


EAP-TTLS / PEAP

TLS-tunnel met **servercertificaat** + **username/wachtwoord**. Wat eduroam meestal gebruikt.



eduroam: de klassieke fout



Een evil twin die ook “eduroam” heet.

Je login reist via RADIUS naar je **eigen instelling**, veilig door de TLS-tunnel.

Maar: valideert je toestel het **servercertificaat** niet, dan oogst een **evil twin** (“eduroam”) je wachtwoord.

Daarom: **eduroam CAT** / **geteduroam** gebruiken, nooit “certificaat niet valideren”.

Conclusie

WEP	fundamenteel gebroken (RC4, IV, CRC, geen sleutelbeheer)
WPA1	tijdelijke patch (TKIP), een wrapper rond WEP
WPA2	AES/CCMP + 4-way handshake, sterk maar KRACK (keystream-hergebruik, net als WEP)
WPA3	SAE, forward secrecy, PMF, Enhanced Open. Enkel WPA3 (of Enhanced Open) op 6 GHz
802.1X	enterprise met eigen sleutels per gebruiker (eduroam); valideer het servercertificaat

Wat neem je mee?

- ✓ **WPA3** waar mogelijk
- ✓ **Enterprise-mode** in een bedrijf
- ✓ Een **sterk wachtwoord** in personal mode
- ✓ AP's **gepatcht**

- ✗ **WEP** en **WPA1**
- ✗ SSID verbergen als “beveiliging”