Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys

Mathy Vanhoef and Frank Piessens, iMinds-DistriNet, KU Leuven

DistriNet
iMinds KU LEUVEN

Security of Wi-Fi group keys?

Protect broadcast and multicast Wi-Fi frames:

- All clients share a copy of the group key

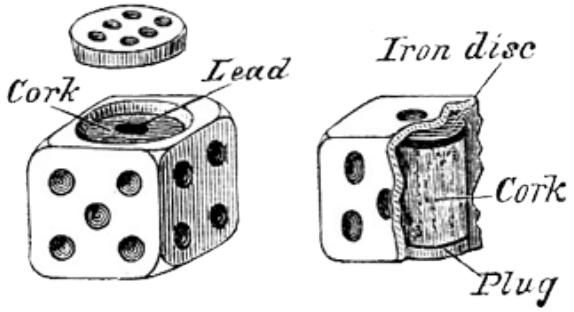
Security of groups keys not yet properly investigated!

- In contrast with preshared & pairwise keys …

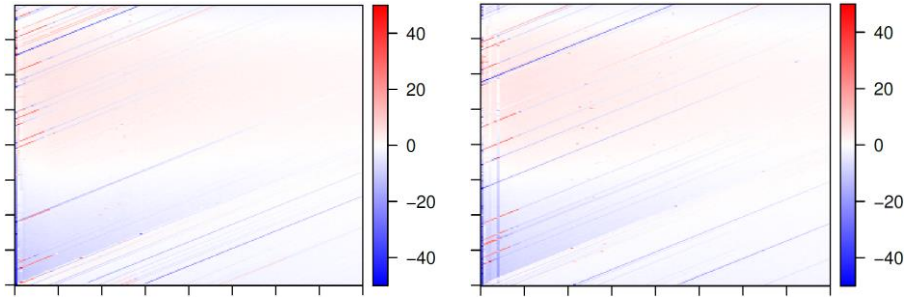
Analyze security of group key during its full lifetime!

DistriNet iMinds KU LEUVEN

Contributions: Security of Group Keys

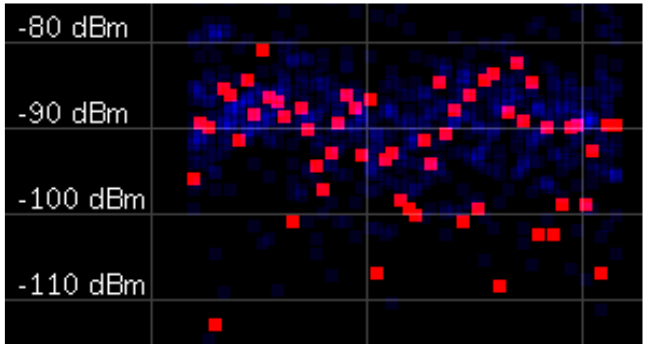


Flawed generation



Force RC4 in handshake

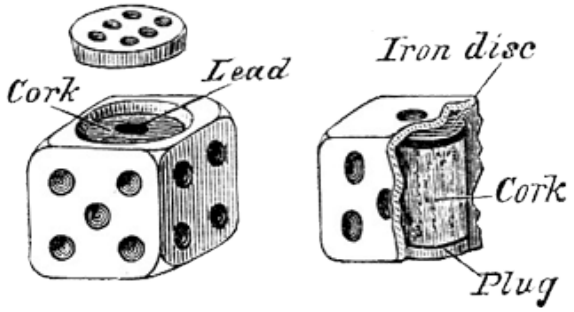
Inject & decrypt all traffic



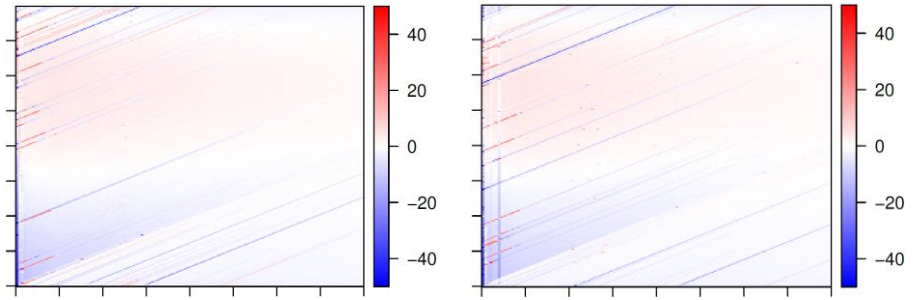
New Wi-Fi tailored RNG

DistriNet
iMinds
KU LEUVEN

Contributions: Security of Group Keys

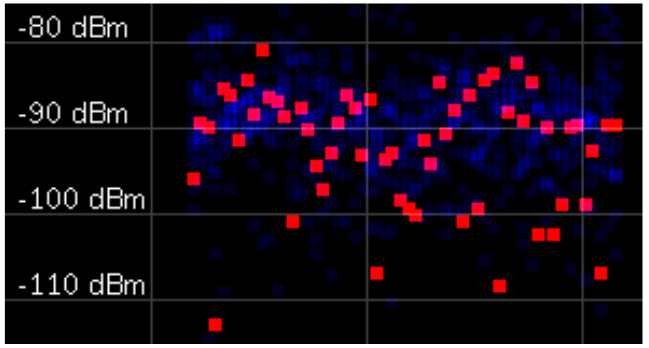


Flawed generation



Force RC4 in handshake

Inject & decrypt all traffic



New Wi-Fi tailored RNG

DistriNet
iMinds
KU LEUVEN

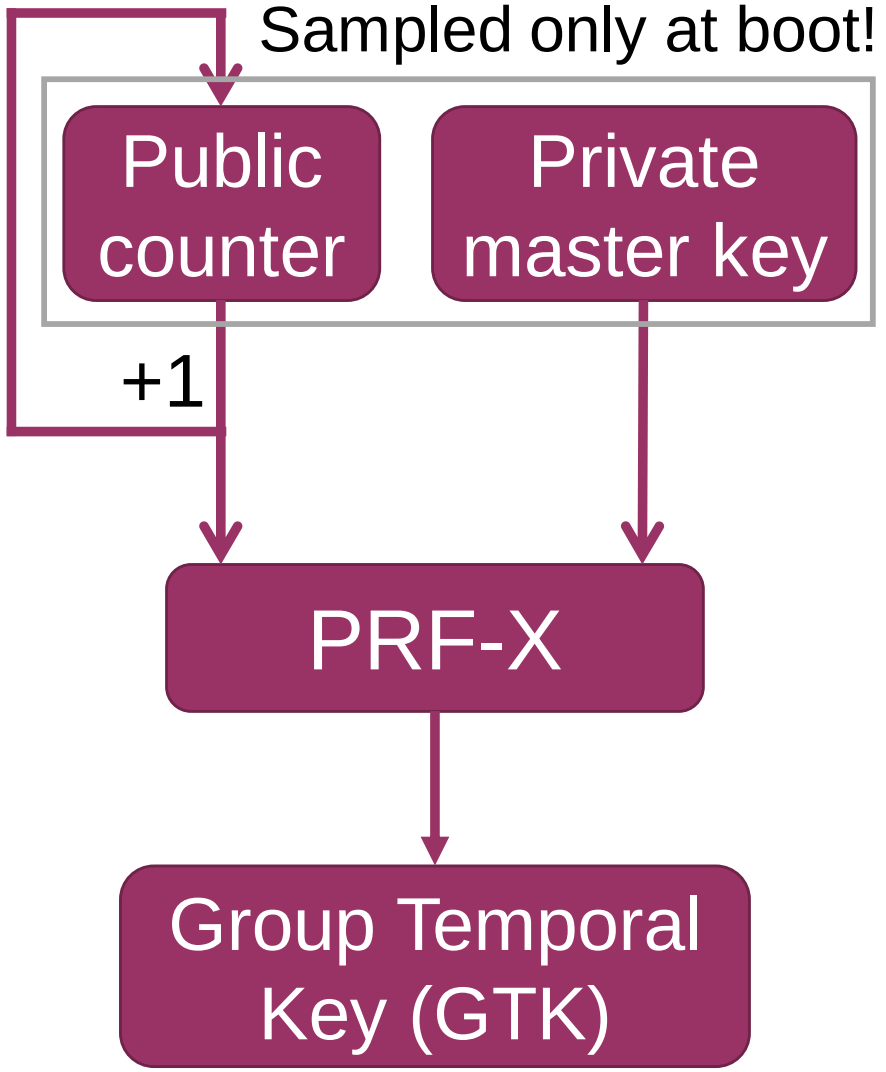
How are group keys generated?

Group key hierarchy:

- AP generates public counter and secret master key
- Derive group temporal keys (GTKs)

Entropy only introduced at boot

- If master key is leaked, all group keys become known



How are random numbers generated?

802.11 standard has example Random Number Generator

- §11.1.6a: "… can generate cryptographic-quality randomness"
- Annex M.5: "This solution is expository only"

Inconsistent description of RNG's security guarantees!

- How secure is the design of the 802.11 RNG?
- How many platforms implement this RNG?

802.11 RNG: Main Design

The 802.11 RNG is a stateless function returning 32 bytes

- Collects entropy on-demand
- Entropy extracted from frame arrival times and clock jitter

Deviates from traditional RNG design:

- No entropy pools being maintained
- Entropy only extracted from events when the RNG is being invoked

802.11 RNG: Entropy sources

Frame arrival times:

- Collected by repeatedly starting & aborting 4-way handshake
- Problem: AP is blacklisted after several handshake failures

Clock jitter and drift:

- Note: Router's current time is leaked in beacons
- Problem: No minimum time resolution → small clock jitter

Surely no one implemented this...?

Weakened 802.11 RNG

Depends on OS

Surely no one implemented this…?

Weakened 802.11 RNG

Depends on OS

MediaTek RNG: Linux-based APs

Uses custom Linux drivers:

- Implements 802.11's RNG using only clock jitter
- Uses *jiffies* for current time: at best millisecond accuracy

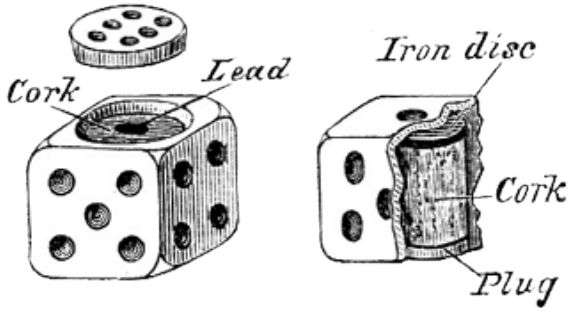
RT-AC51U

OpenCL

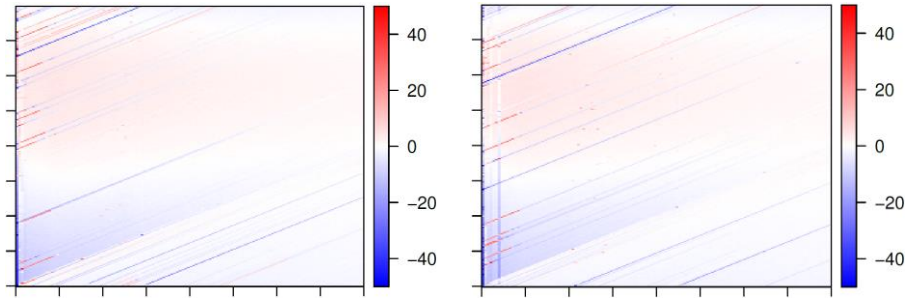
~3 mins

GMK & GTK

Contributions: Security of Group Keys

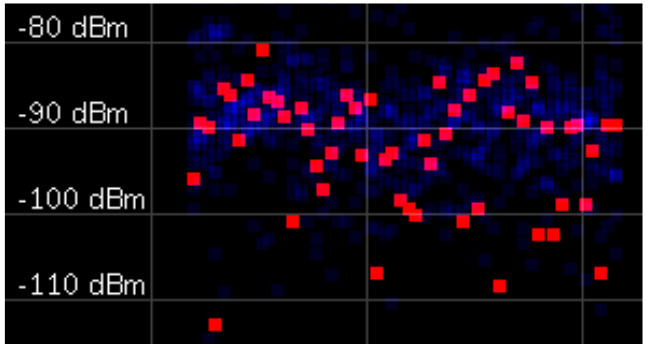


Flawed generation



Force RC4 in handshake

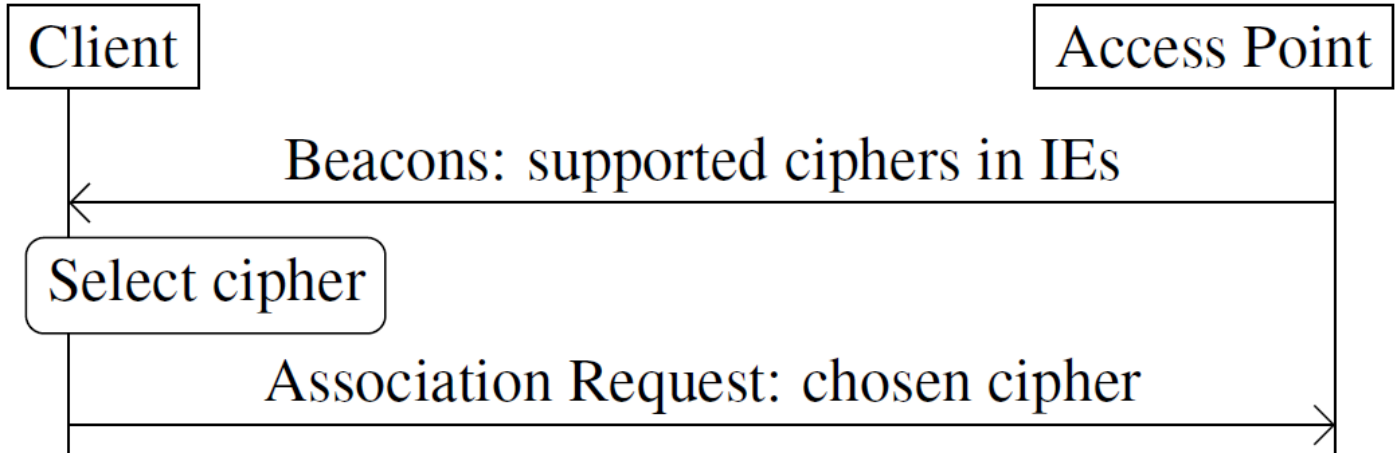
Inject & decrypt all traffic



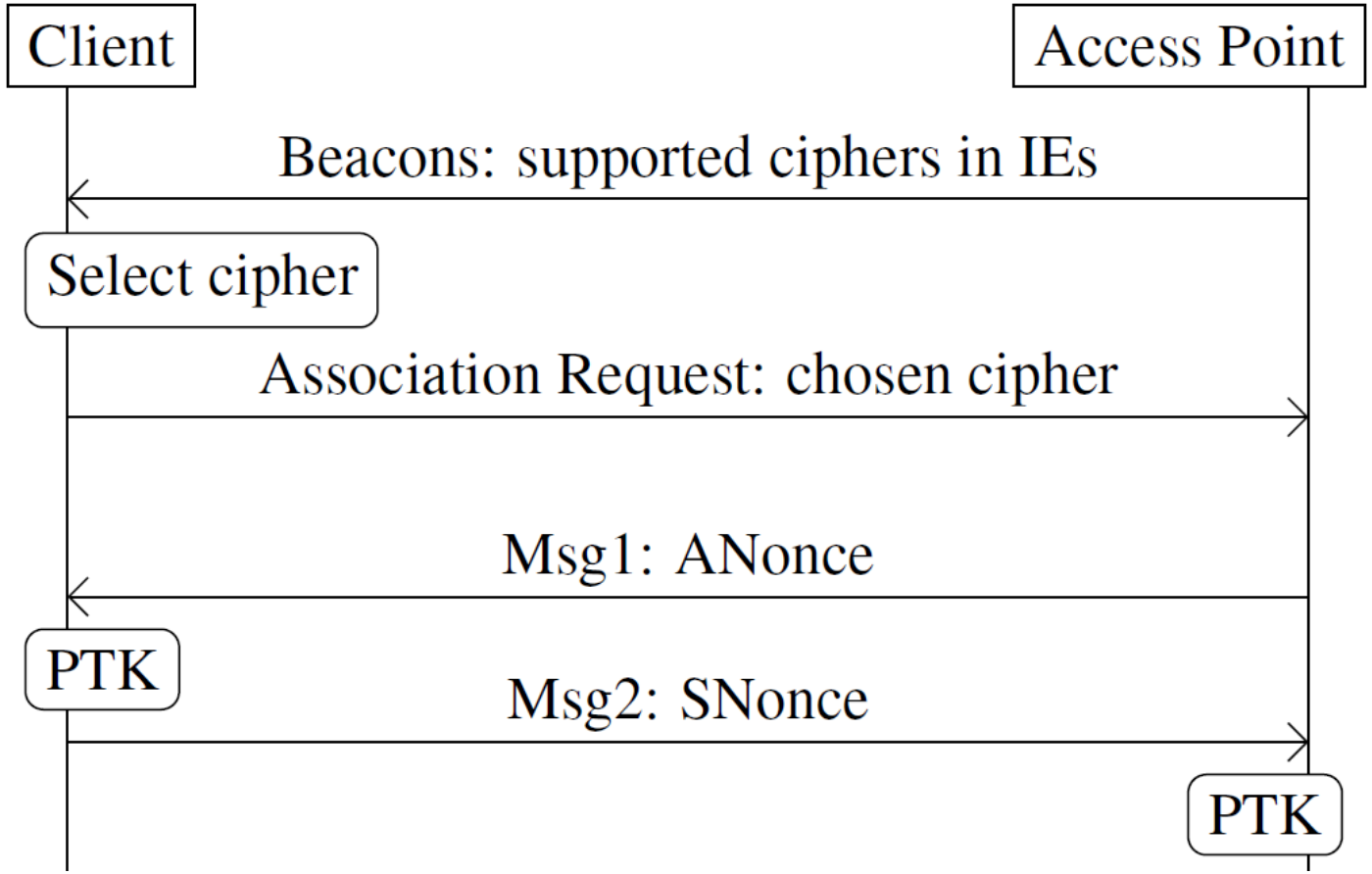
New Wi-Fi tailored RNG

DistriNet
iMinds
KU LEUVEN

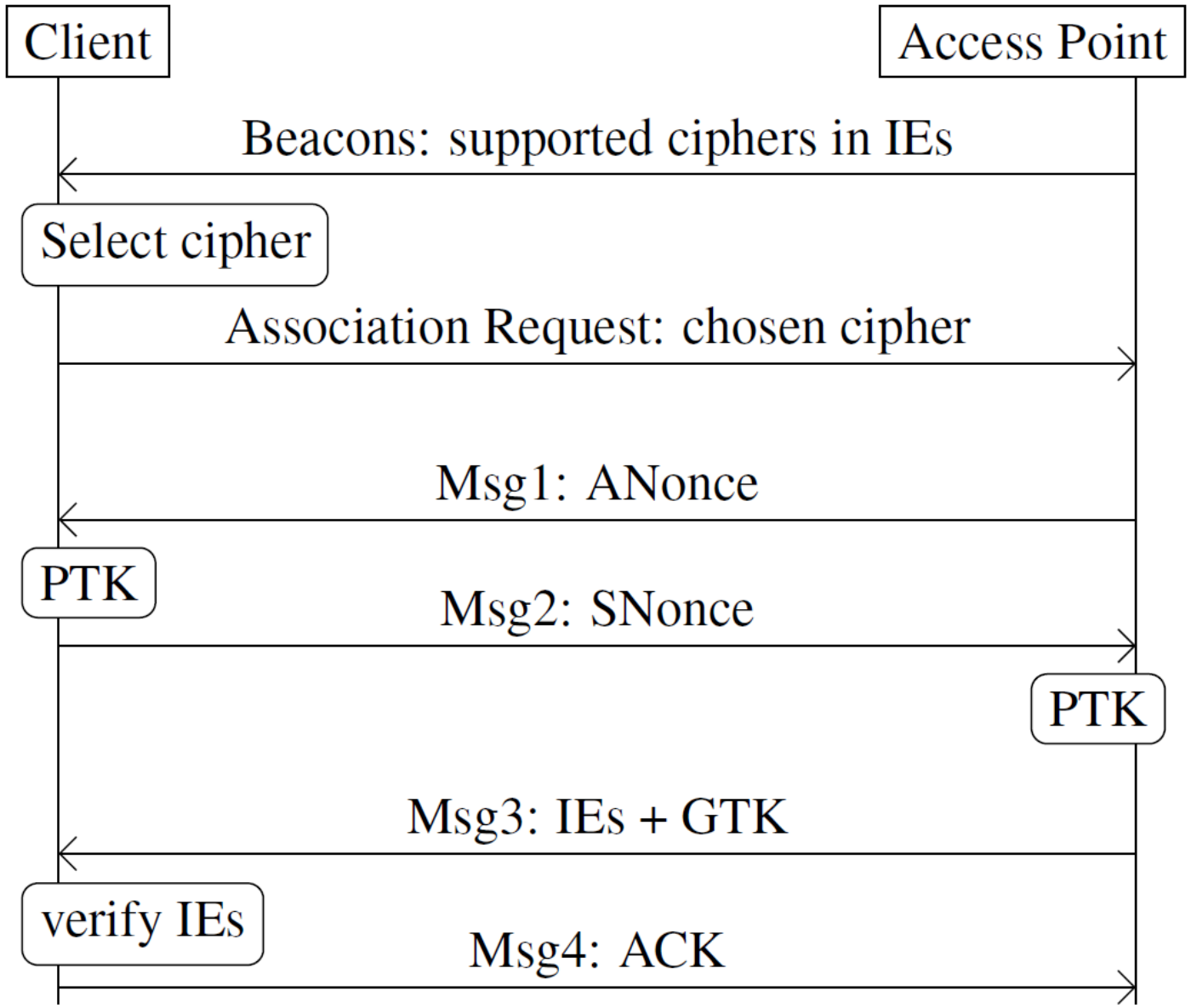
Simplified 4-way hanshake



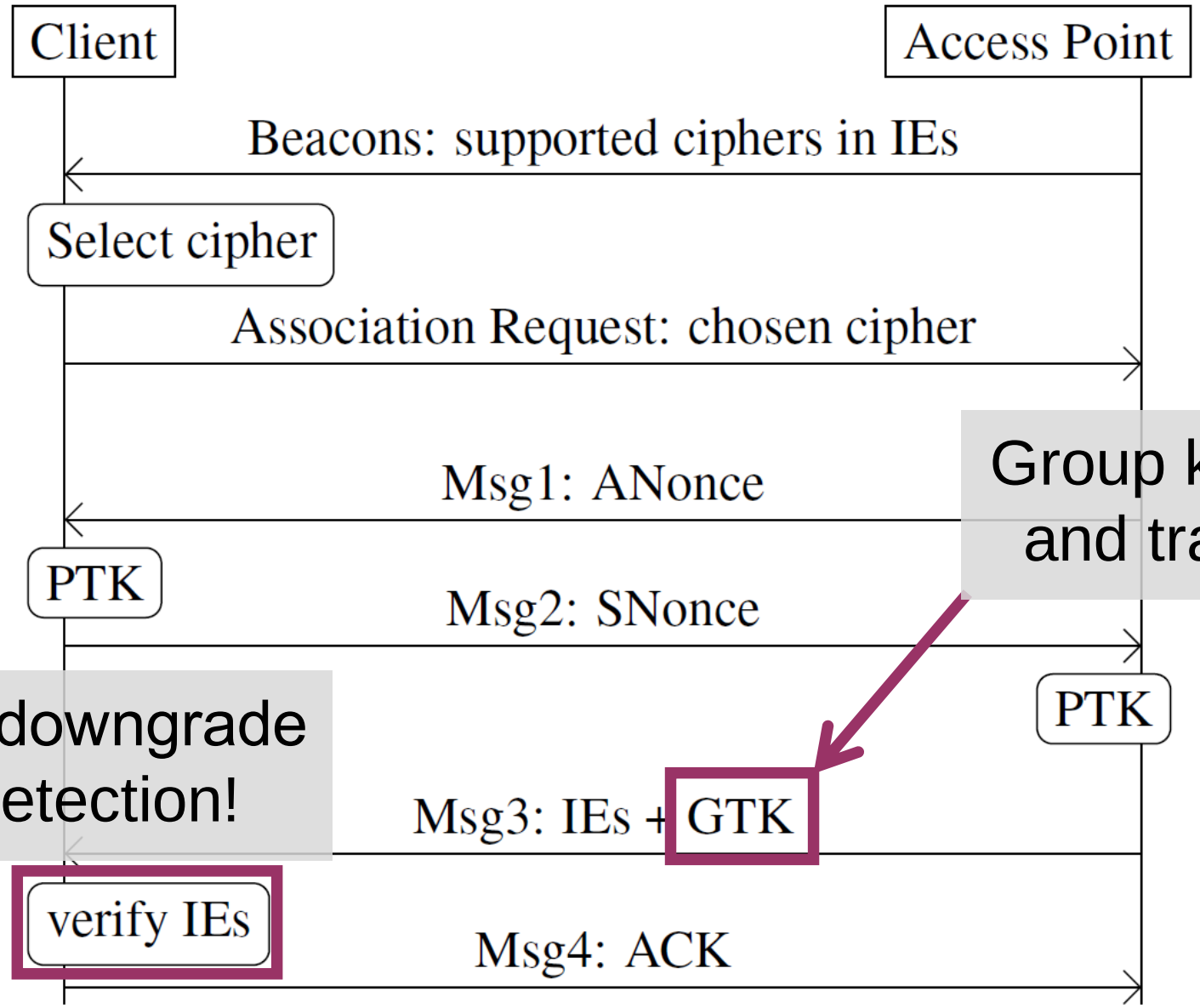
Simplified 4-way hanshake



Simplified 4-way hanshake



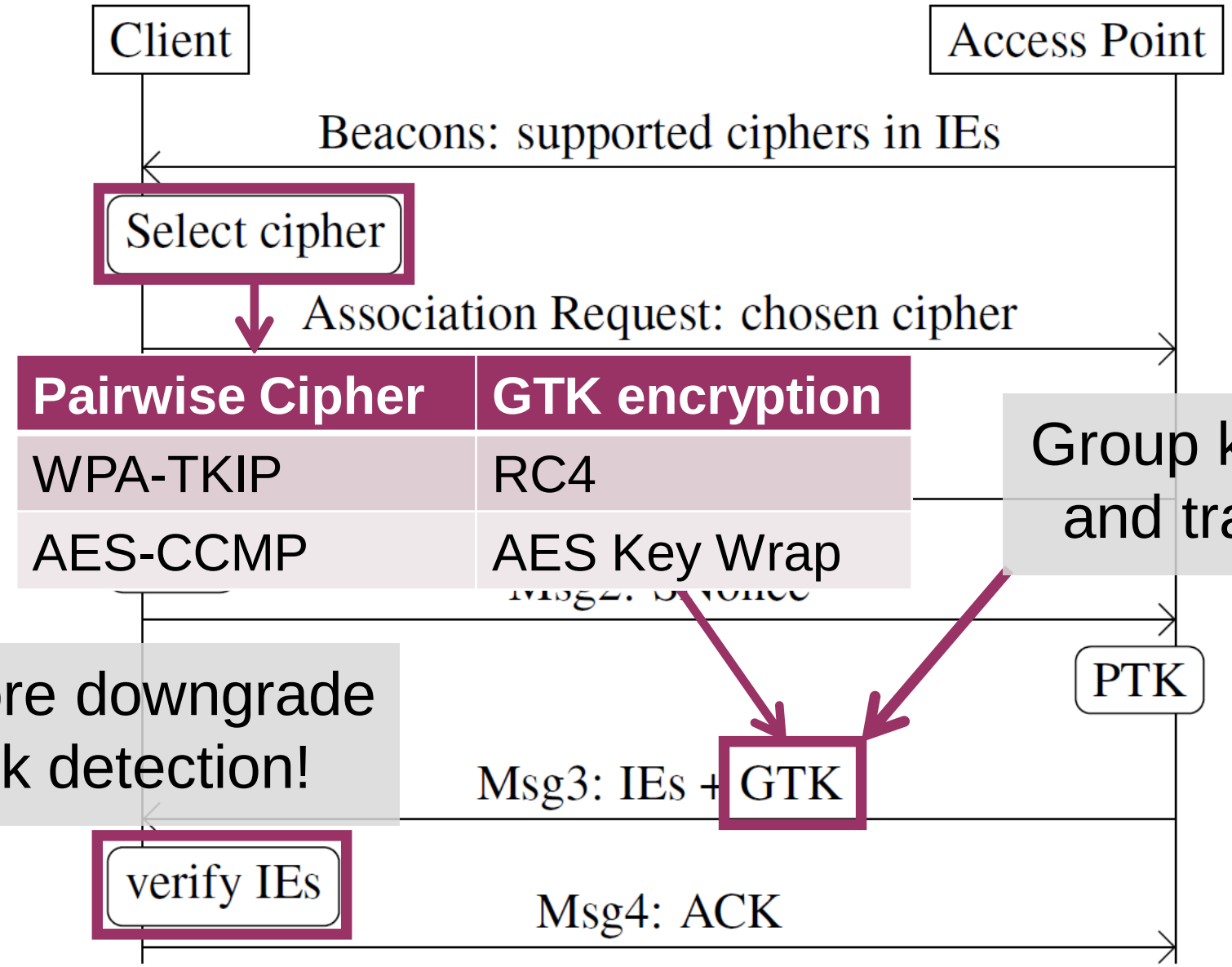
Simplified 4-way hanshake



Group key encrypted and transmitted …

… before downgrade attack detection!

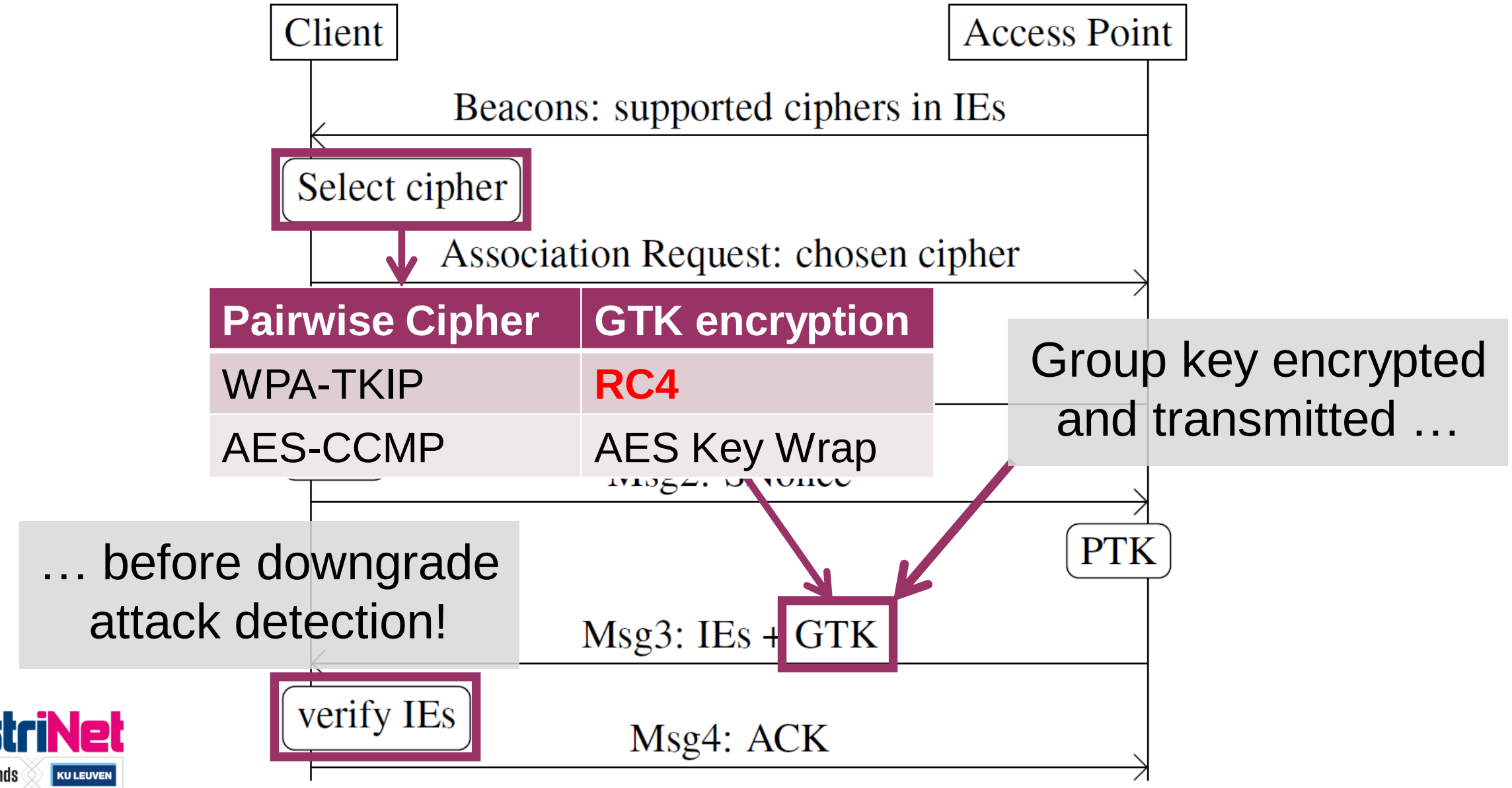
Simplified 4-way hanshake



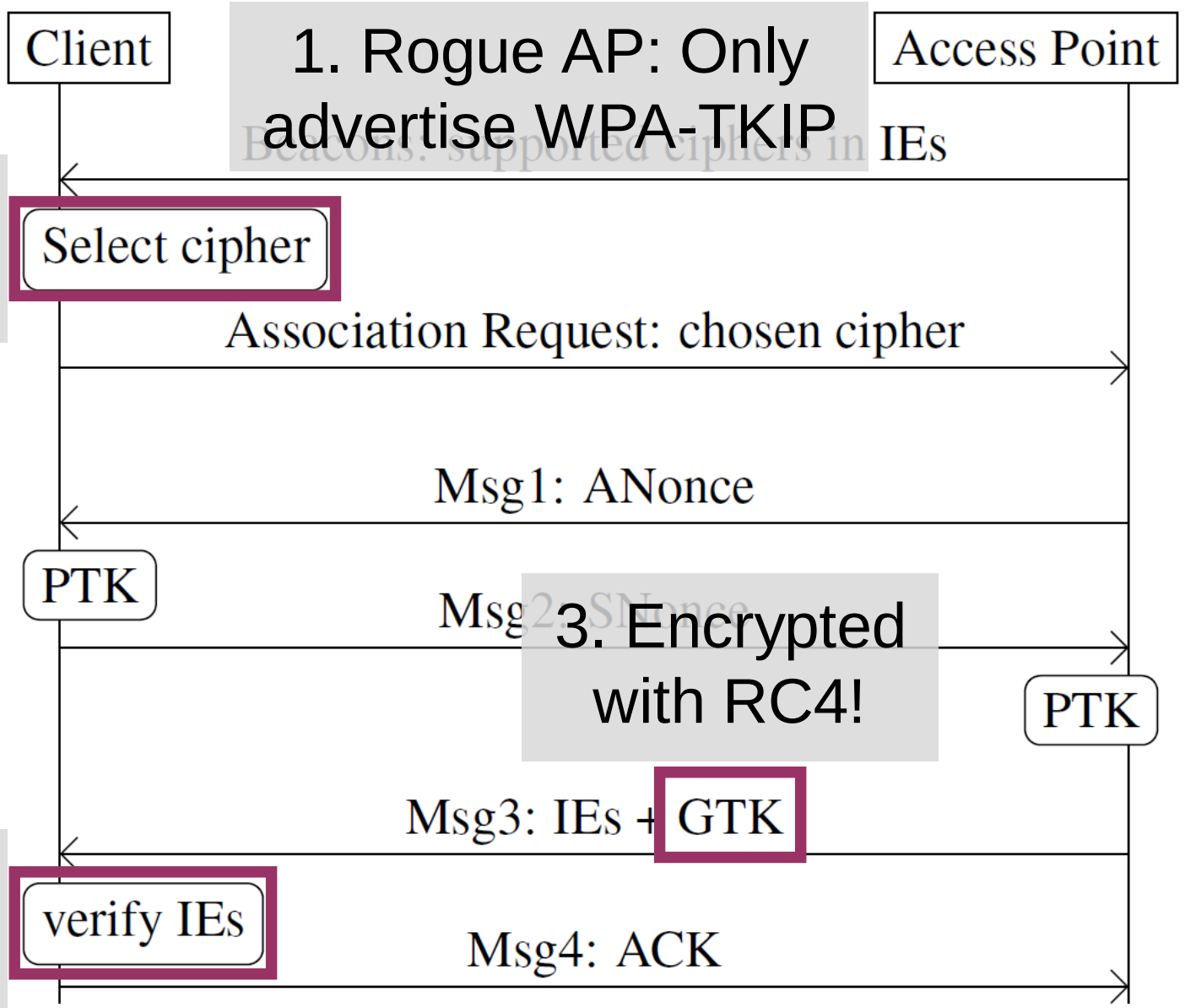
Group key encrypted and transmitted …

… before downgrade attack detection!

Simplified 4-way hanshake



Downgrade attack



Attacking RC4 encryption of GTK

- RC4 Key: 16-byte IV ||16-byte secret key
- First 256 keystream bytes are dropped

Recover repeated encryptions of GTK:

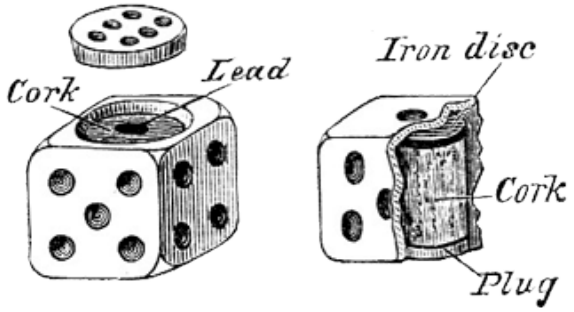
- Requires $\sim 2^{31}$ handshakes: takes >50 years

Countermeasures:

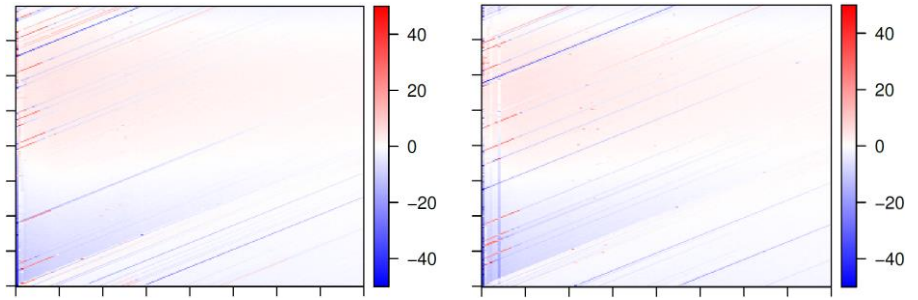
- Disable WPA-TKIP & RC4
- Send GTK after handshake

DistriNet iMinds KU LEUVEN

Contributions: Security of Group Keys

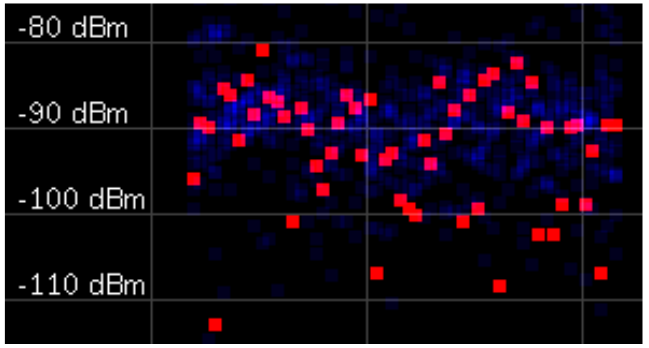


Flawed generation



Force RC4 in handshake

Inject & decrypt all traffic



New Wi-Fi tailored RNG

DistriNet
iMinds
KU LEUVEN

Abusing the group key: Hole 196?

- Inject unicast IP packet in broadcast Wi-Fi frame
- Detected by “Hole 196” check

Hole 196 check done at network-layer…

… but an AP works at link-layer!

Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

Victim

Attacker

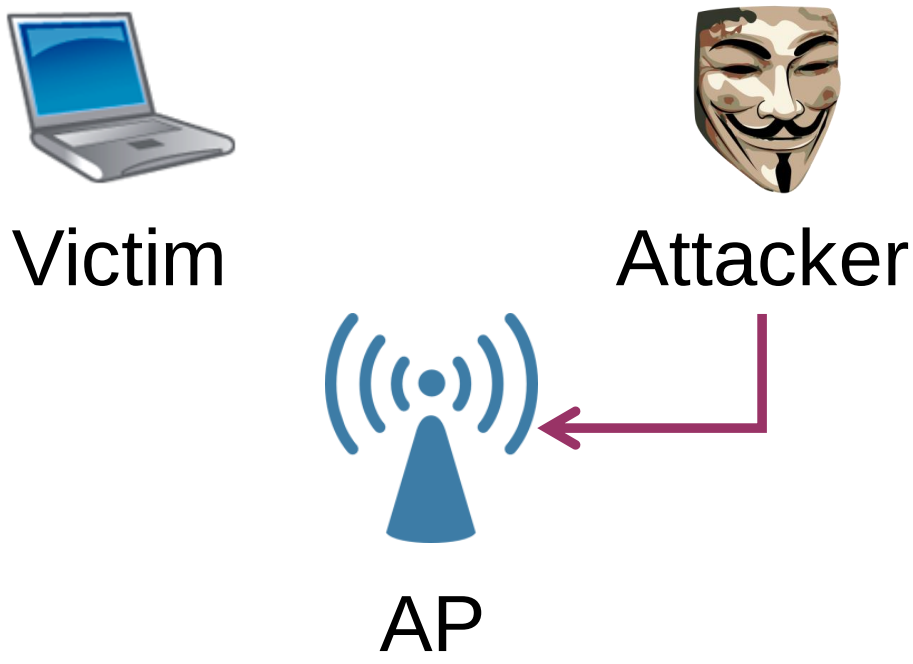
AP

Sender	Destination	Data

Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

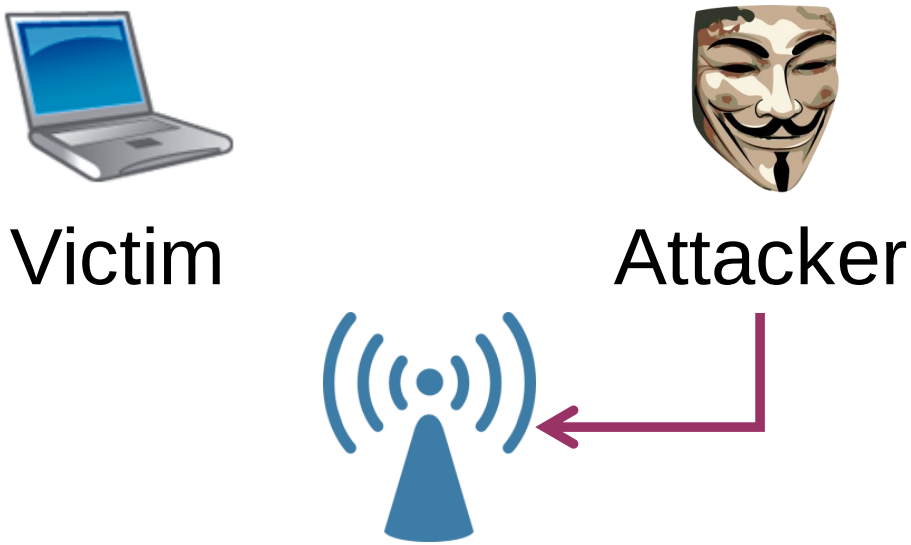
1. Inject as group frame to AP



Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

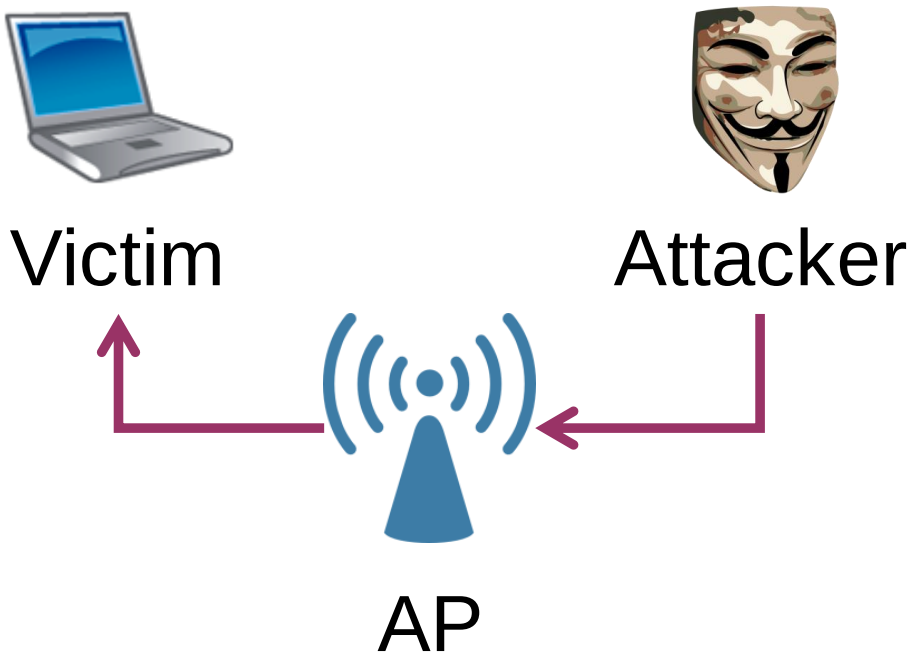
1. Inject as group frame to AP
2. AP processes and routes frame



Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

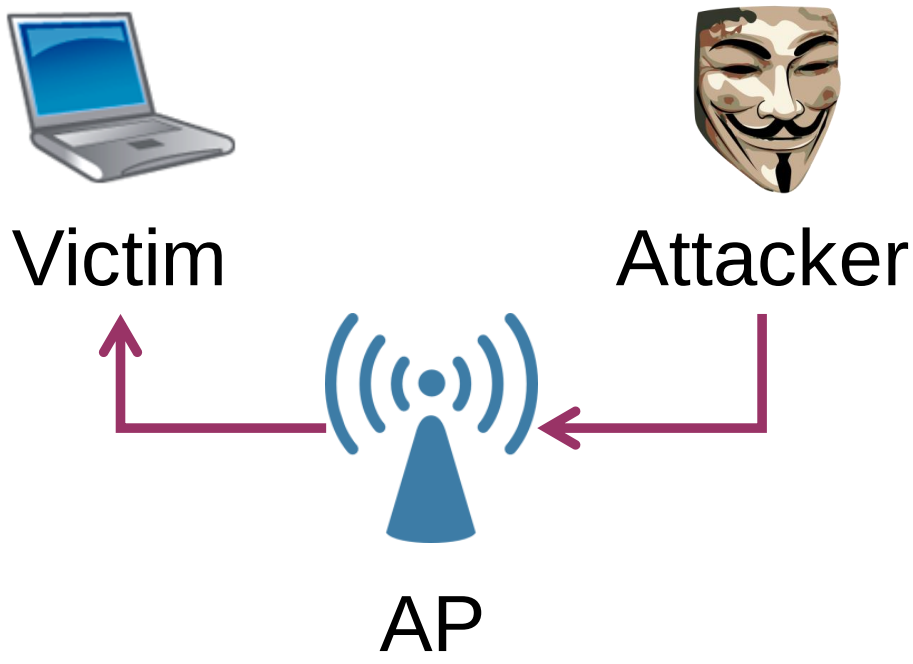
1. Inject as group frame to AP
2. AP processes and routes frame
3. AP transmits it to destination



Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

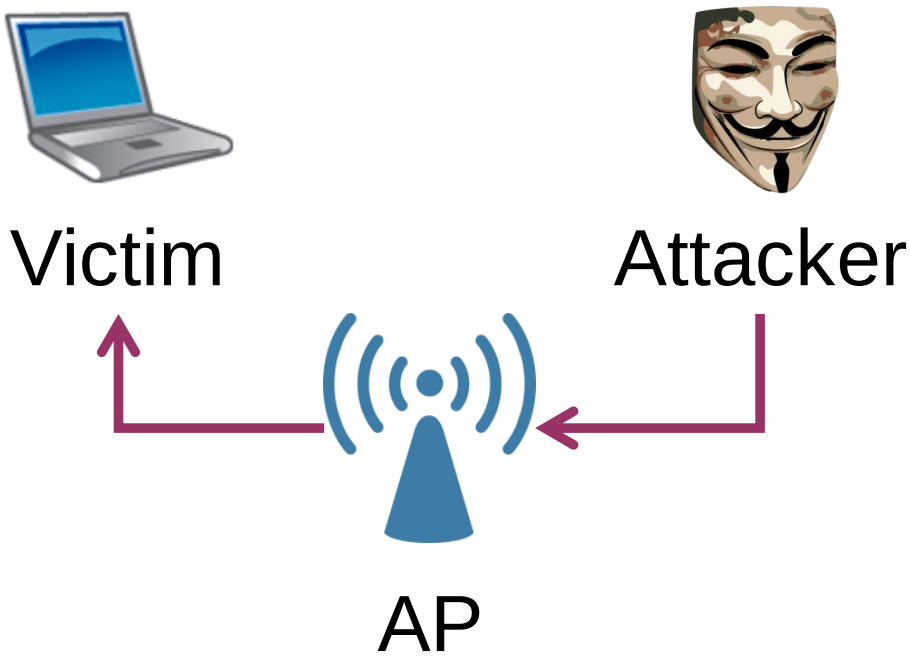
1. Inject as group frame to AP
2. AP processes and routes frame
3. AP transmits it to destination
4. Victim sees normal unicast frame



Forging unicast frames using group key

Abuse AP to bypass Hole 196 check:

1. Inject as group frame to AP
2. AP processes and routes frame
3. AP transmits it to destination
4. Victim sees normal unicast frame



Decrypting all traffic

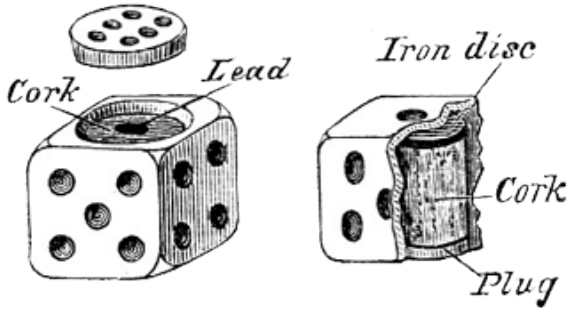
ARP poison to broadcast MAC address

- Poison both router and clients
- Targets network-layer protocols: IPv4, IPv6, …

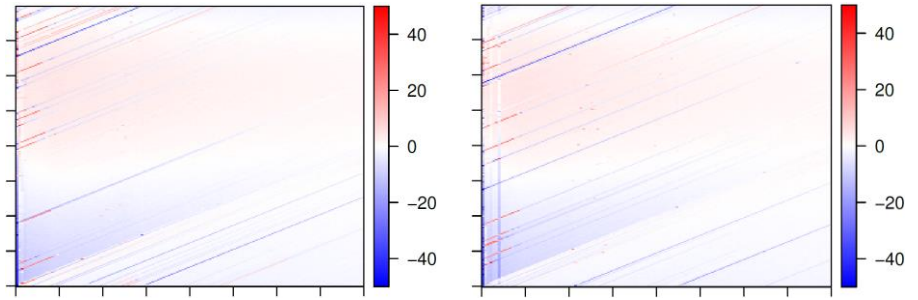
Countermeasure:

- AP should ignore frames received on broadcast or multicast MAC address.

Contributions: Security of Group Keys

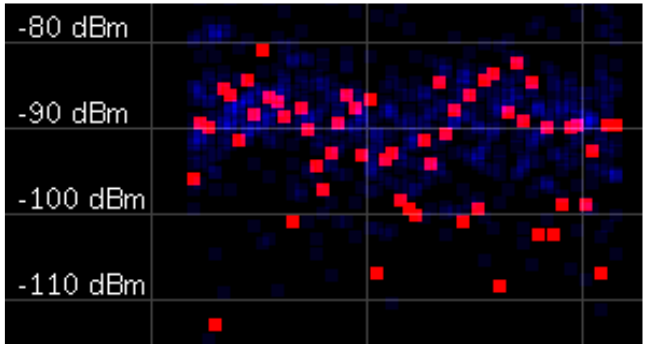


Flawed generation



Force RC4 in handshake

Inject & decrypt all traffic



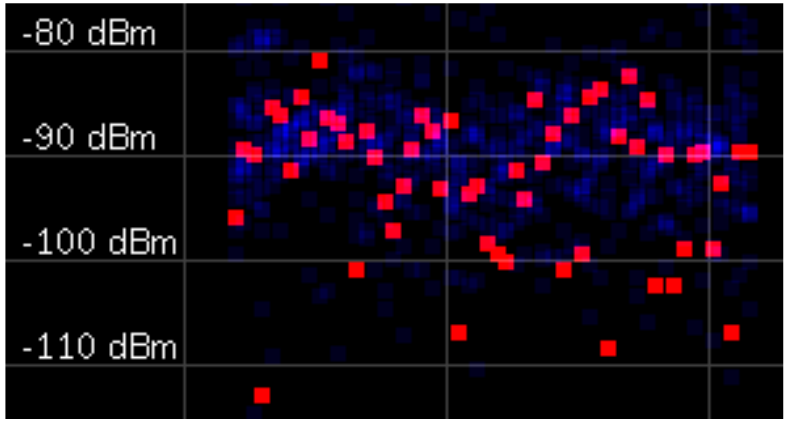
New Wi-Fi tailored RNG

DistriNet
iMinds
KU LEUVEN

An improved 802.11 RNG

Entropy present on al Wi-Fi chips?

- Wi-Fi signals & background noise



Spectral scan feature in commodity chips:

- Can generate 3 million samples / second
- First XOR samples in firmware
- Extract & manage resulting entropy using known approaches

Additional research needed: performance under jamming?

DistriNet
iMinds
KU LEUVEN

Conclusion: lessons learned

1. Use a proper RNG
2. Let AP ignore group-addressed frames
3. Don’t put “expository” security algos in a specification
4. Don’t transmit sensitive data before downgrade detection

Questions?

DistriNet iMinds KU LEUVEN