A Formal Analysis of IEEE 802.11’s WPA2

Countering the Kracks
Caused by
Cracking the Counters

Niklas Medinger, Benjamin Kiesl, and Cas Cremers
What is **WPA2**?

- **Purpose:** Enable secret communication over wireless networks
- **How:** Establish secret keys for encryption
  - **Pairwise transient keys (PTK)** for protecting WiFi traffic (different for each client)
  - **Group transient keys (GTK)** for protecting broadcast messages (same for each client)
The Four-Way Handshake

M1: ANonce, Counter₁

M2: SNonce, Counter₁, MACₚTk

M3: encₚTk(GTK, NonceGTK), Counter₂', MACₚTk

M4: Counter₂, MACₚTk

Generate ANonce

Derive PTK

Accept PTK

Generate SNonce and derive PTK

Accept PTK + GTK
What can go wrong?

- WPA2 had been considered secure (apart from offline attacks)
- **Big shock** in 2017: Vanhoef and Piessens break WPA2 by exploiting subtle behavior of the protocol => KRACK attacks
  - Message retransmissions are exploited to achieve key reinstallation
  - Key reinstallation leads to nonce reuse in WPA2’s authenticated encryption schemes
  - Nonce reuse leaks the key used for encryption
Encrypt data with PTK and nonce +0

Nonce Reuse!
Attacker learns Key
Breaking... and Fixing?

● Vanhoef and Piessens proposed intuitive countermeasures

● However, in 2018 Vanhoef and Piessens found new attack variants...

  ...that circumvent their own countermeasures.

● They then proposed new improved countermeasures
Formal Model using Tamarin

- We created a **formal model** of WPA2 with the **Tamarin prover**
- Modeled 7 state machines for the major mechanisms specified in the standard
- Created a more **accurate model** of the authenticated encryption schemes where nonce reuse leads to key leakage
- This took around **12 person-months** of work
- A lot of time spent on **understanding the WPA2 standard**
Analysis Results

● We proved...
  ○ ...security of the pairwise transient keys and of the group keys
  ○ ...authentication of 4-way-handshake ("injective agreement")

● Verification was not fully automatic

● Tamarin required many intermediate statements
Analysis Results

- Previous analysis did not cover mechanisms such as
  - Key leakage through nonce reuse
  - WNM sleep mode and sleep bit
- Our analysis covers a large class of attacks including these mechanisms
- No attacks on the pairwise keys in the twice patched WPA2 protocol.
Conclusion

- We provide the **first formal security argument** for **WPA2** that covers the major mechanisms.

- **Highly complex** protocols can now be verified **formally**.

- **Read** our paper! **Check out** our Website\(^1\)! **Build** on our model!

---

cremers@cispa.saarland
benjamin.kiesl@cispa.saarland
s8nimedi@stud.uni-saarland.de

\(^1\)https://cispa.saarland/group/cremers/tools/tamarin/WPA2/index.html