Discovering Logical Vulnerabilities in the Wi-Fi Handshake Using Model-Based Testing

Mathy Vanhoef, Domien Schepers, Frank Piessens
imec-DistriNet, KU Leuven
Asia CCS 2017
Introduction

More and more Wi-Fi network use encryption:

Most rely on the Wi-Fi handshake to generate session keys
How secure is the Wi-Fi handshake?

Design: formally analyzed and proven correct (CCS 2005)

Security of implementations?
- Some works fuzz network discovery stage
- Many stages are not tested, e.g. 4-way handshake.
- But do not tests for logical implementation bugs

→ Objective: test implementations of the full Wi-Fi handshake for logical vulnerabilities
Main purposes:

- Network discovery
- Mutual authentication & negotiation of pairwise session keys
- Securely select cipher to encrypt data frames

- **WPA-TKIP**
  
  Short-term solution that sacrificed some security, so it could run on old WEP-compatible hardware

- **AES-CCMP**
  
  Long-term solution based on modern cryptographic primitives
Wi-Fi handshake (simplified)

Client

Beacons: supported ciphers

Association Request: chosen cipher

Msg1: ANonce

Msg2: SNonce + chosen cipher

Session keys

Msg3: supported ciphers

verify supported ciphers

Msg4: ACK

verify chosen cipher

Session keys

Access Point
Wi-Fi handshake (simplified)

- Beacons: supported ciphers
- Select cipher
- Association Request: chosen cipher
- Msg1: ANonce
- Msg2: SNonce + Session keys
- Msg3: supported ciphers
- Msg4: ACK

Defined using EAPOL frames
EAPOL frame layout (simplified)

| header | key info | replay counter | ... | MIC | key data |

| PMI | S | E | R | CA | key version |

key info flags
≈ message ID
EAPOL frame layout (simplified)

- Header
- Key info
- Replay counter
- ... (Continued)
- MIC
- Key data

Key info flags:
≈ message ID

Key version:
PM I S E R C A

- Key version
- MD5/RC4 or SHA1/AES

- EAPOL frame layout (simplified)
How to test implementations?

- Test if program behaves according to some abstract model
- Proved successful against TLS

➤ Apply model-based approach on the Wi-Fi handshake
Model-based testing: our approach

Handshake model

Test generation rules

Correct & incorrect modifications

A test case defines:
1. Messages to send
2. Expected replies
3. Results in successful or failed connection?

Normal handshake

Set of test cases

For every test case

Test failed

Reset

No (or unexpected reply)

Yes

Expected result?

Successful connection?

Inspect failed tests

Expert determines exploitability!

Execute test case

1. Messages to send
2. Expected replies
3. Results in successful or failed connection?
Test generation rules

Test generation rules manipulating messages as a whole:
1. Drop a message
2. Inject/repeat a message

Test generation rules that modify fields in messages:
1. Wrong selected cipher suite in message
2. Bad EAPOL replay counter
3. Bad EAPOL key info flags (used to identify message)
4. Bad EAPOL key version (switch SHA1/AES with MD5/RC4)
5. Bad EAPOL Message Integrity Check (MIC)
6. …
Evaluation

We tested 12 access points:

- Open source: OpenBSD, Linux’s Hostapd
- Leaked source: Broadcom, MediaTek (home routers)
- Closed source: Windows, Apple, Telenet
- Professional equipment: Aerohive, Aironet

Discovered several issues!
Missing downgrade checks

1. MediaTek & Telenet don’t verify selected cipher in message 2
1. MediaTek & Telenet don’t verify selected cipher in message 2
2. MediaTek also ignores supported ciphers in message 3

→ MediaTek clients can be trivially downgraded
Windows 7 targeted DoS

Client

Association Request
Association Request
Association Request
Association Request
Association Rejected

AP

Association Request

Client 2

Msg1

...
Broadcom downgrade

Broadcom cannot distinguish message 2 and 4

- Can be abused to downgrade the AP to TKIP

Hence message 4 is essential in preventing downgrade attacks

- This highlights incorrect claims in the 802.11 standard
- §11.6.6.8: 4-way handshake analysis mentions that:

“While Message 4 serves no cryptographic purpose, it serves as an acknowledgment to Message 3. **It is required to ensure reliability** and to inform the Authenticator that the Supplicant has installed the PTK and GTK and hence can receive encrypted frames.”
Fingerprinting techniques!
Permanent DoS attack against OpenBSD & Broadcom
DoS attack against Windows 10, Broadcom, Aerohive
Inconsistent parsing of selected and supported cipher suite(s)
…
Conclusion

Overall advantages and disadvantages:

- Black-box testing mechanism: no source code needed
  - But time consuming to implement & requires an expert

Detected several issues, for example:

- Missing checks allowing downgrade attacks
- Several implementation-specific flaws
- ...

→ Fairly simple handshake, but still several **logical** bugs!
Discovering Logical Vulnerabilities in the Wi-Fi Handshake Using Model-Based Testing

Mathy Vanhoef, Domien Schepers, Frank Piessens

Questions?