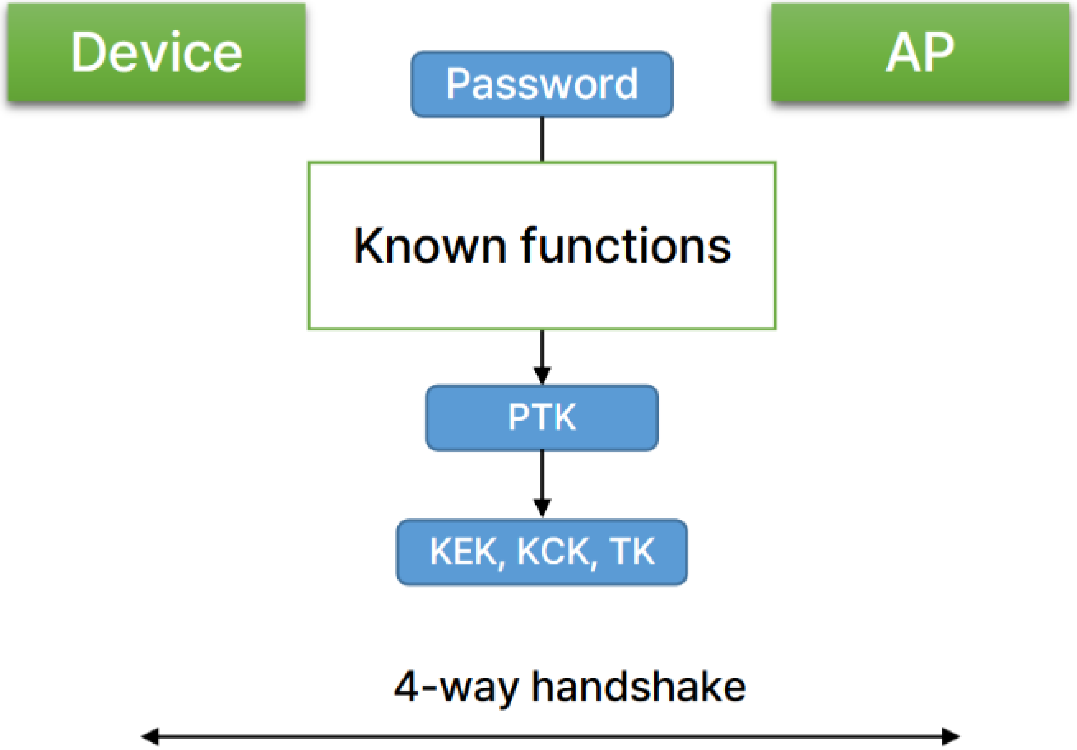
Exam Two

2024.11.13

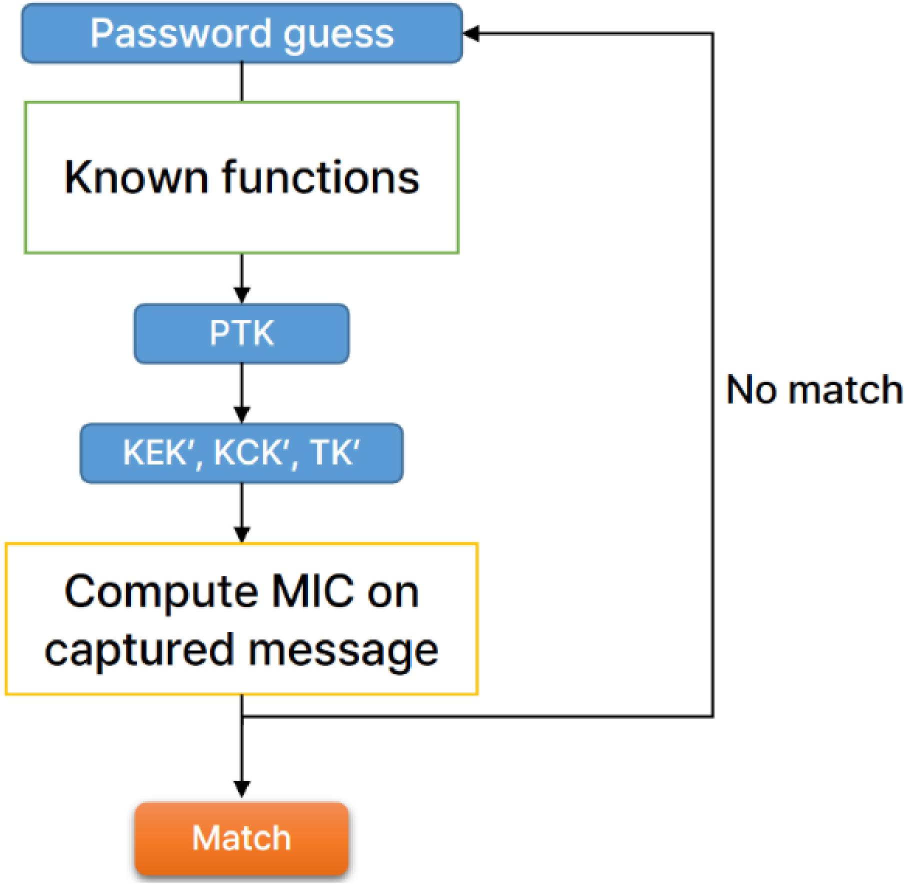
4-Way Handshake in WPA2-PSK

- Devices and an AP (Access Point) share a passphrase in advance
- PSK is derived from the passphrase
- PTK is derived from the PSK in the 4-way handshake



Offline Password Guessing Attack

- Adversary sniffs and records the 4-way handshake packets
- Adversary guesses the password until a match is found
  - If the MIC matches, then you found the password!
- You will launch an offline password guessing attack to find the passphrase of the given APs



Targets

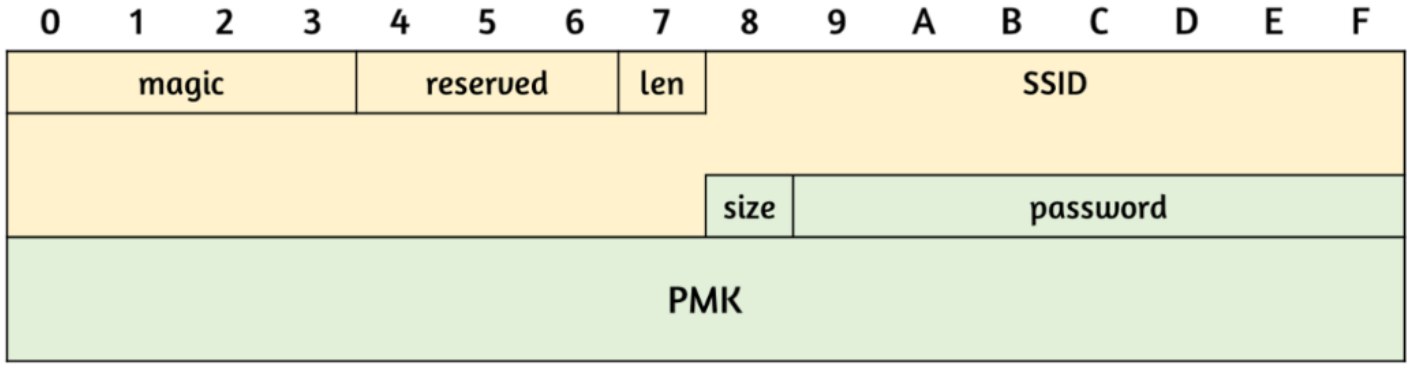
- 3 APs: `DoNotCrack_Bru, DoNotCrack_Dic, DoNotCrack_Rai`
- `DoNotCrack_Bru`
  - Password is 8 characters long, all digits
  - You must brute force the last 6 digits
  - First 2 characters are ‘00’
  - Example passwords: 00727671, 00928715, 00398162
- `DoNotCrack_Dic`
  - Password is 9 characters long, lowercase English characters only
  - You must use online wordlist files to guess the password
  - Example passwords: nevermore, crackdown, abandoned

Targets

- DoNotCrack_Rai
  - Password is 8 characters long
  - Hash file is given to you to assist your password guessing
  - Hash file information is in the next slide
  - Example passwords: ueo@517s, a&7ci11p

Hash File

- Header structure
  - Magic [4 bytes] || reserved [3 bytes] || ssidlen [1 byte] || ssid [32 bytes]
  - Total: 40 bytes
- Body structure
  - Record size [1 byte] || password [x bytes] || PMK [32 bytes]
  - Total: (33+x) bytes per each password



0 1 2 3 4 5 6 7 8 9 A B C D E F

magic

reserved

len

SSID

size

password

PMK

Warnings

- Languages are limited to C, C++ and Java
  - Other languages may NOT be used
- Do not DoS the router
- Routers will be taken offline at 13:30
  - You should finish capturing the packets before then
- You may receive a copy of the captured packets after 12:00
  - Ask the TA for a copy
  - Your score will be deducted by 20%
- You may borrow LAN cards
  - There is no penalty for this

Report

- Prepare a report for the project including followings
  - Description of your attack in detail
  - Any codes created by you for the project
  - Proofs that your attacks were successful
  - All tools used in the attack
  - Your unique experiences earned during the test
  - The three 4-way handshake messages in the form of screenshot and hex dump
- Reports without these will be considered invalid!

Submission

- You must submit the report and the pcap file you captured
  - pcap file must contains the 4-way handshake
- Use MS-Word or other your favorite word processors for the report
- Name your file to your_student_id.[docx|hwp|cap] and place them under the folder before submitting
  - Name the folder as your student ID and compress the file (zip)
- Do not submit codes. Instead copy them in your report
- Submit the compressed file to iCampus before the due date
  - No late submissions will be accepted!