Assignment 4 - Breaking WPA/Protocol implementation

<Simon> <Rommer>, <1225253>

December 7, 2016

The year is 2020, and the entire world is using secure Wifi everywhere and services used on the internet employ only the best protocols provided by libraries used by millions of people. And, speaking of people, every person uses only the most secure passwords which are impossible for machines to crack. Well, not entirely...

The following assignment is split into two parts and it is your job to crack the password of a WPA network and obtain privileged information you should not have access to.

Please document your findings and your solution by filling out this template and upload the resulting PDF to TUWEL.

1 Breaking WPA

Assignment

Somewhere out there a little wifi still exists using WPA to secure connections. As a skilled hacker you read on StackOverflow that this makes it vulnerable to dictionary attacks. Somehow you manage to get hold of a handshake (since you of course are also gifted in the art of social engineering). The source can't recall the exact passphrase, but it's SSID was "wpa2own" and she remembered that the password ended with a number (coincidentally your student ID [Matrikelnummer]) prefixed with a password out of a famous, real-world password list from the Internet (hint: research some famous recent hacks): [password][studentID]). You grab a coffee, warm up your GPUs, and get ready to work ...

Dictionary attacks

A dictionary attack happens when an attacker tries passwords according to a given list of words (Dictionary). This doesn't even have to be a real dictionary like "Oxford Dictionary" or the "Duden". Most of the times attacker use a list of previously gained

passwords from hacks.
Dictionary attacks can also be when you obtained a database with stored passwords as hashes and you cross reference the hashes from the passwords to the hashes you obtained. The hashes from the passwordlist can be precalculated and stored in a list (a so called Rainbowtable) so that the comparison goes much faster. Also you could use graphics cards to calculate hashes since the way graphics card work make them more fitting than cpu's. (GPU achieve great performance by using heavy parallelism, possible because of pipelining and sharing instruction decoding (since many cores will run the same instructions at the same time).)
Countermeasures to dictionary attacks on the admin side are limiting the numbers of tries that a user has to login and set requirements for passwords. Setting requirements for passwords is not usefull if the user doesn't remember the password and chooses to use something really easy like "1234abcd".
Countermeasures to dictionary attacks on the user side choosing passwords that are not single words or easy numbers like "password" or "123456". Also phrases like "passw0rd" are really common. A good approach here would be to use a passwordmanager that stores all your difficult passwords. In this case you only have to remember one master-key and can have different passwords on every account. Also please don't recycle passwords.
TODO: Briefly discuss how and why a dictionary attack can be used to compromise the password of a WPA network, given a handshake

Approach

TODO: Describe in detail how your solved this assignment. If you used any tools or other resources please include a reference or, if you wrote any source code, include it in the report as a listing.

Solutions

WPA key Insert the cracked key here

Password list Insert the password list you used here

2 Breaking a broken protocol

Assignment

After you successfully broke into the WPA network, you decide to sniff the some traffic. As it turns out, some unknown spy agency is communicating over the same network and you find a reference to a secret mission request portal. You have always wanted to become a secret agent, so you decide to participate in their next mission. Maybe they will be impressed and offer you a position. But you do not know where the mission will be. You stare at the mission request portal and decide to hack it.

Note: You do not need to complete the first part of the assignment to solve this one.

Approach

TODO: Describe in detail how you went about solving the assignment. Document every step of your process.

Exploiting the Service

TODO: Describe the security vulnerability present in the mission request service. What is the (likely) underlying cause. How can this bug be prevented?
TODO: Recently, a similar, high-impact, security issue was discovered in OpenSSL. Research and explain it.
TODO: Briefly explain why failing to validate user data is dangerous.

Decrypting the Mission

Mission code Insert mission code here

TODO: Describe how you decrypted the message and include the content.