Final Project Report

CIT 43100

Jake Simpson
IUPUI
Purdue School of Engineering and Technology
Indianapolis, Indiana
jaksimps@iu.edu

***Abstract*—This document is the Final Project Report for my CIT 43100-25878 class. It is topic number 3 which is attacking any modern ciphers or hash functions (developed after 1960). In this case I chose the RC4 stream cipher as the modern cipher that I wanted to investigate and attack.**

I. Introduction

This document is the final project report for CIT 43100. In this report I delve into a background on cryptography, but mainly focus the attention of this paper on attacking the RC4 cipher. The goal is to explore the vulnerabilities that are present within the widely used stream cipher and to give a demonstration on attacking this modern cipher. The attack I will be preforming is a Fluhrer Mantin Shamir attack against the Wired Equivalent Privacy (WEP) protocol.

II. Background

A. Modern Ciphers

Cryptography is the practice and study of different techniques for secure communication. The word come from the ancient Greek words for "hidden" and "writing". Cryptography can be broken down into three different periods in history[1].

The first era is classic cryptography. Unlike modern cipher that will rely on complex mathematics to encrypt and decrypt. They can be thought of as usually substitution or transposition ciphers[1]. Substitution ciphers will replace letters with another letter according to a secret key. The most famous example is the Caesar Cipher. Which is a substitution cipher that shifts the alphabet 3 characters. For example "A" would become "D". Transposition ciphers on the other hand will rearrange the order of letters without altering their values[1]. A major problem with these classic ciphers is that they are vulnerable to cryptoanalysis. Frequency analysis can be used to easily crack these ciphers even if the secret key is not known[1]. This because they inherit language characteristics even in their cipher-text state. Some ciphers like the Vigenere cipher, a polyalphabetic cipher, tried to improve upon this vulnerability but it is also vulnerability thanks to the Kasiski examination[1].

The second era is basically a early computer era. Think of World War II. There was new technology that was available thanks to the war and the desire to get an edge over the enemy. This includes technology like telegram, radio, and early computing[1]. On of the more famous examples from this time is the Enigma machine used during World War II[2]. the Germans made heavy use of the Enigma machine. The German military also used several teleprint stream ciphers[2]. A teleprinter is an electromechanical device that is used to send and receive typed messages through various communication channels both point-to-point and point-to-multipoint[3]. Many of the warring nations invested heavily into cryptanalysis in order to crack enemy encryptions.

Modern cryptography is the last era. It is what we are focusing on in the report. It uses extensive mathematics to aide with the much more complex ciphers. This is thanks to the computing technology that we have. Date is able to be encrypted into binary form now unlike the more classical ciphers. In modern cryptography there are two main methods. They are Symmetric and Asymmetric cryptography[1]. Symmetric key cryptography refers to the method in which both the sender and receiver of a message share the same key[1]. They are implemented as either block ciphers or stream ciphers. A block cipher breaks messages down into blocks of plaintext instead of leaving it as just individual characters, like a stream cipher would[1]. Data in symmetric cryptography is encrypted and decrypted significantly faster than asymmetric cryptography[1]. This is because Asymmetric cryptography uses two keys, a public key and a private key. The advantage of using asymmetric cryptography is that it allows individuals to establish a secure line of communication without needing a shared secret key[1]. Hashing is another thing that us used today in modern cryptography. A hash function is any function that can be used to map data of arbitrary size to a fixed-size value[4]. IBM was the first to use the concept of a hash function in 1953[4]. A hash function is used in a lot of different scenarios but these are some of the most popular: integrity checks, key derivation, message authentication codes, password storage, signatures[4]. The overall theme is integrity. Some of the more popular hashing functions are MD-5, SHA-1, and SHA-256[4].

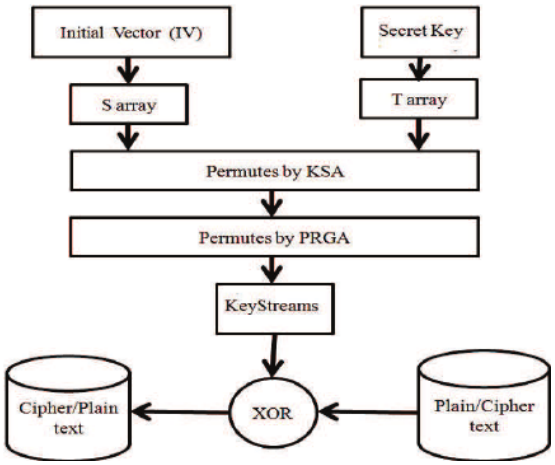
III. The RC4 Stream Cipher/Implementation

Before jumping into the exploitation of the RC4 cipher, it is a good idea to understand what it is and how it works. RC4

other wise known as the Rivest Cipher 4 was designed by Ron Rivest (RSA Security) in 1987 and became public in 1994[5]. It gained massive popularity for being a quick, affordable, and uncomplicated encryption method[5]. The advantages to using RC4 is the simplicity of its implementation and the speed of operation and deployment[5]. This allows the ability to work with massive data streams in a fast and efficient way. It is a stream cipher, a cipher where plain-text digits are encrypted one at a time with a corresponding keysteam[5]. Its key size can variate from 40 to 256 bits [5]. Today is insecure, which will be discussed in detail later.

A. How it works

How the cipher works is that RC4 uses a pseudorandom stream of bits, known as the keystream and combines it with the plain-text bits using an exclusive or[5].



Here is how the Key-sheduling algoritm (KSA) in RC4 works:

```
for i from 0 to 255
S[i] := i
endfor
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
swap values of S[i] and S[j]
endfor
```

Random Key stream generation (PRGA):

```
i := 0
j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap values of S[i] and S[j]
t := (S[i] + S[j]) mod 256
K := S[t]
output K
endwhile
```

The Pseudo-random generatoin algorithm will modify the state and outputs of a byte of a keystream. It will iterate through this process as many times are needed. Each element of S is swapped with another element for at least one time every 256 iterations[5].

B. Vulnerabilities

Over the years since it was created numerous vulnerabilities have been discovered and identified. As a result of this RC4 is now considered an insecure and should not be used[6]. For example, RC4 doesn't require authentication, which means that it is susceptible to a Man-in-the-Middle attack. It is also a stream not block cipher, which makes it vulnerable to bit-flipping attacks, this is where an attacked changes a bit in the cipher-text in a way that hopefully will result in a predictable change in the plain-text. Probably most obviously the RC4 stream cipher is vulnerable to key reuse attacks if it is not implemented correctly because it is a stream cipher.
Here are some of the most prominent RC4 vulnerabilities that have been discovered over the years:

- The Roo's biases. Andrew Roos observed that the first byte of the RC4 keystream is correlated with the first three bytes of the key, and the first few bytes of the permutation after the KSA are correlated with some linear combination of the key bytes. n simpler terms it means that there are correlations and biases in the RC4 structure[5][6].
- RC4 has biased outputs. It will create keystreams that can be biased which makes them vulnerable to distinguishing attacks. For example, the second output byte of the cipher is biased toward zero[5][6].
- The Fluhrer Mantin Shamir attack. This is where the first bytes of the keystreams are not random and because of this information is exposed about the key. The long term key can be discovered by simply analysing a large number of messages encrypted with that key[5][6]. This attack was used to break the Wired Equivalent Privacy protocol or WEP.
- Klein attack. This attack showed more correlations between the keystream and the key. This attack was used to crack the RC4 cipher in under a minuet using aircrack-ptw[5][6].

Those are just a few of the most notable vulnerabilities.

C. Applications

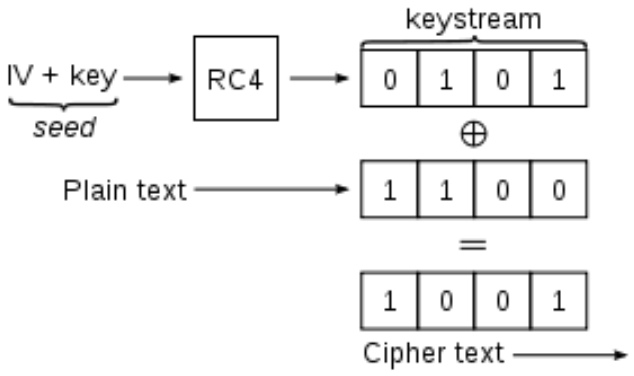
RC4 Stream Cipher is used in a variety of instances. For example, WEP, TKIP, BitTorrent, TLS/SSL (the RC4 option was eventually prohibited), PDF. Then optionally in secure shell, remote desktop, and Kerberos[5].

IV. DEMO/EVALUATION

For this section I will focus on breaking the RC4 stream cipher by using the Fluhrer Mantin Shamir attack. I will be breaking it in the WEP protocol. I will be using is Kali Linux on a Virtual Machine as my test enviroment and the tools airmon-ng, airodump-ng, airplay-ng, and aircrack-ng.

A. WEP

WEP uses the RC4 stream cipher for encryption and a CRC-32 checksum for integrity. WEP uses a 40-bit key along with a 24-bit initialization vector. Both of which are entirely too small. Since WEP uses the RC4 cipher it must never reuse the key otherwise it is vulnerable. The initialization vector was supposed to prevent that but 24 bits is way too short and eventually the IVs will repeat. Once the IV is repeated and it is used in combination with the key in the RC4 cipher a duplicate keystream will be created. If enough packets are passively collected eventually with enough packets we will be able to break RC4 because of the multiple uses of the same key and IVs. **ariodump-ng wlan0mon**



B. Lab Environment

For my lab environment I decided to create a Kali Linux Virtual Machine. Kali Linux is a Linux Distribution designed for digital forensics and penetration testing that is maintained and funded by Offensive Security. It is based on Debian and contains about 600 useful tools for cybersecurity. I downloaded the file and created the VM with the help of VMWare, which is an American cloud computing and virtualixation technology company. Additionally, I used an ALFA AWUS036NH adapter as it is compatible with Kali Linux.

C. Attack

In Kali Linux I started by launching the command line and entering the following command:

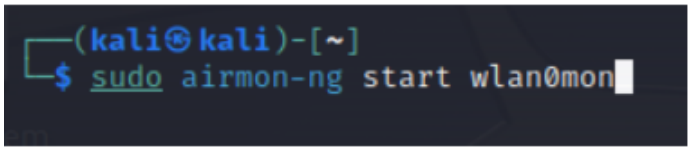
airmon-ng

This command is part of the Aircrack-ng suite. The Aircrack-ng suite is a set of tools that are used to assess WiFi network security. It focuses on these key areas of Wifi Security:

Monitoring - Packet capture and export of data to text fiels for further processing
Attacking - Replay attacksm deauthentication, fake access points and others
Testing - Checking WiFi cards and driver capabilities (capture and injection)
Cracking - WEP and WPA PSK (WPA 1 and 2)

What this airmon-ng command does is it will primarily be used to enable monitor mode on wireless adapters. This allows the wireless adapted to listen to all traffic in the air, even if it is outside of the network the device belongs to.The next command that I ran was:

ariodump-ng wlan0mon

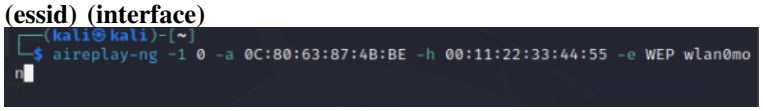


This command allowed my to see a list of wireless networks around me. I chose the test network running that was WEP and its BSSID and its channel. BSSID stands for Basic Service Set Identifier. It is basically the MAC (Media Access Control) of the access point that was running WEP. The next command that I ran was:

airodump-ng -c (channel) -w (filename) –bssid (bssid) (interface)

This command is to watch what is going on with the targeted network. The next command I ran was:

aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 -e (essid) (interface)



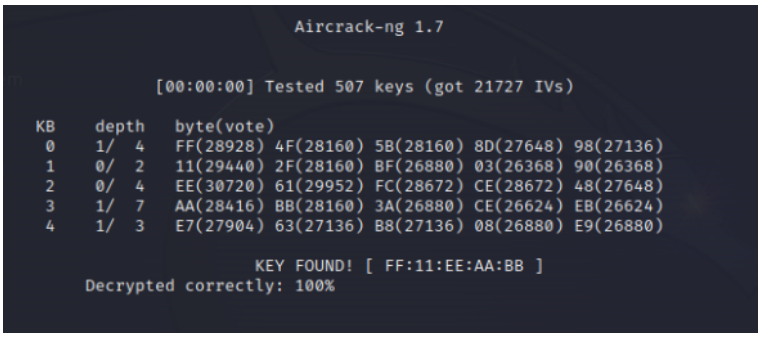
I then ran:

aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 (interface)

This command creates router traffic so that we can capture more throughput faster. Once I had enough packets I was then able to crack it. This was done when I entered the command:

aircrack-ng -b (bssid) (filename)

After that command was entered it uses the thousands of captured packets to crack RC4 and give us the key.



This is a successful example of the Fluhrer Mantin Shamir attack. This entire demo was done in about 10-15 minuets. This is one of the reasons WEP shouldn't be used anymore today. Computing power is simply too strong and attackers can easily crack it. To be more secure a protocol such as WPA2 or WPA3 should be used because they use block ciphers such as Advance Encryption Standard (AES).

V. Conclusion

In this paper I explored the history of cryptography over its three ages, I think went into depth about the RC4 stream cipher as that is the modern cipher I wanted to discuss for my paper. I then showed a demo of how to crack the RC4 stream cipher is WEP using a Fluhrer Mantin Shamir attack. Rc4 is the most widely used and most popular stream cipher in the world. However, with todays technology many expers feel that stream ciphers aren't safe for widespread use. any prefer the use of block ciphers as they are more complex versatile and robust than stream ciphers. Looking into furher projects I would be curious to see whether or not other stream ciphers suffered from similar vulnerabilities to the RC4 stream cipher. I would also be curious to look into block ciphers like AES as it is probably the most popular cipher in the world right now. In fact WEP was eventually replaced with WPA and then WPA2 and WPA3 which utilize AES.

References

[1] Wikipedia Contributors, "Cryptography," Wikipedia, Oct. 23, 2019. https://en.wikipedia.org/wiki/Cryptography
[2] Wikipedia Contributors, "History of cryptography," Wikipedia, Apr. 07, 2019. https://en.wikipedia.org/wiki/Historyofcryptography
[3] "Teleprinter," Wikipedia, May 14, 2020. https://en.wikipedia.org/wiki/Teleprinter
[4] Wikipedia Contributors, "Hash function," Wikipedia, Sep. 08, 2019. https://en.wikipedia.org/wiki/Hashfunction
[5] Wikipedia Contributors, "RC4," Wikipedia, Dec. 31, 2019. https://en.wikipedia.org/wiki/RC4
[6] "What Is Rivest Cipher 4 (RC4) And Why Is It A Vulnerability." https://crashtest-security.com/disable-ssl-rc4/