WEP Attacks and Solutions

Jack Neilson

April 18, 2018

School of Computing Science and Digital Media

Faculty of Design and Technology

Coursework Assignment

Student Name*	Jack Neilson
Matriculation Number*	1506801
Contact Number (in case of urgent need)	07990 850 875
Course	CS Hons Year
Stage	BSc
Time taken to complete (hours)	1-4 5-9 10-14 15-19 20+
Lecturer	Ian Harris
Module Name	Ethical Hacking
Module Number	CM4103
Coursework Title	WEP Attacks and Solutions
Coursework Part	Coursework
Handout Date	26th Mar 2018
Due Date	23rd Apr 2018
Submission Method	Via campusmoodle assessment dropbox

*Declaration ** This **MUST** be affirmed by signing below*

I confirm

- **That the work undertaken for this assignment is entirely my own and that I have not made use of any unauthorised assistance.**
- **That the sources of all reference material has been properly acknowledged.**

Student Signature*	J. Neilson
Date Submitted*	

For Office Use

Marker' Comments

Marker	Grade

Contents

1 Non-Technical Report

1.1 WEP Overview

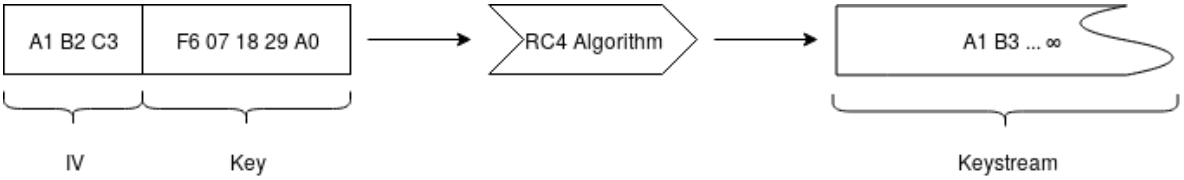
Wired Equivalent Privacy (WEP) is a method of securing over-the-air network traffic. It's used when devices connect to a Wi-Fi access spot to make sure that traffic between an access spot and an end device (such as a laptop or mobile phone) is encrypted, and isn't sent "in the clear" as human-readable, unencrypted text. It is important that traffic is encrypted in this manner, as otherwise an attacker could position themselves between an end device and an access point and read every communication sent between the two devices, capturing sensitive information in the process.

1.2 WEP Implementation

At it's core, WEP encryption consists of two components:

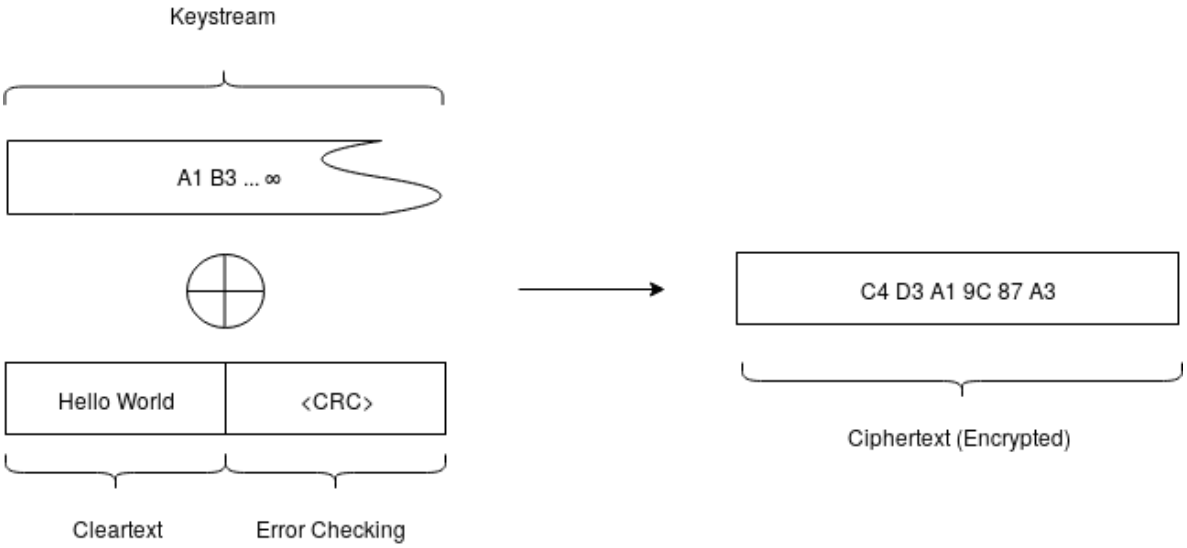
- An "initialisation vector" (IV). This is a random number that is generated for each message sent over the network. It is used in conjunction with the secret key to generate a stream of pseudo-random bits that are suitable for encryption.
- A secret key. This is known to both the access point and end device, and is used when encrypting and decrypting traffic.

First, the IV and the secret key are joined together to give the key for the message. This is then put through the RC4 algorithm, which generates a stream of pseudo-random numbers.



A digest (CRC) of the message is then generated to allow to recipient to check for errors.

The message and the CRC is then encrypted using the keystream.



Finally, the IV is added so that the recipient can do the entire process in reverse to decrypt to message.

1.3 Weaknesses of WEP

WEP was superceded by WPA in 2003, and was deprecated due to security concerns in 2004.

In 2006 a paper was released that showed fundamental flaws in how the WEP standard was designed, allowing attackers to gain access to the key of even the most secure (104-bit) implementations in under 60 seconds(Tews et al., 2007). This is particularly damning as the key allows the attacker to decrypt all traffic he or she captures.

1.4 Business Impact

The business impact of using WEP with no other mitigations could potentially be very large. Should an attacker come in range of a wi-fi access point they could potentially gather traffic to and from multiple users. If this occurs the massive negative press could potentially bankrupt the business, legal implications notwithstanding. Industry regulators could force the business to close if medical or financial information is disclosed.

2 Proposed Solution

2.1 VPN

3 Ethics

3.1 Ethical Framework

3.2 Professional Standards

References

Tews, E., Weinmann, R.-P. and Pyshkin, A. (2007), Breaking 104 bit wep in less than 60 seconds, *in* 'International Workshop on Information Security Applications', Springer, pp. 188–202.