Brief yet Scintillating Article about WEP and WPA2

Ashley Oudenne
The University of Texas at Austin
aoudenne@cs.utexas.edu

Jerremy Adams
The University of Texas at Austin
ja7872@cs.utexas.edu

December 12, 2012

Abstract

Interesting yet vague things about our paper.

1 Introduction

2 Related Work

3 Modeling of Protocols

3.1 Protocol Structures

3.1.1 WEP

WEP, described in [1], uses a one-message protocol to transmit data between two parties that relies on a secret key k that has been shared between them. Before a message is sent, an integrity checksum *C(m)* is computed on the message so that the recipient can verify that the message has not been altered in transit. The message is concatenated to this checksum to form the plaintext P.

The plaintext is now encrypted using the RC4 cipher. The sender chooses an initialization vector IV and uses this vector along with the secret key k to generate a keystream, which is a long sequence of pseudorandom bits. The sender then uses exclusive-or (or XOR, denoted by $\oplus$) to XOR P and the keystream to generate ciphertext C. The complete encryption process can be represented by:

$$C = P \oplus RC4(IV, k)$$

The message is then ready to be transmitted from the sender to the receiver. We will represent this transmission symbolically as:

$$A \rightarrow B : IV, (P \oplus RC4(IV, k)), whereP = \langle m, C(m) \rangle$$

Notice that the initialization vector IV is sent in the clear, meaning that anyone can read the value of the initialization vector. This should not matter because an attacker would need boh the IV and the secret key k to recover the keystream used to decrypt the message, but we will show later in this paper that this is enough to break WEP.

Decryption works by reversing the encryption process described above. The recipient first regenerates the keystream used to encode the message with the secret key k and the IV sent along with the encrypted message. He can XOR the ciphertext with the keystream to recover the plaintext P:

$$\begin{aligned} P &= C \oplus RC4(IV, k) \\ &= (P \oplus RC4(IV, k)) \oplus RC4(IV, k) \\ &= P \end{aligned}$$

The recipient can then verify the integrity of the message by splitting P into $\langle m, C(m) \rangle$ and recomputing the checksum of m. If the computed checksum matches the sent checksum, then the message has not been tampered with.

3.2 Proverif

3.3 Attacker Model

3.4 Modeling Security Properties

4 Analysis of Protocol Models

4.1 WEP

4.2 WPA/WPA2 Four-Way Handshake

5 Conclusions and Future Work

References

[1] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: The insecurity of 802.11. In *MobiCom '01: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pages 180–189, 2001.