

A COMPARATIVE STUDY INTO THE ENCRYPTION ALGORITHMS USED IN
WIRELESS INTERNET SECURITY

by

Christopher R. Harm

A Thesis Proposal

Presented to the Faculty of
Bucknell University
In Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science with Honors in Computer Science and Engineering

October 15, 2002

Approved: _____

Xiannong Meng
Thesis Advisor

Gary Haggard
Chair, Department of Computer Science

Purpose

Wired Equivalent Privacy otherwise known as WEP is an algorithm used in the IEEE 802.11 standard to encrypt data packets that travel over a wireless local area network (WLAN). WLANs lack the physical security of actual wires as compared to traditional wired LANs. The IEEE 802.11b standard specifies that wireless transmissions will occur in 2.4 GHz frequency. This frequency is used by many other consumer devices such as cordless phone, microwaves, and two-way radios. The medium is open for anyone to transmit or listen to signals from such devices [11]. Inherently, there is a higher risk of eavesdropping or unauthorized access to a WLAN than the traditional wired LAN. The WEP algorithm is supposed to provide the same level of security to a WLAN that is found on a wired network. However, security flaws have been documented in the WEP algorithm, and these flaws have lead to successful attacks on WLANs [4]. With the increasing popularity of wireless products, more and more companies and individuals are relying on IEEE 802.11's WEP algorithm to keep their wireless networks secure. In this project I intend to investigate the source of the security holes in the WEP algorithm. I will compare different encryption algorithms and their applications to wireless communications. I intend to investigate why the algorithm behind WEP is successful in some of its other applications and not towards wireless communications. With the knowledge that I gain, I will have a better understanding of how to make packet delivery over WLANs more secure.

WEP Standards and Problems

IEEE 802.11's WEP algorithm has three main objectives: to protect data packets from unauthorized eavesdropping, to guard against unauthorized access to the network, and to protect the integrity of the data packets as they travel across the network. The WEP algorithm relies on the existence of a secret key that is known by the sending and receiving parties [4].

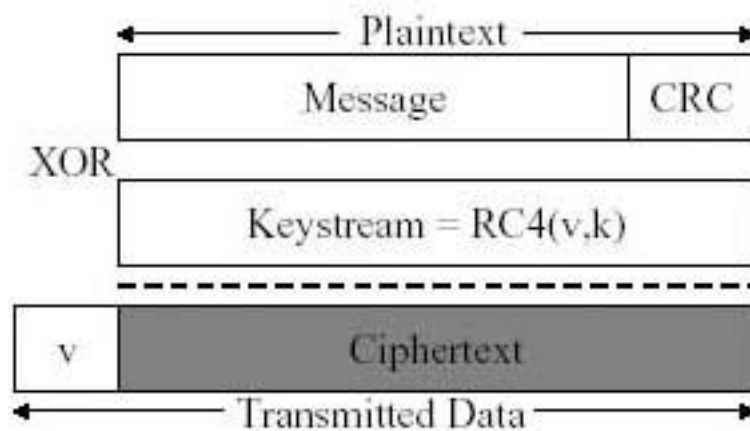


Figure 1 – Encrypted WEP Frame (Borisov)

The first step in the encryption process is to compute the cyclic redundancy check (CRC) checksum on the initial message. The checksum will be used in the decoding process to validate the message that was received correctly. The plaintext is composed of the original message concatenated to the integrity checksum [5]. The Keystream is generated by using the secret key and the initialization vector in the RC4 stream cipher. The RC4 stream cipher is used to create a pseudorandom variable length stream of bits. The Plaintext and the Keystream are then exclusive-ored (XOR) to create the Ciphertext. The initialization vector and the ciphertext are concatenated together and then transmitted across the network. The receiving party will reverse the process and obtain the original

message. The initialization vector that was transmitted is used with the secret key to come up with an identical keystream that was used to encrypt the message. The ciphertext is then XORed with the keystream to produce the original message with the integrity checksum. The received checksum is then compared to the value obtained by computing the checksum on the received message. Matching checksums signifies that the message was received correctly. If they don't match then the message is discarded [4].

The problems in the WEP algorithm arise when the same keystream is used more than once. If two ciphertext packets that are encrypted with the same keystream are XORed together, then the keystreams will cancel out and leave behind the two original plaintext messages XORed together. With some knowledge about one of the original messages, the other message is easy to discover. The keystream is generated by the RC4 stream cipher using the secret WEP code and the Initialization Vector (IV). To prevent duplicate keystreams use, the IV is changed for every data packet that is transmitted. The IV field has a maximum length of only 24-bits, which on a moderately busy access point will lead to keystream reuse in less than one full day. The secret key (WEP Code) can be set to a 40-bit key or can be extended to a larger 128-bit key. However, the 128-bit key WEP Code is subject to the same keystream reuse flaws as the 40-bit code [4].

Project Methodology

My project will look into the theoretical aspects of data encryption and its applications toward WLANs. Some proprietary solutions have been developed to try and solve the security issues with WEP, but a new standard has yet to be adopted. I plan on researching the details of the RC4 stream cipher and the CRC checksum to add more security to wireless transmission. WEP currently uses the RC4 stream cipher as the

engine behind its encryption. The data encryption scheme that is used on secure web sites (SSL) also uses the RC4 stream cipher to encrypt data. However, SSL is not subject to the same attacks as WEP. In my project, I will investigate why the RC4 algorithm works for SSL but not WEP [15]. It is possible that a different encryption scheme would be better suited for wireless data encryption. I will compare how different ciphers work when applied to wireless communications. The CRC integrity check is a vital part to the encryption process. A technique that attackers commonly use, called bit-flipping, is used to modify the ciphertext message portion of the message. When the message is then decrypted, the resulting plaintext will not match the original plaintext. The integrity check is computed to make sure that decrypted message matched the original message. If the integrity check is designed well, attempts to change the ciphertext will fail because the decrypted message will not match the CRC integrity check value of the original message [5]. The WEP algorithm fails to deliver the level of security that it promises [4]. I intend to look into alternatives for using the stream cipher to encrypt the wireless data. The knowledge that I gain will help me to understand the WEP algorithm and its flaws. When the project is finished, the WEP algorithm will be more secure and will better protect information as it travels across a wireless network.

Significance

When wireless networks first began to appear on the market, security was not a major concern. As wireless cards and access-points become cheaper and more available to the public, the security that protects WLANs has become a necessity. The physical security of wires and walls that once protected wired networks is gone; the information is literally out in the air for anyone to grab. The industry standard, IEEE 802.11, does not

provide adequate security for protecting a WLAN against unauthorized access or eavesdropping. As WLANs get larger and greater in number, a solution needs to be found that will provide stronger encryption of data and reliable authentication to network resources. My project will look into the flaws of the WEP algorithm and will present ideas that will make packet delivery over wireless networks more secure.

Bibliography

- [1] Arbaugh, William A. and Narendar Shankar and Y.C. Justin Wan. Your 802.11 Wireless Network has No Clothes. 2001. 16 Sept 2002.
<http://www.cs.umd.edu/~waa/wireless.pdf>.
- [2] Bellare, Steven M. Problem areas for the IP security protocols. In 6th USENIX Security Symposium, San Jose, California, July 1996. USENIX.
- [3] Blaze, Matt and John Ioannidis. Trust management for IPsec. ACM Transactions on Information and System Security. ACM Press. Volume 5, Issue 2, May 2002.
- [4] Borisov, Nikita and Ian Goldberg and David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. 16 Sept 2002.
<http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf>.
- [5] Braden, B., D. Borman, and C. Partridge. Computing the internet checksum. Internet Request for Comment RFC 1071, Internet Engineering Task Force, September 1988.
- [6] Brown, Michael, Donny Cheung, Darrel Hankerson, and Julio Lopez Hernandez. PGP in Constrained Wireless Devices. In 9th USENIX Security Symposium, Denver, Colorado, August 2000. USENIX.
- [7] Chown, P. Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS). Internet Request for Comment RFC 3268, Internet Engineering Task Force, June 2002.
- [8] Kent, Stephen and Randall Atkinson. Security Architecture for the Internet Protocol. Internet Request for Comment RFC 2401, Internet Engineering Task Force, November 1998.
- [9] LAN MAN Standards Committee of the IEEE Computer Society. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ANSI/IEEE Std 802.11, 1999 Edition.
- [10] Mitchell, C.J. Remarks on the security of the *Alpha1* stream cipher, Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2001-8, December 2001, 5 pages.
- [11] O'Hara, Bob and Al Petrick. IEEE 802.11 Handbook: A Designer's Companion. Standards Information Network IEEE Press. 1999.
- [12] Samarati, Pierangela. An authorization model for a public key management service. ACM Transactions on Information and System Security. ACM Press. Volume 4, Issue 4, November 2001.
- [13] Schaad, J. and R. Housley. Advanced Encryption Standard (AES) Key Wrap Algorithm. Internet Request for Comment RFC 3394, Internet Engineering Task Force, September 2002
- [14] Steiner, Michael. Secure password-based cipher suite for TLS. ACM Transactions on Information and System Security. ACM Press. Volume 4, Issue 2, May 2001.
- [15] Walker, Jesse, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000.
- [16] Yeun, Chan Yeob. Design, Analysis and Applications of Cryptographic Techniques. Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2001-5, November 2001.
- [17] Zhang, Yongguang and Bikramjit Singh. A Multi-Layer IPsec Protocol. In 9th USENIX Security Symposium, Denver, Colorado, August 2000. USENIX.