STATE BASED WEP-SECURITY PROTOCOL FOR WIRELESS NETWORKS

VivekAnand.V ,Ravishankar.S,Vijaybalaji.M
College of Engineering,Guindy
Anna University,Chennai-25.

ABSTRACT

SBW(State Based WEP) is a hybrid model of State Based Key Hop (SBKH) and WEP(WIRED EQUIVALENT PRIVACY).It is similar to SBKH except that it has less memory constraints. It provides a strong, light weight encryption scheme for Wireless Devices where battery power is a significant constraint. It eliminates all the security issues with WEP using the existing hardware at a speed greater than WEP and Wi-Fi Protected Access(WPA) 1.0 or 2.0. ***It is a moderate solution between the high memory requirements of SBKH and high power consumption of WPA 1.0 and 2.0.***

GENERAL TERMS
Security, Performance

KEYWORDS
Computer Security, Masker, Synchronization, Low Power Security

1.0 INTRODUCTION

1.1BACKGROUND

1.1.1 Wired Equivalent Privacy (WEP)

[IEEE802.11 1999] defined an encryption scheme called wired equivalent privacy (WEP), to provide security to the 802.11 users. WEP is a symmetric encryption scheme in which a WEP key is known or shared between two communicating nodes. WEP uses RC4 algorithm to do per packet encryption. RC4 algorithm is a stream cipher scheme [FM 2001, Mantin 2001] in which the data is encrypted by XORing data with the cipher stream generated by RC4 from an RC4 seed. WEP concatenates the WEP key (40 or 104 bits) and the initialization vector (IV) (24 bits), as the RC4 seed.

1.1.2 Wi-fi Protected Access (WPA)

IEEE 802.11i [Draft802.11 2003]'s first proposal for 802.11 legacy devices (WPA 1.0) encapsulates WEP functionalities by temporal key integrity protocol (TKIP). TKIP and Michael algorithms add significant processing on every packet. They also add additional overhead of 12 octets in every packet (without fragmentation) which can contribute to additional power consumption during transmission and reception. IEEE 802.11i's second part (WPA 2.0) uses Advanced Encryption Standard (AES) and requires change in hardware. WPA 2.0 also adds an overhead of 8 octets to every packet. Thus WPA 2.0 can also be very expensive.

1.1.3 State Based Key Hop(SBKH)

[SM12004] introduced the concept of SBKH for battery operated devices such as sensors in Wireless sensor network and Small Office Home Office(SOHO). It is indeed a simple, robust, light weight security protocol carrying out power efficient

encryption. Whereas WEP and WPA initialize RC4 state for every packet and generates a cipher stream from the initialized RC4 state, SBKH does not reinitialize RC4 states, rather it maintains a RC4 seed for a duration. Since each state is 258 octets, the total memory requirement for a single duplex connection is around 2KB.

2.0 DETAILED DESCRIPTION

2.1 SBW PROTOCOL OVERVIEW

SBW is also an State Based Encryption model in which the communicating nodes share a common knowledge of the shared state. However SBW invokes the RC4-KSA and the RC4-PRGA for every packet unlike SBKH. This is because the 24-bit Initialization Vector(IV) is used for each packet unlike SBKH. In SBKH the initialization vector was eliminated because the exposure of the IV lead to dictionary attacks. In SBW the dictionary attack is handled in a different way. Even though 24 bits is allocated for the IV, only 23 bits are used for generating the cipher stream. The dummy bit will be one of the 24 bits and the position of the dummy bit is changed for each packet. Since five bits are required to specify the position of the dummy bit, the state information in SBW is five bits unlike 258 octets in SBKH. It provides an effective way to hinder the intruder to impose the traditional dictionary attack on the network. Since the position of the dummy bit changes for each packet the IV is hidden from the intruder

2.2 SBW PROTOCOL DETAILS

Communication State

The State is a five bit information and for successful transmission both the nodes have to be in the same state i.e. encryption state synchronized. Since nodes A and B operate asynchronously, a pair of states are maintained for each communication direction i.e. uplink and downlink. SBW has two pairs of RC4 states: Previous Communication states(PCu and PCd) and Current Communication States(CCu and CCd). PC are the communication states for the previously successfully transmitted SBW encrypted packet. CC are the communication states with which encryption and decryption of the subsequent packets take place. The notation CCu,j,a corresponds to a state CCu for packet j being sent to node B.

Sequence Counter

SBW uses a sequence counter maintained for each direction(SCu and SCd). The sequence counters helps to handle retransmission and packet drops and helps in decision making when we try to decrypt the incoming packet.

2.3 PROTOCOL OPERATION

When the communication begins

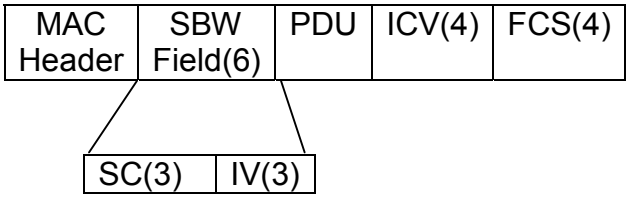
SCu = SCd = 0

PCu = PCd = CCu = CCd = 0

A sends packet j in its uplink encrypted at CCu,j,a to B. After receiving packet j, B compares SCu,j with its SCu,j-1 which according to B was the last successfully acknowledged packet's SCu. If SCu,j - SCu,j-1=1, then B decrypts packet j at CCu,j,b. After successful decryption (CCu,j,b = CCu,j,a) B acknowledges the packet to A and also updates its SCu to SCu,j. B then updates its PCu,j+1,b = CCu,j,b and its CCu = CCu,j+1,b , the state where decryption of the packet corresponding to SCu,j+1 will begin. After the receipt of B's acknowledgment, A updates its PCu,j+1,a = CCu,j,a and its CCU = CCu,j+1,a, the state where encryption of the packet with SCu = j+1 will begin . A also updates SCu = SCu,j+1 which will be used in packet with SCu = j+1. The same discussion applies for packets sent by B to A on its downlink.

If the packet hasn't reached A, PC and CC at both A and B are not updated and hence the subsequent retry doesn't cause any problem. If the transmission of packet j is a retry (retryfield in MAC frame set to 1), and if B previously acknowledged packet j and updated CCU to CCu,j+1,B, and PCu to PCu,j+1,b (= CCu,j,b), then B decrypts the packet from PCu,j+1,b or could optimize by sending an acknowledgment without re-decrypting.

The updation of CCu to CCu,j+1,b is done by using the first generated five bits of the cipher stream generated for the previous IV.



3.0 ANALYSIS

State Based WEP's intelligent IV exposure makes it resilient towards Dictionary attacks since the dummy bit position keeps on changing in a random fashion. It also helps to overcome FMS attack which was also due to the exposure of weak IV's. Replay attacks and modified attacks also fail for the same reason as in SBKH.

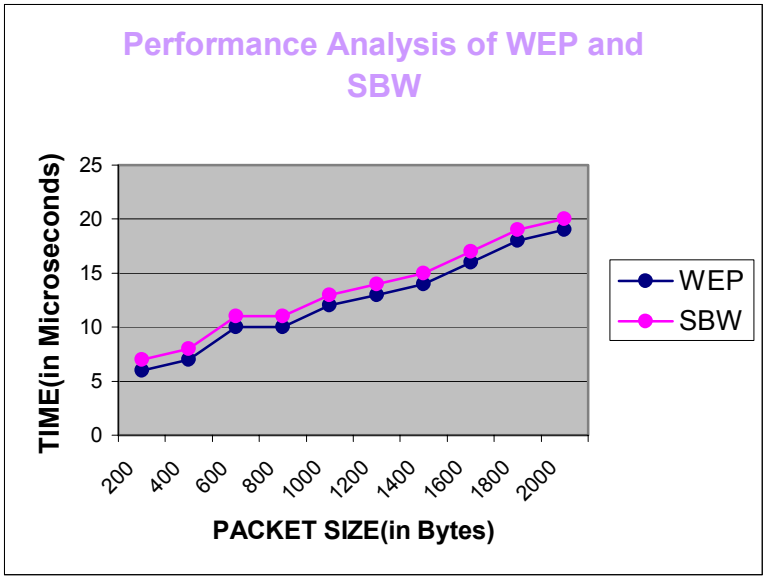
4.0 VERIFICATION OF THE PROTOCOL

The SBW Protocol was verified using the SPIN model checker and PROMELA(Process Meta Language). For the encryption and decryption to be successful both the nodes needs to be state synchronized. This property was verified using the model checker. The sequence counter helps in avoiding out of order packet receptions.

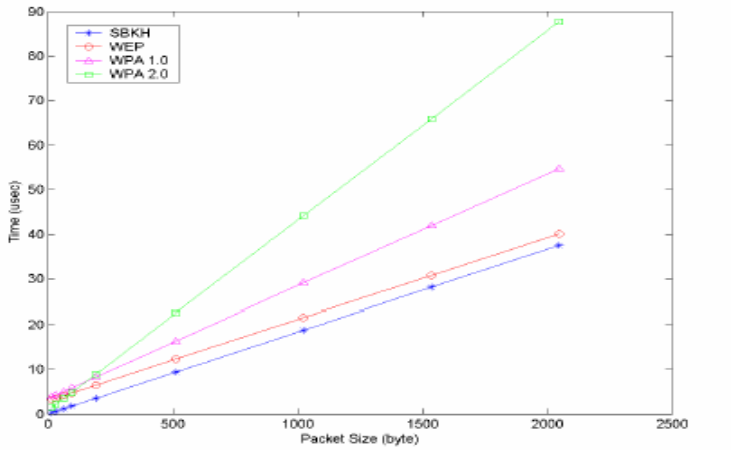
5.0 IMPLEMENTATION SETUP

The test bed consisted of an INTEL PENTIUM 4, 2.6 GHZ processor with LINUX operating system. The Encryption and decryption algorithms were written in C and used the OPENSSL –0.9.7, RC4 library. However the checksum calculation time was neglected since both SBW and WEP require the same operation.

6.0 RESULTS



From our implementation we determined that SBW took 1-2 microseconds more than WEP. From [SM2 2004] we can conclude that SBW has a processing speed greater than WPA 1.0 and 2.0 but less than SBKH. It requires a memory of 20 bits(3 bytes approx) compared to 2KB of SBKH for a Single Duplex connection.



The above result is from [SM2 2004] and shows WEP consumes less time than WPA 1.0 and 2.0.

7.0 CONCLUSION

SBW implements encryption in a state based approach similar to SBKH. It is a moderate solution between the high memory requirements of SBKH and high power consumption of WPA 1.0 and 2.0. Though it uses the simple RC4 algorithm, it still provides cheap and robust security.

8.0 FUTURE WORK

- Use of the dummy bit for intruder detection.
- Extension for broadcast operations.
- Analysis of WPA 1.0 and 2.0 with respect to SBW.

9.0 REFERENCES

[Draft 2003] Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: MAC Security Enhancements, IEEE Std. 802.11i/D7.0, Oct. 2003.

[IEEE802.11 1999]Telecommunications and Information Exchange Between Systems – Local and Metropolitan Networks – MAC and PHY Control, IEEE Press 1999.

[FM 2000] Fluhrer S. and McGrew D. Statistical Analysis of the Alleged RC4 Keystream Generator, FSE: Fast Software Encryption, FSE2000, Springer-Verlag, 2000.

[FMS 2001] Fluhrer S., Mantin I., Shamir I., Weaknesses in the key scheduling algorithm of RC4, SAC'2001, 2001.

[Mantin 2001] Mantin I., Analysis of the Stream Cipher RC4. Weizmann Institute of Science, Nov. 2001.

[PK 2003] Prasithsangaree P., Krishnamurthi P., Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs, Global Telecommns. Conf., Globecom '03, Dec. 2003.

[SM1 2004] Srinivasan K., Michell S., State Based Key Hop (SBKH) Protocol, Wireless 2004 Conference, Jul. 2004.

[SM2 2004] Srinivasan K., Michell S., Performance of State Based Key Hop (SBKH) Protocol for Security on Wireless Networks, IEEE Vehicular Technology Conference 2004 Fall, Sep. 2004.

[SM3 2004] Srinivasan K., Michell S State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks, 1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN 2004). Venice, Italy. October 4, 2004.