The Analyse of Wireless Communication Encryption Technologies. Modificated WEP Protocol

Orest Kavka, Iurii Garasym, Valerii Dudykevych

Abstract – **In this paper wireless communication encryption technologies were alalysed, modificated WEP protocol was proposed.**

Keywords – **encryption technologies, wireless communication, WEP, WPA and WPA2 protocol.**

I. INTRODUCTION

Modern wireless technologies use a limited set of methods and facilities of information security and also network development management facilities. It gives an opportunity to malefactors, who are near from wireless structures to carry out a number of attacks which were impossible in wire communication networks. Nowadays the most popular wireless applications security technologies are WEP, WPA and WPA2 enciphering protocols, which have their advantages and disadvantages.

II. WEP MODIFICATION

The idea of protocol modification is to update the shared secret key between the access point and the wireless nodes. The update procedure depends on the following parameters: network traffic and number of transmitted frames.

From Borisov et al [1] it's always run a risk of repeating IVs after 5000 frames due to birthday paradox [2]. Suppose it would be a WEP system where after every 5000 frames shared secret key is changed. Network traffic determines the number of transmitted WEP frames and that is why these two parameters are important in determining when to change the shared secret key.

The aim is to minimize the information that an attacker can retrieve from the transmitted frames and minimize time available to him to launch an attack.

Access point creates the key mapping for the clients; it can use the MAC addresses of the client to generate the new-shared secret key (fig. 1).

In the conventional WEP frame Key ID field signifies which key out of the four possible keys is used to decrypt the current frame. Key IDs are from 0 to 3. Whenever the value of the Key ID field is greater than 3, one needs to subtract 4 from that key ID value to get the correct key to decrypt the current frame. Whenever the Key ID is greater than 3 it would indicate that the data payload is carrying the new-shared key for future encryptions. In this case this is an indication for the receiver that this frame has new shared secret key in its payload i.e. last 104 bits of the data payload before 32 bit CRC is the new shared key for future encryptions. Out of the four keys this new-shared secret key will replace the first one. On subsequent updates it will replace the second key, third key and so on. At a given point of time there are 4-shared keys and new shared keys arrive at regular intervals and replace the old ones. Data Payload will be as usual except that it makes provision for extra 104 bits when the new shared secret key is being sent. When the receiver decrypts the frame it takes out the last 104 bits in the data payload and uses them as the shared secret key for future encryptions.

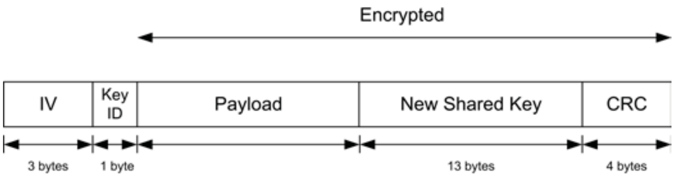

Figure 1. Modificated WEP Frame Structure

There are two different approaches to using keys under WEP; these are default keys and key mapping keys [3]. In the default keys all the wireless nodes and access points have the same set of shared secret keys while in the case of key mapping keys every individual wireless node has different set of shared secret keys. The key mapping keys are more secure but are difficult for access points to handle.

III. CONCLUSION

The possible drawback one can identify with new method is the computational overhead associated with generating, and transmitting the session keys at the access point. In this paper has been shown that proposed modification to the existing WEP protocol makes it more secure and robust in terms of Message Privacy. The fact of frequently change the shared secret keys through the WEP mechanism makes any kind of cryptanalytic attack futile.

REFERENCES

1. Borisov N. Intercepting mobile communications : The insecurity of 802.11 [Text] / N. Borisov, I. Goldberg, D.Wagner. – Rome, Italy, 2001.

2. [Електронний ресурс] Режим доступу : http://en.wikipedia.org/wiki/Birthday_attack

3. Edney J. Real 802.11 Security Wi-Fi Protected Access and 802.11i [Text] / J. Edney, W. A. Arabaugh. – Pearsons Education Inc. – 2004.

Orest Kavka – is a Student at Informational Security Department, Lviv Polytechnic National University, S. Bandery Str., 12, Lviv, 79013, UKRAINE,
E-mail: orestkavka@gmail.com

Iurii Garasym is an Engineer at Informational Security Department, Lviv Polytechnic National University, 12, S. Bandery Str., Lviv, 79013, UKRAINE,
E-mail: garasym_yr@polynet.lviv.ua

Valerii Dudykevych is Professor, the Head of Informational Security Department, Lviv Polytechnic National University, 12, S. Bandery Str., Lviv, 79013, UKRAINE,
E-mail: vdudykev@polynet.lviv.ua