Wep essay examples

Business, Company

ASSIGN BUSTER

Background

WEP refers to Wired Equivalent Privacy. WEP was one of the first encryption policies designed for wireless network security. WEP is a security protocol that is stipulated in the Wireless Fidelity standard, 802. 11b (Networld). This is designed in such a way as to allow wireless local area network. The security level and privacy of WEP is almost similar to that of a wired LAN. For a wired local area network, defence is normally employed by physical security means. These physical security mechanisms are suitable and effective in a controlled environment such as that provided by wired local area networks. However, when it comes to radio waves, it becomes difficult in the sense that the radio waves cannot be contained in a network. In such scenario, developers use the WEP to handle or provide a security solution similar to that offered in a physical environment such as that of a wired local area network. According Mehta (2001), WEP is specifically designed to protect the confidentiality of data from eavesdroppers. Additionally, WEP is designed to maintain data integrity or prevent any modifications of data from unauthorized access.

WEP Protocol Architecture

WEP uses two of the lowest layers of the Open Systems Interconnect reference model, physical layers and data links, which makes it not to offer end-to-end security. Ideally, WEP will depend on a single shared key between the communicating parties. For integrity checking, WEP uses the RC4 PRNG algorithm to check each packet, during communication.

WEP Weaknesses

WEP has been found out to have some weaknesses. These include key management, key size, integrity check vector (ICV) algorithm are not appropriate, small initialization vector (IV) and easy forging of authentication messages. When it comes to key management and key size, WEP does not have a specified key management standard. These make keys to be used for a long time and are of poor quality. In WEP, most wireless networks tend to use a single key being shared between each node on the wireless network. When using WEP, all access points and client stations are programmed with the same WEP key. What makes the key not to be changed is because the synchronizing of keys is a difficult and tiresome process. Additionally, the 802. 11 standard used in WEP does not have specifications for key sizes greater than 40 bits. This makes it difficult to make keys that are more complex.

Another weakness that is common in WEP is the small initialization vector (IV). According to Networld website, the IV for WEP of size 24 bits gives 16, 777, 216 distinct RC4 cipher streams for a specific WEP key. Attackers can easily reuse the IV to produce RC4 cipher streams, which then allows them to decrypt any succeeding packets easily that have been encrypted with the same initialization vector. Additionally, WEP allows easy forging of authentication messages, which allows an unauthorized decryption and infringement of data integrity. This will occur once the WEP key is revealed and can be accessed by a hacker. The hacker then transforms any ciphertext to comprehend the meaning of the data. The hacker then uses the transformed key to change the ciphertext and may forward the changed message to the receiver.

Moreover, WEP has another weakness in the form of the integrity check vector algorithm (ICV). The WEP ICV works on the CRC-32 platform algorithm, which is used for sensing noise and popular errors in the transmission. However, the CRC-32 performs badly when it comes to cryptographic hash.

Future of WEP

Researchers are currently suggesting improvement in the security of WEP. According to Weil (2001), there is a need to have better encryption of WEP. Not even the 128-bit encryption of WEP is considered secure. Vendors of the 802. 11 standard that is used are increasing the number of layers as a way of enhancing the security in WEP. Additionally, companies are being urged to have the wireless networks located outside the companies firewall as a measure of security. Hook (2001) suggested a few methods that can be employed to reduce the vulnerabilities that are posed by WEP. Because of the security issues that are common with the use of WEP, encryptions such as WPA (Wi-Fi Protected Access) are being used to replace it.

There has been an increase on hacking attacks on WEP. This has made most of experts in the computing field to consider the removal or discontinued use of WEP on wireless networks. Hacking has become faster, and efficient making it easier to retrieve the WEP keys. The most common attack that is being used currently is the active packet injection. Other challenges that commonly affect WEP are the denial of service attacks and defeating access control. However, eradicating the use of WEP becomes a challenge to most companies because of the cost implications. According to Wei (2001), most products used on wireless networks use the WEP standard, which makes even reducing the security attacks a problem. For security purposes, it is advisable, in this day of increased technology, is to avoid using WEP as the only solution to security issues.

Bibliography

Mehta, P. 2001. Wired Equivalent Privacy Vulnerability. [online]. Available at <> [Accessed December 12, 2012].

WEP (wired equivalent privacy). (n. d.). Network World. [Online]. Available at <>. [Accessed 12 December 2012].

Weil, N. 2001. Wireless Security Flawed, Researchers Report |
PCWorld. PCWorld - News, tips
and reviews from the experts on PCs, Windows, and more. [online]. Available at < > [Accessed 12 December 2012].