The wep processes encryption computer science essay

Business, Management

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Considered one of the first security mechanisms introduced by industries Wired Equivalent Privacy (WEP) , it ‘ s considered as a portion of 802. 11 criterion for coding WLAN traffic.

Wired tantamount privateness is a shared-secret key encoding system used to code packages transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communicating from listen ining. A secondary map of WEP is to forestall unauthorised entree to a radio web.

WEP encrypts the warhead of informations packages. Management and command frames are ever transmitted in the clear. WEP uses the RC4 encoding algorithm invented by Ron Rivest to code all web informations traffic. The shared-secret key is either 40 or 104 spots long. The system decision maker chooses the key. This cardinal must be shared among all the

Stationss and the AP utilizing mechanisms that are non specified in the IEEE 802.

11. [1]

WEP Procedures:

Encoding:

Figure (1) WEP Encryption [2]Based on Figure (1) , The WEP protocol uses two procedures that are applied to the plaintextinformations. The first one encrypts the plaintext and the 2nd one protects it against anyunauthorised alterations.

Then, the secret key, 40 spots of size is combined with a 24 spotslow-level formatting vector (IV) ensuing in a 64-bit sum cardinal size. The ensuing key is placed intothe pseudorandom figure generator (PRNG) . The PRNG (RC4) on its bend, outputs a pseudorandom cardinal sequence based on the input key. Then, the ensuing sequence is beingused for informations encoding by making a bitwise XOR.

Decoding:

In the decoding procedure The IV (Initialization Vector) of the incoming message is used for the coevals of the sequence cardinal necessary for the decoding of the incoming message. As shown in figure (2)Figure (2) WEP decoding [2]The combination of the ciphertext and the proper cardinal sequence produces the original plaintext and ICV (Integrity Check Value) . The decoding is verified by executing the unity cheque algorithm on the

recovered plaintext and comparing the end product ICV to the ICV transmitted with the message.

In instance where the end product ICV is different from the ICV transmitted, the receive message is in mistake and an mistake indicant will be sent to the MAC direction and to the directing station. Mobile clients with erroneous messages caused by the inability to decode will non be able to authenticate and entree the web resources. In fact, the WEP protocol provides some security steps for the IEEE 802. 11 but it still remains uneffective face to certain onslaughts.

Several researches or paperss prove the ineffectualness of the WEP. [7, 20, and 43] .

WEP Authentication:

Authentication in WEP involves authenticating a device when it foremost joins the LAN.

The hallmark procedure in the radio webs utilizing WEP is to forestall devices/stations fall ining the web unless they know the WEP key. Figure (3) shows the WEP hallmark procedure. Figure (3) WEP AuthenticationIn WEP-based hallmark, wireless device sends authentication petition to the radio entreepoint, so wireless entree point sends 128 spot random challenge in a clear text to the requestingclient. The wireless device uses the shared secret key to subscribe the challenge and sends it to thewireless entree point. Wireless entree point decrypts the signed message utilizing the shared secretkey and verifies the challenge that it has sent earlier.

If the challenge lucifers, so hallmark succeeds otherwise non. Unfortunately, in WEP, no secret key is exchanged after hallmark. The same secret key orshared key is used for both hallmark and encoding. So there is no manner to state whether thesubsequent messages come from the sure device or from an imposter.

This sort ofhallmark is prone to adult male in the in-between onslaught. This hallmark is truly non a best attempthere. In the Wi-Fi specification, hallmark was wholly dropped, despite being in theIEEE 802. 11 criterion.

A history of WEP and RC4 [6]

WEP was antecedently known to be insecure. In 2001 Scott Fluhrer, Itsik Mantin, and Adi Shamir published an analysis of the RC4 watercourse cypher.

Some clip subsequently, it was shown that this onslaught can be applied to WEP and the secret key can be recovered from approximately 4, 000, 000 to 6, 000, 000 captured informations packages. In 2004 a hacker named KoReK improved the onslaught: the complexness of retrieving a 104 spot secret key was reduced to 500, 000 to 2, 000, 000 captured packages. In 2005, Andreas Klein presented another analysis of the RC4 watercourse cypher. Klein showed that there are more correlativities between the RC4 keystream and the key than the 1s found by Fluhrer, Mantin, and Shamir which can to boot be used to interrupt WEP in WEP like use manners.

Aircrack-ptw onslaught

Aircrack-ptw is able to widen Klein ‘ s onslaught and optimise it for use against WEP. Using aircrack-ptw ‘ s version, it is possible to retrieve a 104 spot WEP key with chance 50 % utilizing merely 40, 000 captured packages. For 60, 000 available informations packages, the success chance is about 80 % and for 85, 000 informations packages about 95 % . Using active techniques like deauth and ARP re-injection, 40, 000 packages can be captured in less than one minute under good status.

The existent calculation takes about 3 seconds and 3 MB chief memory on a Pentium-M 1. 7 GHz and can to boot be optimized for devices with slower CPUs. The same onslaught can be used for 40 spot keys excessively with an even higher success chance.

WEP Vulnerabilities:

Execution of IV Mechanisms: The procedure of implementing IV mechanisms has the protocol vulnerable in the antonym of strengthen the encoding.

The intent of IV in RC4 procedure is to do certain that no key is repeated, therefore WEP uses 40 spot protection with a 24 spot IV, therefore the 24 spot Four infinite can be used within few hours and IV ‘ s are repeated once more As the shared key is fixed, the key to RC4 cardinal watercourse generator is repeated if IV ‘ s are repeated. This violates the RC4 regulation of ne’er reiterating the keys. As IV is sent in clear text, the aggressor can place when IV hit occurs. IV hits help aggressor to find the cardinal

watercourse. By analysing the two packages derived from the same IV, cardinal watercourse can be obtained.

Same key is shared: The same key is shared between entree point and wireless device. If there are multipleUsers/devices utilizing the same key, this helps to do the onslaughts on WEP more practical andincreases the opportunities of IV hit. The cardinal alteration at entree point requires every user toalter their cardinal consequently.

So, the cardinal direction is hard to administrate manually. Hence, most of the users do n’t alter acesspoint keys often. They keep the same key for many months or old ages or everlastingly which buys the aggressor more clip to analyse the traffic and place the keystream and IV reuse [4] . Checksum failure to protect informations unity: In WEP, information unity is verified utilizing the CRC checksum operation. The thought behind CRC is toto forestall anyone from fiddling with the message in theodolite.

The CRC is performed on theplaintext but non on the ciphertext. CRC was designed to observe random mistakes in the message butnon to forestall from any harmful onslaughts. It is possible to do alterations to the ciphertext withoutimpacting the checksum. This shows that the WEP checksum failed to protect informations unity (one of the chief ends of the WEP) [4] .

Known plaintext onslaughts: If an aggressor knows the plaintext he/she can easy calculate the checksum and can shoot the bad messages into the web. An aggressor can besides alter the finish reference of the package and replace the old CRC with the modified CRC and besides recomputed the IP

checksum. The entree point wo n’t be able to detect the alterations to the original package and send on it to the selected IP reference [5] . Denial of Service Attacks: Missing strong hallmark methods, DoS are fiddling to implement. An aggressor can enter valid WEP packages and so retransmit them subsequently (play back onslaught) [5] .