Security of the WEP algorithm (Wired Equivalent Privacy)

By:

- **Nikita Borisov**
- **Ian Goldberg**
- **David Wagner**, UC BERKELY

What is WEP?

- The IEEE came up with the 802.11 standard for wireless ethernet.
- The 802.11 standard describes wireless Local Area Networks (LANs).
- Wired Equivalent Privacy algorithm is part of 802.11 standard.

Why WEP?

- Wireless connections has important security issues to keep the intruders from accessing, reading and modifying the network traffic.
- But mobile systems need to be connected.
- We need an algorithm which provides the same level of security that physical wire does.

WEP algorithm is used to:

- **Protect wireless communication from eavesdropping.**
- **Prevent unauthorized access to wireless network** (feature of WEP, but not an explicit goal in the 802.11 standard)

Three security goals of WEP protocol

- **Access Control**
  - Ensure that your wireless infrastructure is not used.
- **Data Integrity**
  - Ensure that your data packets are not modified in transit.
- **Confidentiality**
  - Ensure that the contents of your wireless traffic is not learned

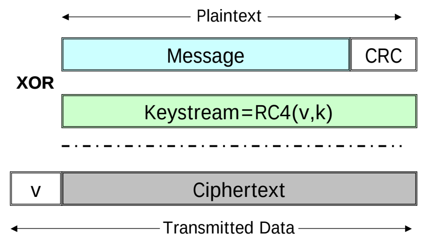
Description of WEP Protocol

- WEP relies on a ***secret key*** which is shared between the sender and the receiver.
  - SENDER: Mobile station (eg.Labtop with a wireless ethernet card)
  - RECEIVER: Access Point (eg. base station)
- ***Secret Key*** is used to encrypt packets before they are transmitted
- ***Integrity Check*** is used to ensure packets are not modified in transit.
  - The standard does not discuss how shared key is established
  - In practice, most installations use a **single key** which is shared between all mobile stations and access points.

Description of WEP Protocol (Cont.)

- To send a message M:
  - Compute a checksum c(M) (is not depend on secret key k)
  - Pick an IV v and generate a keystream RC4(v,k)
  - XOR <M,c(M)> with the keystream to get the ciphertext
  - Transmit v and ciphertext over a radio link
- When received a message M
  - Use transmitted v and the shared key k to generate the keystream RC4(v,k)
  - XOR the ciphertext with RC4(v,k) to get <M',c'>
  - Check is c'=c(M')
  - If it is, accept M' as the message transmitted

Picture of WEP



RC4 (Stream Cipher)

- WEP uses RC4 encryption algorithm known as "stream cipher" to protect the confidentiality of its data.
- Stream cipher operates by expanding a short key into an infinite pseudo-random key stream.
- Sender XORs the key stream with plaintext to produce ciphertext.
- Receiver has the copy of the same key, and uses it to generate an identical key stream.
- XORing the key stream with the ciphertext yields the original message.

This operation creates some attacks.

- If an attacker flips a bit in ciphertext, then after decryption, that bit in the plaintext will be flipped.
- If an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts.
- Knowledge of this XOR can enable the statistical attacks to recover the plaintexts.

Defenses of WEP to these attacks

- Integrity Check(IC) field
  - Used to ensure that packet has not been modified in transit
- Initialization Vector(IV)
  - Used to avoid encrypting two ciphertexts with the same key stream
  - Used to argument the shared key and produce a different RC4 key for each packet

Attack types

- Passive attacks
  - to decrypt traffic based on statistical analysis
- Active attacks
  - To inject new traffic from authorized mobile stations, based on known plaintext
- Active attacks
  - To decrypt traffic, based on tricking the access point
- Dictionary building attacks
  - Allows real-time automated decryption of all traffic

Passive attack

- A passive eavesdropper can intercept all wireless traffic.
- By XORing two packets, attacker obtains the XOR of two plaintext message.
- The resulting XOR can be used to infer data about the content of the two messages.

Active attack

- If attacker knows the exact plaintext fro encrypted message , he can use this knowledge to construct correct encrypted packets

Active attack from both ends

- The attacker makes a guess about not the contents, but the headers of the packet.

Table-based attack

- Small space of possible initialization vector allows attacker to build a decryption table.Once he learns the plaintext for some packet, he can compute the RC4 key stream.

Conclusion

- WEP isn't.

References

- N. Borisov, I. Goldberg, D. Wagner.Intercepting mobile communications:The insecurity of 802.11. *7th Annual International Conference on Mobile Computing and Networking*. July 16-21,2001. Rome, Italy.
- I. Goldberg. An analysis of the Wired Equivalent Privacy protocol. *Black Hat Briefings*, July 11, 2001. http://www.cypherpunks.ca/bh2001/
- Security of the WEP algorithm, uc Berkeley. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html