

Homework 2 solution:

“Wired Equivalent Privacy” (WEP) is the encryption protocol standardized in the IEEE 802.11 Wireless LAN standard. Hacker “warez” are readily available for download on the Internet to analyze WLAN traffic and recover the cleartext traffic.

Research the publicly available literature on WEP attacks and briefly summarize how these attacks work. Suggest a few simple changes that could be made to 802.11 that would have made these attacks much more difficult.

---

There are two primary weaknesses with popular implementations of WEP that subject 802.11 networks to compromise:

1. Short Initialization Vectors (IVs) are used
2. Fixed, system-wide Key Variables are used

These weaknesses are compounded by two characteristics of 802.11 networks:

1. The data protocol contains fixed, repetitive patterns
2. The network is a wireless network

Since the IVs are short, the probability that an IV “collision” will occur, that is the probability that two packets will be sent using the same IV, is moderately high. For a large corporate network, a high level of utilization is likely to occur. Estimates suggest that in less than one business day, a sufficient number of 802.11 packets will be transmitted to virtually guarantee an IV collision. Remember that, although the number of independent IVs is rather large ( $\sim 2^{24}$ ), the “Birthday paradox” increases the likelihood that some pair of IVs will match. It is not necessary that we observe a match with any specific IV. Finding that an IV collision has occurred, the attacker can now rely on the occurrence of fixed patterns in the plaintext to attack the key stream. He knows that the key generator initial state of the two messages was the same, given the IV collision, and knows that the plaintext matches for fixed fields in the message. This gives an unnecessary advantage to knowing the value of the key stream. Note that in residential applications, far less traffic is expected, so it will probably take much longer for an attacker to gather sufficient packets to observe an IV collision.

The second major issue is a key management problem. For most implementations, it is not convenient to change the key variable with any frequency. Often a user organization will set a single key variable system wide and leave it unchanged for the lifetime of the system. This means that the attacker has all the time in the world to attack the system. Yesterday’s collected IVs are useful today, since the key variables are the same. A more significant threat, and one that any well designed cryptosystem should not fall prey to is compromise of past information with a current attack. If a hacker discovers the current key variable, then they can use this to recover ALL historical information that was encrypted in the same variable.

Since so much of the WEP is static, the attacker can precompute much of the information they need to attack a system. With large amounts of data storage readily available, this type of attack is quite feasible and becoming more so.

Finally, since 802.11 is a wireless network, physical proximity to the network is not needed to mount an effective attack. Realistically, an attacker who is a thousand feet from a corporate AP, using only the antenna in their PCMCIA card will probably not be able to easily monitor traffic, given signal losses through walls and over the distance, but with high gain antennas, in campus-like office settings, attacks may well be feasible. The greatest wireless threat comes from the home users AP, which might be well within range of their neighbor.

These attacks are the worst kind – passive attacks requiring only monitoring of transmissions. WEP is also susceptible to active attacks, through the manipulation of messages and

checksums. Users who can modify and replay messages can disrupt the integrity of a data network. Users who can insert arbitrarily generated and modified messages can direct them to their own IP address, using the APs to decrypt messages for them.

The simplest and most obvious fix to WEP is to reduce the attackers advantage in short, repetitive IVs. By using longer IVs, the collision rate can be reduced substantially. IVs can be reinitialized less frequently if the terminal and AP treat an association as a unit and bridge the state of the KG from one transmission to the next. This requires more bookkeeping, maintaining a session index for each terminal-AP association, accounting for lost packets, but would have less overhead than a longer IV per packet.

All users using the same KV for long periods of time is another item that requires a fix. As a minimum, smaller user groups are needed, each with a separate net KV. This would probably cause the greatest complexity for an attacker, since he would not necessarily know which transmission was associated with which net. Ideally, each user should use their own KV to communicate with the AP. In this way, a significant amount of traffic would be needed for each user under attack. This would also have the effect of compartmentalizing user vulnerability – a successful attack against one user would not compromise another. Finally, a key variables should be updated on a much shorter schedule than “whenever we get around to it.” Historical traffic must be protected against future compromise, which can only be accomplished with shorter “crypto-periods,” intervals of time between key variable changes. High volume users, with more exposed IVs could have shorter crypto-periods than low volume users, high sensitivity users might have shorter crypto-periods as well.

Some other intrinsic changes to 802.11 that would counter the weaknesses in WEP:

1. APs should throttle back power output to the minimum needed for effective communications. This reduces the threat of monitoring
2. APs should not broadcast their System ID in the clear – if a network cannot be identified reliably, it is much more difficult to attack
3. MAC address filtering at the AP reduces, but does not eliminate, the risk of active attack. MAC addresses can be cloned, but not as easily as the other attacks can be mounted.