Wired Equivalent Privacy Protocol

Author(s):

Summary: The Wired Equivalent Privacy (WEP) protocol, described in [80299], is used to protect data during wireless transmission.

Protocol specification (in common syntax)

```
A, B :  principal
Kab :   symkey
RC4 :   message, symkey -> message
C :     message -> message

1.   A  ->  B  :    v, ((M,C(M)) xor RC4(v,Kab))
```

Description of the protocol rules

To encrypt the message `M`, `A` applies the operator xor to `RC4(v,Kab)` and `(M,C(M))` where `C(M)` is the *integrity checksum* of the message `M` and `RC4` is a function modeling the RC4 algorithm which is used to generate a *keystream* (*i.e.* a long sequence of pseudo-random bytes) from the initial vector `v` and the secret key `Kab` shared between `A` and `B`. To decrypt the received message, `B` computes `RC4(v,Kab)` and after applying exclusive or, he obtains `(M,C(M))` and can verify that the checksum is correct.

The properties of exclusive or are:

$$
\begin{aligned}
\texttt{x xor (y xor z)} &= \texttt{(x xor y) xor z} \quad \text{(E1)}\\
\texttt{x xor y} &= \texttt{y xor x} \quad \text{(E2)}\\
\texttt{x xor 0} &= \texttt{x} \quad \text{(E3)}\\
\texttt{x xor x} &= \texttt{0} \quad \text{(E4)}
\end{aligned}
$$

References

[80299]

Claimed attacks

We present below attacks given in [BGW01] that require the following properties:

$$
\begin{aligned}
\mathtt{C(x\ xor\ y)} &= \mathtt{C(x)\ xor\ C(Y)} \quad \text{(E5)}\\
\mathtt{(x1,y1)\ xor\ (x2,y2)} &= \mathtt{(x1\ xor\ x2,y1\ xor\ y2)} \quad \text{(E6)}
\end{aligned}
$$

According to [BGW01], (E5) is a general property of CRC checksum.

The first attack uses the fact that encrypting two messages `P1` and `P2` with the same initial vector `v` and with the same key `k` can reveal information. Indeed, we have the following equalities between the ciphers `C1` and `C2` and their associated plain text `P1` and `P2`:

$$
\begin{aligned}
\mathtt{C1\ xor\ C2} &= \mathtt{((P1,C(P1))\ xor\ RC4(v,k))\ xor\ ((P2,C(P2))\ xor\ RC4(v,k))} &\\
&= \mathtt{((P1,C(P1))\ xor\ (P2,C(P2)))\ xor\ (RC4(v,k)xor\ RC4(v,k))} & \text{(E1)(E2)}\\
&= \mathtt{(P1,C(P1))}\ \text{xor}\ \mathtt{(P2,C(P2))} & \text{(E3)(E4)}
\end{aligned}
$$

This allows an intruder who knows a plain text `P1` and its cipher `C1` to decrypt any cipher `C2`. Indeed, thanks to this equality, the intruder can easily get `(P2,C(P2))` and obtain the plaintext `P2`.

The second attack allows the intruder controlled modifications to a cipher text without disrupting the checksum. Assume that the intruder has intercepted `(M,C(M))xor RC4(v,Kab)` and knows `D`. He can now obtain the cipher text associated to the message `Mxor D` by computin g:

$$
\begin{aligned}
\mathtt{((M,C(M))\ xor\ RC4(v,Kab))\ xor\ (D,C(D))} &= \mathtt{RC4(v,Kab)xor((M,C(M))\ xor\ (D,C(D)))}\\
&= \mathtt{RC4(v,Kab)\ xor\ (M\ xor\ D,C(M)\ xor\ C(D))}\\
&= \mathtt{RC4(v,Kab)\ xor\ (M\ xor\ D,C(M\ xor\ D))}
\end{aligned}
$$

Notice that this attack can be applied without full knowledge of `M`. For example, to flip the first bit of `M`, the attacker can set `D = 100...0`. Now, if the intruder knows the plaintext `M` (and its associated cipher) he can generate the ciphertext associated to any message he wants.

Citations

[80299] IEEE 802.11 Local and Metropolitan Area Networks: Wireless LAN Medium Acess Control (MAC) and Physical (PHY) Specifications, 1999.

[BGW01] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. In *Proc. 7th Annual International Conference on Mobile Computing and Networking (MOBICOM'01)*, pages 180–188, Rome (Italy), 2001. ACM Press.