Security (Part 2) 2001 Second Question

P 89b
RJA

In the Wired Equivalent Privacy protocol used in IEEE 802.11 networks, data are protected at the link level during transmission on a wireless LAN. Each frame has a 32-bit CRC appended to it; it is then encrypted using the RC4 stream cipher, initialised with a shared key and a 24-bit initial value; and finally, the initial value is ~~prep~~ sent with the encrypted frame.

(1) Why is the initial value used?

(2) Is the CRC an appropriate mechanism, and, if not, what should be used instead?

(3) Describe one passive attack on this system.

(4) Describe one active attack on this system.

(5) What would be the effect of upgrading from RC4 to a stronger cipher, such as AES used in output feedback mode?

Model answer

(1) To prevent keystream reuse + resulting attack in depth

(2) No, as it's linear over GF2 – just like the stream cipher
Use hash function instead

(3) Wait for IV reuse and get a depth; or recognise housekeeping traffic ~~[illegible]~~; or keysearch (keys are 40 bit in the standard)

(4) Inject known traffic to get IV + keystream, or tweak bits in known (guessed) traffic. The goal could be to copy observed packets to

an IP address under the control of the attacker, or to insert messages that defeat access controls directly (e.g., overwrite the password file).

(5) No effect so long as the cipher is additive. However, use of AES in CBC mode would fix the problem

(More details : http:// www.isaac.cs.berkeley.edu)