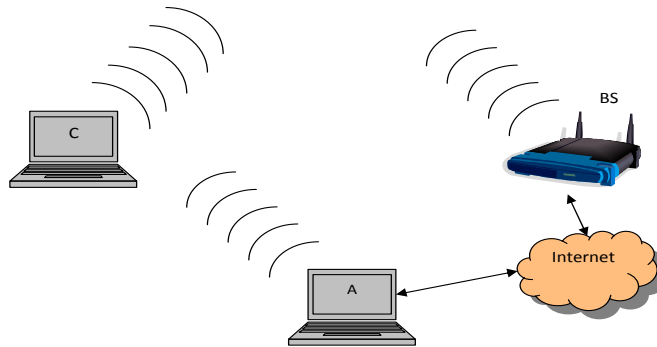


Network Security

Sumeet Priyadarshee Dash

September 14, 2009

Another Weak Point of WEP



Suppose the attacker is the BS's ISP.

1. The attacker can flip some bits in the ciphertext corresponding to the destination IP address and recompute the CRC to reflect the modified data.
2. He can then transmit the new ciphertext on the wireless channel and observe outgoing packets from the BS to the Internet.
3. Doing so the attacker can route any packet originating at the user to its own network. The BS then serves as a decryption oracle for the attacker. If the attacker owns a class A IP address network then he only needs to guess the position of the first byte of the destination IP.

How to design a good stream cipher?

In order to design a good stream cipher we need a good and secure pseudorandom number generator. The definition of a good random number generator would be as follows.

A function $G : \{0, 1\}^l \rightarrow \{0, 1\}^L$ is a (t, ϵ) secure pseudorandom number generator if $G \circ u_l \stackrel{t}{\sim} u_L$.

Theorem

If $G_1 : \{0, 1\}^l \rightarrow \{0, 1\}^L$ is a (t, ϵ_1) secure PRG and $G_2 : \{0, 1\}^L \rightarrow \{0, 1\}^M$ is a (t', ϵ_2) secure PRG running in time t' ; then $G_2 \circ G_1$ is a PRG which is $(t - t', \epsilon_1 + \epsilon_2)$ secure.

Proof

By Definition:

$$u_L \overset{t}{\sim} \epsilon_1 G_1 \circ u_l$$

By Data Processing Inequality and the above definition:

$$G_2 \circ u_L \overset{t-t'}{\sim} \epsilon_1 G_2 \circ G_1 \circ u_l$$

$$\Rightarrow G_2 \circ u_L \overset{t}{\sim} \epsilon_1 G_2 \circ G_1 \circ u_l \text{ [1]}$$

(If a PRG is $t-t'$ secure, it would indeed be secure in time $t > t - t'$)

By Definition:

$$u_M \overset{t}{\sim} \epsilon_2 G_2 \circ u_L \text{ [2]}$$

By transitivity of expressions [1] and [2]

$$G_2 \circ G_1 \circ u_l \overset{t-t'}{\sim} \epsilon_1 + \epsilon_2 u_M \square$$

Lemma

If $G_1 : l_1 \rightarrow L_1$ is (t_1, ϵ_1) secure and runs in time t'_1 and $G_2 : l_2 \rightarrow L_2$ is (t_2, ϵ_2) secure and runs in time t'_2 , then $G_1 \parallel G_2$ is $(t_3, \epsilon_1 + \epsilon_2)$ secure where $t_3 = \text{poly}(t_1, t_2)$.

Proof

$$\text{By Definition: } G_1 \circ u_{l_1} \overset{t_1}{\sim} \epsilon_1 u_{L_1}$$

Let us consider a function $f(x)$ s.t. $f(x) = x \parallel G_2(y)$ where $y \leftarrow u_{l_2}$.

The running time of f will almost be same as that of G_2 which is t'_2 .

Now, by data processing inequality:

$$f(G_1 \circ u_{l_1}) \overset{t_1-t'_2}{\sim} \epsilon_1 f(u_{L_1})$$

$$\Rightarrow G_1 \circ u_{l_1} \parallel G_2 \circ u_{l_2} \overset{t_1-t'_2}{\sim} \epsilon_1 u_{L_1} \parallel G_2 \circ u_{l_2} \text{ [1]}$$

$$\text{By Definition: } G_2 \circ u_{l_2} \overset{t_2}{\sim} \epsilon_2 u_{L_2} \text{ [2]}$$

By transitivity of expressions [1] and [2]

$$G_1 \circ u_{l_1} \parallel G_2 \circ u_{l_2} \overset{\min(t_1-t'_2, t_2)}{\sim} \epsilon_1 u_{L_1} \parallel u_{L_2}$$

$$G_1 \circ u_{l_1} \parallel G_2 \circ u_{l_2} \overset{\text{poly}(t_1, t_2)}{\sim} \epsilon_1 u_{L_1+L_2} \square$$

Goldreich, Goldwasser, and Micali construction

The GGM construction provides a mechanism to construct a pseudorandom function family using a pseudorandom number generator. The idea is that no algorithm should be able to distinguish between a function chosen randomly from the PRF family and a random oracle whose outputs are completely random.