

Network Security

Class 4, Lecture Notes

September 18, 2009

1 WEP contd...

Suppose the attacker is the Base station's ISP, then the attacker captures some ciphertext. If 'C' sends an encrypted message destined to some other person, first the Base Station decrypts the message and sends it across to the destination. If the attacker wants to attack, then he just changes the destination IP address to his address.

Attack:

- Flip some bits of the ciphertext corresponding to the destination IP address.
- Transmit new ciphertext on the wireless channel.
- Observe the outgoing packet from the Base Station to the internet.

Base Station acts as the decryption oracle.

In RC4 encryption, the key (104-bit) is concatenated with IV (24-bit). This is a very bad way of selecting the key. $IV \parallel K$ is stronger than $K \parallel IV$.

1.1 Definition:

A function $G : \{0, 1\}^l \rightarrow \{0, 1\}^L$ is a t, ϵ -secure Pseudo Random Generator if

$$G(u_L) \stackrel{t, \epsilon}{\sim} u_L$$

i.e. If we combine a string of 0's and 1's with G (which in turn expands the string) and compare with a long randomly generated bit string, then these 2 would be computationally indistinguishable.

1.2 Theorem:

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

By definition, $u_L \stackrel{t}{\sim}_{\epsilon} G_1(u_L)$.

By data processing inequality, $G_2 \circ u_L \stackrel{t-t'}{\sim}_{\epsilon_1} G_2 \circ G_1(u_L)$.

By definition, $G_2 \circ u_L \stackrel{t, \epsilon_2}{\sim} u_M$.

Hence, by transitivity, $u_M \stackrel{t-t', \epsilon_1 + \epsilon_2}{\sim} G_2 \circ G_1(u_L)$.

1.3 Lemma:

If $G_1is(t_1, \epsilon_1)$ secure that runs in time t'_1 and $G_2is(t_2, \epsilon_2)$ secure that runs in time t'_2 that runs in time t'_2 , then $G_1||G_2ist_3, \epsilon_1 + \epsilon_2$ -secure, where $t_3 = poly(t_1, t_2)$.

Proof: $G_1ou_{l_1} \overset{t}{\sim}_{\epsilon_1} u_1 \cdot f(X) = X||G_2(Y)$.

By DPI, $G_1ou_{l_1}||G_2ou_{l_2} \overset{t_1-t'_2, \epsilon_1}{\sim} u_{L_1}||G_2ou_{l_2}$

By transitivity, $G_1ou_{l_1}||G_2ou_{l_2} \overset{min(t_1-t'_2, t_2)}{\sim}_{\epsilon_1+\epsilon_2} u_{L_1+L_2}$