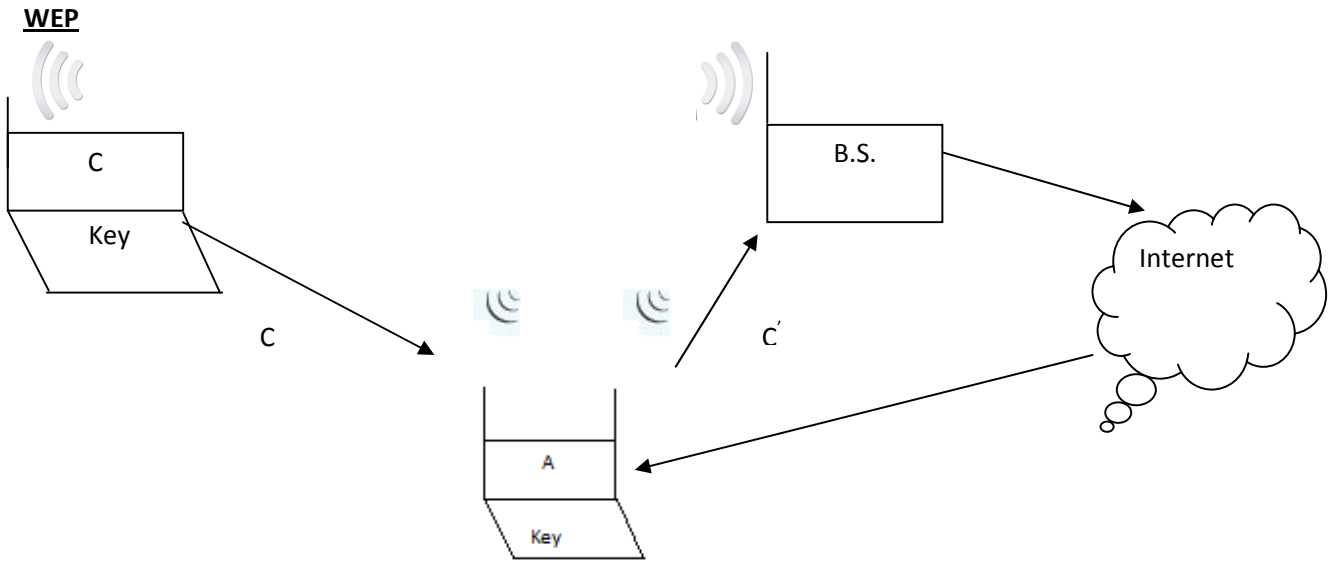


Network Security Notes (September 14 2009)

By Supreet Padhi



Chosen Ciphertext attack

Suppose attacker is BS'ISP.

Attack Scenario

1. Flip some bits in ciphertext corresponding to the destination IP address.
2. Transmit new ciphertext on wireless scheme.
3. Observe outgoing packet from BS to internet.

Here BS acts as decryption oracle.

Computational Indistinguishability

Theorem-Transitivity

$$D_1 \stackrel{t}{\sim}_{\epsilon_1} D_2 \text{ and } D_2 \stackrel{t}{\sim}_{\epsilon_2} D_3 \text{ then } D_1 \stackrel{t}{\sim}_{\epsilon_1 + \epsilon_2} D_3$$

Theorem – Data Processing Inequality(DPI)

if $D \stackrel{t}{\sim}_{\epsilon} D'$ and f is any function computable in time t' then

$$f(D) \stackrel{t-t'}{\sim}_{\epsilon} f(D')$$

How to design a good stream cipher?

We need a good and secure pseudo random number generator in order to design a good stream cipher.

Definition: A function $G: \{0,1\}^l \longrightarrow \{0,1\}^L$ is a t, ϵ pseudo-random generator if

$$G.U_1 \stackrel{t}{\sim}_{\epsilon} U_L$$

Theorem: if $G_1: \{0,1\}^l \longrightarrow \{0,1\}^L$ is (t, ϵ) secure PRG and $G_2: \{0,1\}^L \longrightarrow \{0,1\}^M$ is (t', ϵ_2) secure in time t' then $G_2 \circ G_1$ is $(t', \epsilon_1 + \epsilon_2)$ secure PRG

Proof: By definition

$$U_L \stackrel{t}{\sim}_{\epsilon_1} G_1.U_1$$

By DPI:

$$U_L \stackrel{t-t'}{\sim}_{\epsilon_1} G_2.G_1.U_1$$

By def :

$$G_2.U_L \stackrel{t}{\sim}_{\epsilon_2} U_M$$

By transitivity :

$$U_M \stackrel{t-t'}{\sim}_{\epsilon_1 + \epsilon_2} G_2.G_1.U_1$$

Hence, $G_2 \circ G_1$ is $(t-t', \epsilon_1 + \epsilon_2)$ secure PRG

Lemma

$G_1(t_1, \epsilon_1)$ secure runs in t_1'

$G_2(t_2, \epsilon_2)$ secure runs in t_2'

$\Rightarrow G_1 || G_2$ is $(t_3, \epsilon_1 + \epsilon_2)$ secure where t_3 is $\text{poly}(t_1, t_2)$

Proof:

$$G_1.U_{11} \stackrel{t_1}{\sim}_{\epsilon_1} U_{L1}$$

Let $f(x) = x || G_2(y)$ where $y \leftarrow U_{L2}$

The running of f is t_2' which is same as that of G_2

By DPI:

$$f(G_1.U_1) \stackrel{t_1-t_2'}{\sim}_{\epsilon} f(U_{L1})$$

$$\Rightarrow G_1.U_{11} || G_2.U_{12} \stackrel{t_1-t_2'}{\sim}_{\epsilon} U_{L1} || G_2.U_{12}$$

By def:

$$G_2.U_{12} \stackrel{t_2}{\sim}_{\epsilon_2} U_{L2}$$

By transitivity:

$$G_1.U_{11} || G_2.U_{12} \stackrel{\min(t_1-t_2', t_2)}{\sim}_{\epsilon_1 + \epsilon_2} U_{L1} || U_{L2}$$

$$G_1.U_{11} || G_2.U_{12} \stackrel{\text{poly}(t_1, t_2)}{\sim}_{\epsilon_1 + \epsilon_2} U_{L1} + U_{L2}$$