Tutorial 9

SOEN-321

Exercise 6 – Problem 4

Alice would like to send a message M to Bob with confidentiality and integrity. Alice and Bob share symmetric keys k1; k2. Bob's public key is KB; we assume that Alice knows KB. Below, MAC is a secure message authentication code, H is a secure cryptographic hash, and E_{k_1} is a secure stream cipher.

Consider the following two schemes:

S1: Alice sends $E_{k_1}(M)$; $MAC_{k_2}(M)$ to Bob

S2: Alice sends $E_{k_1}(M)$; $H(M)$ to Bob

(a) Which scheme is better for confidentiality? Why?

(b) Which scheme is better for integrity? Why?

Answer: (a)

S1 is better. S2 lets the attacker test a guess at M (given a guess g, compute H(g); if H(g) = H(M), then he can conclude his guess was correct)

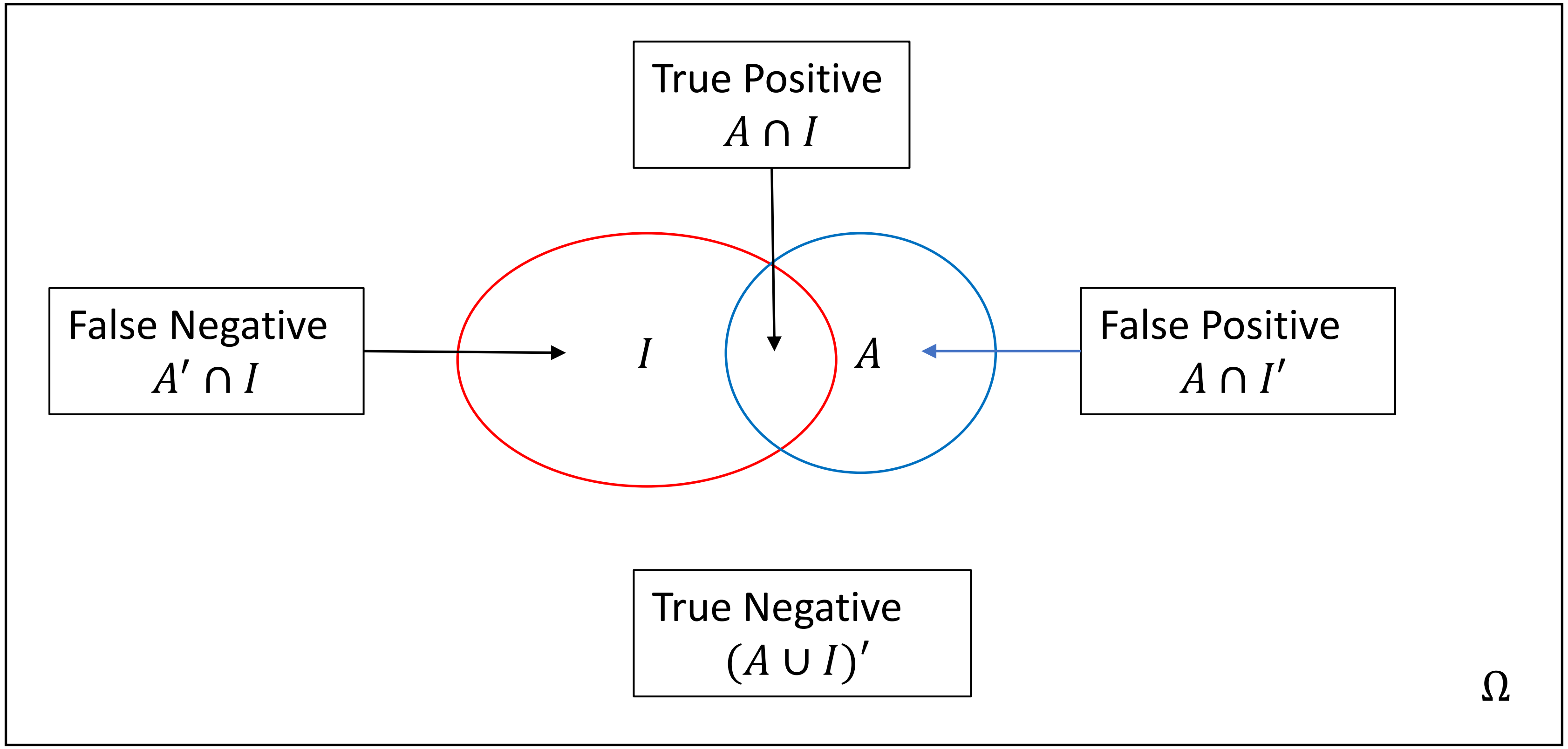
Answer: (b)

S1 is better. With S2, if the attacker knows M, he can modify the ciphertext to turn it into a valid encryption of M'. Since E is a stream cipher, he can flip bits in $E_{k_1}(M)$ to change it to an encryption of $E_{k_1}(M')$, and then replace $H(M)$ with $H(M')$

Detection Theory

Let $\Omega, \mathrm{I}, \mathrm{A}$ denote the set of all events, intrusion events, and alert events, respectively.

We define intrusion rate as $P(I) = \frac{|I|}{|\Omega|}$ and alert rate as $P(A) = \frac{|A|}{|\Omega|}$



Detection Theory

We define detection rate as $P(A|I) = \frac{P(A \cap I)}{P(I)}$ which is the set of all detection normalized by the set of all intrusions.

Example:

Suppose $|\Omega| = 1000000, \;\; |I| = 20, \;\; |A| = 22, \;\; |A \cap I| = 18$, what is the detection rate?

$$P(A \cap I) = \frac{18}{100000}, and\ P(I) = \frac{20}{1000000}$$

$P(A|I) = \frac{18}{20} = .9 = 90\%$, which means 10% of all intrusions pass undetected (i.e. false negative)

Detection Theory

Another metric to judge on the effectiveness of an IDS is to compute Bayesian detection rate which is the set of all detections normalized by the set of all alerts as $P(I|A) = \frac{P(A \cap I)}{P(A)}$

Example:

Suppose $|\Omega| = 1000000, \; |I| = 20, \; |A| = 22, \; |A \cap I| = 18$, what is the Bayesian detection rate?

$$P(A \cap I) = \frac{18}{100000}, and\ P(A) = \frac{22}{1000000}$$

$P(I|A) = \frac{18}{22} = .82 = 82\%$, which means 18% of all alerts are false positives!

Calculating Bayesian Detection Rate

Sometimes, we know the detection rate (i.e. accuracy) and intrusion rate only, and we want to find Bayesian detection rate.

Fact: $P(A) = P(I) \times P(A|I) + P(I') \times P(A|I')$

$$P(I|A) = \frac{P(I \cap A)}{P(I) \times P(A|I) + P(I') \times P(A|I')}$$

Example:

In a city of 1000 people, there is one terrorist. Suppose we have terrorist recognition system that is 99% accurate, and the alarm was triggered. Is the suspect really a terrorist?

$$P(T) = \frac{1}{1000} = 0.001, \qquad P(T') = 0.999 \qquad P(A|T) = 0.99 \qquad P(A|T') = 0.01$$

We want to know $P(T|A)$

$$P(T|A) = \frac{P(T \cap A)}{P(A)} = \frac{P(T \cap A)}{P(T) * P(A|T) + P(T') * P(A|T')} = \frac{P(A|T) * P(T)}{P(T) * P(A|T) + P(T') * P(A|T')}$$

$$P(T|A) = \frac{0.99 * 0.001}{0.001 * 0.99 + 0.999 * 0.01} = 0.09 = 9\%$$