

Security, Interference and Information Theory

S.Hunt-City



P.Malacaria-Queen Mary

D.Clark-Kings

How can we **measure how secure** is a software system? For example someone stole a cash card and is trying his luck at a cash machine.

He can guess the 4 digits pin number **so** the account is **not secure**.

If the thief knows the pin the account has no security, because he knows all 4 digits (13.3 bits of information). If he knows nothing about the pin then the account is maximally secure (he can only know 0.000147 bits of information by an attempt at guessing it).

How do we get those numbers?

Given two states of a program s, s' and two program variables X, Y we measure

$$H(X(s)|Y(s)) - H(X(s)|Y(s), Y(s'))$$

I.e. the **difference** between the information about X at s knowing Y at s **and** the information about X at s knowing Y at s and s' . This quantity is the **information leakage** or **interference** from X at s to Y at s' .

We can determine safe bounds on interference of program variables **without** having to run the program. This is a **static analysis** and makes important use of Fano Inequality

Shannon's **Information Theory** measures the **minimum** amount of space which is on **average** required to store or transmit information about a set of data. This amount depends on the likelihood of data, e.g. a horse race outcome with 4 horses will in general require 2 bits for storage or transmission but if only two horses in that set can win 1 bit will be enough

Given a set of events $X=e_1 \dots e_n$ with probabilities p_1, \dots, p_n , Shannon's basic **information measure** is called **entropy** and is defined as

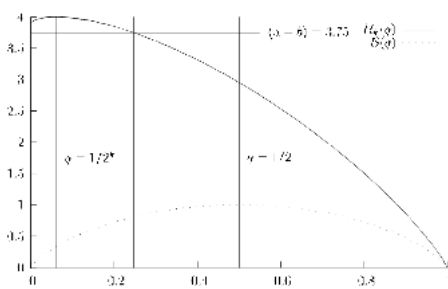
$$H(X) = -\sum p_i \log(1/p_i)$$

The related notion of **conditional entropy** is defined as

$H(X|Y) = H(X, Y) - H(Y)$ and measures the information about X given knowledge of Y

Fano Inequality: Suppose message X was sent and Y was received. Let $p(e)$ be the probability of **error** I.e. of X being different from Y .

$$\text{Then } H(X|Y) \leq H(p(e)) + p(e) \log(\#X - 1)$$



The diagram shows how to compute bounds on leakage of an equality test $X=n$ for X a 4 bits variable. Known a lower bound for $H(X)$ (in the figure 3.75) we intersect it with the solid curve which comes from Fano inequality. We then project that intersection on the lower curve obtaining $0 \leq q \leq 0.25$ which gives (projecting on the vertical axe) an upper bound of 0.75 for the leakage of $X=n$.

The background

The problem

The theory

The application