

Uma implementação de Quantitative Information Flow

Artur Vaz¹ and Mário S. Alvim¹

Universidade Federal de Minas Gerais, Brazil

1 Introdução

Qual o problema a ser resolvido ou questão a ser investigada no projeto? Por que ele é importante? Listar os objetivos gerais e específicos do trabalho.

2 Referencial Teórico

No campo de QIF, modelos de segurança são modelados como canais de informação. Um canal é definido como uma função $C : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$ onde \mathcal{X} é o grupo das entradas, ou valores secretos, e \mathcal{Y} é grupo dos outputs, ou observáveis:

$$C(x, y) = p(y|x)$$

$C(x, y)$ é a probabilidade do sistema produzir o observável y dado o segredo x , $\forall x \in \mathcal{X}$ e $\forall y \in \mathcal{Y}$.

Por exemplo, podemos modelar um sistema de login onde \mathcal{X} é o grupo de todas as possíveis senhas e \mathcal{Y} um grupo de 2 elementos, se a senha é certa ou errada. Nesse sistema apenas um elemento é correto e o restante incorreto. Esse

C	Correto	Incorreto
"123455"	0	1
"123456"	1	0

Table 1: Representação matricial de um canal

exemplo é determinista e interessante para perceber a interpretação do canal porem em sistemas de segurança é comum ter varios observáveis possíveis para cada segredo.

Para entender como a informação vaza é preciso modelar também o *atacante*, é assumido que o observável e o sistema é conhecido. Alem disso, o adversário pode saber um pouco sobre o segredo antes do sistema executar e é definido como distribuição apriori π em \mathcal{X} , uma distribuição de probabilidades sobre os segredos.

3 Metodologia

Quais os principais passos previstos (com uma breve descrição) para execução do projeto? Como pretende-se abordar o problema?

4 Resultados Esperados

O que se pretende obter ao final do trabalho?

5 Etapas e Cronograma

Descrever o cronograma previsto para a realização dos passos definidos na Metodologia com resolução em nível de semanas.