TBA

Artur Vaz[1] and Mário S. Alvim[1]

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, sistemas de segurança são modelados como canais de informação. Um canal é definido como uma função $C : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ 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 probilidade 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*, que conhece o observável e como o sistema funciona. Alem disso, o adversário pode saber alguma coisa sobre o segredo antes do sistema executar e é defindo como a distribuição apriori π em $\mathcal{X}$ sobre os segredos.

3 Metodologia

O projeto consiste em implementar as ferramentas e analisar a diferença entre a aproximação do vazamento, usando os operadores, e o cálculo exato feito diretamente no canal.

A primeira parte do projeto é implementar uma biblioteca em C++ que contenha o ferramental mínimo para fazer a analise. Essa biblioteca vai conter:

- Parser
- Estrutura do canal
- Métricas antigas
- Métricas novas
- Operadores de composição

O Parser foi implementado para permitir operações de composição com vários canais de forma simples. O canal vai ser definido como uma classe onde as métricas e operadores serão métodos.

A segunda parte é analisar a efetividade dos operadores de composição, a maior dificuldade do processo de medir o vazamento de informação é a propria modelagem do sistema.

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.