A definir

Artur Vaz[1] and Mário S. Alvim[1]

Universidade Federal de Minas Gerais, Brazil

1 Introdução

Proteger informação sensível do público é um objetivo importante de segurança. O campo do Fluxo Quantitativo de Informação(QIF) se preocupa com em quantificar o quanto de informação sensível um sistema vaza, e tem sido muito ativo na ultima decada [1]-[X].

A representação do sistema é chamada de *Canal* e é a distribuição de probabilidade das saidas de cada entrada, essa definição modela o comportamento do sistema. O problema com a modelagem é que intuitivamente a abordagem é pensar no sistema como uma coisa só, que é suficiente para sistemas simples e pequenos mas para sistemas robustos não é uma tarefa trivial.

A partir disso, foi proposto uma abordagem aproximativa que modela o canal a partir da composição de partes do sistema e é proposto operadores que capturam as interações que ocorrem entre os componentes. Essa abordagem simplifica o processo de modelagem.

O objetivo desse projeto é comparar a análise de fluxo de informação pela aproximação usando os operadores e pelo calculo exato no canal e modelar protocolos como composição de canais e analisar o fluxo de informação. Na primeira parte do Projeto Orientado em Computação será feita uma comparação do vazamento de informação em protocolos já estudados, usando as diferentes abordagens, e será implementada uma biblioteca em C++ para auxiliar esse projeto, e futuros. Na segunda parte novos protocolos serão analisados usando o método aproximativo.

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. A Tabela 1 mostra como o canal do login é simples e interessante para perceber a

C	Correto	Incorreto
"123456"	1	0
Restante	0	1

Table 1: Representação matricial de um canal

interpretação do canal. Em sistemas de segurança é comum ter varios observáveis possíveis para cada segredo(Tab. 2).

C	y_1	y_2	y_3
x_1	0.4	0.3	0.3
x_2	0.2	0.8	0

Table 2: Representação matricial de um canal

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 que é defindo como a distribuição a priori π em $\mathcal{X}$ sobre os segredos.

O conhecimento a priori

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 para analise. Essa biblioteca vai conter:

- Estrutura do canal
- Utilidades para a classe do canal
- Métricas antigas
- Métricas novas
- Operadores de composição

O canal vai ser definido como uma classe onde as métricas e os operadores são métodos. Será implementado algumas utilidades, por exemplo gerar um canal aleatorio.

A segunda parte é analisar a efetividade dos operadores de composição. Existem dois protocolos de segurança, *Dining Cryptographers* e *Crowds*, comuns na literatura de QIF que podem ser usados para comparar o vazamento de informação usando os métodos diferentes.

4 Resultados Esperados

Ao final do POC I teremos uma implementação para o framework de QIF, com metricas e operações, que por sí só já em um boa contribuição para futuras pesquisas. Além disso, mostrar que metodos aproximativos são uma alternativa viável para modelar sistemas de segurança contribui para a modelagem de sistemas cada vez maiores e complexos.

No POC II é esperado expandir a quantidade de sistemas de segurança modelados e analisados na literatura.

5 Etapas e Cronograma

O cronograma foi definido dividindo as etapas em blocos de semana, e pelo planejado a implementação e a análise vai estar pronta na época da aprensetação parcial.

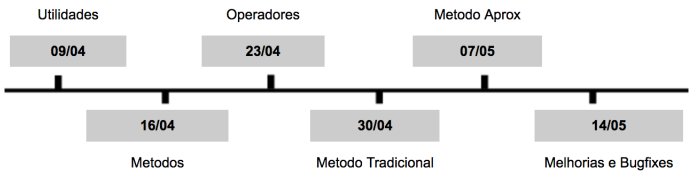

Fig. 1: Cronograma

O restante do tempo será reservado para melhorar a usabilidade da biblioteca e procurar problemas.