Trabalho de Lógica em Programação

Mario Benevides

June 14, 2019

Descrição

Implementar e Verificar, o modelo de Dolev Yao para três agentes A, B e Z, onde Z é um intruso. A deseja enviar uma mensagem para B. E o intruso pode interceptar qualquer mensagem. Eles usam um protocolo de chave pública. Todos os agentes tem duas funções E_X e D_X tal que:

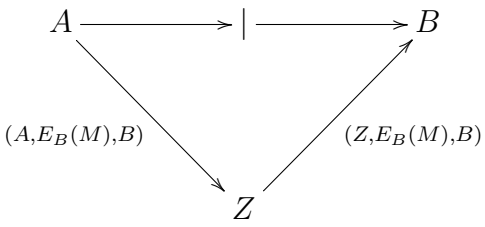
- User X has:
  - encryption function E_X (public)
  - decryption function D_X (known only by user X)
- Requirements:
  - $E_X D_X = D_X E_X$
  - for any user Y knowing $E_X(M)$ does not reveal anything about M

Example 1 *A sends msg M to B*

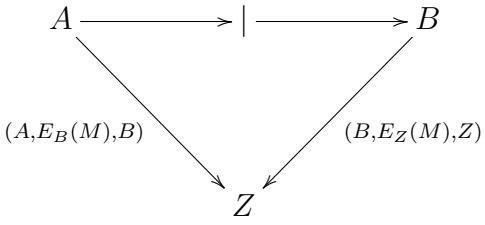
$$A \longrightarrow (A, E_B(M), B) \longrightarrow B$$

Intruder Z intercepts the message sent from A to B

Intruder Z sends message $(Z, E_B(M), B)$ to B



B sends message $(B, E_Z(M), Z)$ *to* Z



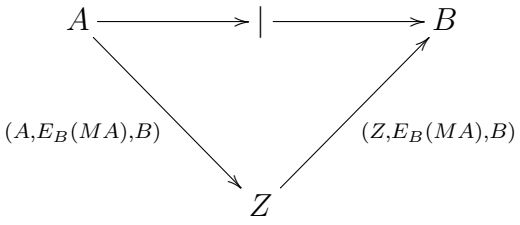
Intruder Z *decodes* $E_Z(M)$ *and obtains* M

Example 2 *A sends msg* MA *to* B *and* B *replies to the user that is encrypted with the message* M *and not to the sender*

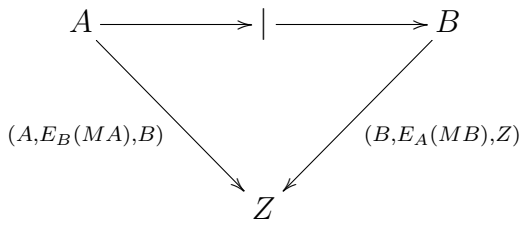
$$A \longrightarrow (A, E_B(MA), B) \longrightarrow B$$

Intruder Z *intercepts the message sent from* A *to* B

Intruder Z *sends message* $(Z, E_B(MA), B)$ *to* B



B sends message $(B, E_A(MB), Z)$ *to* Z



Intruder Z **cannot** *decode* $E_A(MB)$ *to obtain* M

It can be proved that this protocol in secure against arbitrary behaviour of the intruder.

Implemente este sistema em Nu-SMV ou NuXMV e verifique para os dois exemplos se o intruso Z consegue obter a mensagem ou não.

Todos os componentes devem executar assincronamente.

Observação

- **Entrega**: até 05/07/19 (máximo).
- Programas copiados não serão aceitos.
- Trabalhos deverão ser apresentados com o programa rodando.
- Um descrição do trabalho deve ser entregue junto com uma cópia impressa do programa.
- Trabalhos devem ser psresentados pelos alunos com hora marcada.