GAC119 - REO 2: Mapeamento de riscos e ameaças

Mateus Carvalho Gonçalves - 201810245
Pedro Antônio de Souza - 201810557

Introdução

Este trabalho objetiva mapear riscos e ameaças da aplicação **Quero falar**. O mapeamento será feito utilizando o modelo STRIDE, mnemônico para Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege.

Spoofing (Propriedade violada: autenticação)

- A mulher que relatou uma agressão não é ela mesma, é alguém querendo se passar por ela.
- Um agressor acessa a conta da vítima para verificar se ele está sendo denunciado.

Tampering (Propriedade violada: integridade)

- Uma pessoa pode mudar ou remover os dados de contato dos órgãos de segurança para inviabilizar os chamados.
- Uma pessoa pode mudar os dados de outra.
- Um agressor pode remover relatos de agressão nos quais é acusado.
- Um atacante pode remover o botão de “pânico”.

Repudiation (Propriedade violada: autenticidade)

- Uma pessoa pode informar, propositalmente, falsos relatos de agressão (trote).
- Uma pessoa pode utilizar o botão de “pânico” para iniciar transmissões de áudio e vídeo a fim de sobrecarregar o sistema e alegar que não executou essa ação.

Information Disclosure (Propriedade violada: confidencialidade)

- Uma pessoa acessa os relatos feitos por outra pessoa.
- Uma pessoa intercepta comunicações.

Denial of Service (Propriedade violada: disponibilidade)

- Um atacante pode indisponibilizar os servidores a fim de cobrar resgate do sistema.
- É necessário garantir que o sistema esteja sempre disponível para todos.
- É necessário garantir que a comunicação entre usuários padrões e órgãos de segurança esteja sempre disponível.

Elevation of Privilege (Propriedade violada: autorização)

- Uma pessoa obtém privilégios de autoridade policial para receber transmissões de áudio e vídeo.