ATIVIDADE 5

NOME: LUCAS MARTINS OLIVEIRA
MATRÍCULA: 202465058A

Texto relativo ao artigo "R-STELLAR: A Resilient Synthesizable Signature Attenuation SCA Protection on AES-256 with built-in Attack-on-Countermeasure Detection":

O artigo "R-STELLAR: A Resilient Synthesizable Signature Attenuation SCA Protection on AES-256 with Built-in Attack-on-Countermeasure Detection" aborda uma questão crucial na segurança de sistemas embarcados: os ataques de canal lateral (Side-Channel Attacks - SCAs). Mesmo algoritmos criptográficos que são matematicamente seguros, como o AES-256, podem inadvertidamente vazar informações através de assinaturas físicas, como consumo de energia, radiação eletromagnética, emissões de luz e emanações acústicas durante sua implementação em hardware. Esses vazamentos físicos podem reduzir significativamente o espaço de busca de um atacante, tornando a quebra da criptografia muito mais viável. Para combater isso, o artigo propõe R-STELLAR, uma contramedida para o AES-256 que atenua essas assinaturas de canal lateral e, o que é inovador, inclui uma detecção embutida de ataques contra a própria contramedida. Isso significa que o sistema não apenas tenta se proteger, mas também identifica se um atacante está tentando "burlar" sua proteção, aumentando a resiliência contra técnicas adversárias mais avançadas.

Minha visão crítica sobre o tema é que, embora a criptografia seja fundamental para a segurança da informação, a atenção aos detalhes da sua implementação em hardware é igualmente vital e frequentemente subestimada. O trabalho apresentado em "R-STELLAR" ilustra perfeitamente essa complexidade, pois mostra que a segurança de um sistema não se limita apenas à robustez matemática do algoritmo, mas se estende à forma como ele é fisicamente executado. A inclusão de uma capacidade de "detecção de ataque à contramedida" é um avanço significativo, pois reflete uma mentalidade de segurança proativa, reconhecendo que os atacantes estão constantemente aprimorando suas técnicas. Contudo, é importante considerar a sobrecarga (overhead) que tais contramedidas podem introduzir em termos de área, energia e desempenho em dispositivos embarcados, que muitas vezes possuem recursos limitados. Equilibrar segurança máxima com a viabilidade prática em ambientes restritos continua sendo um desafio central e um campo de pesquisa promissor na engenharia de segurança.

Texto relativo ao paper “C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC”:

O artigo "C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC" apresenta uma abordagem inovadora no campo da esteganografia. Diferente dos métodos tradicionais que modificam uma imagem portadora para ocultar informações, a esteganografia coverless ("sem capa") busca incorporar dados secretos sem alterar perceptivelmente a imagem original, o que resolve vulnerabilidades inerentes a essas abordagens clássicas. Contudo, os métodos coverless existentes frequentemente exigem a transmissão de metadados, o que pode comprometer a segurança da informação oculta. C-HIDE propõe uma solução para isso, utilizando uma criptografia híbrida de imagem com AES e ECC, combinando a ocultação robusta de dados com segurança avançada, sem a necessidade de modificar a imagem "capa" e eliminando a transmissão de metadados.

Minha visão crítica sobre esta pesquisa é que a esteganografia coverless representa um avanço significativo na busca por métodos mais seguros e imperceptíveis de ocultação de dados. A eliminação da necessidade de modificar a imagem portadora e a não transmissão de metadados são pontos cruciais que mitigam riscos de detecção e comprometimento da informação secreta. Em um cenário onde a vigilância e a análise de dados estão cada vez mais sofisticadas, a capacidade de esconder informações de forma que nem mesmo a existência de dados ocultos seja perceptível é de valor inestimável. No entanto, é fundamental que a complexidade computacional e a eficiência desses métodos sejam cuidadosamente avaliadas, especialmente para aplicações em tempo real ou em dispositivos com recursos limitados. A combinação de algoritmos robustos como AES e ECC no processo é promissora, mas a eficácia prática e a escalabilidade do C-HIDE em diferentes tipos e tamanhos de imagens, bem como contra atacantes com conhecimento do sistema, demandarão testes e validações rigorosos.