ANÁLISE DA APLICAÇÃO DA ESTEGANOGRAFIA COMBINADA COM O MÉTODO CRIPTOGRÁFICO AES

Orientador: KUEHLKAMP, Andrey
Acadêmica: GRAFF, Suelen
Curso: Ciência da Computação
Área de Conhecimento: ACET

A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, despertar atenção ou prejudicar alguém. Fica claro então que tornar uma rede segura envolve muito mais do que simplesmente mantê-la livre de erros de programação. Também é visto que a maioria dos ataques provém de pessoas conhecidas, que tenham alguma desavença ou rancor com o alvo do ataque. Esses detalhes consequentemente levam os sistemas de segurança a serem projetados considerando esses fatos. A criptografia nasceu da necessidade de manter a privacidade de informações. Desde a antiguidade já se tinha conhecimento da substituição ou troca dos símbolos com o objetivo de confundir um possível interceptador. Para a computação, esse princípio é mantido, porém, a escrita é substituída pelo processamento digital e com capacidade de processamento de dados. A segurança de dados criptografados é inversamente proporcional à facilidade de quebra do código cifrado, geralmente fundamentado na utilização de chaves de codificação, que são do conhecimento somente do remetente e do destinatário das informações. A esteganografia é um método de segurança capaz de encobrir informações em outras informações que, após esse processo, pode ser criptografado para a rede. Este trabalho trata da proposta de aplicação da esteganografia com o método criptográfico AES. A proposta de aplicação da esteganografia ocorreu por informações ocultadas em imagens. A técnica criptográfica AES foi a escolhida, por ser uma das mais utilizadas atualmente para a criptografia, padrão de criptografia do Governo dos Estados Unidos. A junção das duas técnicas é uma forma de melhorar a confidencialidade e a integridade dos mecanismos usados para prover segurança às informações. Foram realizados testes no protótipo para avaliar a junção das duas técnicas de acordo com as métricas e os testes descritos na literatura. Foram realizados teste de tempo, memória, integração, estresse, desempenho e relação imagem/mensagem. O resultado obtido foi que as duas técnicas funcionaram bem juntas, viabilizando o aumento da segurança. A imagem, após a aplicação da técnica, não obteve alterações de qualidade nem alterações relevantes de tamanho. A eficácia não foi prejudicada e o tempo de execução se alterou em poucos milissegundos.
Palavras-chave: Esteganografia. Criptografia. AES. Segurança.

suelengraff@hotmail.com
andrey.kuehlkamp@unoesc.edu.br