Anais do II Congresso de Ciência e Tecnologia da PUC Goiás
Disponível em: http://pucgoias.edu.br/ucg/prope/pesquisa/anais/2016
ISSN: 2177-3327

CRIPTOGRAFIA HÍBRIDA BASEADA EM IDENTIDADE

TAYNAN MINA MUNIZ, JOSÉ LUIZ DE FREITAS JÚNIOR
tmmuniz92@gmail.com

Objetivo: Criação de um novo esquema de autenticação e geração de chaves com base na Criptografia Baseada em Identidade que forneça mais eficiência no processo de autenticação e negociação de chaves em comparação ao modelo híbrido atual. **Método:** Utilizar ao máximo a criptografia simétrica para que o sistema tenha mais desempenho, descartando o uso e a consequente procura de certificados digitais entre os participantes, reservando esta ferramenta apenas ao centro de distribuição de chaves. A criptografia one-time-pad (OTP), funções de hash, nonce e autenticação por desafio-resposta são as principais ferramentas utilizadas para fornecimento de integridade, autenticidade e confidencialidade no novo esquema. **Resultados:** Uma nova estratégia para negociação de chaves foi descoberta através da divisão em n partes iguais do cálculo de funções Hash (h) em master keys (h(MK)) e aplicação da operação XOR entre elas, processo nomeado por Hash self-xored (Hsx). Esta função resulta em um único bloco de tamanho n e, por ser uma operação reversível, o bloco resultante é utilizado para criptografar via OTP um nonce do qual possui a funcionalidade de autenticação por desafio resposta, envolvendo geração de números aleatórios entre uma dupla de usuários. O uso do Hsx e o nonce possibilitou a extração de uma chave simétrica para formação do canal seguro e geração de uma nova MK, tornando a negociação independente do distribuidor de chaves. **Conclusão:** A única operação assimétrica presente no novo esquema é a transmissão segura da primeira MK compartilhada por parte do master key generator aos participantes, que negociarão de forma ágil, novas MKs entre ambos. O objetivo do projeto foi então alcançado, pois criptografias assimétricas realizam operações complexas, computacionalmente mais caras quando comparadas ao método simétrico, do qual, no novo esquema de autenticação, desfruta de operações lógicas triviais através do OTP.

Palavras-chave: one-time-pad. criptografia híbrida. IBE.