FACULDADE ENGENHARIA
Departamento de Informática

Comparação, uso e aplicação de algoritmos criptográficos para IoT.

Orientador: Professor Dr. Valderi R. Q. Leithardt (valderi.leithardt@ubi.pt)

Área de pesquisa: Sistemas distribuídos, privacidade de dados.

Objetivos

A Internet das Coisas (IoT - Internet of Things) está cada vez mais presente no cotidiano das pessoas, como na medicina, em redes elétricas inteligentes (Smart Grids), automação residencial, agricultura e mobilidade urbana. Com isto surge a necessidade de proteger os dados processados pelos dispositivos IoT contra e invasores. Um bom modo de resolver este problema é através de algoritmos criptográficos, em contra partida criptografias demandam muito poder computacional. Sistemas embarcados possuem poder computacional limitado, assim, o desempenho de algoritmos criptográficos é bem menor, gerando tempo de execução maior. O AES, originalmente chamado Rijndael, foi desenvolvido na década de 1990 por Vincent Rijmen e Joan Daemen para participar do concurso que substituiria o algoritmo criptográfico padrão do governo dos Estados Unidos, o DES, que já estava inseguro. O algoritmo Rijndael acabou sendo escolhido como o melhor algoritmo do concurso e a partir de então passou a chamar-se AES. Desde sua criação, já foram realizadas várias modificações no algoritmo original e ataques específicos quebraram apenas algumas rodadas da criptografia. O AES possui quatro etapas de transformação, sendo elas: SubBytes, ShiftRows, AddRoundKey e MixColumns, cada uma indispensável para a segurança do algoritmo. O RC6 é um algoritmo derivado do RC5, e desenvolvido por Ron Rivest, Matt Robshaw, Ray Sidney e Yiqun Lisa Yin. Foi concorrente do Rijndael no concurso para o Advanced Encryption Standard, onde foi derrotado pois além de necessitar de uma quantidade grande de memória, seu desempenho em FPGA (Field Programmable Gate Array) não foi satisfatório. Assim, possui desempenho superior em software do que em hardware se comparado à outros algoritmos criptográficos, em Linguagem C foi o algoritmo mais rápido entre os concorrentes. O algoritmo é baseado na cifra de Feistel, com entrada de texto pleno de 128 bits dividido em 4 entradas de 32 bits e tamanho de chave de até 256 bits. O RC6 é um algoritmo simples de compreender e

menos complexo que o AES, que possui várias etapas baseadas em princípios algébricos sofisticados. Como têm base na cifra de Feistel, o RC6 conta com muitas operações de rotação de bits, XOR e rotação de posições das entradas. Outros exemplos de criptografias baseadas em cifra de Feistel são: Blowfish, CAST, DES e 3DES. Portanto, o principal objetivo deste projeto é analisar, considerando tamanhos de pacotes e chaves variadas, os algoritmos de chave simétrica AES e RC6 em relação aos algoritmos e chaves criptograficas já implementadas pelo professor.

Tarefas a Realizar e Cronologia

T1 Estudo do problema e estado da arte;

T2 Escrita da literatura comparando algoritmos de criptografia existentes;

T3 Definição do algoritmo de criptografia e comunicação a desenvolver;

T4 Desenvolvimento da aplicação;

T5 Escrita do relatório do projeto;

T6 Escrita de um short paper.

Cronograma

	Fev	Fev	Mar	Mar	Abr	Abr	Mai	Mai	Jun	Jun
T1	X	X	X							
T2		X	X							
T3			X							
T4				X	X	X	X	X		
T5								X	X	
T6									X	X

Requisitos Técnicos / Académicos

Ter boas classificações e conhecimentos em programação, segurança da informação.

Elementos de Avaliação a Entregar

A(o) aluna(o) deverá entregar os seguintes elementos para avaliação:

- relatório impresso (ver regulamento sobre número de exemplares);

- CD ou DVD (ou outro elemento de memória de massa) com os vários

cenários e ambiente de testes e simulação e cópia do relatório em formato PDF;

- Short paper em formato digital a incluir no CD ou DVD;

- Para além do relatório e itens elencados anteriormente, o(a) aluno(a) deverá entregar todos os *scripts* e código fonte desenvolvido no CD ou DVD.

Resultados Esperados

- Um protótipo da aplicação;
- O levantamento do estado da arte e trabalhos relacionados;
- Um relatório de projeto;
- Um Short Paper.

Referências Bibliográficas

Biham, E., Dunkelman, O., and Keller, N. (2005). **Related-key boomerang and rectan-gle attacks**. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 507–525. Springer.

da Silva, B. A., de Mello, G., Silva, L. A., and Leithardt, V. R. Q. (2018**). Comparative study of aes cryptographic algorithm in limited capacity device**. Workshop em Sistemasde Informação do IFC, 1. Brasil.

Daemen, J. and Rijmen, V. (2013). **The design of Rijndael: AES-the advanced encryptionstandard**. Springer Science & Business Media. Mendes, M. A. L. (2001).

Naru, E. R., Saini, H., and Sharma, M. (2017**). A recent review on lightweight crypto-graphy in iot**. In 2017 International Conference on I-SMAC (IoT in Social, Mobile,Analytics and Cloud) (I-SMAC), pages 887–890.

Ochôa, I. S., Teive, R. C., Alonso, E. E., and Leithardt, Valderi (2018). **Uma anáalise de desempenho criptográfico de algoritmos implementados no microcontrolador msp430f6749 utilizando o protocolo osgp**. Anais SULCOMP, 9 – Brasil 2018.

SILVA, L. A. ; DAZZI, R. L. S. ; Silva, Jorge Sá ; Leithardt, Valderi R. Q. . PRISER - **Utilização de BLE para localização e notificações com base na privacidade de dados.** REVISTA ELETRÔNICA ARGENTINA-BRASIL DE TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO, v. 2, p. 1-13, 2018. Doi: http://dx.doi.org/10.5281/zenodo.1336806

Soewito, B., Gunawan, F. E., Diana, and Antonyov́ a, A. (2016). **Power consumption forsecurity on mobile devices**. In 2016 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS), pages 1–4.