UNIVERSIDADE FEDERAL DE PERNAMBUCO

Graduação em Engenharia da Computação
Centro de Informática

Um comparativo de performance entre o uso de smart card baseado em FPGA e leitores unitários com interface USB

Aluno: Bruno Albuquerque de Barros {bab@cin.ufpe.br}
Orientador: Djamel Sadok {jamel@cin.ufpe.br}

Outubro de 2016

Sumário

1. Contexto
2. Objetivo
3. Cronograma
4. Referências
5. Possíveis Avaliadores
6. Assinaturas

Contexto

Smart cards são dispositivos de processamento embarcados em um cartão plástico. Contêm microprocessador e memória própria, e podem ser acessados através de conexão física ou utilizando RFID (*Radio-Frequency IDentification*). São conhecidos devido a sua elevada segurança, principalmente sua resistência a adulteração física, possuindo mecanismos para impedir que dados internos sejam roubados (VEDDER, 1992). Tais características, juntamente com o processamento próprio e a capacidade de executar algoritmos de encriptação, tornaram seu uso popular na telefonia móvel (HUSEMANN, 1999).

Além da sua aplicação no ramo de telefonia móvel, *smart cards* são utilizados em cartões de identificação, sistemas de controle de acesso, armazenamento de dados seguro, assinaturas eletrônicas, comércio eletrônico e cartões multifuncionais que incorporam várias aplicações em um único cartão (COOKE; BREWSTER, 1993). Urian (2004) em seu trabalho demonstra um método de autenticação segura utilizando *smart cards*.

Há alguns serviços de segurança contra-ataques externos bastante seguros. No entanto, nem todos os serviços são capazes de garantir a proteção quando existe o acesso ao meio físico. Mas, com o uso do *smart card* é possível garantir a proteção dos dados, devido ao alto nível de segurança, mesmo que o usuário tenha acesso ao local em que os dados estão armazenados. Pois, os *smart cards* implementam protocolos de criptografia de chave assimétrica e executam algoritmos de criptografia, que garante ao projetista uma segurança nas informações (RANKL; EFFING, 2004).

A conexão entre o computador e o *smart card* é realizada por um dispositivo (leitor ou terminal) de *smart cards*, que estabelece conexão de dados e fornece energia para o chip, um dispositivo com acesso simultâneo a mais de um *card* é chamado de *smart grid*. Portanto, compete a ele a responsabilidade de detecção de erro nas conexões elétricas responsáveis pelas transmissões de dados. Para evitar danos ao chip, sequencias de ativação e desativação são realizadas, devendo seguir a norma ISO/IEC 7816-3 (ISO/IEC 7816-3, 2006). Os terminais normalmente contêm um gerador de clock, uma memória associada e um microcontrolador, que são programados usando linguagens de alto nível como C, C++ e Java.

Objetivo

Este trabalho propõe a análise comparativa entre o desempenho do uso de um *smart grid* baseado em FPGA para conexão com vários *cards* simultaneamente com a utilização de terminais de *smart card* USB comuns, que acessam apenas um *card*. Também é do escopo do mesmo utilizar de métricas para avaliar a viabilidade do uso do *smart grid*, levando em consideração rapidez de processamento e escalabilidade.

Serão realizadas várias rotinas de inicialização do *card*, o envio de várias mensagens onde estas serão divididas em dois grupos, mensagens de status que são processadas no smart grid, e mensagens de processamento, que são processadas no *card*. Para realizar os testes comparativos, serão utilizados vários leitores comuns ligados através de um hub USB, de forma que a tecnologia usada possa ser abstraída para a aplicação.

Para atingir o objetivo, será utilizada a seguinte metodologia:

- Primeiramente será escolhido um conjunto de mensagens para ser enviadas aos *cards*, tal conjunto deve ser grande e diversificado o bastante para um resultado satisfatório;
- Será desenvolvido um sistema de captura de métricas, como o tempo de execução e taxa de erros para automaticamente colher os dados da execução de cada mensagem, assim como enviar tais mensagens através do driver.
- Serão realizados testes tanto com um quanto com mais *cards*, como dito acima, no caso dos leitores USB, será utilizado um hub para a conexão de vários leitores.
- Serão comparados entre si os tempos de execução e os erros do sistema para finalizar a análise.

Cronograma

Atividade	Agosto	Setembro	Outubro	Novembro
Escrita da proposta	X			
Revisão Bibliográfica	X			
Implementação da proposta		X	X	
Avaliação de resultados			X	
Escrita de relatório			X	X
Elaboração de Apresentação				X

Referências

VEDDER, Klaus. Smart Cards. In: **CompEuro '92. 'Computer Systems and Software Engineering',Proceedings.** p. 630 - 635, 1992.

HUSEMANN, Dirk. The smart card: don't leave home without it. **Concurrency, IEEE**, v.7, n.2, p. 24-27, 1999.

COOKE, J. C.; BREWSTER, R. L. The use of smart cards in personal communication systems security. In: **Fourth IEE Conference on Telecommunications.** 1993. p. 246-251.

RANKL, Wolfgang; EFFING, Wolfgang. **Smart card handbook**. John Wiley & Sons, 2010.

ISO/IEC 7816-3. **Cards with contacts Electrical interface and transmission protocols, ISO/IEC Std.** 2006. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-3:en. Acessado em: 28/mar/2016.

Possíveis Avaliadores

Professora Edna Natividade
Professora Judith Kelner

Assinaturas

Djamel Sadok
(*orientador*)

Bruno Albuquerque de Barros
(*Aluno*)