IMPLEMENTAÇÃO DE FERRAMENTA PARA ANÁLISE DE ESPECTRO EM AMBIENTES INDUSTRIAIS

Bruno Albuquerque de Barros[1] ; Djamel Fawzi Hadj Sadok[2]

[1]Estudante do Curso de Engenharia da Computação - CIn – UFPE; E-mail: bab@cin.ufpe.br,
[2]Docente/pesquisador do Centro de Informática – CIn – UFPE. E-mail: jamel@gprt.ufpe.br.

Sumário: Considerando que cada vez mais serviços remotos são utilizados, tecnologias de autenticação se fazem extremamente necessárias, assim sendo, este projeto visa criar um servidor de autenticação baseado em *smart cards*. Visando uma maior capacidade de processamento e de armazenamento, o projeto focou na criação de um servidor com acesso a vários cartões. Para manter um processamento constante de todos os cartões conectados, a pesquisa optou pela utilização de um FPGA. Como resultado do projeto foi finalizada a arquitetura interna ao FPGA, e como trabalho futuro a finalização da arquitetura para comunicação com a rede.

Palavras–chave: FPGA; smartcard

INTRODUÇÃO

A virtualização de redes - técnica que permite executar vários servidores diferentes, com sistemas operacionais diferentes em uma mesma máquina - e a computação na nuvem - serviços computacionais disponíveis via Internet - serão as bases para a arquitetura da internet do futuro devido ao número crescente de dados processados, armazenados e compartilhados em tempo real. A segurança do acesso às nuvens é um dos desafios para a implementação de uma arquitetura de redes virtualizadas.

As tecnologias mais utilizadas para a criação de servidores de autenticação como RADIUS, LDAP e SecurID RSA armazenam as chaves de segurança nos servidores através de memória convencional. No entanto, não é uma tecnologia perfeitamente segura, pois caso haja acesso ao servidor físico as chaves de segurança estão em risco.

Dentre as tecnologias de segurança disponíveis atualmente os *smart cards* se destacam por apresentar um processamento próprio, técnicas de criptografia embutidas e resistência a adulterações físicas. Devido a isso, chaves privadas criptografadas armazenadas em sua memória são quase impossíveis de serem descobertas. [1] diz que o *smart card* provou ser uma forma ideal, fornecendo um alto nível de segurança (baseado em criptografia) disponível para todos, uma vez que pode armazenar chaves privadas e executar algoritmos de criptografia.

Com a finalidade de utilizar *smart cards* para a implementação de uma arquitetura de redes virtualizadas, foi desenvolvido um servidor de autenticação. Nos cartões as chaves criptografadas são armazenadas e as verificações são processadas, diminuindo a possibilidade de quebra de segurança.

Um esquema de autenticação baseada em *smart cards* foi proposto em [2], no qual o servidor utiliza uma senha e um *smart card* como dois fatores para alcançar a autenticação do usuário excluindo assim, o uso de uma tabela de verificação, dessa forma é possível reduzir a chance de algum usuário ou software sem boas intenções modificá-la. Em [3], o

autor faz uso de *smart cards* para proteção contra tentativas de ataques que reenviem requisições de login interceptadas previamente.
Este projeto não limita a utilização de *smart cards* apenas para o armazenamento da chave, mas permite também o armazenamento das informações sobre o usuário contidas no servidor. Além disto, a proposta é permitir a utilização de vários *smart cards* em um mesmo servidor, visando ampliar a sua capacidade. Os cartões podem ser utilizados para armazenar e verificar as chaves dos usuários, assim sendo, a autenticação do usuário nunca será feita na memória do servidor dificultando dessa forma, ataques e quebras de segurança.
O foco deste projeto foi o desenvolvimento de uma plataforma em hardware de baixo custo, porém segura, para ser utilizada em larga escala. Tal plataforma terá dois componentes: a BASE - prover a interface com a rede - e o hardware projetado com o uso do FPGA -responsável pela comunicação com todos os cartões conectados a ele.
O bolsista tem como principal atividade definir as tecnologias de hardware que serão utilizadas através de pesquisa de mercado e das tecnologias disponíveis, buscando quais se adequariam melhor ao problema abordado, assim como desenvolver a arquitetura completa interna ao FPGA. As informações sobre leitores de cartões disponíveis no mercado foram utilizadas como base para o desenvolvimento da pesquisa.

MATERIAIS E MÉTODOS

Inicialmente foi realizado o estudo de estado da arte através da leitura de livros, artigos, e do estudo de tecnologias existentes com propósito similar. Em seguida, o bolsista estudou qual tecnologia seria mais apropriada para realizar a comunicação com os cartões, optando pelo FPGA pelo seu paralelismo e número de IO disponíveis. Então, foi possível iniciar o desenvolvimento dos módulos, assim como de suas FSM (*Finite State Machine)*. Para cada conjunto de módulos desenvolvido, foram realizados testes em software para, além de buscar erros, verificar o consumo de memória e lógica programável. Com todos os módulos testados em separado e em alguns grupos, foi desenvolvido um conjunto de testes para toda a arquitetura, para assim, testar a comunicação e funcionamento dos mesmos em conjunto.

RESULTADOS

A pesquisa foi dividida em 3 etapas: escolha dos componentes utilizados e definição da arquitetura utilizada; na etapa seguinte foi definida a arquitetura interna do FPGA; e por fim a implementação da arquitetura interna do FPGA.
Na etapa 1 foi desenvolvida a arquitetura em alto nível, figura 1. A BASE é responsável pela conexão e gerenciamento da rede, isto é, conexão do servidor desenvolvido no projeto com a rede. A escolha do Raspberry para essa tarefa fundamental, foi realizada devida a sua alta versatilidade e ao seu baixo custo.
O FTDI é responsável em fazer a ligação entre a BASE e o FPGA, através da conversão da comunicação USB e a comunicação paralela. Outras tecnologias poderiam ter sido utilizadas, mas o FTDI mostrou ser o mais adequado devido seu baixo custo, facilidade de implementação e pequeno número de pinos.
O gerenciamento dos cartões é responsabilidade do FPGA devido ao seu nível de paralelismo e a elevada quantidade de GPIO (*General Purpose IO*), além de operar com uma frequência de 50Mhz, dessa forma é possível utilizar os *smart cards* com *clock* máximo.

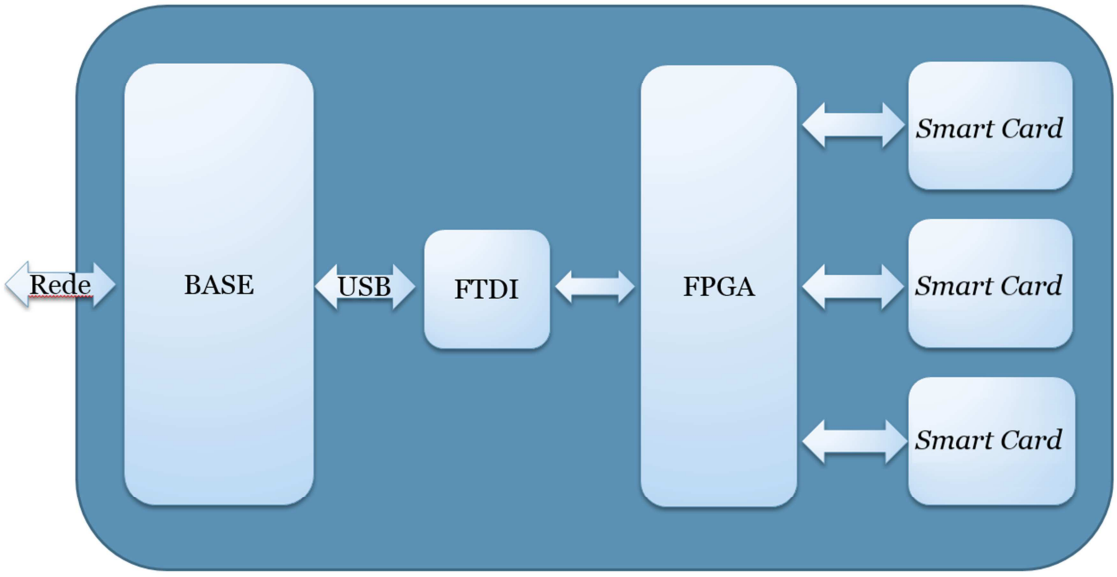

Figura 1 – Arquitetura em alto nível

Após a definição da arquitetura mostrada na Figura 1, a etapa 2 foi iniciada com a definição da arquitetura interna do FPGA, Figura 2. O Módulo de Comunicação é responsável por selecionar os dados dos cartões e fazer a comunicação com o FTDI.
O SLOT é responsável pela realização das rotinas necessárias para a comunicação com o *smart card*, isto é, são nos SLOTs que há a implementação dos protocolos utilizados pelos *smart cards*, tais protocolos serão descritos a seguir. Foi utilizado o paralelismo presente no FPGA para replicar os SLOTs para cada cartão conectado.
As FIFOs (*First in First Out*) são utilizadas como interface entre os SLOTs e o Módulo de Comunicação, servindo também para armazenar os dados enviados.

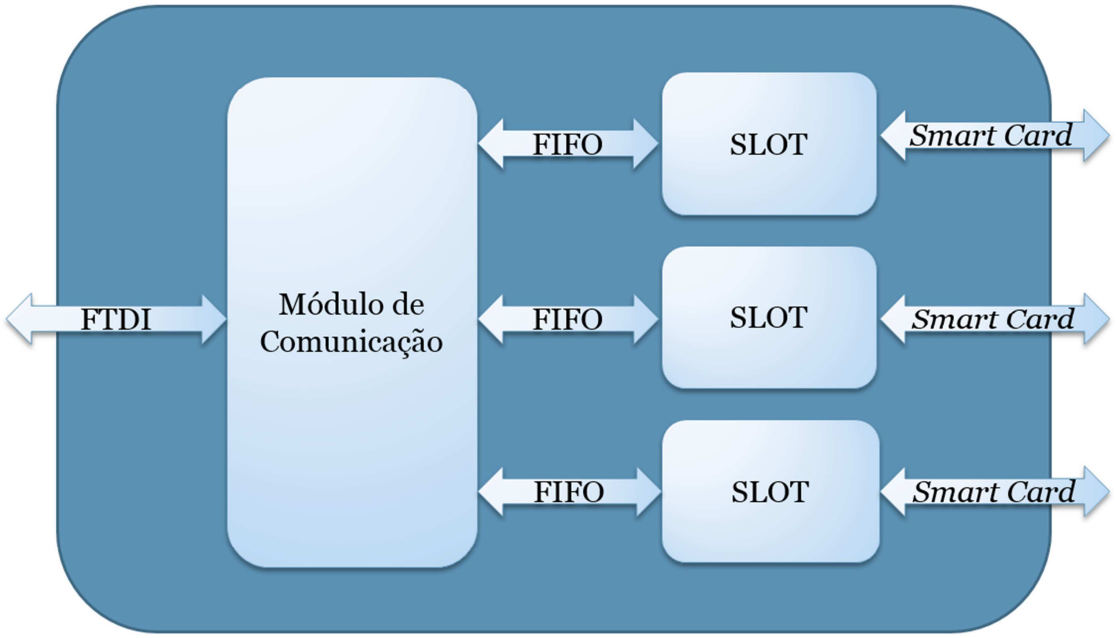

Figura 2 – Arquitetura interna do FPGA

Na etapa 3 é iniciado o desenvolvimento das FSM (*Finite State Machine*) que fazem parte do Módulo de Comunicação e do SLOT. Nesta etapa foram estudados os protocolos existentes para a comunicação com o *smart card* e o seu funcionamento, além das rotinas de inicialização e finalização. Após o desenvolvimento das FSM, foi iniciada a etapa de implementação das mesmas, utilizando a linguagem de descrição de hardware SystemVerilog.

DISCUSSÃO

Ao iniciar a etapa de desenvolvimento da BASE para se comunicar com o USB, se percebeu que não era viável manter a comunicação como tinha sido planejada, então foram necessárias mudanças para que a comunicação seja feita usando o protocolo CCID (*Chip Card Interface Device*). Tais modificações tiveram que ser realizadas tanto no Módulo de Comunicação, quanto no SLOT, sendo maior no Módulo de Comunicação.
Devido a estas alterações, a finalização e testes sofreram atrasos, e estão em andamento e devem ser concluídos até a realização do CONIC.

CONCLUSÕES

Num mundo cada vez mais digitalizado, a segurança é um fator crucial para a vida cotidiana, e abordagens confiáveis se fazem cada vez mais necessárias. Através dos estudos realizados é possível notar que o uso de *smart cards* tem uma grande importância nas tecnologias de segurança, e pode ser bastante abrangente, porém, as tecnologias atuais exploram apenas um lado da capacidade dos mesmos. Este trabalho propõe uma nova forma de utilizar os cartões para segurança de redes, com a finalidade de aumentar a segurança das mesmas.

AGRADECIMENTOS

Agradeço a PROPESQ por disponibilizar o auxílio financeiro e ao grupo do GPRT pelo fornecimento do espaço e do equipamento necessário para que a pesquisa fosse realizada sem maiores problemas. Agradeço também ao professor orientador pelo suporte durante toda a pesquisa.

REFERÊNCIAS

[1] Rankl, W.; Effing, W.: Smart Card: Handbook. Fourth Edition. United Kingdom: John Wiley & Sons Ltd, 2010.

[2] Chang, C. C., & Wu, T. C. (1991). Remote password authentication with smart cards. IEE Proceedings E: Computers and Digital Techniques, 138, 165–168.

[3] Pippal, Ravi Singh, Jaidhar, C. D. & Tapaswi, Shashikala. (2013). Robust Smart Card Authentication Scheme for Multi-server Architecture. Wireless Personal Communications, Volume 72, Issue 1, pp 729-745.