UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA

2012.1

AUTENTICAÇÃO DE USUÁRIO UTILIZANDO PLATAFORMA SEGURA

PROPOSTA DE TRABALHO DE GRADUAÇÃO EM REDES DE COMPUTADORES

Aluno – Matheus Bispo Arrais de Souza, mbas@cin.ufpe.br.
Orientador – Djamel Fawzi Hadj Sadok, jamel@cin.ufpe.br.
Coorientador – Eduardo Luzeiro Feitosa, efeitosa@icomp.ufam.edu.br.

10 de abril de 2012

1. Contexto

As redes de computadores são parte fundamental para o funcionamento adequado dos sistemas computacionais das empresas. Manter essa comunicação segura depende de inúmeras medidas, como o uso de criptografia para esconder as mensagens trocadas e a autenticação dos usuários para liberar os recursos de acordo com as permissões dadas ao usuário.

Essa área, a segurança da informação, é desafiadora devido ao valor que pode estar envolvido nos sistemas. Uma pequena vulnerabilidade pode trazer um grande prejuízo para as empresas. Essas ameaças são as mais variadas possíveis como falhas nos algoritmos ou nas suas implementações; vulnerabilidade de hardware (por exemplo, interceptar os barramentos de comunicação para extrair informações acerca do texto cifrado); vírus; ataque de negação de serviço, entre outros. Portanto, desenvolver soluções com menores possibilidades de ataque é fundamental para assegurar as informações dos sistemas.

Com a finalidade de tratar algumas dessas vulnerabilidades foi desenvolvido o TPM - *trusted plataform module*. Um TPM é um chip que fornece maior nível de segurança que um software, pois possui uma infraestrutura capaz de executar instruções de criptografia e armazenar as chaves necessárias diretamente em hardware [1,2]. A especificação desse hardware é um padrão definido pelo *trusted computing group*, um grupo formado por grandes empresas que estabelece padrões de tecnologia [3]. O TPM pode ser integrado em uma grande gama de dispositivos como celulares e computadores pessoais, onde o uso de computação segura se faz necessária. Esse *chip* já pode ser encontrado em alguns *laptops* de forma integrada.

2. Objetivos

Esse trabalho tem como objetivo o desenvolvimento de uma solução para autenticação de usuários, fazendo uso da uma plataforma segura. Nessa abordagem o usuário teria um TPM que armazena suas credenciais e pode confirmar sua identidade ao tentar acessar informações ou recursos restritos do sistema.

Especificamente pretende-se:

- Realizar um estudo acerca do estado da arte na área segurança da informação com ênfase em dispositivos seguros, como *smartcards* ,TPMs e outras possíveis soluções existentes.
- Instalar, testar e avaliar plataformas segura como, por exemplo, os projetos TPM Gateway [4] e Throusers [5], afim de verificar o uso de TPM para a identificação de usuários.
- Projetar e desenvolver uma proposta para autenticação de usuários utilizando TPM, real ou simulado, como o TPM Emulator [6].

3. Cronograma

O Quadro 1 mostra o cronograma previsto, dividido em semanas, para a realização das atividades necessárias ao desenvolvimento desse trabalho.

Quadro 1 - Cronograma

Mês	Abril				Maio				Junho				Julho			
Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Revisão bibliográfica																
Analisar o escopo do projeto																
Definir a estrutura do projeto																
Implementação da solução																
Avaliação da solução																
Avaliar resultados e problemas encontrados																
Redigir o documento final																
Revisão final																

4. Referências

[1] Cryptographic Processors - A Survey, Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov
[2] A Formal Analysis of Authentication in the TPM, Stephanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel
[3] http://www.trustedcomputinggroup.org/, acessado em 03 de abril de 2012
[4] http://www.cs.tau.ac.il/~orkaplan/TPMWorkshop/, acessado em 03 de abril de 2012
[5] http://trousers.sourceforge.net/, acessado em 03 de abril de 2012
[6] A Software-Based Trusted Platform Module Emulator, Mario Strasser and Heiko Stamer

_____

Matheus Bispo Arrais de Souza
Orientando

_____

Djamel Fawzi Hadj Sadok
Orientador

Recife, 10 de abril de 2012