Grupo de Resposta a incidentes de Segurança

Biometria

Thiago Elias
thiago@gris.dcc.ufrj.br
Breno G. De Oliveira
breno@gris.dcc.ufrj.br

03 de Dezembro de 2008

Biometria

Grupo de Resposta a Incidentes de Segurança
UFRJ – IM – DCC – GRIS

- Objetivos
- O que é biometria?
- Senha X Impressão Digital
  - Senha
  - Impressão Digital
- Experiências Realizadas
- Próximos Trabalhos
- Bibliografia

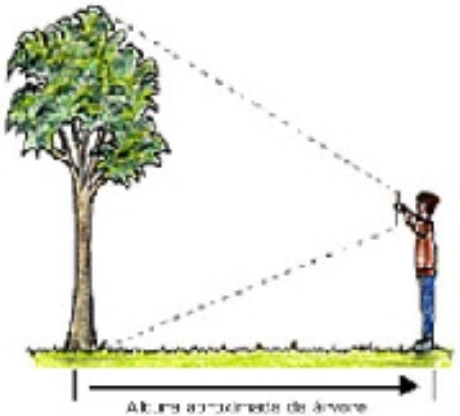
Grupo de Resposta a
Incidentes de Segurança
UFRJ – IM – DCC – GRIS

O que é Biometria?

O que é Biometria?

Biometria
BIO (vida) + METRIA (medida)

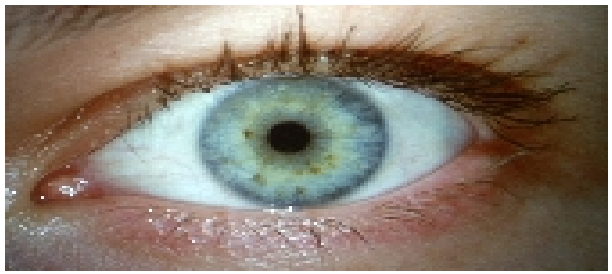
É o estudo estatístico das características físicas ou comportamentais dos seres vivos. Recentemente este termo também foi associado a medida de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente.



O que é Biometria?

Grupo de Resposta a Incidentes de Segurança
UFRJ – IM – DCC – GRIS

Hoje a biometria é usada na identificação criminal, controle de ponto, controle de acesso, etc. Os sistemas chamados biométricos podem basear seu funcionamento em características de diversas partes do corpo humano, por exemplo: a palma da mão, as digitais do dedo, a retina ou íris dos olhos. A premissa em que se fundamentam é a de que cada indivíduo é único e possui características físicas e de comportamento (a voz, a maneira de andar, etc.) distintas.



http://myhometheater.homestead.com/files/milla_eye.jpg

http://thumbs.dreamstime.com/thumb_187/11902508732A9kAv.jpg

Objetivo do Trabalho

Objetivo do Trabalho

O Objetivo deste trabalho é alertar sobre a utilização de sistemas de autenticação baseados em impressão digital (é a técnica biométrica com melhor custo/benefício).

Uma experiência feita em 2001(Sandström) burlou todos os leitores testados.

Outra em 2002(Matsumoto) verificou falhas em diversos leitores, além disso, analisou a possibilidade de burlar um sistema de impressão digital usando uma digital latente deixada em um copo, por exemplo.

Desde então diversas teses que tratam sobre como identificar uma digital viva vêm sendo publicadas.

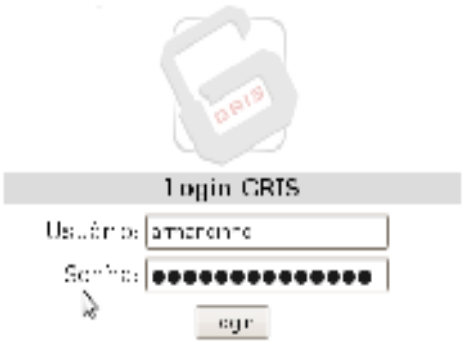
Biometria

Senha X Impressão Digital

Senha X Impressão Digital

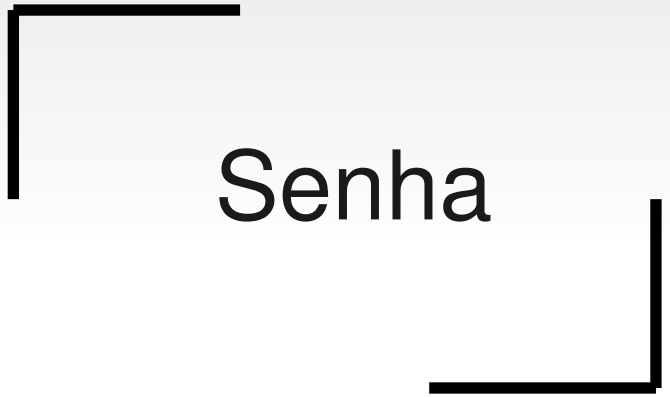
Grupo de Resposta a Incidentes de Segurança
UFRJ – IM – DCC – GRIS

Gradativamente a autenticação por senha está sendo substituída pela de impressão digital. Porém, devemos ter cuidado, pois a senha já está consolidada e devidamente estudada e a de impressão digital ainda necessita de mais estudos, principalmente estudo de vulnerabilidades. Cada uma tem seus pontos positivos e negativos que veremos a seguir.



http://1.bp.blogspot.com/_41Ti2-JCYWY/SLa94bo3m2I/AAAAAAAAAF0/NbjS9sdtV-U/s1600-h/leitora+impress%C3%A3o+digital.jpg

Biometria



Senha

Este é o modo de autenticação mais usado até hoje. Consiste em um par de cadeia de caracteres sendo eles o nome de usuário e a senha. Em alguns casos, como no controle de acesso físico, pode existir apenas uma senha numérica.

Ela é considerada por muitos peritos em segurança da informação como o elo mais fraco por diversos motivos. Porém, com o uso de políticas rígidas de utilização e troca, ela se torna forte e muito útil contra pessoas mal intencionadas.

http://lh3.ggpht.com/_UpHsVX9pF5w/Rs2hM47eOZI/AAAAAAAAAP4/-JYmxqMgORA/13_05_besafer.jpg

Grupo de Resposta a
Incidentes de Segurança
UFRJ – IM – DCC – GRIS

Vantagens e Desvantagens

Vantagens:

- Não pode ser roubada da sua mente;
- Pode ser alterada caso alguém tenha acesso a ela;
- Pode ser emprestada em casos emergenciais;
- Não precisa de aparelhos especializados.

Desvantagens:

- Pode ser esquecida;
- Sua eficiência depende do usuário seguir a política de senhas;
  - Trocar de 3 em 3 meses;
  - Ter mais de 6 caracteres sendo eles maiúsculos, minúsculos, especiais e numéricos;
  - Ser de fácil digitação;
  - Etc.

Mais informações: https://www.gris.dcc.ufrj.br/artigos/GRIS-2005-A-002.pdf

Biometria

Impressão Digital

Impressão Digital

Este método de autenticação vem sendo amplamente divulgado como o método que traz mais segurança aos usuários. Consiste em submeter sua digital a um leitor que captura a imagem e através de um software, faz o reconhecimento utilizando uma base de dados. Traz comodidade e uma sensação ao usuário de estar tecnologicamente atualizado, ou seja, virou moda.

http://img.dailymail.co.uk/i/pix/2007/10_03/fingerpMS2010_468x665.jpg

Vantagens e Desvantagens

Vantagens:

- Solução para a maioria dos problemas das senhas;
- Fácil utilização do usuário;
- Não depende da forma de utilização;
- Não pode ser esquecida.

Desvantagens:

- Vem sendo utilizada sem estudo de segurança;
- Pode ser capturada;
- Pode ser roubada;
- Necessita de aparelhagem específica;
- Forjamento de provas.

Impressão Digital

Grupo de Resposta a Incidentes de Segurança
UFRJ – IM – DCC – GRIS

O Método

A Impressão digital é formada por sulcos presentes nos dedos. As formas como estes sulcos estão dispostos formam as características da impressão digital. Estas características são extraídas através de um software de processamento de imagem. Sendo assim:

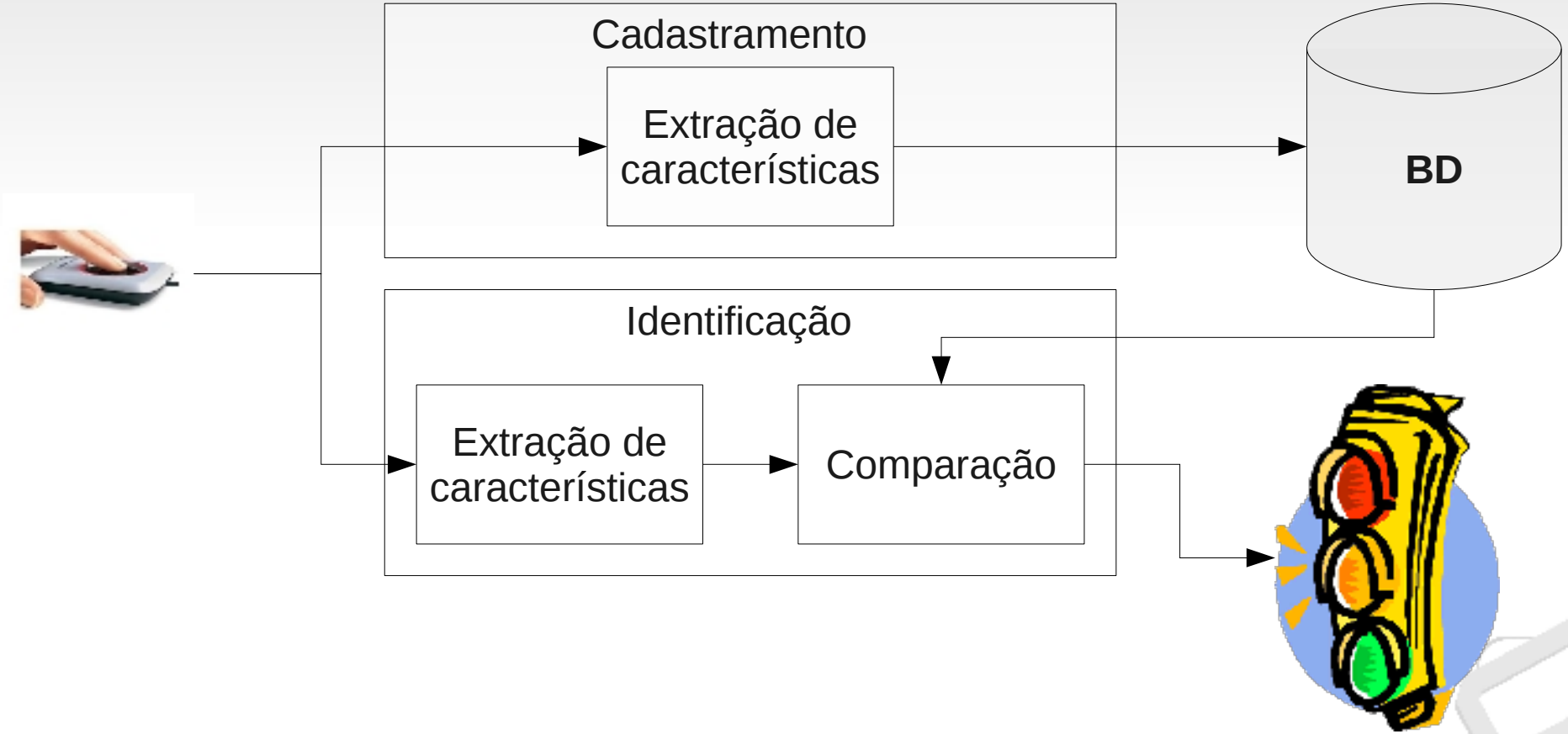
Imagem gerada pelo leitor

Processamento de imagem

Informação armazenada no BD

Impressão Digital

O Método



Métodos de ataque

Um criminoso poderia aplicar os seguintes ataques:

- Obrigar uma pessoa a apresentar a digital por coação ou droga;
- Cortando o dedo de alguém, que está cadastrado;
- Força bruta;
- Clone genético da digital;
- Clone artificial de uma digital.

Grupo de Resposta a
Incidentes de Segurança
UFRJ – IM – DCC – GRIS

Experiências Realizadas

Experiências Realizadas

Tentando comprovar que ainda hoje existem falhas nos leitores de impressão digital, estamos realizando alguns testes em parceria com a empresa Kognitus. O método de ataque utilizado foi um clone artificial e para isso, seguimos o artigo publicado por Matsumoto para fabricar as digitais falsas de gelatina utilizando um molde feito por uma digital viva.

Artigo lido para as experiências:
http://cryptome.info/0001/gummy/gummy.htm

Experiências Realizadas

O teste consistia em:

- Cadastrar o indivíduo A no banco de dados;
- Clonar a digital do indivíduo A;
- O indivíduo B conseguir ser aceito utilizando a digital clonada;

e

- Clonar a digital do indivíduo A;
- Cadastrar a digital clonada no banco de dados;
- O indivíduo A conseguir ser aceito;

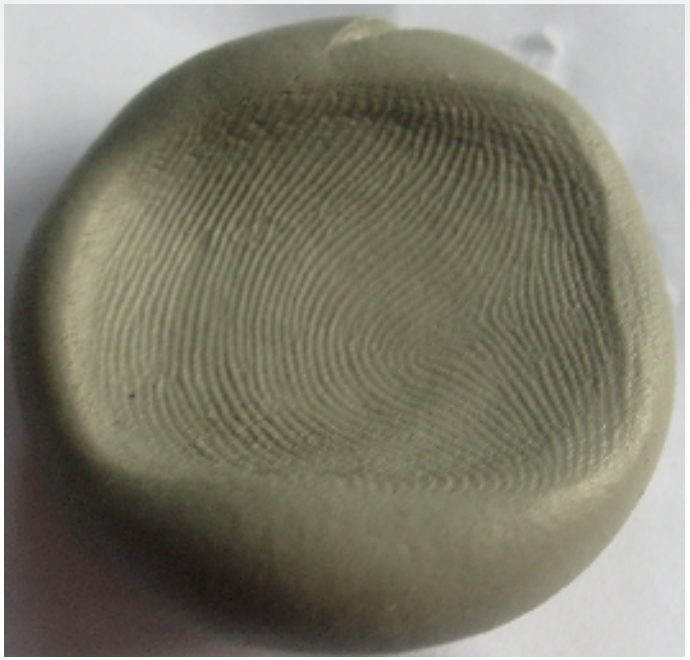
Experiências Realizadas

Resultados

O único resultado que conseguimos chegar por enquanto é que o leitor testado não rejeitou a digital falsa, ou seja, ele faz a leitura, mas por mal formação do molde e a falta de recursos, ainda não conseguimos fazer com que a digital falsa seja identificada.

Experiências Realizadas

Algumas fotos das experiências

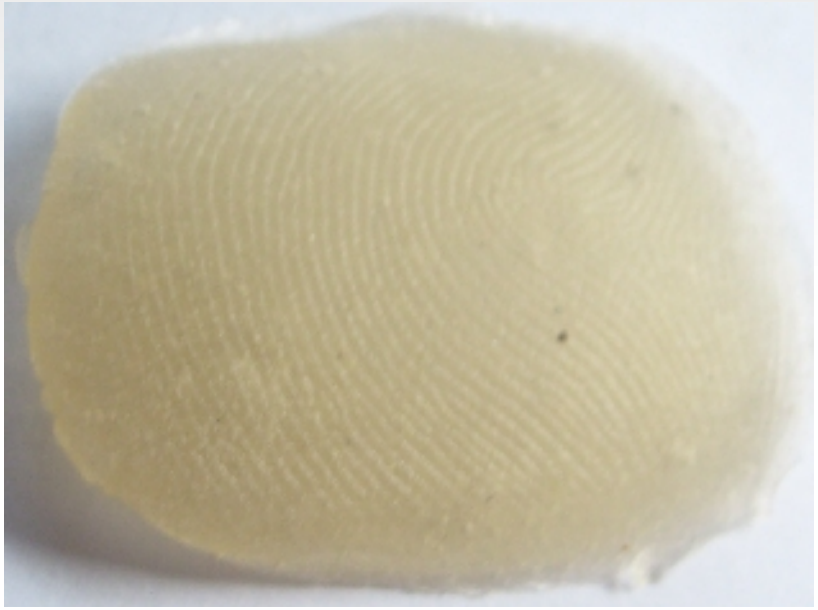


Molde

Gelatina no molde

Experiências Realizadas

Algumas fotos das experiências



Gelatina com a impressão digital falsa

Próximos Trabalhos

Próximos Trabalhos

Daremos continuidade a esta pesquisa e as principais tarefas a serem realizadas são:

- Fazer com que a digital falsa obtida através da digital viva seja identificada utilizando tipos diferentes de leitores;
- Fazer um molde utilizando uma digital latente(alto custo);
- Fazer com que a digital falsa obtida através da digital latente seja identificada utilizando tipos diferentes de leitores;
- Catalogar quais os leitores são burlados com esses métodos.

Bibliografia

Bibliografia

- Wikipédia: http://pt.wikipedia.org/wiki/Biometria
- OLIVEIRA, Breno G. de. *Como Escolher uma senha.* RJ, 2005.
- JARDINI, Evandro de Araújo. *MFIS: Algoritmo de Reconhecimento e Indexação em Base de Dados de Impressões Digitais em Espaço Métrico.* SP, 2007.
- MATSUMOTO, Tsutomo e Hiroyuki. YAMADA, Koji. HOSHINO, Satoshi. *Impact of Artificial "Gummy" Fingers on Fingerprint Systems.* Japão, 2002.
- SANDSTRÖM, Marie. *Liveness Detection in Fingerprint Recognition Systems.* Linköping, 2004.

Dúvidas?

Thiago Elias
thiago@gris.dcc.ufrj.br