# Projeto de Formatura – Turmas 2018

## PCS - Departamento de Engenharia de Computação e Sistemas Digitais

### Engenharia de Computação

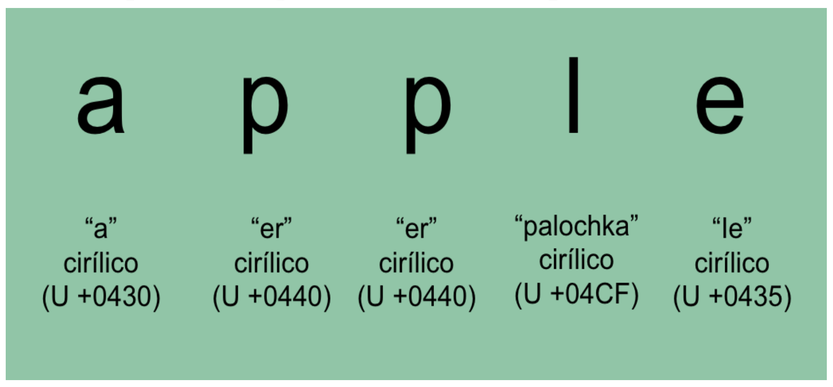
**Tema:**

Módulo de segurança web para hashing de senhas e proteção contra phishing

## PROPOSTA

O projeto consiste em um plugin de segurança para browsers que acrescenta uma camada extra de *hashing* de senhas durante a autenticação em algum site e como atividade paralela verifica possíveis ataques de *phishing* por caracteres homógrafos (de grafia semelhante ou idêntica).

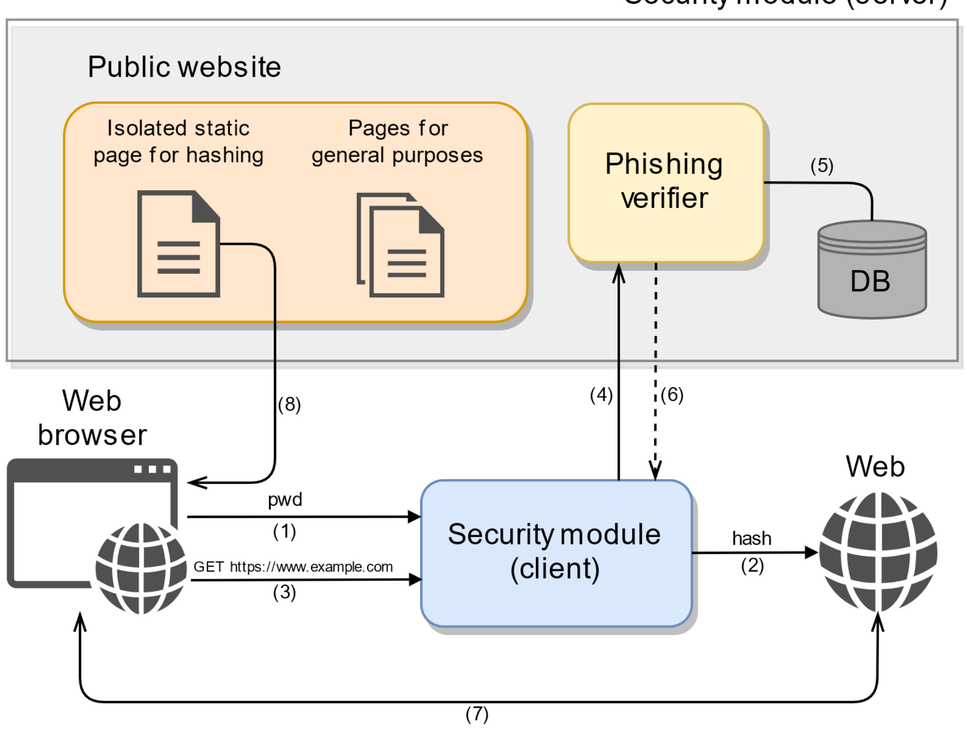
Figura 1 – Ataque homógrafo utilizando apenas caracteres cirílicos (1).




- **Contexto:** Diversos esquemas de *hashing* de senhas estão presentes no cotidiano do usuário da Internet, em diversos sistemas. O IDNA é um protocolo de internacionalização de domínios que permite visualizar domínios por caracteres Unicode.
- **Problema:** O usuário não pode optar por um esquema de *hashing* mais seguro. Reuso de senhas possibilita invasões bem sucedidas em sistemas distintos. Outro problema é o *phishing* utilizando caracteres Unicode idênticos de outro alfabeto em registro de domínios.
- **Solução:** Desenvolvimento de um plugin que interceptará as tentativas do usuário de se logar em um website e realizar o *hashing* da senha utilizando um algoritmo seguro (Lyra2) com sal composto do domínio acessado. Como atividade complementar irá verificar ataques de *phishing* complexos por *address spoofing*.

## ESPECIFICAÇÃO DA ARQUITETURA

Figura 2 – Arquitetura do sistema.





Integrantes: Daniel Norio Takasu Rabelo
Victor França Ferreira

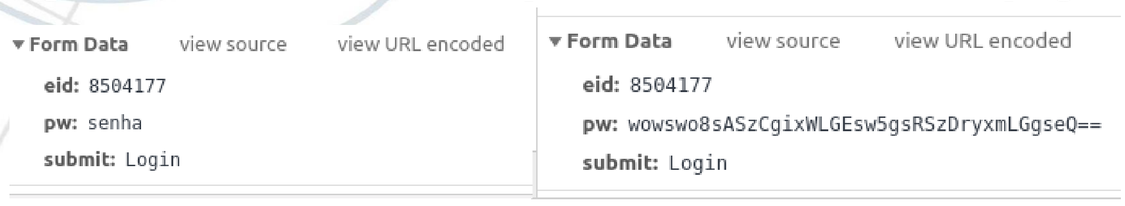
Professor Orientador: Prof. Dr. Marcos A. Simplicio Jr


## IMPLEMENTAÇÃO E RESULTADOS

Implementamos o plugin com as funcionalidades abaixo:

- Hash automático da senha com Lyra2 em Javascript nativo, através da WebExtensions API;
- Configuração de tamanho, tempo e memória para geração de hashs e restrição de caracteres por domínio;
- Geração do hash base variável de saída para satisfazer restrição de caracteres na autenticação em sistemas;

Figura 3 – Form Datas enviados para o Tidia-AE sem, e com o plugin.




- Geração de uma base de homógrafos;
- Implementação das práticas recomendadas pelo *Unicode Technical Standard #39 – Security Mechanisms* (2), da própria Unicode;
- Opção de sempre exibir endereços em punycode (apenas o Firefox disponibiliza isso nativamente);
- Detecção de diversos tipos de ataques de phishing por homógrafos: *Mixed-Script*, *Whole-Script*, *Single-Script* e *Numeric*, fazendo inferências através do idioma do usuário, da qualidade da página, e da existência de algum homógrafo com maior perfil de segurança;
- Cacheamento das consultas ao phishing verifier.

Além disso, implementamos um servidor DNS simples a fim de demonstrações e implantamos na Web uma página para realizar o hashing onde o plugin não puder ser instalado.

## REFERÊNCIAS


1 ZHENG, XUDONG. Phishing with Unicode Domains. Disponível em https://tinyurl.com/ksmqfr5, 2017.

2 Unicode Security Mechanisms. Disponível em https://tinyurl.com/y885u4s8, 2018.