Titulo : Acesso aos Tokens Criptográficos via Web

Orientadores(s) (UBI)

- Prof. Dr. Paul Crocker : Email: crocker@di.ubi.pt
- Prof. Dr. Simão Melo de Sousa (Co-Orientador)

Descrição

Hoje em dia os browsers têm vindo a restringir cada vez mais o acesso aos plugins no browser. Exemplo disso é o Chrome que já não permite a execução de Java applets. Esta restrição dificulta os processos de autenticação e de assinatura de documentos em páginas web que necessitam acesso aos recursos como smart cards ou outros elementos seguros como tokens USB. Existem alternativas aosplugins como por exemplo o Web Cryptography API [1] que descreve um API de JavaScript para executar operações básicas de criptografia, por exemplo a criação de Hashs e Assinaturas digitais. No entanto este API não trate do acesso aos elementos seguros. Encontra-se a ser desenvolvida pela Google uma Web API de acesso às portas USB. Apesar desta especificação ainda ser *draft* [3] já esta implementada no browser de desenvolvimento da Google [2].

Os objectivos deste projecto visam explorar esta API para implementar aplicações web que aceda aos Smart cards ou Tokens USB e efectue assinaturas digitais com as chaves criptográficas presentes nestes equipamentos. Também faz parte do desafio analisar o desempenho das aplicações via Web e fazer uma analise das propriedades da segurança propondo também modelos de ameaça apropriados.

Os Middlewares necessários para a interacção com smart cards, por exemplo o cartão de cidadão, serão disponibilizados pelos orientadores deste trabalho. Este tese de mestrado poderá contar com a colaboração da empresa MultiCert.

Plano de Trabalho

1. A realização de um estudo e levantamento do estado arte das soluções existente assim como de soluções alternativas;
2. Analise do estado das propostas das API's;
3. Análise, comparação e proposta de evolução dos vários Standards;
4. Desenho de um sistema, incluindo aplicação cliente e servidor que permita a criação de um protótipo de uma solução real para o problema;
5. Implementação da solução desenhada e analise do seu desempenho;
6. Modelo de Segurança e Analise.

Resultados Esperados

Dissertação e prova de conceito para aceder aos tokens criptográficos via Browser.

Referencias

[1] https://www.w3.org/TR/WebCryptoAPI/
[2] https://www.chromestatus.com/features/5651917954875392
[3] https://wicg.github.io/webusb/

Hide

[4] https://code.google.com/p/chromium/issues/detail?id=492204
[5] https://wiki.mozilla.org/Security/WebAPI/Web_USB
[6] https://bugzilla.mozilla.org/show_bug.cgi?id=674718