Seguridad Informática.

Formalidades de trabajo en equipo.

Grupos.

- No más de 4 personas.

Fecha de Entrega: 11/11/2016

Objetivos del Trabajo.

- Analizar diferentes soluciones de control de acceso lógico.
- Analizar los diferentes algoritmos criptográficos, comparando soluciones simétricas y asimétricas.
- Analizar las principales debilidades existentes en soluciones de control de acceso y criptográficas; y los ataques existentes, de forma de realizar una implementación robusta.
- Analizar las mejores prácticas para el desarrollo seguro.
- Realizar un aprendizaje práctico en la implementación de mecanismos de control de acceso lógico y soluciones criptográficas en las aplicaciones.
- Realizar un trabajo de investigación que incluya el uso de la nueva cedula de identidad uruguaya.

Descripción del Trabajo.

Documentar el análisis, especificación técnica y desarrollar un prototipo operativo de una solución que:

1. Permita Identificar, Autenticar y Autorizar a sus usuarios, almacenando las contraseñas de forma que se preserve en todo momento su seguridad por medio del uso de algoritmo de one-way hash.

2. Permita cifrar y descifrar archivos por medio del uso de algoritmos simétricos, formalizando mecanismos seguros para el intercambio de la clave.

3. Utilice algoritmos probados, implementados por APIs criptográficas.

4. Realice una implementación robusta y segura de los algoritmos.

5. Permita firmar digitalmente (y verificar la firma) archivos por medio del uso de algoritmos asimétricos, considerando mecanismos seguros para el intercambio de las claves requeridas.

6. Se haga un uso de dispositivos criptográficos en Hardware (Ej. Nueva Cedula Uruguaya) para las funciones de control de acceso y criptográficas.

Entregables:

- Informe formal del análisis realizado, detallando la especificación técnica y las fortalezas de la solución diseñada e implementada ante las principales vulnerabilidades y ataques conocidos.
- Código y Aplicación operativa junto con los elementos de demuestren su desempeño.
- Presentación y defensa del trabajo.

Referencias:

AGESIC – Drivers CI Uruguaya.

http://www.agesic.gub.uy/innovaportal/v/5314/1/agesic/documentacion-y-drivers-de-firma-digital.html

Micrtosoft Windows DEV Center – Using Cryptography

https://msdn.microsoft.com/en-us/library/windows/desktop/aa388162(v=vs.85).aspx

Microsoft - Cryptographic Services .NET Framework 4.6 and 4.5

https://msdn.microsoft.com/en-us/library/92f9ye3s.aspx

Java ™ Cryptography Architecture - (JCA) Reference Guide

http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

Libros:

https://www.schneier.com/books/applied_cryptography/