Formulario de Aprobación Curso de Posgrado 2015

Asignatura: Dispositivos móviles de alta seguridad

Profesor de la asignatura [1]:
Dr. ing. Eduardo Gimenez, Investigador asociado del PEDECIBA

Profesor Responsable Local [1]:
Msc. Ing. Maria Eugenia Corti, Profesor Adjunto, Instituto de Computación

Otros docentes de la Facultad:

Docentes fuera de Facultad:
Ing. Daniel Pedraja

Instituto ó Unidad: Instituto de Computación
Departamento ó Area: Seguridad Informática

Fecha de inicio y finalización: 30 de junio al 14 de agosto
Horario y Salón: Martes, jueves y viernes de 18:00 a 21:00 – Salón a confirmar

Horas Presenciales: 53
(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

Nº de Créditos: 6
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem metodología de la enseñanza)

Público objetivo y Cupos: Profesionales y estudiantes interesados en los temas de seguridad informática y/o en la programación de dispositivos móviles como por ejemplo: tarjetas SIM, tarjetas de transporte STM, dispositivos NFC, etc.
Sin cupo

Objetivos: La última década ha sido testigo del desarrollo de dos conceptos que han impactado significativamente en las tecnologías de la información: la seguridad informática y la movilidad. Este curso se focaliza en una tecnología que está en el cruce de esas dos áreas temáticas y que se conoce habitualmente bajo el nombre de tarjetas inteligentes (smart cards). Estos dispositivos se componen de un micro-controlador que brinda capacidad de cálculo (en especial, de cálculo criptográfico) a un objeto o soporte físico de pequeño tamaño en el cual va inserto (una tarjeta plástica, una libreta de papel, un pendrive, un teléfono celular, etc) y que está sometido a elevados requerimientos de seguridad. Ejemplos de este tipo de dispositivos son: la tarjeta SIM en un teléfono celular, una tarjeta de transporte como las utilizadas en el Sistema de Transporte Metropolitano de Montevideo, tarjetas bancarias con micro-chip conforme al estándar EMV, pasaportes electrónicos como los que utilizan los países de la Union Europea, etc. El curso introduce al estudiante a las diferentes tecnologías subyacentes a estos dispositivos y a los estándares industriales internacionales que regulan su implementación. Al final del curso el estudiante será capaz de comprender proyectos que integren la utilización de tarjetas inteligentes y de diseñar y desarrollar código Java destinado a ser embarcado en este tipo de dispositivos.

Conocimientos previos exigidos: Conceptos de Programación en Java.

Conocimientos previos recomendados: Conocimientos básicos de programación y arquitectura de sistemas.

Metodología de enseñanza:
(comprende una descripción de las horas dedicadas por el estudiante a la asignatura y su distribución en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

- Horas clase (teórico): 30
- Horas clase (práctico):
- Horas clase (laboratorio): 15
- Horas consulta: 6
- Horas evaluación: 2
    - Subtotal horas presenciales: 53
- Horas estudio: 20
- Horas resolución ejercicios/prácticos:17
- Horas proyecto final/monografía: 0
    - Total de horas de dedicación del estudiante: 90

Forma de evaluación:
El curso se evaluará a partir de:

- los laboratorios
- un examen final de 2 hs.

Temario:

1 Introducción a los dispositivos móviles de alta seguridad (DMAS)
1.1 Principales características tecnológicas
1.1.1 Modelo computacional
1.1.2 Formatos (form factors)
1.1.3 Tipos de memorias
1.1.4 Terminales de lectura
1.2 Casos de uso: banca, transporte, telecomunicaciones e identificación
1.3 Formatos y componentes
1.4 Estándares industriales

2 Tecnología
2.1 Arquitectura interna
2.2 Microcontroladores: principales características
2.3 Soportes físicos del microcontrolador: materiales y formatos
2.4 Interfaces de comunicación: ISO7816, ISO 14443 y NFC

3 Ambiente de ejecución de aplicaciones
3.1 Dispositivos abiertos multiaplicación: la tecnología Java Card
3.2 Java Card Runtime Environment:
3.2.1 Selección de applets
3.2.2 Canales lógicos
3.2.3 Objetos Transcientes
3.2.4 Protección de applets: el Java Card Firewall
3.2.5 Transacciones
3.2.6 Java Card API
3.3 La máquina virtual Java Card
3.3.1 Restricciones respecto a Java
3.3.2 El formato CAP
3.3.3 Bytecodes Java Card
3.3.4 Bytecode verification y su rol en la arquitectura de seguridad

4 Administración de dispositivos móviles: la tecnología GlobalPlatform

4.1 Componentes de la arquitectura GlobalPlatform
4.2 Dominios de seguridad
4.3 Canales de comunicación seguros: los protocolos SCP
4.4 Ciclo de vida del dispositivo y de las aplicaciones
4.5 Privilegios de las aplicaciones
4.6 Administración delegada
4.7 Administración OTA (Over the Air)

5 Aplicaciones
5.1 Aplicaciones de firma electrónica: el estándar ISO
5.2 Aplicaciones de identificación: el estándar ICAO 9303
5.3 Aplicaciones de banca: el estándar EMV

6 Ciclo de vida de un dispositivo móvil de alta seguridad
6.1 Diseño
6.2 Inicialización y personalización
6.3 Mantenimiento

7 Estándares de certificación de seguridad
7.1 El estándar ISO 15408 "Common Criteria"
7.2 El estándar FIPS 140-2

Bibliografía:

Chen, Zhiqun. Java Card technology for Smart Cards :architecture programmer's guide
Rankl, Wolfgang. Smart card applications :design models for using and programming smart cards
Rankl, Wolfgang. Smart card Handbook, fourth edition
Jurgensen, Timothy M. Smart cards :the developer's toolkit
Hendry, Mike. Multi-application smart cards :technology and applications

Java Card Platform Specification, v2.2.2, Sun Microsystems.
GlobalPlatform Card Specification v2.1.1, GlobalPlatform Consorcium.
ICAO Document 9303, International Civil Aviation Organization.