



GRUPO DE SEGURIDAD INFORMÁTICA

Seguridad Informática en Ingeniería

Gustavo Betarte

Grupo de Seguridad Informática
Instituto de Computación
Facultad de Ingeniería - UdelaR



JIAP 2007



GRUPO DE SEGURIDAD INFORMÁTICA

Plan

- Contexto
- El Grupo de Seguridad Informática (GSI)
- Enseñanza
- Actividad de Investigación
- Proyectos en curso
- Asesoramiento especializado



- Creciente importancia de la temática a nivel académico e industrial
- Ausencia en Fing-UdelaR de
 - actividad formal de investigación en Seguridad Informática
 - formación curricular de grado y posgrado
- Buen nivel de conocimiento y experiencia, pero dispersos y no coordinados



Grupo de Seguridad Informática

- Formado a comienzos del año 2006
- Integrado por docentes y profesionales del InCo, IIE y la URI de la Facultad de Ingeniería
- Objetivos
 - Formación de RRHH (grado y posgrado)
 - Investigación
 - Asesoramiento especializado



GRUPO DE SEGURIDAD INFORMÁTICA

Formación de RRHH



GRUPO DE SEGURIDAD INFORMÁTICA

Cursos

- ***Fundamentos de la Seguridad Informática***
 - Curso opcional de grado (Ing. en Computación)
 - Curso de posgrado (Pedeciba Informática)
- ***Seguridad de Sistemas Informáticos***
 - *Curso del diploma de especialización del Centro de Posgrados y Actualización Profesional (CPAP)*



GRUPO DE SEGURIDAD INFORMÁTICA

Áreas de Estudio

- Criptografía aplicada
- IAA
- Control de acceso: modelos y políticas
- Sistemas Operativos
- Redes
- Aplicaciones
- Bases de datos



GRUPO DE SEGURIDAD INFORMÁTICA

Laboratorios

- Formación teórica complementada con experimentación
- Familiarización con técnicas y herramientas
- Diversidad de dominios
- Infraestructura informática y de comunicaciones configurable y escalable
- Plataformas customizables



Concepción, Diseño e Implantación

- Características y elementos de diseño
 - Escenario complejo y altamente variable
 - Fácil replicación e independencia del hardware
 - Proteger al resto de las máquinas pertenecientes al laboratorio
 - Las máquinas involucradas (y vulnerables) no tienen que quedar expuestas
 - Ensayos multiplataforma
- Infraestructura basada en tecnología de Máquinas Virtuales



- Equipos que actúan de clientes
 - Equipos con instalación fija utilizados como terminal
 - Software cliente de Máquina Virtual
- Framework de trabajo
 - Servidores dedicados
 - Software que implementa núcleo del ambiente virtual
- Equipos virtuales preinstalados
 - Servidores: web, ssh, correo
 - Estaciones de trabajo: Windows, Linux
 - Máquinas atacantes: diferentes herramientas instaladas



GRUPO DE SEGURIDAD INFORMÁTICA

Explotación de Vulnerabilidades

- Man in the Middle
- Password cracking
- Vulnerabilidades de MD5
- Intrusión
- Tests de penetración
- SQL injection, cross-site scripting



GRUPO DE SEGURIDAD INFORMÁTICA

Protección y Reacción

- Password checkers
- Password managers
- Firewalls
- IDSs
- VPNs
- PKI



GRUPO DE SEGURIDAD INFORMÁTICA

Investigación



Situación actual y enfoque

- Estado inicial
- Énfasis en la formación de posgrado
- Se comienza a profundizar en líneas de trabajo
- Tesis/Estudios de Maestría en curso
- Interacción con grupo de Métodos Formales del InCo
- Cooperación internacional



- Análisis Forense Digital
- Computación distribuida segura
- Honeypots y honeynets
- Especificación y verificación formal de sistemas críticos
- Análisis estático de programas
- Virtualización y Seguridad



- Modelos de Seguridad
- Sistemas embebidos
 - Java Card
 - J2ME – MIDP (2.0, 3.0)
- Asistentes de prueba
- Verificadores lógicos
- Análisis estático de código móvil



GRUPO DE SEGURIDAD INFORMÁTICA

Arquitectura de Seguridad de J2ME - MIDP

- Plataforma implantada en más de 1000 M dispositivos
- Estándar y portable
- Ejecución de aplicaciones Java (MIDlets)
- Plataforma abierta
 - Descarga e instalación de aplicaciones
 - Escalabilidad de funcionalidades
- Interacción con plataforma Java Card (SIM)



Especificación y Verificación

- Especificación formal de modelo de permisos y reglas de control de acceso a funcionalidades sensibles del dispositivo
- Formulación y prueba de propiedades
- Máquinas de estado
- Lenguaje formal: Cálculo de Construcciones Inductivas
- Asistente de pruebas: Coq



GRUPO DE SEGURIDAD INFORMÁTICA

Proyectos



GRUPO DE SEGURIDAD INFORMÁTICA

Proyecto CERTuy

- Metodologías y herramientas para la gestión de incidentes de seguridad
- Diseño e Implantación de un CSIRT nacional
- Actividad específica en el contexto del convenio marco de cooperación entre ANTEL y FING-UdelaR
- Integrantes del proyecto
 - Gerencia de Seguridad de la Información, CSIRT (ANTEL)
 - Grupo de Seguridad Informática (FING)



Proyecto STEVE

- Seguridad a Través de Evidencia Verificable
 - Computación distribuída segura
- Especificación y Verificación de Sistemas de Componentes
 - Modelo seguridad J2ME – MIDP 3.0
 - Modelo de permisos de MIDP
- Actividad enmarcada en proyecto internacional de cooperación científico-tecnológica STIC Amsud “*ReSeCo: Reliability and Security of Distributed Software Components*”.



Proyectos de grado

- Honeypots de bajo nivel de interacción (InCo)
- Herramienta para gestión de incidentes en CSIRT (InCo)
- Control de acceso en sistemas de aplicaciones (InCo)
- Automatización de implantación y mejora continua de SGSI (InCo)
- Modelo de Seguridad de J2ME – MIDP 3.0 (InCo)
- Formalización del Controlador de Acceso de J2ME (Universidad de Rosario, Argentina)



GRUPO DE SEGURIDAD INFORMÁTICA

Asesoramiento



GRUPO DE SEGURIDAD INFORMÁTICA

Técnico - Organizacional

- Análisis y diagnóstico del estado de la seguridad informática de la División Informática de la Oficina Central de la DGR
- Recomendaciones
- Alcance
 - Infraestructura tecnológica de hardware y de software
 - Seguridad física y prácticas operativas
 - Evaluación de la Seguridad: perimetral, de la red local, de los servidores, de los puestos de trabajo



GRUPO DE SEGURIDAD INFORMÁTICA

Técnico - Estratégico

- Participación en el grupo de trabajo de Seguridad de la Información auspiciado por AGESIC
- Cometidos del grupo
 - Analizar y proponer un marco legal para regular el accionar de los diversos actores en los incidentes de seguridad informática mayores
 - Analizar y promover la implementación de un Centro de Respuesta a Incidentes Informáticos nacional, para el Estado Uruguayo



- Consolidación del equipo
- Formación curricular de grado y posgrado
- Ambiente de experimentación
- Desarrollo de líneas de investigación
- Tesis de posgrado y de grado
- Intensa actividad de proyectos: cooperación nacional e internacional
- Asesoramiento especializado

1967

Computador Universitario



Analista en Computación
Ingeniería en Computación
Estudios Avanzados en Computación
Maestría en Ingeniería en Computación
Maestría en Informática
Doctorado en Informática

InCo

2007