Actividades del Grupo de Seguridad Informática

Dr. Ing. Gustavo Betarte (Prof. Titular)
Ing. Alejandro Blanco (Prof. Adjunto)

Grupo de Seguridad Informática
Instituto de Computación, Facultad de Ingeniería
Universidad de la República

www.fing.edu.uy/~[gustun,ablanco]
www.fing.edu.uy/inco/grupos/gsi

Encuentro TICAL - Abril 2015

Plan

1. Formación Curricular
   - Cursos
   - Laboratorio
2. Proyectos I + D
   - XOval, Indicadores de compromiso, Forensia digital
   - Hacia un CSIRT nacional (ANTEL)
   - Gestión de Identidad Electrónica (AGESIC)
3. Asesoramiento especializado

Grupo de Seguridad Informática (GSI - FING)

- 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

Cursos de grado y posgrado

- Fundamentos de la Seguridad Informática
  - Curso electivo de grado (Ing. en Computación)
  - Curso de posgrado (Pedeciba Informática)
  - `http://www.fing.edu.uy/inco/cursos/fsi`

Cursos de grado y posgrado

- Fundamentos de la Seguridad Informática
  - Curso electivo de grado (Ing. en Computación)
  - Curso de posgrado (Pedeciba Informática)
  - `http://www.fing.edu.uy/inco/cursos/fsi`
- Taller de Seguridad Informática
  - Focalizado en aplicación de metodologías y uso de herramientas
  - `http://www.fing.edu.uy/inco/cursos/tallersi`

Cursos de grado y posgrado

- Fundamentos de la Seguridad Informática
  - Curso electivo de grado (Ing. en Computación)
  - Curso de posgrado (Pedeciba Informática)
  - `http://www.fing.edu.uy/inco/cursos/fsi`
- Taller de Seguridad Informática
  - Focalizado en aplicación de metodologías y uso de herramientas
  - `http://www.fing.edu.uy/inco/cursos/tallersi`
- Diploma de Especialización en Seguridad Informática
  - Diploma de posgrado del CPAP
  - `http://www.fing.edu.uy/cpap/carreras/`

Laboratorio de Seguridad Informática

- El laboratorio brinda un ámbito que permite complementar la teoría con la experimentación
- Familiarización con técnicas y herramientas
- Diversidad de dominios
- Infraestructura informática y de comunicaciones configurable y escalable
- Características
  - Escenario complejo y altamente variable
  - Fácil replicación e independencia del hardware
  - Proteger al resto de las máquinas pertenecientes al laboratorio
  - Previene exposición de las máquinas involucradas (y vulnerables)
  - Ensayos multiplataforma

Áreas de trabajo

- Especificación y verificación formal de arquitecturas de seguridad de sistemas críticos
  (BBCL 2011, BBCL 2012, BBCCL 2014)

Áreas de trabajo

- Especificación y verificación formal de arquitecturas de seguridad de sistemas críticos (BBCL 2011, BBCL 2012, BBCCL 2014)
- Análisis de seguridad basado en procesos automatizados (BBR 2011)

Áreas de trabajo

- Especificación y verificación formal de arquitecturas de seguridad de sistemas críticos (BBCL 2011, BBCL 2012, BBCCL 2014)
- Análisis de seguridad basado en procesos automatizados (BBR 2011)
- Análisis estático y dinámico de seguridad de aplicaciones web

Áreas de trabajo

- Especificación y verificación formal de arquitecturas de seguridad de sistemas críticos (BBCL 2011, BBCL 2012, BBCCL 2014)
- Análisis de seguridad basado en procesos automatizados (BBR 2011)
- Análisis estático y dinámico de seguridad de aplicaciones web
- Ambientes para el entrenamiento en Seguridad Informática (BCR 2007, BCEPR 2009)

Áreas de trabajo

- Especificación y verificación formal de arquitecturas de seguridad de sistemas críticos (BBCL 2011, BBCL 2012, BBCCL 2014)
- Análisis de seguridad basado en procesos automatizados (BBR 2011)
- Análisis estático y dinámico de seguridad de aplicaciones web
- Ambientes para el entrenamiento en Seguridad Informática (BCR 2007, BCEPR 2009)
- Gestión de Seguridad de la Información (BCF 2005, CP 2009)

XOval

Un framework para la recolección de evidencia digital

Aspectos metodológicos

- Promueve la modularización de las actividades desarrolladas por investigadores forenses
- Provee guías metodológicas para identificar y especificar en forma precisa primitivas forenses
- Facilita la especificación de procedimientos forenses en forma independiente de la tecnología usada para implementarlos (experimentación basada en el modelo de (LK 2004))

XOval

Un framework para la recolección de evidencia digital

Aspectos metodológicos

- Promueve la modularización de las actividades desarrolladas por investigadores forenses
- Provee guías metodológicas para identificar y especificar en forma precisa primitivas forenses
- Facilita la especificación de procedimientos forenses en forma independiente de la tecnología usada para implementarlos (experimentación basada en el modelo de (LK 2004))

Aspecto tecnológico

Incorpora XOvaldi una herramienta multiplataforma y extensible basada en OVAL (OVAL) que puede ser usada para interpretar y ejecutar las primitivas forenses

XOval

Un framework para la recolección de evidencia digital

Aspectos metodológicos

- Promueve la modularización de las actividades desarrolladas por investigadores forenses
- Provee guías metodológicas para identificar y especificar en forma precisa primitivas forenses
- Facilita la especificación de procedimientos forenses en forma independiente de la tecnología usada para implementarlos (experimentación basada en el modelo de (LK 2004))

Aspecto tecnológico

Incorpora XOvaldi una herramienta multiplataforma y extensible basada en OVAL (OVAL) que puede ser usada para interpretar y ejecutar las primitivas forenses

Presentado en IEEE Symposium on Privacy, Security and Trust 2011 (BBR 2011)

Automatización del análisis de ciber-amenazas

Herramienta

- Asiste a un analista de seguridad en la detección de compromisos informáticos, apoyándose en una base de conocimiento de indicadores de compromiso definidos en los lenguajes (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados
- Recolección de evidencia definida en los indicadores derivados.
- Realiza evaluación de compromiso verificando que la evidencia obtenida determina la existencia de un ataque.
- Proyecto de cooperación internacional STIC AMSUD *AKD* (Brasil (UFRGS), Chile (UTSM), Francia (INRIA Nancy), Uruguay (InCo, UdelaR)).

Automatización del análisis de ciber-amenazas

Herramienta

- Asiste a un analista de seguridad en la detección de compromisos informáticos, apoyándose en una base de conocimiento de indicadores de compromiso definidos en los lenguajes (STIX) y (CybOX) (MITRE - NIST)
- Derivación de indicadores a partir de hallazgos encontrados
- Recolección de evidencia definida en los indicadores derivados.
- Realiza evaluación de compromiso verificando que la evidencia obtenida determina la existencia de un ataque.
- Proyecto de cooperación internacional STIC AMSUD *AKD* (Brasil (UFRGS), Chile (UTSM), Francia (INRIA Nancy), Uruguay (InCo, UdelaR)).

Una aplicación

- Se estudió el malware ZBot utilizado por la botnet Zeus, especializada en robo de información de tarjetas de crédito y cuentas bancarias.
- Estudiando su comportamiento se logró que la herramienta detecte este popular bot.

Hacia un CSIRT nacional

- 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)

Sistema único de gestión de Identidades

Motivación y objetivos

- Contar con un sistema de identificación y autenticación unificado para los servicios de la plataforma nacional de gobierno electrónico
- Los ciudadanos puedan identificarse con las mismas credenciales ante los distintos proveedores de servicios de la plataforma y contar con SSO (Single Sign On)
- Establecer guías para el desarrollo de un sistema de gestión de identidades electrónicas (e-IdMS)

Sistema único de gestión de Identidades

Motivación y objetivos

- Contar con un sistema de identificación y autenticación unificado para los servicios de la plataforma nacional de gobierno electrónico
- Los ciudadanos puedan identificarse con las mismas credenciales ante los distintos proveedores de servicios de la plataforma y contar con SSO (Single Sign On)
- Establecer guías para el desarrollo de un sistema de gestión de identidades electrónicas (e-IdMS)

Resultados

- Relevamiento y análisis de requerimientos de la plataforma tecnológica de AGESIC
- Estado del Arte y experiencia de otros países y regiones
- Propuesta de solución para la implementación de un e-IdMS
- Reportado en (GSISUGI 2012)

Dispositivo de Identificación Electrónica

Tecnología de estudio

Dispositivo de identificación físico + un microchip de alta seguridad con capacidades de almacenamiento y cálculo criptográfico

Dispositivo de Identificación Electrónica

Tecnología de estudio

Dispositivo de identificación físico + un microchip de alta seguridad con capacidades de almacenamiento y cálculo criptográfico

Objetivos

- Identificación de funcionalidades y requerimientos
- Estado del arte y experiencias de uso en otros países

Dispositivo de Identificación Electrónica

Tecnología de estudio

Dispositivo de identificación físico + un microchip de alta seguridad con capacidades de almacenamiento y cálculo criptográfico

Objetivos

- Identificación de funcionalidades y requerimientos
- Estado del arte y experiencias de uso en otros países

Resultados

- Arquitectura funcional y de seguridad (Roles, arquitectura interna, ejemplo de aplicación)
- Ciclo de vida
- Prototipo de firma electrónica utilizando simuladores
- Reportado en (GSIDIE 2012)

Asesoramiento Técnico - Estratégico

- Participación en el grupo de trabajo de Seguridad de la Información auspiciado por AGESIC

Asesoramiento Técnico - Estratégico

- Participación en el grupo de trabajo de Seguridad de la Información auspiciado por AGESIC
  - Analizar y proponer un marco legal para regular el accionar de los diversos actores en los incidentes de seguridad informática mayores

Asesoramiento Técnico - Estratégico

- Participación en el grupo de trabajo de Seguridad de la Información auspiciado por AGESIC
  - 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 la Administración Pública Uruguaya

Asesoramiento Técnico - Estratégico

- Participación en el grupo de trabajo de Seguridad de la Información auspiciado por AGESIC
  - 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 la Administración Pública Uruguaya
- Representante de la UdelaR en el Consejo Asesor Honorario de Seguridad de la Información de la AGESIC

Referencias (GSI)

G. Barthe, G. Betarte, J.D. Campo, C. Luna.

Formally verifying isolation and availability in an idealized model of virtualization.
En Proceedings of FM2011: 17th International Symposium on Formal Methods, Lecture Notes in Computer Science, vol. 6664, pp 231-245, Ireland, June 2011.

G. Barthe, G. Betarte, J.D. Campo, C. Luna.

Cache-leakage resilience in an idealized model of virtualization.
En Proceedings of CSF12: 25th IEEE Computer Security Foundations Symposium, IEEE Computer Society Press, pp 231-245, Harvard University, Massachusetts, USA, June 2012.

G. Barthe, G. Betarte, J.D. Campo, J. Chimento, C. Luna.

Formally verified implementation of an idealized model of virtualization.
En Post-Proceedings of TYPES 2013: Workshop on Types for Proofs and Programs. To appear in LIPcs, 2014.

M. Barrère; G. Betarte; M. Rodríguez

Towards machine-assisted formal Procedures for the Collection of Digital Evidence.
En Proceedings of IEEE Symposium on Privacy, Security and Trust (PST 2011), Montreal, Canada, July 2011.

G. Betarte, M.E. Corti, M. Rodríguez

Concepción, Diseño e Implementación de un Laboratorio de Seguridad Informática
En Proceedings of the IV Congreso Iberoamericano de Seguridad Informática, Mar del Plata, Argentina, 2007.

Referencias (GSI)

A. Blanco, J.D. Campo, L. Escanellas, C. Pintado, M. Rodríguez

Generación de Ambientes para Entrenamiento en Seguridad Informática
En Proceedings of the V Congreso Iberoamericano de Seguridad Informática, Montevideo, Uruguay, 2009.

G. Betarte, M.E. Corti, R. de la Fuente

Hacia una Implementación Exitosa de un SGSI
En Proceedings of the III Congreso Iberoamericano de Seguridad Informática, Valparaíso, Chile, 2005.

M.E. Corti, G. Pallas

Metodologi?a de Implantación de un SGSI en grupos empresariales de relación jerárquica
En Proceedings of the V Congreso Iberoamericano de Seguridad Informática, Montevideo, Uruguay, 2009.

G. Betarte; A. Blanco; P. López; R. López

Sistema de Gestión de Identidades: Descripción de la Solución
Entregable de actividad de asesoramiento a AGESIC, GSI, febrero 2012.

M.E. Corti; E. Giménez

Dispositivo de Identificación Electrónica
Entregable de actividad de asesoramiento a AGESIC, GSI, setiembre 2012.

Referencias

R. Leigland; A. Krings

A Formalization of Digital Forensics.
International Journal of Digital Evidence, 3(2), 2004.

The Mitre Corporation.

Open Vulnerability and Assessment Language (OVAL).
`http://oval.mitre.org/` (Última visita: 27 de febrero de 2014).

The Mitre Corporation.

Cyber Observable eXpression (CybOX).
`http://cybox.mitre.org/` (Última visita: 27 de febrero de 2014).

The Mitre Corporation.

Structured Threat Information eXpression (STIX).
`http://stix.mitre.org/` (Última visita: 27 de febrero de 2014).