

Experiencias en la Especificación y el Análisis de Modelos de Seguridad para Dispositivos Móviles Interactivos

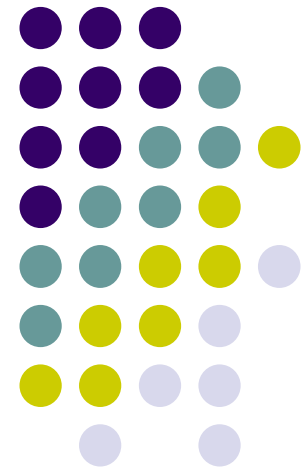
Carlos Luna

cluna@fing.edu.uy

Instituto de Computación, Facultad de Ingeniería,
Universidad de la República, Uruguay

Responsable del grupo de Investigación:
Gustavo Betarte (gustun@fing.edu.uy)

CIBSI 2009



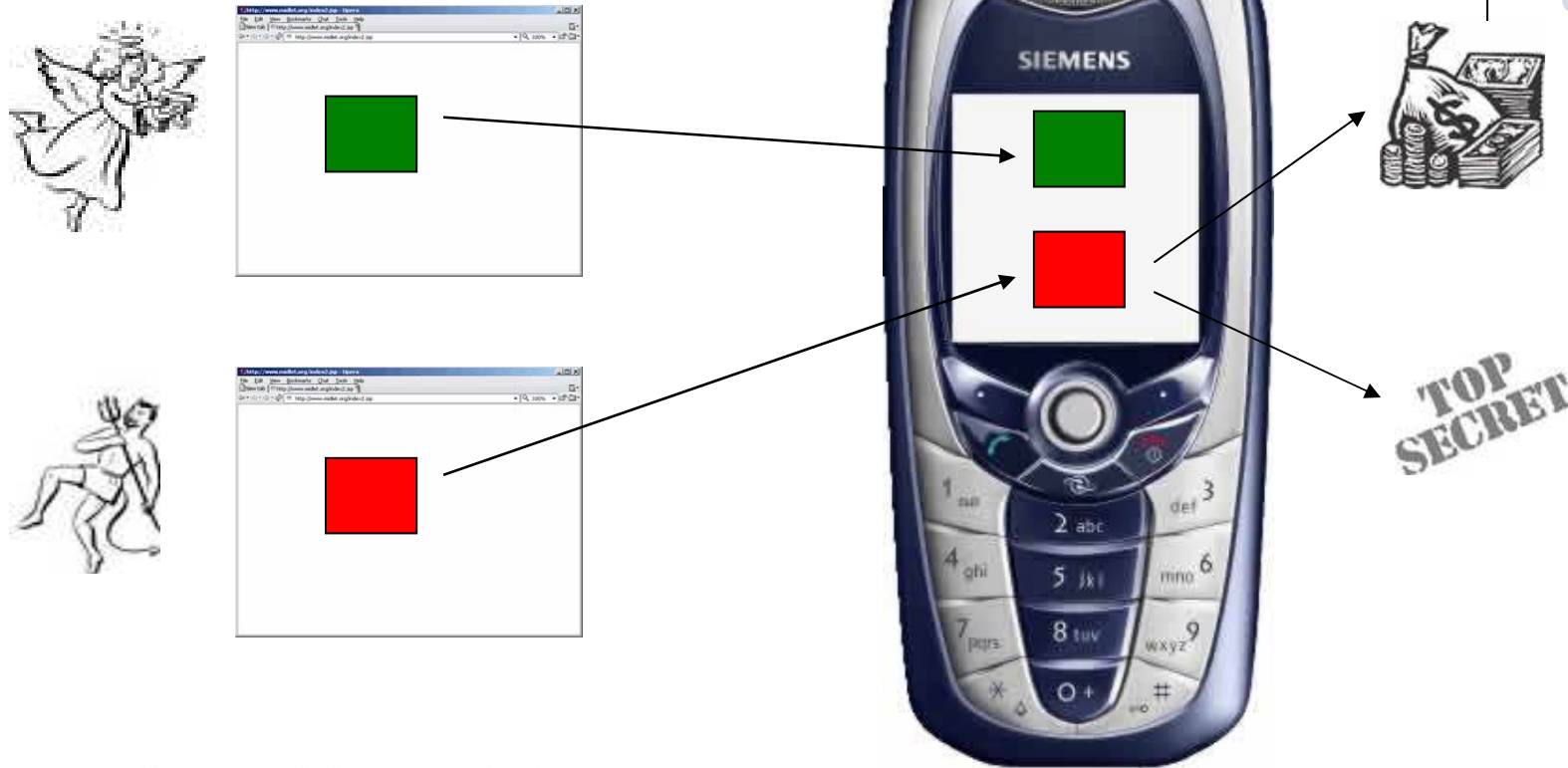
Dispositivos Móviles Interactivos



Estos dispositivos permiten:

- Almacenar información confidencial
- Establecer comunicaciones con entidades externas
- Descargar aplicaciones de fuentes desconocidas
- Incurrir en gastos

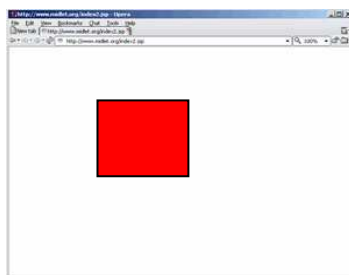
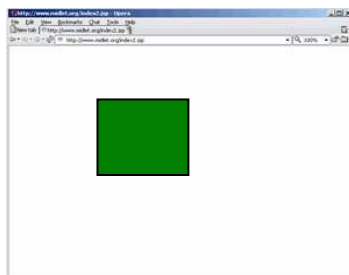
Un problema



Estos dispositivos deben asegurar:

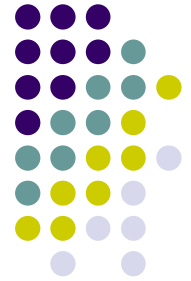
- La confidencialidad e integridad de los datos
- El control de los costos
- La disponibilidad del servicio

Una solución



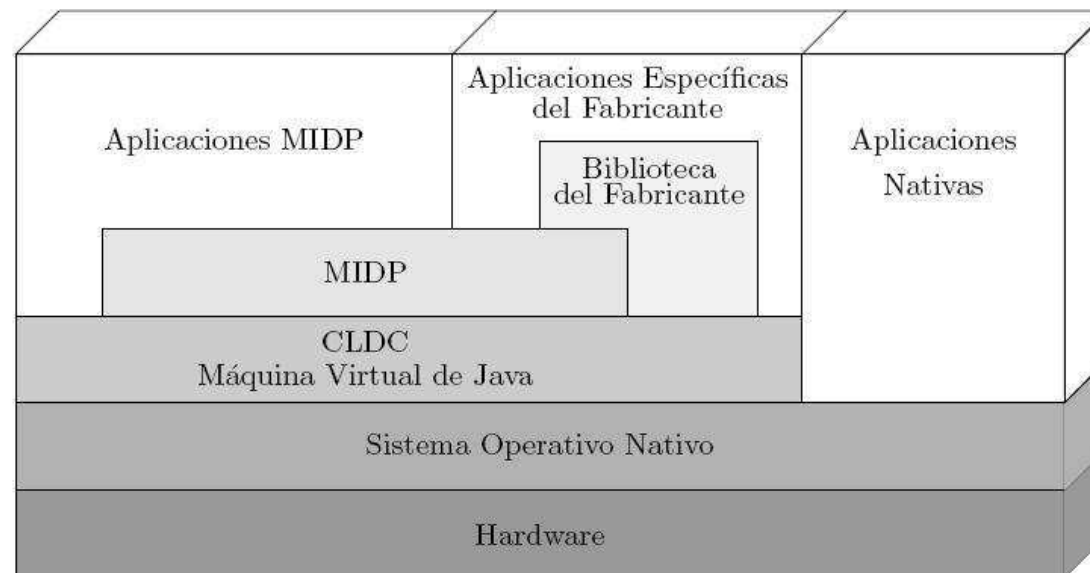
Política de Seguridad

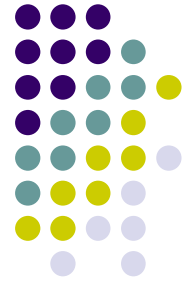




Arquitectura JME

- Máquina virtual: KVM
- Capa Configuración: CLDC/CDC
- Capa Perfil: **Mobile Information Device Profile (MIDP)**
- Paquetes opcionales
- Aplicaciones: MIDlet suites

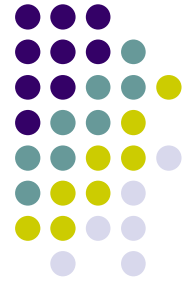




Generaciones MIDP

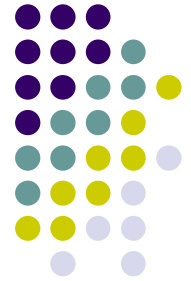
- Nivel de Plataforma
 - Permisos para acceder a funciones sensibles
 - MIDP 1.0: Cajón de Arena
 - MIDP 2.0: Dominio de Protección
 - Permisos: *allowed* y *user* (*one-shot*, *session*, *blanket*)
- Nivel de Aplicación
 - Autorizaciones para acceder a recursos compartidos
 - MIDP 3.0: Autorización de Acceso

Especificaciones Informales



Desventajas:

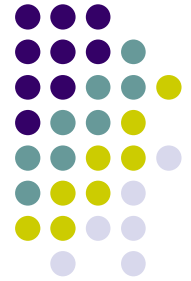
- Los modelos pueden estar subespecificados
- Pueden contener ambigüedades o contradicciones que sean difíciles de detectar
- Es muy complejo saber cuáles son las propiedades de seguridad que satisfacen



Formalizaciones

Desarrolladas en una teoría constructiva de tipos (CIC), utilizando el asistente de pruebas Coq.

- A Formal Specification of the MIDP 2.0 Security Model [Fast06]
- A Certified Access Controller for JME-MIDP 2.0 enabled Mobile Devices [ChWFM08, SCCC09]
- Formal Specification and Analysis of the MIDP 3.0 Security Model [ChWFM08, SCCC09]
- Autorización de Acceso en MIDP 3.0 [CIBSI09]



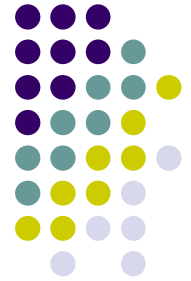
Desarrollo de un Framework

Basado en:

- Besson, Dufay, Jensen: [A Formal Model of Access Control for Mobile Interactive Devices](#) [ESORICS06]

Extiende los permisos presentes en MIDP:

- Introduce una noción de multiplicidad
- Flexibiliza la forma en la que el usuario puede conceder a las aplicaciones que son utilizadas en el dispositivo, accesos a los recursos del mismo



El Framework

A framework for the analysis of access control models
for interactive mobile devices [TYPES'08]

Está formalizado en CIC, utilizando Coq. Permite:

- la definición de políticas de control de acceso
- el análisis formal de cuándo una política de concesión de permisos es más restrictiva que otra
- analizar si un modelo de permisos es más general que otro
- la verificación de propiedades de seguridad



Trabajo Futuro

- El análisis formal de diferentes componentes de seguridad de MIDP 3.0
- La especificación, utilizando el framework definido, de algoritmos para forzar políticas de seguridad derivadas de distintos tipos de modelos de permisos
- La extensión del framework para permitir la construcción de prototipos certificados a partir de las definiciones formales de dichos algoritmos



Proyectos y Publicaciones

Proyectos:

- **STEVE: Seguridad a Través de Evidencia VERificable**. Proyecto PDT, DINACYT, Uruguay
- **ReSeCo: Reliability and Security of Distributed Software Components**. Proyecto STIC-AMSUD

Publicaciones:

- S. Zanella, G. Betarte, and C. Luna. “**A formal specification of the MIDP 2.0 security model**”. T. Dimitrakos et al. (Eds.): FAST 2006, LNCS 4691, pp. 220–234, 2007. Springer-Verlag 2007
- J. M. Crespo, G. Betarte, and C. Luna. “**A Framework for the Analysis of Access Control Models for Interactive Mobile Devices**”. S. Berardi, F. Damiani, and U. de'Liguoro (Eds.): Types for Proofs and Programs (TYPES) 2008, LNCS 5497, pp. 49–63, 2009. Springer-Verlag Berlin Heidelberg 2009
- G. Mazeikis y C. Luna. “**Autorización de Acceso en MIDP 3.0**”, CIBSI'09, Uruguay, 2009
- R. Roushani, G. Betarte, and C. Luna. “**A Certified Access Controller for JME-MIDP 2.0 enabled Mobile Devices**”, XXVIII International Conference of the Chilean Computer Science Society. Session: Formal Methods, to be published by IEEE CS Press in 2009
- G. Mazeikis, C. Luna, and G. Betarte. “**Formal Specification and Analysis of the MIDP 3.0 Security Model**”, XXVIII International Conference of the Chilean Computer Science Society. Session: Formal Methods, to be published by IEEE CS Press in 2009