Actividades prácticas para la asignatura de Seguridad de sistemas de información

Félix J. García Clemente
Departamento de Ingeniería y Tecnología de Computadores
Universidad de Murcia
Campus de Espinardo
30100 Murcia
fgarcia@um.es

Resumen

La gran mayoría de los nuevos planes de estudios están incorporando nuevas asignaturas dedicadas a la Seguridad de Sistemas Informáticos. Un aspecto clave de estas asignaturas es el trabajo práctico y determinar qué actividades pueden ser las más idóneas para mostrar a los alumnos los diferentes aspectos de la Seguridad. En este artículo presentamos dos actividades prácticas que combinan los conceptos relativos a la autenticación basada en tarjetas inteligentes y el control de acceso en sistemas operativos Windows y Linux.

1. Introducción y motivación

La materia de Seguridad se ha incorporado en la definición de los nuevos planes de estudios de Grado y Máster en Ingeniería en Informática, fundamentalmente a raíz de la adaptación de dichos planes para el cumplimiento del Acuerdo del Consejo de Universidades [2] por el cual se establecen las competencias que los alumnos deben adquirir para dichas titulaciones. Concretamente esta resolución recoge varias competencias que consideran la Seguridad, estas son:

- "Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, **seguridad** y calidad, conforme a principios éticos y a la legislación y normativa vigente" dentro del módulo Común a la rama de la informática en el título de Grado.
- "Capacidad para comprender, aplicar y gestionar la garantía y **seguridad** de los sistemas informáticos" dentro del módulo de Ingeniería de Computadores en el título de Grado
- "Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de **seguridad** y cumplimiento de la normativa y la legislación vigente" dentro del módulo de Sistemas de Información del título de Grado.
- "Capacidad para comprender, aplicar y gestionar la garantía y **seguridad** de los sistemas informáticos" dentro del módulo Tecnologías de la Información para el Grado en Ingeniaría en Informática.
- "Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de **seguridad** en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido" dentro del módulo de Tecnologías Informáticas para el Máster en Ingeniería en Informática.

Estas competencias han sido cubiertas en la gran mayoría de los títulos de grado y máster propuestos incluyendo una o más asignaturas relativas a la Seguridad de los Sistemas Informáticos.

Es cierto que los planes de estudio no han incluido tradicionalmente asignaturas de Seguridad, a pesar de que esto ha sido apuntado con anterioridad [10] y de que el Computer Curricula 2005 de ACM [1] reflejaba su relevancia incluyendo dos materias (*Security: issues and principles* y *Security: implementation and management*). En todo caso, podemos encontrar diferentes propuestas de diseño de estas asignaturas [12][11] que pueden servir de base para los nuevos planes de estudios.

En este trabajo se presenta un recurso para apoyar la docencia práctica de una asignatura de Seguridad. Concretamente el recurso se centra en la autenticación y el control de acceso en sistemas operativos. Además, el autor tiene probada experiencia con el recurso ya que lo ha puesto en uso en la asignatura optativa *Sistemas Integrados* [13] de quinto curso de Ingeniería en Informática en los últimos años.

El resto del trabajo se estructura como sigue. La sección 2 presenta y describe el recurso, la sección 3 explica su uso, la sección 4 describe nuestra experiencia con el recurso y, por último, la sección 5 presenta las conclusiones y los trabajos futuros.

2. Descripción del recurso propuesto

El recurso se subdivide en tres partes y cada una de ellas viene acompañada de un paquete software que incluye ejemplos y plantillas. Estas tres partes son el acceso a la tarjeta inteligente, la autenticación en Windows y la autenticación en Linux. A continuación dedicamos una sección a cada una de estas partes.

Los componentes software del recurso se encuentran disponibles para su descarga en [5].

2.1. Acceso a la tarjeta inteligente

Existen diferentes tecnologías para el acceso a una tarjeta inteligente, pero nuestro recurso se basa en la más utilizada y extendida, el estándar PC/SC (Personal Computer/Smart Card) [8]. PC/SC es un conjunto de especificaciones para la integración de tarjetas inteligentes en ordenadores personales. En particular se define un API de programación que permite a los desarrolladores de aplicaciones acceder de forma uniforme a las tarjetas a través de lectores (terminales) de distintos fabricantes que cumplan con la especificación.

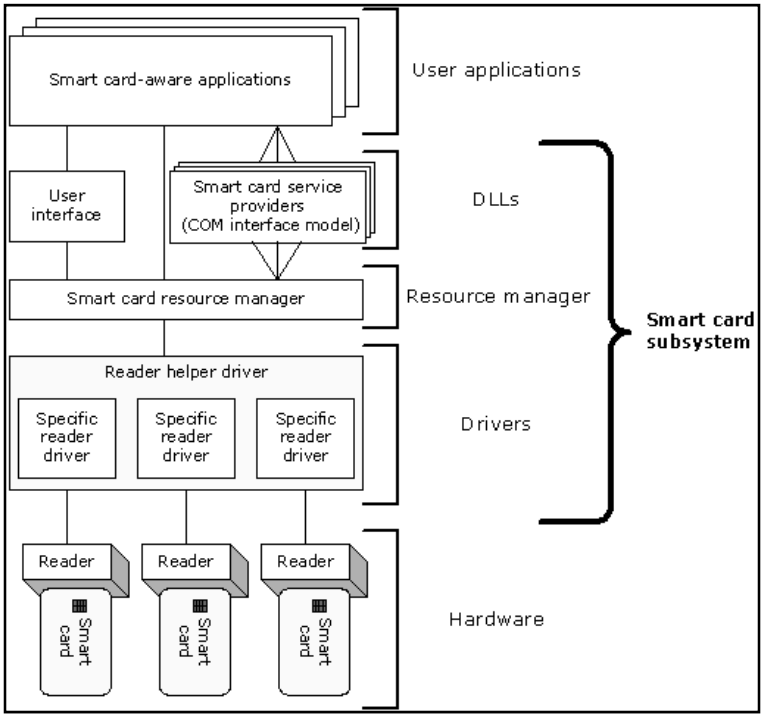

Figura 1. Arquitectura de tarjeta inteligente de Microsoft Windows

El API de PC/SC está incluida en los sistemas Microsoft Windows 200x/XP y también existe una implementación libre, de código abierto, llamada PC/SC Lite (proyecto MUSCLE) [9] para sistemas operativos GNU Linux. Esto permite a un desarrollador poder reutilizar sus aplicaciones basadas en PC/SC en ambos sistemas operativos.

Para mostrar la programación y uso del API se utilizan las tarjetas inteligentes que los propios alumnos tienen, estas son, su tarjeta universitaria y su DNI electrónico. Ambas tarjetas son tarjetas inteligentes con contactos con soporte ISO 7816 [14] y pueden ser utilizadas en las prácticas.

En la Figura 1 se muestra la arquitectura PC/SC de Microsoft Windows donde se distingue el hardware necesario (tarjeta inteligente y lector), el subsistema PC/SC del sistema operativo y la aplicación de usuario desarrollada. En nuestro recurso la aplicación accede a la tarjeta utilizando el Resource Manager del subsistema PC/SC.

Por último, el alumno debe conocer cómo y dónde está almacenada la información en el interior de la tarjeta para que a través de comandos ISO 7816 poder acceder a la información deseada del interior de la tarjeta (número de DNI, fecha de caducidad, certificado digital, etc.). Para esto al alumno se le proporciona la estructura interna de la tarjeta inteligente que en el caso de la tarjeta universitaria tiene una estructura propietaria pero que en el caso del DNI electrónico sigue el estándar PKCS#15 [4].

Para facilitar el trabajo docente y el aprendizaje al alumno, esta parte del recurso se complementa con un conjunto de ejemplos de código en lenguaje C que muestran el acceso/lectura a la tarjeta inteligente universitaria y al DNI electrónico. Estos ejemplos fundamentalmente consisten en:

- Verificar el número PIN
- Leer el número de DNI
- Leer la fecha de caducidad de la tarjeta
- Extraer el certificado digital de la tarjeta

También se introducen ejemplos más avanzados relativos a funciones criptográficas relativos a la firma digital y su verificación

2.2. Autenticación en Windows 200x/XP mediante tarjeta inteligente

El elemento clave en el proceso de autenticación en los sistemas operativos Windows 200x/XP es el módulo GINA [3].

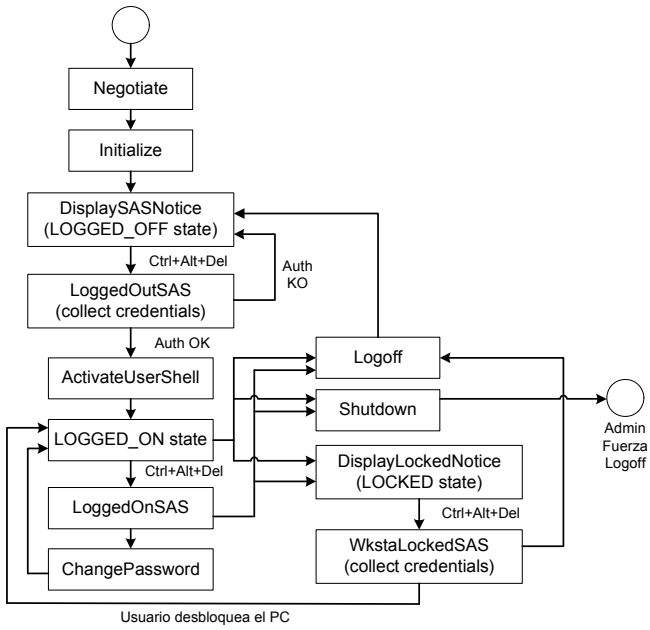

Figura 2. Diagrama de estados GINA

GINA es una parte intercambiable de WinLogon que un desarrollador o administrador del sistema puede reemplazar para incorporar la funcionalidad de inicio de la sesión de Windows (logon) que se desee. Por tanto, reemplazando el GINA se puede sustituir el mecanismo de autenticación de los usuarios y controlar el acceso al sistema operativo. En este sentido, esta parte del recurso propone al alumno diseñar y desarrollar un módulo GINA basado en tarjetas inteligentes para controlar el acceso al sistema.

Winlogon controla el inicio, bloqueo y cierre de una sesión Windows. Esto lo hace definiendo tres estados: logged-off (no hay sesión), logged-on (sesión activa) y locked-workstation (sesión bloqueada). Partiendo de estos estados, la Figura 2 muestra un diagrama en el que se muestran las funciones que Winlogon invoca del módulo GINA, y el orden en que se ejecutan.

La función más importante de cara a la autenticación es LoggedOutSAS. Esta es la función que se ejecuta cuando se está mostrando la ventana de espera de un evento SAS (secure attention sequence), no habiendo por tanto, iniciado una sesión ningún usuario. En esta función se obtienen los credenciales con los que se selecciona a un usuario registrado en el sistema para iniciar la sesión. Aquí es por tanto donde se indica que se va a iniciar la sesión de Windows con uno de los usuarios creados.

El desarrollo de un módulo GINA desde cero es un trabajo muy costoso. Por tanto, se le propone al alumno que realice un módulo GINA que invoque al módulo GINA por defecto en aquellas funciones que no son relevantes.

La autenticación mediante la tarjeta inteligente puede hacerse de diferentes maneras. Al alumno se le indican tres:

- Mediante un identificador de la tarjeta (ATR, SCard ID u otro interno).
- Mediante el contenido de un fichero interno de aplicación (número de dni, identificador de aplicación u otro).
- Mediante el certificado digital que alberga la tarjeta inteligente.

Independientemente de la manera que se utilice el usuario deberá verificar su PIN. Esto obligará al alumno a desarrollar una ventana para que el usuario pueda introducir el número de PIN por teclado y así poder verificarlo.

En relación a esta parte del recurso docente, al alumno se le proporciona un módulo GINA que implementa todas las funciones relevantes reenviado la llamada al módulo GINA que incorpora por defecto el sistema. Además se le proporciona la documentación oportuna para la instalación y configuración del módulo GINA en el sistema operativo.

2.3. Autenticación en Linux mediante tarjeta inteligente

La autenticación en los sistemas operativos Linux es proporcionada por los módulos PAM (Pluggable Authentication Modules) [7]. El *framework* que se define para PAM consiste en cuatro partes: clientes, librería PAM, fichero de configuración *pam.conf* y los módulos de servicios PAM (o proveedores).

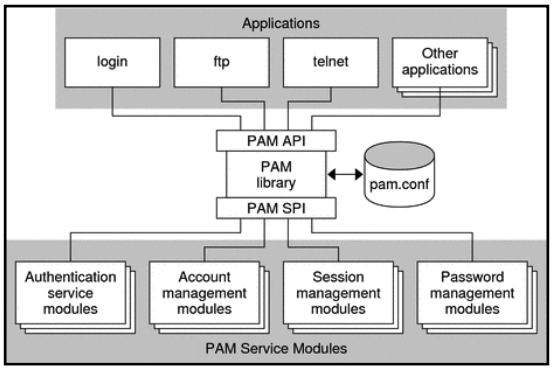

Figura 3. Arquitectura PAM

El *framework* proporciona un camino uniforme para realizar los procesos de autenticación en el sistema. Asimismo permite a los desarrolladores de aplicaciones que usen los servicios PAM sin tener que conocer la semántica de las políticas de autenticación del sistema. Y por otro lado los algoritmos y métodos de autenticación pueden ser modificados independientemente de las propias aplicaciones. En definitiva, con PAM, los administradores pueden confeccionar el proceso de autenticación del sistema sin tener que cambiar las aplicaciones. Los cambios son hechos a través del fichero de configuración *pam.conf*.

La Figura 3 muestra la arquitectura PAM. Las aplicaciones se comunican con la librería PAM a través de la API PAM. Los módulos PAM se comunican con la librería PAM a través de la SPI PAM. Por tanto, la librería PAM permite a las aplicaciones y los módulos comunicarse entre ellos.

El desarrollo de un módulo PAM para incorporar la autenticación mediante la tarjeta inteligente no es un trabajo muy costoso y aún menos si lo comparamos con el trabajo que puede llevar desarrollar su equivalente en Windows, el módulo GINA.

La autenticación mediante la tarjeta inteligente puede hacerse de las mismas tres maneras que se indican para el módulo GINA, estas son mediante un identificador de la tarjeta, el contenido de un fichero interno de aplicación o el certificado digital que alberga la tarjeta inteligente. Igualmente, independientemente de la manera que se utilice el usuario deberá verificar su PIN.

En relación a esta parte del recurso docente, al alumno se le proporciona un módulo PAM sin funcionalidad. Además se le proporciona la documentación oportuna para la instalación y configuración del módulo PAM en el sistema operativo.

3. Uso del recurso propuesto

De cara a la puesta en práctica de esta propuesta nos encontramos que el alumno debe trabajar con los módulos clave del arranque del sistema operativo y esto puede llevar a que si se realiza una mala configuración o implementación del módulo, el sistema quede en un estado no recuperable y obligue al alumno a reinstalar el sistema o a utilizar alguna técnica de recuperación del sistema. Para evitar estos problemas, se propone a los alumnos el uso de la virtualización [15].

Por otro lado, los alumnos deben disponer de un PC con un lector interno de tarjetas inteligentes instalado, o al menos, de un lector externo que ellos mismos puedan instalar y configurar en su PC de trabajo. Se debe elegir un lector con driver PC/SC en Windows y Linux. Este detalle es importante porque no todos disponen de un driver PC/SC para Linux.

Para facilitar el aprendizaje del alumno, a continuación se detalla una propuesta de sesiones prácticas:

- *Sesión 1. Configuración básica*. Esta sesión práctica tiene dos objetivos: instalación y configuración de un driver PC/SC en Windows y Linux; y, la instalación y configuración del sistema de virtualización.
- *Sesión 2. Acceso a la tarjeta.* Esta sesión tiene como objetivo desarrollar un programa que acceda a la tarjeta inteligente universitaria y al DNI electrónico.
- *Sesión 3. Instalar un módulo GINA.* El objetivo es que instalen un módulo GINA sin funcionalidad en Windows.
- *Sesión 4. Módulo GINA basado en tarjeta inteligente.* El objetivo es desarrollar un módulo GINA que base su autenticación en un identificador de la tarjeta (por ejemplo, el ATR).
- *Sesión 5. Módulo GINA avanzado basado en tarjeta inteligente.* El objetivo es realizar un módulo GINA que solicite la verificación del PIN y, si es posible, realice una autenticación más compleja basada en contenido de un fichero interno o en el certificado digital.
- *Sesión 6. Instalar un módulo PAM.* El objetivo es que instalen un módulo PAM sin funcionalidad en Linux.
- *Sesión 7. Módulo PAM basado en tarjeta inteligente.* El objetivo es desarrollar un módulo PAM que base su autenticación en el contenido de un fichero de aplicación (por ejemplo, el número de DNI).
- *Sesión 8. Módulo PAM avanzado basado en tarjeta inteligente.* El objetivo es realizar un módulo PAM que solicite la verificación del PIN y, si es posible, realice una autenticación más compleja basada en el certificado digital.

La duración estimada para cada sesión es de una hora. Por tanto, con un total de 8 horas podría desarrollarse la propuesta.

Esta propuesta también asume un trabajo autónomo del alumno por el cual trabaja la documentación técnica que se le proporciona. Esta documentación [5] que se incluye junto con los programas de ejemplo, el módulo GINA y el módulo PAM, contiene los siguientes documentos:

- Arquitectura PC/SC para Windows y Linux.
- Comandos y respuestas APDU para la tarjeta universitaria y el DNI electrónico.
- Estructura interna de la tarjeta universitaria y el DNI electrónico.
- Módulo GINA. Desarrollo, instalación y configuración.
- Módulo PAM. Desarrollo, instalación y configuración.

La duración estimada de este trabajo autónomo se cuantifica en que cada alumno deberá dedicar una hora y treinta minutos previos a cada sesión a leer y comprender la documentación relativa a la sesión correspondiente.

4. Experiencia docente con el recurso

El recurso que este trabajo propone ha sido utilizado en la asignatura optativa *Sistemas Integrados* [13] de quinto curso de Ingeniería en Informática en los últimos seis años. Esta asignatura ha tenido un número aproximado de 20 alumnos cada año. Por tanto, han sido más de 100 alumnos los que han tenido la oportunidad de trabajar estas prácticas.

Nuestra experiencia nos permite asegurar que los alumnos que han participado en las prácticas han conseguido comprender la importancia de la autenticación en la seguridad de los sistemas informáticos, el valor añadido que introduce el uso de tarjetas inteligentes y la capacidad de diseñar aplicaciones que combinen autenticación y tarjeta inteligente.

5. Conclusiones y trabajo futuro

El recurso docente que aquí se presenta tiene suficientes características para poder ser integrado como parte de las sesiones prácticas de una asignatura dedicada a la Seguridad. El alumno a través de actividades prácticas que combinan los conceptos relativos a la autenticación basada en tarjetas inteligentes y el control de acceso en sistemas operativos Windows y Linux, adquiere suficientes conocimientos para ser capaz de diseñar y desarrollar aplicaciones que combinen autenticación y tarjetas inteligentes.

Como trabajo futuro se está trabajando para incluir la autenticación en Windows Vista, donde no aparece GINA y se utiliza una nueva arquitectura con proveedor de credenciales [6].

Referencias

[1] ACM/IEEE Joint Task Force for Computing Curricula (2005). Computing Curricula 2005: The Overview Report. Disponible en web http://www.acm.org/education/curricula.html #CC2005

[2] Acuerdo del Consejo de Universidades, por el que se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Informática, Ingeniería Técnica Informática e Ingeniería Química. Disponible en web: http://www.boe.es/boe/dias/2009/08/04/pdfs/ BOE-A-2009-12977.pdf

[3] Brown, K. *Customizing GINA*. MSDN Magazine, 2005. Disponible en web http://msdn.microsoft.com/en-us/magazine/cc163803.aspx

[4] Estándar PKCS#15. Disponible en web: http://www.rsa.com/rsalabs/node.asp?id=214 2

[5] García, F.J. Recursos prácticos para la. Disponible en web http://www.ditec.um.es/~fgarcia/si/

[6] Griffin, D. *Create Custom Login Experiences With Credential Providers For Windows Vista*. MSDN Magazine, 2007. Disponible en web http://msdn.microsoft.com/es-es/magazine/cc163489.aspx

[7] PAM (Pluggable Authentication Modules). Disponible en web: http://www.linuxdocs.org/HOWTOs/User-Authentication-HOWTO/x101.html

[8] PC/SC Workgroup. Disponible en web: http://www.pcscworkgroup.com/

[9] Proyecto MUSCLE. Disponible en web: http://www.linuxnet.com/middle.html

[10] Ramió Aguirre, J. *Introducción de las enseñanzas de seguridad informática en los planes de estudios de las ingenierías del siglo XXI*. VII Jornadas de Enseñanza Universitaria de la Informática (JENUI), 2001.

[11] Ribadas, F.J., Barcala, F.M., Darriba, V., Otero, J. *Diseño de un entorno virtualizado para la docencia práctica de Seguridad en Sistemas de Información*. XIV Jornadas de Enseñanza Universitaria de la Informática (JENUI), 2009.

[12] Riesco, M., Díaz, M.A., Redondo, J.M., García, N. *Propuesta de diseño de la asignatura de Seguridad de Sistemas Informáticos*. XV Jornadas de Enseñanza Universitaria de la Informática (JENUI), 2009.

[13] Sistemas Integrados. Programa de la asignatura accesible a través de la web http://www.um.es/informatica/index.php?pagina=planificacion&seccion_plan=programas

[14] The ISO 7816 Smart Card Standard: Overview. Disponible en web: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

[15] Virtual Box. Disponible en web: http://www.virtualbox.org/