Universidad Carlos III de Madrid

OO/UC3M/22 - EVALUACIÓN E INTEROPERATIVIDAD DE PROTOCOLOS Y ARQUITECTURAS DE SEGURIDAD

Durante los últimos años, el uso de protocolos de seguridad ha crecido significativamente, la protección de las comunicaciones ha sido llevada a cabo mediante el empleo de protocolos y arquitecturas de seguridad que están poniendo de manifiesto diversos problemas que no habían aparecido hasta ahora. Los problemas de interoperatividad están dificultando la expansión potencial de las tecnologías TIC. Nuestro grupo ha desarrollado trabajos que permiten evitar los problemas de interoperatividad en protocolos y arquitecturas de seguridad mediante la definición y aplicación de una metodología para la evaluación de la conformidad de la implementación de protocolos y arquitecturas de seguridad, así como el análisis específico del rendimiento centrado en los parámetros más relevantes de los protocolos de seguridad.

Descripción de la Tecnología

Recientemente, las investigaciones realizadas sobre tarjetas inteligentes aspiran a considerar estos dispositivos como un nodo dentro de una red (Network Smart Card). Para ello, debe incorporar distintos mecanismos de autenticación y protocolos de red con el objetivo de participar de forma transparente en un contesto de red heterogéneo. Sin embargo, el diseño de los protocolos de autenticación para tarjetas inteligentes han estado tradicionalmente orientados a funcionalidades de tipo “dispositivo criptográfico seguro” frente a un potencial diseño más orientado hacia la conectividad en red. Más allá, la tarjeta inteligente es fuertemente dependiente del Terminal de acceso, siendo esta dependencia no deseable, especialmente cuando se trata de terminales desconocidos o de confianza cuestionable. Nuestro trabajo está centrado en obtener el mayor grado de integración e interoperabiliad posible de la tarjeta inteligente en la red, con el fin de desarrollar seguros y robustos sistemas para la identificación de usuarios que porten este tipo de dispositivos específicamente diseñados con este propósito. Para ello, se propone una arquitectura completa de autenticación -eficiente y efectiva- basada en este tipo de tarjetas de identificación electrónica. Este enfoque es especialmente interesante si consideramos escenarios que pueden ser críticos por las operaciones que los caracterizan: identificación de ciudadanos, control de fronteras, centrales nucleares, hospitales, transporte de mercancías peligrosas, etc.

Como fundamento tecnológico, nuestro trabajo define una arquitectura de protocolos de autenticación con las siguientes características.

- Solicitante de autenticación “compacto” (stand-alone supplicant): se propone un modelo para tarjeta inteligente en el que ésta participa autónomamente en un esquema de autenticación, en una versión stand-alone supplicant versus split-supplicant (solicitante de autenticación dividido). En entornos críticos, el Terminal de acceso debe ser considerado como no confiable y por tanto son definidas medidas de seguridad adicionales en nuestro proyecto.

- Diseño atómico del protocolo en la tarjeta inteligente: el protocolo de autenticación debe diseñarse íntegramente dentro de la tarjeta. Nuestro trabajo propone una pila de protocolos específica en la tarjeta con objetivos de identificación del portador.

- Autenticación mutua extremo-a-extremo: donde la tarjeta inteligente participa como extremo de la comunicación. En el otro extremo en la red, un servicio centralizado de autenticación controla y autoriza el acceso (lógico o físico) al sistema. Este túnel de autenticación evita posibles ataques realizados desde un Terminal de acceso potencialmente manipulado.

- Autenticación en capa 2. Nuestro enfoque trata de explotar las ventajes en términos de seguridad y computacional que presenta un esquema de autenticación basado en capa 2 para la integración de la tarjeta inteligente en el sistema en red.

Este proyecto, por tanto, trata de desarrollar un sistema de autenticación de la identidad de usuarios basado en “tarjetas inteligentes en red” con las anteriores características. Este sistema está diseñado para la identificación de ciudadanos o empleados, especialmente en entornos de seguridad crítica.

Universidad Carlos III de Madrid

Aspectos innovadores
Se puede considerar que la tecnología de tarjetas inteligentes en red se encuentra en una fase de estudio/prototipado. En la actualidad, existen pocos -aunque muy interesantes- trabajos en esta línea y con diferentes estrategias en función de los servicios finales a dotar. Nuestro proyecto está orientado concretamente hacia la explotación de las capacidades en capa 2 (OSI) de la tarjeta inteligente en red, con propósitos específicos para la autenticación de credenciales de identidad electrónica. Este enfoque facilita la compatibilidad con las tarjetas inteligentes convencionales, así como, la integración en sistemas de acceso a redes heterogéneo (cableado o inalámbrico), al tiempo que proporciona interoperabilidad con protocolos de red estandarizados. Esta forma de abordar la identificación electrónica resulta innovadora respecto a la tecnología existente de tarjetas inteligentes o propuestas relacionadas (a menudo orientadas a soportar impracticables pilas de protocolos de red, entre los que se incluyen protocolos de seguridad: SSL, IPSec, etc.). Por tanto, nuestro proyecto aspira a desarrollar un sistema de identificación específico, basado en estas innovadoras tarjetas ID en red (ID-NSCards).

Ventajas competitivas
Las ventajas competitivas que supondría la incorporación de esta tecnología en una empresa o institución estarían centradas en la seguridad del sistema, pero también el ahorro de tiempo y coste de mantenimiento y actualización de software de seguridad. La centralización de ciertos servicios de identificación y autenticación de personas en determinadas empresas o instituciones donde se desarrollan actividades críticas, se verían mejoradas mediante la incorporación de esta tecnología. El hecho de disponer de un sistema de autenticación basado en *network id-cards* permitiría una autenticación robusta mutua *on-line*, así como la interoperación entre la tarjeta y el servidor de autenticación central. En esta interoperación podrían incluirse operaciones de mantenimiento y actualización del software relativo a ambos extremos sin que el Terminal/Host tuviera que ser modificado. Esto se traduce en ahorro de tiempo y costes que permite un despliegue dinámico, efectivo y seguro, lo que en los entornos críticos es muy requerido.

Estado de la propiedad industrial: ☒ Patente solicitada

Palabras clave
Tarjetas inteligentes y sistemas de acceso; Protección de datos, tecnología de almacenamiento, criptografía, seguridad de datos; Comercio electrónico, pago electrónico; Firma electrónica; Tele-gobierno (e-Government)

Persona de contacto: María Dolores García-Plaza
Teléfono: + 34 91 624 9016 / 9030
E-mail: comercializacion@pcf.uc3m.es