SEGURIDAD EN SISTEMAS EMBEBIDOS

G. Escudero, A. Bertello, O. Jalón
INTI Electrónica e Informática
ohj@inti.gob.ar

Introducción

En este trabajo se presenta la experiencia de la Unidad Técnica Informática (UTI) del Centro INTI-Electrónica e Informática en el campo de los sistemas embebidos de aplicación en el ámbito regulado, tanto desde su rol de asesor tecnológico de los organismos de regulación en el desarrollo de las normativas técnicas, como desde su rol de laboratorio de verificación y validación de equipos electrónicos, *hardware y software*, para la aprobación de modelo. En particular, se proponen mecanismos necesarios para brindar a los sistemas embebidos un mayor nivel de seguridad, y facilitar las tareas de verificación sobre los mismos por parte de los organismos de control.
Generalmente, el tipo de sistemas embebidos a los que se hace referencia, tienen principalmente funciones de registración, almacenamiento, manipulación y generación de reportes de operaciones, siendo necesario verificar que cada una de las funciones de interés se ajuste a las correspondientes regulaciones.

Objetivo

El objetivo del presente trabajo fue desarrollar distintas plataformas que permitiesen evaluar ventajas, facilidad de implementación y factibilidad de aplicación de estrategias y mecanismos de seguridad para afrontar las diversas demandas que recibe la UTI. A partir de la evaluación de estos modelos, se desarrollarán especificaciones técnicas referentes a seguridad de *software*, información y parámetros críticos para este tipo de sistemas embebidos.
Dichas especificaciones técnicas alcanzan a la definición de la arquitectura y a la descripción de los mecanismos necesarios para:

- Preservar la integridad de la información almacenada y transmitida.
- Asegurar la integridad del *software*.
- Facilitar la verificación de la integridad del *software* por parte del organismo de control.

Descripción

Como base de la estrategia adoptada para implementar la seguridad en los sistemas embebidos se utilizó criptografía de clave asimétrica o esquema de Clave Pública. (Figura 1.).
Se evaluaron soluciones criptográficas basadas en *software* (librerías SSL) y soluciones basadas en *hardware* dedicado (chips criptográficos) con certificación NIST-FIPS 140-2 o superior. Finalmente se optó por la solución por *hardware* dado que el mercado actualmente ofrece chips criptográficos, a un costo razonable, que presentan las siguientes ventajas:

- Generan internamente el par de claves.
- Configurados adecuadamente no permiten la exportación de la clave privada.
- Las operaciones criptográficas se realizan dentro del chip, evitando la circulación de la clave privada en el bus de comunicaciones del sistema.
- Posibilitan la comunicación con el procesador central del sistema a través de un canal seguro.
- Implementan fuertes medidas de protección contra ataques de *software* y/o *hardware*, las cuales incluyen desde el borrado de las claves hasta la inutilización definitiva del chip.

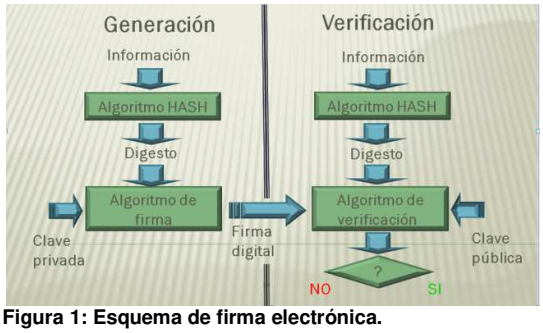

Figura 1: Esquema de firma electrónica.

Como mecanismo para asegurar el almacenamiento, se adoptó agrupar la información en bloques de datos con un campo verificador. Este campo verificador puede consistir en una suma de comprobación, el resultado de una función hash o la firma electrónica del bloque. De esta forma, al modificarse algún dato del bloque, el campo verificador deja de ser válido lo cual es fácilmente detectado por un auditor externo o por el mismo dispositivo cuando realiza su auto diagnóstico.

Para el proceso de exportación y transmisión de los datos a puntos remotos, también se adoptó el mecanismo de firma electrónica con clave asimétrica, garantizando así que la entidad receptora pueda verificar la integridad de la información como también su origen (no repudiabilidad). En este caso, las capacidades de los chips criptográficos utilizados, permiten implementar una infraestructura PKI (*Private Key Infrastructure*).
Con respecto a asegurar la integridad del *software* principal del equipo, se implementó un esquema de firma electrónica utilizando un par de claves propias de la UTI (Figura 2.). Una vez que el equipo ha cumplimentado los requisitos funcionales de *software* y *hardware*, el *software* es firmado con la clave privada perteneciente a la UTI, y el fabricante debe embeber en el producto a comercializar, el *software* así aprobado junto con la firma en una memoria que no permita sobreescritura (OTP).

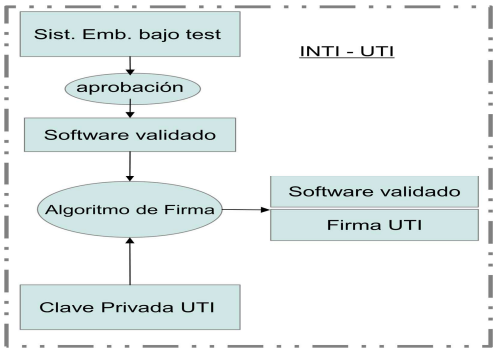

Figura 2: Firmado del *software* validado.

Para el caso en que la memoria que almacena el *software* principal sea de tipo *FLASH* (se puede borrar y volver a escribir muchas veces) se implementó un mecanismo de carga segura (*secure boot*) e indicadores de confianza (*roots of trust*). Para ello se requiere que el sistema embebido posea una pequeña porción de *software* residente en memoria OTP junto a la clave pública de la UTI y la firma correspondiente al *software* principal.
Este *software* residente es el encargado de leer el módulo de *software* principal de la memoria tipo *FLASH* y realizar la verificación de la firma del mismo. Si el resultado es positivo, lo carga en la memoria ejecutable permitiendo el normal funcionamiento del sistema embebido, caso contrario lo bloquea.

Resultados

Los conocimientos desarrollados se aplicaron en la Nueva Generación de Controladores Fiscales reglamentada por la Administración Federal de Ingresos Públicos (AFIP). Esta Administración oportunamente requirió gestionar electrónicamente la información generada por los Controladores Fiscales (CF) y reemplazar la guarda de documentos impresos por documentos electrónicos con el respaldo tecnológico de la estructura de Firma Digital.
En este caso, dada la infraestructura informática de la AFIP, este organismo además de ser el destino de la información generada por los CF, es la Autoridad Certificante que valida la clave pública de cada CF antes de salir de fábrica. El certificado generado por la AFIP debe ser embebido por el fabricante en el CF para habilitar su funcionamiento.

En este proyecto:

- Se desarrollaron herramientas de firmado electrónico por *software* y por *hardware*, para uso en los ensayos de aprobación de modelo que realiza la Unidad Técnica Informática.
- Se estableció la especificación técnica de la nueva generación de Controladores Fiscales, incluida como parte de la Resolución General AFIP Nº 3561/2013
- Se transfirió a las empresas fabricantes de controladores fiscales la experiencia adquirida en el manejo de los esquemas de firmado de clave asimétrica y el uso adecuado de los chips criptográficos para cumplir con la normativa de AFIP.

Conclusiones

Se transfirió exitosamente la tecnología a empresas fabricantes de CF, se hicieron los ensayos de aprobación de modelo de diez modelos de CF y ya se encuentran en funcionamiento en el mercado varios cientos.
Se está trabajando con otros organismos para incorporar esta tecnología en nuevos reglamentos técnicos (Controlador de Faena, controlador de molienda de granos, etc.).
La experiencia generada nos permite el abordarje de temas tales como Smart Grids, IoT e Industria 4.0.

Bibliografía

- National Institute of Standards and Technology, FIPS PUB 140-2,“ Security Requirements for Cryptographic Modules”.
- National Institute of Standards and Technology, FIPS PUB 186-3,“Digital Signature Standard”.
- Ley 25506, Ley de Firma Digital de la República Argentina, 2001.
- Resolución General AFIP Nº 3561/2013.