tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

083

PROYECTOS TECNOLÓGICOS DE SEGURIDAD EN EL MINISTERIO DE DEFENSA

Miguel Ángel Rego Fernández
Comandante de la Armada
Área de Seguridad
Inspección General CIS
Secretaría de Estado de Defensa
Ministerio de Defensa

Miguel Ángel Rego Fernández

Palabras clave

Seguridad de la Información, Seguridad
PKI (Public Key Infrastructure)
Infraestructura de Clave Pública
Certificados Digitales
Certificación
Identidad digital
Cifrado
Firma electrónica
Tarjeta electrónica
Tarjeta chip
Autoridad de Certificación, CA
Autenticación
Identificación
Control de acceso
Confidencialidad
SIM (Security Information Management)
Gestión y correlación de eventos de Seguridad
Intrusos, detección de intrusos
IPS (Intrusion Protection System)
IPSec (Internet Protocol Security)
Protocolo de Seguridad IP
Protección
CISCO
I+D
Token criptográfico
SSF (Secuware Security Framework)

Resumen de su Comunicación

La comunicación trata sobre los proyectos tecnológicos que se están llevando a cabo en el Ministerio de Defensa en el ámbito de la Seguridad de la Información.

En ella se describirán los proyectos y los beneficios que con ellos se pretenden obtener.

Miguel Ángel Rego Fernández

PROYECTOS TECNOLÓGICOS DE SEGURIDAD EN EL MINISTERIO DE DEFENSA

1. Pilares de la Seguridad de la Información

La Seguridad de la Información se basa en tres pilares: Políticas, Organización y Medidas Técnicas. El Ministerio de Defensa apuesta por el fortalecimiento de éstas últimas definiendo y acometiendo una serie de proyecto de carácter tecnológico.

2. Proyectos tecnológicos del Área de Seguridad

Los proyectos tecnológicos que el Ministerio de Defensa está llevando a cabo en materia de Seguridad de la Información son los siguientes:

2.1. Proyecto de Identidad Digital

En este "macro-proyecto" se enmarcan los siguientes subproyectos:

- Implantación de una Infraestructura de Clave Pública (PKI), como herramienta fundamental para la implementación de servicios de seguridad en los sistemas de información y en las aplicaciones (autenticación, firma digital, cifrado, no repudio y sellado de tiempo).
- Implantación de la Tarjeta Electrónica de Defensa (TEDEF), como elemento seguro de identificación ante sistemas electrónicos y soporte de certificados y claves emitidos por la PKI (control de acceso físico, control de acceso lógico, soporte seguro de información, etc.).
- Proyecto de Real Decreto de Firma Electrónica que desarrolla el artículo 4.4 de la Ley 59/2003 de Firma Electrónica.

Mediante la gestión de claves y certificados a través de una PKI en una organización se facilita la posibilidad de utilización de los servicios de firma electrónica y cifrado en una amplia variedad de aplicaciones, estableciendo y manteniendo un entorno de red seguro.

La implantación de una PKI proporciona a una organización, entre otras, las siguientes funcionalidades:

- Autenticación y cifrado de redes de comunicación.
- Acceso Remoto Seguro.
- Identificación de usuarios.
- Firma electrónica de documentos.
- Cifrado de documentos.
- No repudio de mensajes.

El modelo de PKI desarrollado por el Ministerio de Defensa permite alcanzar altos niveles de servicio y seguridad, por la autonomía que proporciona la gestión interna que se hace de los certificados digitales y la utilización de productos certificados por el CCN [1] Este modelo es exportable al resto de organismos de la Administración General del Estado, que habitualmente ha trabajado con arquitecturas de PKI gestionadas externamente.

1 CCN: Centro Criptológico Nacional.

Por otra parte, la Tarjeta Electrónica de Defensa (TEDEF), certificada por el CNI [2] con altas prestaciones de seguridad, tanto criptográficas como gráficas, es la única tarjeta con la posibilidad de manejar información clasificada SECRETO.

2.2. Implantación y despliegue de una herramienta de Gestión y Correlación de Eventos de Seguridad (SIM)

El proyecto consiste en la realización de un estudio de mercado, en la selección y en la implantación de las tecnologías y herramientas para la gestión centralizada de registros de eventos de seguridad del Ministerio de Defensa.

Los beneficios que este proyecto aporta al conjunto de la Organización son los siguientes:

- Aumento en el grado de cohesión y respuesta frente a los incidentes de seguridad realizados o intentados contra la Red de Área Extensa de Propósito General (en adelante, WAN-PG) [3] del Ministerio de Defensa.
- Mejora del grado de protección de la WAN-PG del Ministerio.

2.3. Implantación de IPS (Intrusion Protection System)

Este proyecto tiene por objeto la obtención e implantación de herramientas hardware que previenen contra el ataque de intrusos, aumentando, por tanto, el grado de protección de la red.

2.4. Autorización/ Certificación de dispositivos de encaminamiento (router) de CISCO a Difusión Limitada

El proyecto consiste en el Análisis de Viabilidad de la certificación, por parte del CCN, de la tecnología IPSec (Internet Protocol Security) de los equipos de CISCO hasta nivel DIFUSIÓN LIMITADA.

Los beneficios que se persiguen con este proyecto son los siguientes:

- Emplear los propios equipos de comunicación (router) para cifrar la transmisión de información en la WAN-PG (un solo equipo para comunicación y cifrado), y evitar de esta manera la necesidad de incorporar equipos específicamente dedicados para el cifrado (1 equipo dedicado a la comunicación y 1 equipo para cifrar).
- Reducir los costes de material, gestión y administración.
- Permitir el manejo de información clasificada (DIFUSIÓN LIMITADA) en la WAN-PG.
- Cumplir los requisitos exigidos para la acreditación de la WAN-PG.
- Garantizar el intercambio seguro de información.

2 CNI: Centro Nacional de Inteligencia.

3 El Ministerio de Defensa dispone de dos redes de área extensa (WAN), físicamente aisladas, que dan soporte a todos los sistemas de información del Ministerio. Por una parte, una WAN para Mando y Control Militar (WAN-C2), y por otra parte, la WAN Corporativa de Propósito General (WAN-PG).

2.5. Proyectos I+D

Dentro de los proyectos I+D del Ministerio de Defensa se encuentran los siguientes:

- **Incorporación de Biometría en la Tarjeta Electrónica de Defensa:** Consiste en el almacenamiento de la huella dactilar dentro de la Tarjeta Electrónica de Defensa, para su empleo en lugar del PIN.

- **Token Criptográfico:** Consiste en el desarrollo de una "llave USB", conocida como "TOKEN USB", que es capaz descifrar ficheros hasta un nivel de clasificación de CONFIDENCIAL. Los beneficios perseguidos a través del mismo son los siguientes:

  - Dotar al Ministerio de un dispositivo de pequeño tamaño y portátil, certificado para el cifrado off-line y transporte seguro de claves criptográficas e información clasificada CONFIDENCIAL.
  - Permitir la protección de la información almacenada en ordenadores portátiles.
  - Garantizar el intercambio seguro de información.

- **Protección de Confidencialidad e Integridad en dispositivos portátiles:** Consiste en la elaboración de un piloto de la herramienta SSF (Secuware Security Framework), para valorar el incremento de protección conseguido sobre la seguridad de los ordenadores portátiles de la WAN-PG del Ministerio de Defensa. Permite:

  - Determinar el entorno de uso de los ordenadores portátiles y PDA's del Ministerio.
  - Valorar el incremento de seguridad y cumplimiento de normativa al cifrar los discos duros.

3. Conclusiones

El fortalecimiento de las medidas técnicas, uno de los pilares de la Seguridad de la Información, a través de los proyectos mencionados deriva fundamentalmente en un incremento del grado de protección de la Red de Área Extensa del entorno de Propósito General (WAN-PG) del Ministerio de Defensa, constituyendo todos ellos un referente para otros organismos de la administración pública.