

TESIS
Aplicaciones de PKI al Homeworking

Maestría en Auditoría de Sistemas

Universidad del Salvador



Autor: Ing. Tania Cecilia Cozzi
Tutor: Lic. Andrea Karina Sartor

Diciembre, 2000



USAL
UNIVERSIDAD
DEL SALVADOR

Abstract

El mundo del trabajo está cambiando rápidamente gracias a las diversas herramientas provistas por la tecnología de la información. En virtud de la cantidad y calidad de los datos que se están transmitiendo sobre la red, es que se hace imprescindible contar con técnicas de seguridad que aseguren con un nivel probabilístico aceptable estos nuevos activos organizacionales.

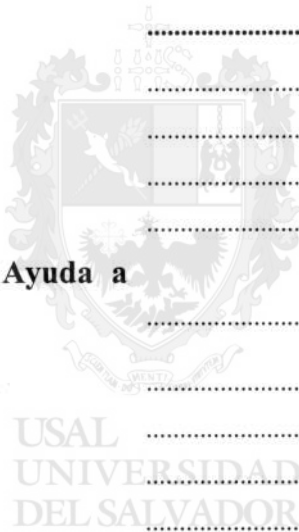
La criptografía de clave pública se está convirtiendo rápidamente en la base de estas prestaciones. Su uso general requiere que los PKI sean capaces de publicar y manipular valores de clave pública. Sin esta infraestructura funcional, la criptografía de clave pública es muy poco más que la tradicional criptografía de clave secreta.

Esta tesis analiza el impacto de esta clase de infraestructura de seguridad en el llamado e-work (electronic-work). Además proporciona elementos simples y concisos para la comprensión de estas nuevas herramientas, así como de otras tendencias emergentes en materia de seguridad.

La información provista en el presente ensayo intenta realzar los rasgos distintivos de estas herramientas y para nada llevar adelante un análisis exhaustivo de las mismas. La intención del autor es efectuar un estudio crítico de los diversos aspectos de PKI aplicados al trabajo hogareño y la visión de los futuros usuarios respecto a esta nueva y revolucionaria manera de llevar adelante sus actividades laborales.

Indice

Abstract
Introducción
Capítulo I: La Tecnología de la Información lo Cambiará Todo
<i>Tres temas para el futuro</i>
<i>La nueva moneda</i>
<i>Nuevas interacciones fundamentales</i>
<i>Porqué trabajar en casa?</i>
Capítulo II: Networks for Homes
<i>Las líneas telefónicas se alistan</i>
<i>El mundo Wirless</i>
<i>El guardián de la puerta</i>
<i>Y del futuro qué?</i>
Capítulo III: PKI la Tecnología Ayuda a Lograr la Seguridad
<i>Características básicas de un PKI</i>
<i>Qué es un PKI?</i>
<i>Certificación</i>
<i>Disposiciones de las CAs</i>
<i>Relaciones entre entidades</i>
<i>Validación</i>
<i>Autenticación</i>
<i>Limitaciones de la autenticación PKI</i>
<i>Anonimato</i>
<i>Sumario</i>
<i>Un mundo sin PKI</i>
E-mail inseguro
FTP y Control de Acceso
<i>Tendencias en seguridad y PKI</i>
Capítulo IV: Elementos de Seguridad a tener en Cuenta para Plantear un Esquema



de Trabajo Hogareño

Confianza en la Red de Telefonía Pública (RTP)

e Internet

Red de Telefonía Pública

Autenticación

Internet

Posibles fallas de las redes y soluciones

Trastornos ambientales

Errores operacionales

Fallas de hardware y software

Ataques maliciosos

A la red telefónica

A Internet

Temas emergentes

Telefonía en Internet

Seguridad y PKI aplicados al homeworking

Políticas de Control de Acceso

Mecanismos de Identificación y Autenticación

Criptografía y PKI

El problema de la administración de las claves

Esquemas de seguridad

Capítulo V: Estudio Estadístico

Ficha Técnica y Objetivos

Totales Generales

Totales por Sexo

Totales por Edades

Totales por Ocupación

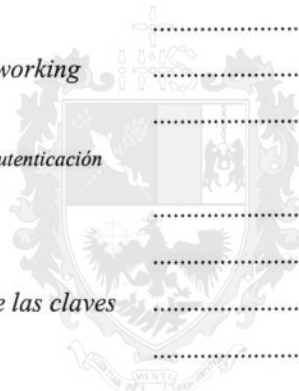
Análisis de Resultados

Conclusión

Glosario

Bibliografía

Otras Fuentes



USAL
UNIVERSIDAD
DEL SALVADOR

Lista de Figuras

<i>Número</i>	<i>Página</i>
Figura 1 - Un Certificado Básico	
Figura 2 - Un Camino de Certificación entre Alice y Bob	
Figura 3 - Una Jerarquía General con Certificación Cruzada	
Figura 4 - Jerarquía Top-Down	
Figura 5 - Comunicaciones en Internet	
Figura 6 - El Protocolo FTP	
Figura 7 - Arquitectura de Detección de Intrusos	
Figura 8 - Gateway/Firewall Honey Pot Networks	
Figura 9 - Arquitectura de una Autoridad Certificadora	
Figura 10 - Arquitectura Criptográfica de Tunneling	

USAL
UNIVERSIDAD
DEL SALVADOR

Lista de Tablas

<i>Número</i>	<i>Página</i>
Tabla 1 - Características Básicas de un PKI	
Tabla 2 - Tipos de Servicios Criptográficos	

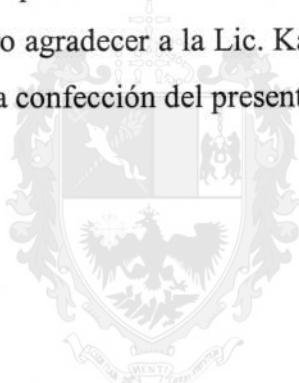
Agradecimientos

El autor desea agradecer a todos aquellos que de una manera u otra han posibilitado que este trabajo haya sido realizado.

Puntualmente quiero reconocer la valiosa ayuda recibida por parte del Committee on Information Systems Trustworthines y del Ph.D. Marc Branchaud por brindarme el material solicitado sin demoras.

Gracias a Consultores Asociados y a su socio principal Bernardo Cuadra por la ayuda en la confección y procesamiento de la encuesta del Capítulo V.

También estoy muy agradecida con todos aquellos que han contribuido indirectamente, haciendo que sus investigaciones estuvieran libremente disponibles en Internet. Esta tesis no hubiera sido posible sin su excelente disposición para compartir abiertamente su labor. También quiero agradecer a la Lic. Karina Sartor y Enzo Taibi por sus prontas respuestas y por guiarme en la confección del presente trabajo.



USAL
UNIVERSIDAD
DEL SALVADOR

A mi familia, por su apoyo y amor incondicional
A mi abuelo Julio, Nono, mirame volar



USAL
UNIVERSIDAD
DEL SALVADOR

Introducción

El presente ensayo consta de cinco capítulos que intentan efectuar un acercamiento a la aplicación de la tecnología de PKI a lo que se ha dado a conocer como home-working. En el primero de ellos se pretende plasmar la manera en que la tecnología de la información ha ido y seguirá cambiando nuestra forma de percibir el mundo que nos rodea. En una segunda sección se brinda la estructura genérica de red que se necesitará plantear para llevar adelante el proyecto del “trabajo casero”. La tercer parte analiza en profundidad el rol del esquema de PKI y sus características más significativas. El capítulo cuatro plantea ciertos aspectos de la seguridad para esta clase específica de trabajo. En el último apartado se ofrece un e sondeo de opinión acerca del parecer de la gente acerca del teletrabajo. Como último punto se brinda una conclusión.



USAL
UNIVERSIDAD
DEL SALVADOR