Esquema de integridad de bitácoras

Roberto Gómez Cárdenas, Ricardo C. Lira Plaza, Adolfo Grego
ITESM-CEM, Departamento de Ciencias Computacionales
Apdo. Postal 50, Módulo Servicio Postal, Atizapán Zaragoza, 52926, México
{rogomez,rlira,agrego}@campus.cem.itesm.mx

ABSTRACT

Computer security is defined as the mechanisms and policies set that assures confidentiality, integrity and availability of systems resources. In a forensics analysis is necessary that data logs remain unchanged. Our work proposes a schema, based in secret sharing theory that assures the integrity and confidentiality of log information. Furthermore our proposition allows fault tolerance, so the availability feature of the data log is also considered.

Keywords: crytology, computer security, networks, distributed systems

RESUMEN

La seguridad computacional se define como el conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema. En un análisis forense es necesario que los datos contenidos en las bitácoras sean íntegros. Nuestro trabajo propone un esquema que involucra la teoría de secretos compartidos en un ambiente distribuido que permite salvaguardar la integridad así como la confidencialidad de la información para su futuro análisis. Además nuestra propuesta incorpora tolerancia a fallas por lo que el aspecto de la disponibilidad también es considerado.

Palabras clave: criptología, seguridad computacional, redes, sistemas distribuidos