Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles

Resumen

Introducción: El desarrollo de tecnologías móviles ha facilitado la creación de aplicaciones mHealth, las cuales son consideradas herramientas clave para la atención segura y de calidad a los pacientes de poblaciones apartadas y con carencia de infraestructura para la prestación de servicios de salud. El artículo considera una propuesta de un modelo de evaluación que permite determinar las debilidades y vulnerabilidades a nivel de seguridad y calidad de servicio (QoS) en aplicaciones mHealth.

Objetivo: Realizar una aproximación de un modelo de análisis que apoye la toma de decisiones referentes al uso y producción de aplicaciones seguras, minimizando el impacto y la probabilidad de ocurrencia de los riesgos de seguridad informática.

Materiales y métodos: El tipo de investigación aplicada es de tipo descriptivo, debido a que se detallan cada una las características que deben tener las aplicaciones móviles de salud para alcanzar un nivel de seguridad óptimo. La metodología utiliza las normas que regulan las aplicaciones y las mezcla con técnicas de análisis de seguridad, empleando la caracterización de riesgos planteadas por Open Web Application Security Project -OWASP y las exigencias de QoS de la Unión Internacional de Telecomunicaciones -UIT.

Resultados: Se obtuvo un análisis efectivo en aplicaciones reales actuales, lo que muestra sus debilidades y los aspectos a corregir para cumplir con parámetros de seguridad adecuados.

Conclusiones: El modelo permite evaluar los requerimientos de seguridad y calidad de servicio (QoS) de aplicaciones móviles para la salud que puede ser empleado para valorar aplicaciones actuales o generar los criterios antes de su despliegue.

Palabras clave: Confidencialidad; sistemas de información en hospital, seguridad computacional.

Abstract

Introduction: The development of mobile technologies has facilitated the creation of mHealth applications, which are considered key tools for safe and quality care for patients from remote populations and with lack of infrastructure for the provision of health services. The article considers a proposal for an evaluation model that allows to determine weaknesses and vulnerabilities at the security level and quality of service (QoS) in mHealth applications.

Objective: To carry out an approximation of a model of analysis that supports the decision making, concerning the use and production of safe applications, minimizing the impact and the probability of occurrence of the risks of computer security.

Materials and methods: The type of applied research is of a descriptive type, because each one details the characteristics that the mobile health applications must have to achieve an optimum level of safety. The methodology uses the rules that regulate applications and mixes them with techniques of security analysis, using the characterization of risks posed by Open Web Application Security Project-OWASP and the QoS requirements of the International Telecommunication Union-ITU.

Results: An effective analysis was obtained in actual current applications, which shows their weaknesses and the aspects to be corrected to comply with appropriate security parameters.

Conclusions: The model allows to evaluate the safety and quality of service (QoS) requirements of mobile health applications that can be used to evaluate current applications or to generate the criteria before deployment.

Keywords: mHealth Apps, data security, Quality of service (QoS), risk assessment and management