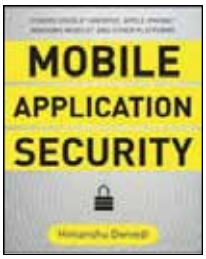

By Himanshu Dwivedi, Chris Clark and David Thiel

Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS, distinguished professor in the law department of the Universidad de los Andes, Colombia. He has been a practitioner and researcher in information and computer security and in computer forensics for more than 15 years in different industries. Cano is a member of ISACA's Publications Subcommittee.

Mobile Application Security

According to an April 2010 Morgan Stanley study on Internet trends,[1] within 10 years there will be a consolidated mobile Internet domain in which applications and interactions between users will become the norm, and information flow will be part of the reason for the services available on that platform.

Similarly, the presence of mobile devices such as smartphones and tablets is an inherent part of the era of mobility and instant information that exists today. In a world dominated by mobility, interaction and loss of privacy, it is necessary to adopt new practices of security and control that enable organizations to meet the challenges of a moving society exposed to continuous data leakage.

In this sense, *Mobile Application Security* introduces the details of current mobile platforms (such as Java Mobile Edition; Symbian OS; webOS; Windows Mobile; and the operating systems of iPhone, Android and BlackBerry) as a way to understand the key aspects of their technical architecture and security issues to establish assurance and control elements that facilitate coexistence in an adequate and reliable mobile reality.

> "New practices of security and control… enable organizations to meet the challenges of a moving society exposed to continuous data leakage."

The book presents a series of suggestions and security tips for developing mobile applications, including the use of protocols such as Transport Layer Security/Secure Sockets Layer (TLS/SSL), input validation, an assurance permission model for the OS, configuration of least privilege and access strategy, proper storage of sensitive information, code signing applications, knowledge of the limitations and advantages of the mobile devices browsers, and safe use of URL.

The authors clearly outline the benefits, risks and security measures for each of the mobile platforms, with examples indicating the actions required for each. Additionally, a review of other mobile services, such as Bluetooth, Wireless Application Protocol (WAP), Short Message Service (SMS) and geolocation, that are inherent parts of the features offered on mobile devices is also provided.

Moreover, analysts offer guidelines based on corporate assurance in the use of these mobile devices, knowing that this is one way to realize data leakage, loss of information and entry of malicious code in the computing infrastructure of enterprises.

Mobile Application Security is intended for information security specialists, information systems (IS) auditors and professionals in IT governance because it includes clear answers about the requirements, risks and control measures required in a mobile information society.

For IS professionals and IT managers faced with securing mobile applications, this book provides a set of best practices that are adaptable to the requirements and business strategies of organizations. These best practices can improve the level of protection and control of information flows on mobile devices while balancing the need for monitoring and control.

ENDNOTE

[1] Morgan Stanley, Internet Trends, 12 April 2010, *www.datam.co.nz/Files/Whitepaper-Internet-Trends-apr2010.pdf*

EDITOR'S NOTE

Mobile Application Security is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650. Another resource is the ISACA white paper *Securing Mobile Devices*, posted at *www.isaca.org/research.*