Chapter VIII

Developments in Security Mechanism Standards

Chris Mitchell
University of London, UK

International Standardisation

Over the last ten years, in parallel with the enormous growth in the use of cryptography, major efforts have been devoted to assembling a set of internationally agreed standards for cryptographic mechanisms. These standards have been prepared by ISO/IEC JTC1/SC27, a committee devoted entirely to security standardisation. Of course, the standards produced by SC27 are not the only cryptographic standards in existence. A number of important standards have been produced by a variety of other bodies, including the following:

• From the early 1980s onwards, the US banking community has produced a range of US (ANSI) standards covering the use of cryptography in retail and wholesale banking. The standards have had a very strong influence on subsequent international banking standards on cryptography and its use. In turn, these banking standards have motivated some of the general purpose standards developed by SC27.
• The Internet community has produced a number of RFCs covering a range of cryptographic algorithms. These RFCs have been primarily aimed at providing algorithms for use in specific secure...
Internet protocols (e.g. for secure e-mail and secure IP). Nevertheless, some of the schemes adopted as RFCs have become widely used in many applications outside of the Internet sphere.

- A variety of national, regional and industry bodies have proposed standards for cryptographic techniques. Examples include the pioneering US standards for the DES block cipher, the DSA signature algorithm, and the SHA-1 hash algorithm, and the European ETSI standards for cryptographic algorithms for use in mobile telecommunications (some of which remain confidential).

**Scope of This Chapter**

However, despite this wide range of standardisation activity, the ISO/IEC JTC1/SC27 work is unique in being both truly international and also aimed at general applications. As such, while we mention the relevant work of other standards bodies, the main focus of this chapter is the work of ISO/IEC JTC1/SC27. The main purpose of this chapter is to bring the international standards for cryptographic techniques to the widest possible audience. Adoption of these standards, which have received detailed scrutiny from experts worldwide, can only help to improve the quality of products incorporating security features.

Note that much of the work described in this chapter is based on recent research. For brevity, references to research papers are not included here. For further information the interested reader should consult the bibliographies in the quoted standards, or the excellent encyclopaedic work (Menezes, van Oorschot and Vanstone, 1997).

**Contents**

The chapter will consider the full spectrum of international standardisation of cryptographic techniques. Thus, it will involve covering the following areas:

- Encryption algorithms,
- Modes of operation for block ciphers,
- Message Authentication Codes (MACs),
- Digital signatures and Hash-functions,
- Entity authentication,
- Non-repudiation, and
- Key management.
The Impacts of Risk on Deploying and Sustaining Lean Six Sigma Initiatives
www.igi-global.com/article/the-impacts-of-risk-on-deploying-and-sustaining-lean-six-sigma-initiatives/191219?camid=4v1a