Progress in Data Security Standardisation

Wyn L Price

NPL, Teddington, UK

1 Introduction

This short paper is intended to provide a statement of current activities in the preparation of data security standards and is directed at the community active in research and development in cryptology, some of whom may not be aware of this aspect of the application of their work; it concentrates on the period since August 1987 when a previous statement was made on this subject in the same context.

2 Reorganisation

During the period since August 1987 the data security standards work within ISO has seen considerable reorganisation. In 1987, the committee with overall responsibility for information processing standardisation within ISO was Technical Committee 97 (TC97). The work of TC97 has now been allocated to the new body, Joint Technical Committee 1 (JTC1), which is joint between ISO and the International Electrotechnical Commission (IEC). The remit of JTC1 is very similar to that of TC97, though the title of the committee changes from "Information Processing" to "Information Technology".

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 620-623, 1990.

Within JTC1 there has been significant dissatisfaction with the organisation of the work in preparing data security standards. There have been signs of substantial overlap of interest between the various constituent bodies of JTC1. The former structure of the work involved Sub-Committee 20 (SC20), with the remit of producing standards for data cryptographic techniques, and other sub-committees, such as SC6 (Data Communication), SC18 (Office Systems) and SC21 (Open Systems Interconnection (OSI)) and others, having responsibility for standards for the application of cryptography in achieving secure services within particular areas. The boundary between these activities was never very precise, with the result that overlapping work took place in some areas, particularly those involving communication protocols. Existing liaison channels were not found to be particularly effective.

During 1988 and the early part of 1989 meetings took place between the various interested parties in efforts to create a more viable structure for the work. It is not necessary here to rehearse all the different arguments that arose at various stages of the consultation, suffice it to say what has been decided by JTC1 and must now be acted upon.

Perhaps the most striking change is the abolition of SC20 and its replacement by SC27 with an extended remit which will include the cryptographic techniques work of SC20 (but not that part of the work which addressed the enhancement of communication protocols with security capability), with the addition of general security techniques which do not involve cryptography. The formal title of the new sub-committee is "Information Technology Security Techniques". The change of title and of remit is meant to take account of the numerous security-relevant techniques in which cryptographic methods do not figure. Obvious examples are those involving access control, where identity tokens and biometric methods will be relevant. Management of passwords for access control is another area where SC27 can be expected to have an interest.

So much for the field of activity of the new sub-committee SC27. The other interested sub-committees are expected to use and apply the techniques and mechanisms developed and standardised by SC27 in creating security services relevant to the standards they are preparing.

The accounts that follow of published standards and of work in progress take note only of activities within the orbit of JTC1. It is relevant to say that another area of ISO, TC68 on banking procedures, also has work proceeding on security standards particularly intended for financial systems, with several standards already published. The latter include procedures for message authentication and for key management.

3 Published Standards

In the field of SC20 two data security standards achieved published status during the period 1987 – 1989. These related to modes of operation for a 64–bit block cipher (ISO 8372–1988) and to the interoperability requirements for data encipherment at the physical layer of OSI (ISO 9160–1987). Note that the latter came from SC20 and not from SC6, which has general responsibility for that part of the OSI structure which includes the physical layer; in the future, as a result of the reorganisation, we may expect that standards of this type will be published by the parent technical sub-committee.

Without doubt the security relevant standard of greatest significance published within the period is ISO 7498/2–1988. ISO 7498/1–1984 provides the basic open systems interconnection reference model. ISO 7498/2 describes the security architecture that may be adopted for providing security services within the OSI context. Note particularly that ISO 7498/2 describes an architecture; thus advice is given on where within OSI particular security services should be located, together with suggestions as to the individual security mechanisms that may be invoked in order to provide these services. Nowhere in ISO 7498/2 is there any attempt to define details of these services or mechanisms. An important section of the standard discusses aspects of security management.

4 Work in Progress

We begin this part of the review with algorithms; in 1986 ISO decided not to standardise algorithms, but rather to establish a register where users can refer for information on what is available. The rules under which this register will run have been embodied in a draft proposal (ISO DP 9979), which has already had one round of voting, but has not yet received approval. (Note: the progression of texts within ISO is from working draft, to draft proposal (DP), to draft international standard (DIS), to international standard.) This specifies the kind of information that may be expected to be found in a register entry, such as name, supplier, external characteristics, speed of operation of implementations, etc. It must be stressed that appearance of an algorithm on the register implies no guarantee of level of security. Optional information may include a description of how an algorithm works.

Another algorithm-related text is ISO DP 10116, which concerns modes of operation for n–bit block cipher algorithms. This is directly related to ISO 8372 and is a generalisation from that standard.

Significant effort has been devoted within SC20 to developing techniques for peer entity authentication. Three texts exist, and will be carried forward by SC27, forming eventually a single standard. These are ISO DP 9798, on peer entity authentication mechanisms using an n–bit secret key algorithm, ISO DP 9799, on a peer entity authentication mechanism using a public-key algorithm with two-way handshake, and ISO DP 10117, on a peer entity authentication mechanism using a public-key algorithm with a three-way handshake. Eventually we may have a fourth peer entity authentication text, based on zero knowledge techniques.

Considerable work has also been devoted to preparing texts for digital signature. It is recognised that two kinds of digital signature are required. One will sign a message after first inserting redundancy information according to specified rules. Recovery of a message is a direct result of verification and removal of the redundancy information. This technique is described in ISO DP 9796. The second technique will first calculate a hash function on the message and will then sign the hash result. Verification proceeds by recalculating the hash function from the received message and comparing it with that obtained in the verification process. No text has yet been prepared describing this signature mechanism, but ISO DP 10118 describes various ways of calculating hash functions.

Work is also in progress in preparing working drafts for the subject of key management, which is critical in successful data security operation. This work will be divided between key management using secret key techniques and that using public key techniques. There will also be a section on the operation of a public key register (not to be confused with the register of algorithms).

A recent development of great significance to SC27 and the other groups working on data security standards is the preparation of "frameworks" or "models" for security techniques and services. These are strongly oriented to applications and seek to proceed by analysing the need for a security function, with the management structure needed to support it, and then identifying the general category of service, technique or mechanism required to fulfill this need. The result of working in this way is that user requirements are given greater prominence than has been the case hitherto. In the past there has been a tendency to think of interesting mechanisms and to seek to develop these into services which users may wish to use. Now the process is being turned on its head, with likely benefit for all concerned.