STANDARDS FOR DATA SECURITY - A CHANGE OF DIRECTION

Wyn L.Price
National Physical Laboratory
Teddington, Middlesex, UK

Standards for data security - the achievement of acceptable privacy and integrity in data communication and storage - have been in preparation for the last fourteen years, beginning with the US Data Encryption Standard (DES). The DES was adopted as a US federal standard (1) in 1977, followed by adoption as an ANSI standard (2) in 1981. Since 1980 work has been in progress to develop a corresponding International Standards Organisation (ISO) text. For most practical purposes the ISO text was identical with the ANSI text; the only significant departure was that the eight parity bits allocated to the key in the US standard were left unallocated in the ISO text. The responsible ISO body was at first Technical Committee 97 (information processing), Working Group 1, TC97/WG1, which was followed by Sub-Committee 20 (data cryptographic techniques) of TC97, TC97/SC20. In May 1986 a discussion, followed by a resolution, took place in TC97, meeting in Washington, as a result of which a reference was made to the central governing body of ISO on which all national member bodies are represented, ISO Council, to decide whether it was wise to proceed to publication of the ISO standard. The outcome of this reference was that ISO Council decided to abandon work on the DES as a potential international standard. The decision was taken very late in the process of preparing the standard text, publication had been imminent.

The chief argument advanced in favour of the decision was that adoption as a standard might encourage overdependence on the DES algorithm. It is well-known that the financial institutions (banks, building societies, savings and loan, etc.) make very widespread use of the algorithm and the value of their daily transactions protected by the algorithm must be very substantial. This offers a very attractive potential target for criminal cryptanalysts. It was evidently feared within ISO that publication of an ISO standard for data encipherment would increase the attractiveness of the target by influencing even more users to depend on the one algorithm.

No-one is seriously suggesting that the useful lifetime of the DES

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 3-8, 1988.

is already over, but it is felt that preparation must be made for that time when it is judged no longer safe for use in protecting transactions of significant value or sensitivity. Various interesting academic results have been obtained in research investigations of the DES (3,4,5), but none of the people or groups involved is yet seriously claiming that the DES is broken. No one is yet able to predict whether the algorithm will succumb first to an analytic attack or to an exhaustive search for a key.

In the US the wish to replace the DES with more appropriate algorithms has led to the establishment of the Commercial COMSEC Endorsement Program (CCEP). This was originally meant to cover two security classes, Type I solely for US federal use and Type II for US federal and domestic commercial use, with the DES being phased out after 1988. However, it seems that the US financial institutions have requested that the DES be continued for financial applications beyond this date; the American Bankers Association has let it be known that the request for extension of approval for the DES has been granted. Neither Type I nor Type II CCEP algorithms are to be exportable and cannot therefore ever be put forward as candidates for international standardisation, should this be considered again in the future; the algorithms wil not be published.

In ISO the approach is somewhat different. ISO has decided to adopt the principle of a register of encipherment algorithms as a means of encouraging some degree of diversification in choice of encipherment algorithms. Algorithms, published and unpublished, will be entered on the register. Unpublished algorithms may be represented by name, supplier(s), block size and key domain; possibly speeds of operation may be entered. Published algorithms may be represented by a reference to a full and formal description of the algorithm; it is quite conceivable that the DES itself will figure in the register. Suppliers of algorithms will be free to offer their algorithms to ISO for entry on the register. Such an entry, however, is unlikely to offer any indication of the strength of an unpublished algorithm; it will be a matter for exercise of user judgement in choosing an algorithm to decide whether an algorithm is suitable for the proposed use. The decision to set up the register was noted by SC20, meeting in Ottawa in April 1987; the first relevant action was to establish a work item which is aimed at setting down the rules under which the register will operate. It is hoped that the operational rules will become

available sometime in 1988, though a formal starting date for the register has not yet been decided.

Until recently work was also in progress within ISO to prepare a standard text for the RSA public key cryptosystem; this was a simple statement of the algorithm, the text of an implementation in Pascal, some sample parameters and an indication of the rules to be applied in choosing key material. However, a recent decision within ISO is to discontinue all work on standards for data encipherment; the embargo on data encipherment standards is therefore extended beyond the DES and now embraces public key algorithms and all others. Working Group 2 of SC20 (SC20/WG2) had been preparing not only the text of an RSA standard but also a technical report surveying recent developments in work on public key cryptography (a first edition of this technical report was published some years ago); the secretariat of TC97 now advises that work on the parts of the technical report relating to encipherment algorithms should also be discontinued. Regarding the RSA algorithm, this too is now fairly widely used in protecting transaction processing. It therefore seems likely that it will be offered as a candidate entry on the algorithm register. There will then be a need for a definitive statement of the algorithm in a form to which reference can be made; the academic papers in which the idea was first disclosed and later discussed and elaborated are not suitable for this purpose. The form that the definitive statement will need to take - it cannot be a formal standard text - has yet to be worked out.

In view of the removal of all the work on encipherment standards one might wonder what was left for TC97/SC20 to do. In fact the work programme of this committee is now heavier and more extensive than it was prior to the recent decisions.

The work programme adopted in April 1987 concentrates on operation of the register of algorithms and on standards for data security applications, including modes of operation for data encipherment, enhancement of communication protocols with security capability and security management (including management of encipherment keys).

One of the early effects of the removal of the work on data encipherment standards was to hold up work on two other standards which were also in an advanced state of preparation. These were respectively

for 64 bit block cipher modes of operation and for enhancement of the physical layer of OSI (Open Systems Interconnection) with encipherment capability. The modes of operation document needed little doing to it to take into account the decision not to publish the DES standard text; this was because the modes of operation text had already been deliberately written in a general way, so that it applied to all 64 bit block ciphers and not just the DES. A little more effort was needed to change the physical layer standard. Publication of the 64 bit block modes of operation standard can be expected without undue further delay. Advancement of the physical layer text to Draft International Standard may also take place soon.

Work is in hand to prepare a standard for modes of operation of a block cipher not restricted to 64 bit blocks; this should present little difficulty, using the 64 bit block text as a basis. Any work on security enhancement at the link layer of OSI is now in abeyance because it was agreed that the demand for a standard in this context has not been established. The need for security enhancement at three other layers of OSI, namely network (layer 3), transport (layer 4) and presentation (layer 6) is recognised and work is now going ahead to prepare standard texts for these functions; the words of the respective work items specify 'conditions for the practical operation of cryptographic protection' at the various layers. Also in the context of secure communications architecture we have a new work item on 'practical conditions for the Associated Control Service Element (ACSE) authentication'.

In the area of key management the work programme is now more detailed; separate items on management of keys for secret key algorithms using secret key techniques, for management of keys for secret key algorithms using public key techniques and for management of keys for public key algorithms using public key techniques have been established. A further work item is to define a register of public keys and its functionality (not to be confused with the register of algorithms); the public key register is a service which will be required for many practical implementations of public key cryptography.

Peer entity authentication has a prominent place in the work programme. Texts are being circulated for draft proposal voting on a method for peer entity authentication using secret key algorithms and for two methods using public keys with two- and three-way handshakes. Work

on digital signatures is strongly represented, with items on digital signature with 'shadow' and with 'imprint' (respectively reflecting direct signature of data and signature of data through the medium of a hash function); methods of generating hash functions are also included.

An important issue that arose during 1986 was the division of responsibilities between the committees of ISO working on communication protocols and architectures and SC20 working on data security. It was recognised that there was a common area of interest between TC97/SC6 (layers 1 - 4 of OSI), TC97/SC21 (layers 5 - 7 of OSI and general architectural matters) and TC97/SC20. The chairmen of SC6, SC20 and SC21 have agreed the details of a definition of responsibilities; the effect of this is to leave the controlling responsibilities for protocols and architectural matters with SC6 and SC21 as appropriate, whilst SC20 has controlling responsibility for security matters with an emphasis on application of encipherment algorithms. We should note that a second part of the OSI architecture definition standard covering data security is in an advanced stage of preparation; this work is proceeding within SC21.

To complete this short review of present activities and trends in the data security standards area we must mention the work of TC68 (banking procedures). TC68 is producing a series of standards with emphasis on message authentication and key management. Work is proceeding on a standard describing the mechanism of message authentication (wholesale) and on a standard specifying algorithms (including the DES) that may be used for message authentication. Another important standard in preparation is that on wholesale financial key management, developed from ANSI standard X9.17. Standards for retail message authentication and key management can be expected to follow. Note, however, that there is no sign as yet of work under TC68 to use public key cryptography for banking purposes; all the known standards work uses symmetric cipher systems.

Much work remains to be done on data security standards and the abandonment of work on encipherment standards will free effort for making progress in the remaining areas.

References

1. National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standard 46, January 1977.

2. American National Standards Institute. Data Encryption Algorithm. American National Standard X3-92, 1981.

3. Desmedt, Y., Quisquater, J-J, & Davio, M. Dependence of output on input in DES; small avalanche characteristics. Proc. Crypto'84, Springer-Verlag, Lecture Notes on Computer Science 196, 1985, pp. 359-376.

4. Kaliski, B.S., Rivest, R.L., & Sherman, A.T. Is DES a pure cipher? (results of more cycling experiments on DES). Proc. Crypto'85, Springer-Verlag, Lecture Notes on Computer Science 218, 1985, pp. 212-226.

5. Shamir, A. On the security of DES. Proc. Crypto'85, Springer-Verlag, Lecture Notes on Computer Science 218, 1985, pp. 280-281.