only exceptional cases, means that the system must be regarded as flawed.

It could also be argued that *B* will receive two messages both secured using the same DEK, which would be a rather suspicious event. However, if *C* was in league with the network provider, then *A*'s original message could be prevented from getting to *B*, and no unusual event would be detectable by *B*.

We have therefore discovered a major drawback with the use of the suggested system for sending secure mail to a multiplicity of users. Although it would be desirable to try and 'repair' the above system to preclude the type of fraud described, it is by no means obvious how to do this. The basic problem is that user *C* knows both the MAC and the key used to generate the MAC for the original message, and it is this, in combination with the fact that the CBC function can be inverted, which makes the fraud possible.

Possible secure modifications must either provide distinct authentication keys and MACs for each intended recipient, or use a one-way function to compute the MAC thus preventing the inversion operation. The first possible modification could be very time-consuming since the MAC computation would need to be done for every possible recipient. It is certainly true that all proposed solutions need to be very carefully examined for possible flaws.

Finally, observe that the motivation for one aspect of the system described above is less than obvious, namely the encryption of the MAC under the IK. It is interesting to speculate that this is present to try and prevent the type of fraud described here. Certainly it is true that without this MAC encryption it would be even easier to construct fraudulent messages, since the MAC could be changed without detection and the 'garbage' block would not be necessary.

REFERENCES

1. J. Linn, Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures. *Request for comments 989 (RFC 989), IAB Internet Privacy Task Force* (Feb. 1987).
2. ANSI X3.106–1983, *Modes of operation of the DEA.* American National Standards Institute (New York) (1983).
3. FIPS 81, *DES modes of operation.* Federal Information Processing Standard, National Bureau of Standards (Washington, DC) (Dec. 1980).
4. FIPS 46, *Data encryption standard.* Federal Information Processing Standard, National Bureau of Standards (Washington, DC) (Jan. 1977).
5. ANSI X3.92–1981, *Data encryption algorithm.* American National Standards Institute (New York) (1981).
6. ANSI X9.9–1982, *Financial institution message authentication.* American Bankers Association (Washington, DC) (April 1982).

Announcement

12–14 APRIL 1989

ETC 89, the First European Test Conference, Palais des Congrès, Paris, France.

Topics: Component, board and system testing; test development; test systems; design for testability; and new test technologies.

Supported by: SEE, EUREL, IEEE Computer Society, AICA, GME, IEE.

Contact: Colin Maunder, British Telecom Research Labs, Martlesham Heath, Ipswich, Suffolk, IP5 7RE, UK. Tel.: (+44) 473 642706.

12–14 APRIL 1989

Artificial Intelligence and Software Engineering: Promise and Problems. An International Workshop sponsored by the AAAI, University of Exeter.

The purpose of this workshop is to present and discuss a broad set of issues relating to the promise and problems of exploiting AI in practical software. The four foci of the workshop are: AI-based support environments; AI mechanisms and techniques in practical software; software engineering tools and techniques for practial AI software: and methodological issues.

The workshop will be structured around invited presentations from both practitioners and researchers from the USA and from Europe. Each such presentation will be followed by ample discussion time. In addition, some short presentations of relevant submitted papers will be scheduled. Several panel discussions are also planned.

In order to facilitate the possibility of useful, open discussion the workshop will be limited to approximately 40 persons. If you would like to participate, present a paper, or organise a panel discussion, please send a one-page summary of your interests in this area to:

Professor Derek Partridge, Department of Computer Science, University of Exeter, Exeter EX4 4PT, U.K. email: derek@uk.ac.exeter.cs. Tel: 0392 264069; fax: 0392 263108.

12–14 JULY 1989

BNCOD-7, Seventh British National Conference on Databases, Heriot-Watt University, Edinburgh, in association with The British Computer Society.

Papers will be presented on various aspects of databases and database systems. This includes topics such as:

- Deductive databases
- Object-oriented databases
- Multimedia databases
- Knowledge bases
- Expert database systems
- Distributed databases
- Data models
- Database performance
- Information retrieval
- Database design
- Advanced user interfaces
- Geographic/cartographic databases

For further information contact:
Professor M. H. Williams, Computer Science Department, Heriot-Watt University, 79 Grassmarket, Edinburgh EH1 2HJ.