M.I.T. Laboratory for Computer Science
Computer Systems Research Division

14 July 1976
Request for Comments No. 119

IRIA WORKSHOP ON PROTECTION AND SECURITY IN DATA NETWORKS
Trip report

by Philippe Janson

The following is a report on the Workshop on Protection and Security in Data Networks, sponsored by the IRIA, the IFIP TC-6 and the Canadian Department of Communications, that was held in Rocquencourt, France, last June 28-30.

This note is an informal working paper of the Computer Systems Research Division, M.I.T. Laboratory for Computer Science. It should not be reproduced without the author's permission and it should not be referenced in other publications.

WORKSHOP ON SECURITY AND PROTECTION IN COMPUTER NETWORKS

PROGRAM

June 28 :

	9.30	Welcome L. POUZIN (IRIA)
*	10.00	Security in Datapac W. CLIPSHAM (BNR)
CACM	11.30	Verification of Security Kernels J. MILLEN (MITRE)
* (also RFC 115)	14.30	Présentation d'un Projet de Validation d'un Système P. JANSON (MIT)
CACM	15.30	Lattice Model of Information Flows D. DENNING (Purdue University)

June 29 :

	9.30	Capability Machines Dr. PATEL (ICL)
*	11.00	Cryptography D. BELL (NPL)
	14.30	Distributed Data Bases W. CHU (UCLA)
	16.00	Practical Aspects of Security J. FISK (DOC)

June 30 :

*	9.30	Discussion groups on Risk Analysis K. WONG (NCC)
*	14.00	Fuzzy Computer Security Metrics L. HOFFMAN (U.C. Berkeley)

END OF THE WORKSHOP

* paper available in Protection Library (NE43-512)
CACM paper in CACM 19 5 (May 1976)

1. Summary.

The program of the workshop is outlined on the previous page. In short, ten different speakers were invited to present papers. Presentations lasted between thirty and sixty minutes and were followed by discussion periods of about thirty minutes.

The style of the workshop was highly informal, which facilitated communication among the attendants, fostered discussion after each presentation and made life easier considering the heat wave that struck Europe in those days.

Unfortunately, the organization of the workshop may have been somewhat too informal. As a result, the level of preparation of speakers varied widely. For instance, Denning and Patel volunteered to speak at the last minute. The latter speaker did not have any notes to speak or any slides to show.

As a result, there will be no such thing as proceedings for the workshop. Reprints of the papers marked * in the program were distributed individually to participants. Copies of those papers are available in our protection library. Presentations marked CACM in the program were reruns of presentations given at the ACM Fifth Symposium on Operating Systems Principles held in Austin, Texas, last November. Reprints of the corresponding papers can be found in the May 1976 issue of the Communications of the ACM. Other speakers did not submit any paper unfortunately.

2. Evaluation.

About eighty people attended the workshop, which is a clear indication of an interest in protection and security in data networks. As far as I can tell from discussions with other participants, that interest stems from two sources.

First, many attendants were eager to find out more about encryption-based protection in networks. Clearly, research has been performed in that field. However, it is often classified and unavailable to the general public. The workshop certainly did not fulfill this lack. Many attendants expressed a definite interest in Steve Kent's recently published thesis on encryption, which I alluded to and briefly commented on during the discussion period on Bell's presentation.

Second, there seems to be a concern for certain information security problems proper to networks and not found in individual systems, noteably the confinement of data to compartments in a physically distributed system handling classified information. The workshop did not bring any answer to that problem either.

In fact, when considering the titles of the presentations, one notices that few of them dealt with protection and security of information in data networks. Most of them dealt with individual systems. Some people suggested that this may be a result of research on protection in networks being classified. While this may be partly true, it cannot be totally true. Why would such research be classified when research on the same topic but concerning individual systems is so widely publicized? I personally suspect that the topic of protection in networks is not yet quite mature.

On the whole, the workshop was somewhat disappointing to me. Most papers were not very deep in content. They discussed old or superficial or obvious solutions to known problems. Deeper papers (Millen, Denning) were not new. Yet, I think our French hosts got a lot out of the workshop.

3. Comments.

Clipsham's paper was a clear discussion of security threats in a public data network (Datapac in particular). However, it does not appear to be the fruit of a very deep research effort and discusses only common sense issues.

Millen's and Denning's papers were very interesting. I will not discuss them here as I suspect readers are familiar with them. Unfortunately for their authors, particularly Dorothy Denning who spoke "fast American" rather than slow English, the presentations passed way above the heads of the audience.

While all speakers were of English speaking origin and spoke little or no French, most participants were of French origin and many had only a poor command of English. As a result, the audience had difficulties in following some of the more complex presentations while the speakers had difficulties in understanding some questions and giving some answers during the discussions.

In that respect, our presentation was a success. While the paper was written in English, the talk was (the only one) delivered in French and had a much greater impact on the audience. Reportedly, it was the first presentation ever in French on the topic of security kernel certification. Members of the Academie Française would have barked at some of the words we had to make up to render concepts related to our topic. However, the audience seemed to appreciate the presentation as indicated by the wide participation in the discussion that followed. The discussion was lead in a bilingual mode for thirty minutes and resumed for another thirty minutes after Dorothy Denning's presentation. At the end of the day, we were invited by several French firms and organizations to say more about our project sometime next year in the course of informal visits to them.

Patel's presentation was a clear description of the functioning of capabilities in the ICL 2900 system. It focused on the conversion of capabilities between out-form and in-form, and on the possibility to partition the security kernel of a capability system into several protection domains.

Bell's presentation was a discussion of the importance of encryption and of the NBS algorithm.

Unfortunately, an attempt to cash traveller's checks 15 miles away from Paris prevented us from attending Chu's presentation.

Fisk's presentation was a rather uninteresting and low level discussion of the roles and duties of security officers in a public data network.

Wong's presentation started with an hour long discussion of a method for identifying, assessing and controlling risks related to information security in an information system. After the presentation, the audience was divided into four groups, which tried, in one hour, to use the risk analysis method in four different case studies. The conclusions of the four groups on their respective studies were vague at the very least. They indicated that the proposed method was in fact too vague itself and too superficial yet to perform a systematic risk analysis of any system.

Hoffman's presentation was clear but the technique he proposes to assess the security of a system is very fuzzy indeed. It sounds like he wants to assess the security of a system statistically with respect to a Gaussian curve plotting the number of (non-existant) systems versus their respective (not really assessed) security.

4. Future.

Another conference on the topic of protection and security in data networks is planned in a year or two. Interested people are welcome to contact L. Pouzin at IRIA.