AD-A065 420 GEORGIA INST OF TECH ATLANTA SCHOOL OF INFORMATION A--ETC F/G 9/2
CONFERENCE ON FOUNDATIONS OF SECURE COMPUTATION HELD ON 3-5 OCT--ETC(U)
DEC 78 R A DEMILLO N00014-77-G-0030

UNCLASSIFIED NL

1 OF 1
AD
A065420

END
DATE
FILMED
4-79
DDC

Final Report

6

CONFERENCE ON FOUNDATIONS OF SECURE COMPUTATION

Held on 3-5 October 1977 at Atlanta, Georgia.

15

ONR GRANT N00014-77-G-0030

9 Final rept.,

10

Dr. Richard A. DeMillo
Project Director

11 1 December 1978

12 7p.

This work relates to Department of the Navy Research Grant N00014-77-G-0030 issued by the Office of Naval Research. The United States Government has a royalty-free license throughout the world in all copyrightable material contained herein.

page -1-

Final Report on ONR Grant #N00014-76G-0030

The point of the meetings funded under this grant was to collect together the major researchers in the theoretical and practical areas of computer security. ~~It was~~ our initial hope that a dialogue between theoreticians and practitioners ~~would~~ result, that many results would flow from the meeting. It was also our hope that the papers resulting from the meeting would receive the widest possible dissemination. A collection of new research contributions from the major researchers in computer security should be influential as a textbook and as a reference work in the area. ~~As I will discuss below,~~ the meeting exceeded ~~our~~ any expectations in the areas cited in ~~our~~ the proposal, and provided a number of unexpected dividends.

On October 3, 4, and 5, 1977 the "Foundations of Secure Computation" workshop was held at the Atlanta Townhouse Hotel across from the Georgia Tech campus. In attendance were the following invited participants:

Timothy Budd, Yale University
James Burns, Georgia Tech
Ellis Cohen, University of Newcastle
George Davida, University of Wisconsin
Richard DeMillo, Georgia Tech
Dorothy Denning, Purdue University
David Dobkin, University of Arizona
Robert Fabry, University of California, Berkeley
Fredrick Furtek, Mitre Corporation
Stockton Gaines, Rand Corporation
Robert Grafton, ONR
Leonard Haines, ONR
Michael Harrison, University of California, Berkeley
Anita Jones, Carnegie-Mellon University
John Kam, Columbia University
Charles Kline, University of California, L.A.
Richard Lipton, Yale University
Nancy Lynch, Georgia Tech
Leonard McNeil, Management Science America
Jonathan Millen, Mitre Corporation
Naftaly Minsky, Rutgers University
Michael Rabin, Hebrew University and MIT
Steven Reiss, Brown University
Ronald Rivest, MIT
Walter Ruzzo, University of Washington
Norman Shapiro, Rand Corporation
Lawrence Snyder, Yale University

All attendees who requested travel funds were supplied with grants which at least partially subsidized their expenses in attending the meeting. No additional honoraria were given to the attendees.

Workshop participants were asked to distribute preliminary drafts of their contributions prior to the meeting. At the time of the workshop, we had the opportunity to review the written summaries provided by the attendees.

The logistics of the meeting's technical sessions proved to be remarkably simple to arrange. Although the papers fall naturally into four categories -- we will use these natural divisions in discussing the papers -- we made an early decision not to segregate the papers at the workshop. Since a major point of the meetings was to have been the cross fertilization between adjacent fields, we thought that a random interleaving of the papers would help promote this attitude. This technique seemed to work very well. The common situation in a conference or a workshop in which topics are segregated is that an attendee who does not perceive himself as having a specific research interest in a particular topic elects to not attend that session or attends as a mere observer. With our technique, attendees are kept "off guard". The topics shift as the session goes on and there is a tendency to participate uniformly throughout the sessions. The structure of the workshop was that attendees would be allocated each a half hour for informal presentation of his paper. Following these presentations was a fifteen minute discussion session. The responsibility of the session chairperson was to record the text of the discussion and attempt to guide its course. During the three days of the meeting, ample time was allowed for informal discussion groups, each devoted to specialized topics, and this aspect appeared to be enormously successful.

The afternoon of October 4th was devoted to a round table discussion covering topics raised in informal and formal discussion sessions. This round table lasted approximately three hours and was also recorded. All discussion topics were edited, condensed, reviewed by the attendees, and appear in the conference volume. The response of the attendees appears to be that the discussion sessions and their subsequent recording was the most successful aspect of the meeting.

The papers presented at the meeting fall naturally into those dealing with database security, encryption, practical aspects of operating systems security, and theoretical aspects of operating systems security. I will give a brief description of what resulted in each of these four areas.

I. Database Security

1. "A View of Research and Statistical Database Security" by Dorothy Denning

2. "Combinatorial Inference" by Richard DeMillo, David Dobkin and Richard Lipton

3. "Database System Authorization" by Don Chamberlain, Jim Graves Patricia Griffiths, Moishe Miesse, Irv Traiger, Bradford Wade

4. "Mediams in Database Security" by Steven Reiss

The four papers concerning database security addressed tradeoffs between usability and security. Dorothy Denning's survey of statistical database security reminds us how far we have come in realizing the limits of the notion of database security. The usual methods of compromising large statistical databases almost always involve transparent uses of information delivered in responses to queries. The article by Richard DeMillo, David Dobkin and Richard Lipton discusses the more subtle kinds of combinatorial inferences which can be formed out of query responses. Compromising the statistical sense is not the only security problem in database design. The pragmatic issues stemming from the authorization of access to database and database communication systems are outlined in the contribution by Chamberlain, Gray, Griffeths, Mresse, Traiger and Wade. The final paper of this section by Steven Reiss returns to statistical compromise with a detailed study of the insecurity inherent in databases which allow a certain statistical query strategy.

II. Encryption as a Security Mechanism

1. "A Structure Design of Substitution Permutation Encryption Networks" by John Kam and George Davida

2. "Proprietory Software Protection" by Richard DeMillo, Richard Lipton and Leonard McNeil

3. "Encryption Protocols, Public Key Algorithms and Digital Signatures in Computer Networks" by Gerald Popek and Charles Kline

4. "Digital Signatures" by Michael Rabin

5. "On Data Banks and Privacy Homomorphisms" by Ronald Rivest, Leonard Adleman and Michael Dertouzos

The five papers presented here are truly representative of current research in data encryption. George Davida and John Kam proposed the type of substitution-permutation encryption design. Their intent is to provide a variant of the NBS Data Encryption standard which obviate several of the difficulties raised by Hellman and Diffie and others. Richard DeMillo, Leonard McNeil and Richard Lipton raised a novel application for encryption research: the protection by encryption of commercial software from overt theft. Gerald Popek and Charles Kline correctly point out that oftentimes the protocol through which encryption algorithms are made available have significant impact on their effectiveness. They examine several encryption methods from this perspective. A surprising probabilistic method for creating secure digital signatures is the subject of Michael Rabin's article. He presents a method which can be based upon any block encoding function that satisfies two simple axioms. Ronald Rivest, Len Adleman and Michael Dertouzos address the serious defect of current methods for encrypting data: coded information must be decoded before it can be manipulated. Out of all possible privacy transformations, the authors select the privacy homomorphisms which allow data to be operated upon in its encrypted form.

III. Design Oriented Models of Operating Systems Security

1. "One Perspective on the Results About the Decidibility of Systems Security" by Robert Fabry

2. "Constraints" by F. Furtek and J. Millen

3. "Some Security Principles in the Application of Computer Security" by Stockton Gaines and Norman Shapiro

4. "Protection Mechanism Models: Their Usefulness" by Anita Jones

5. "The Principle of the Attenuation of Privilege and Its Ramifications" by Naftaly Minsky

In Robert Fabry's article we see a designer struggling to come to grips with the real world implications and with theoretical results: the Harrison, Ruzzo, Ullman Decidibility Theorem. The two part paper by F. Furtek and J. Millen attempts a simplification of several design concepts; they represent a system of "prime constraints", a concept similar to prime implicants of switching theory. Stockton Gaines and Norman Shapiro take a step back from detailed considerations to give us an overview. They provide us with some general perspectives and the state of security research based on some fairly pragmatic insights. The contribution by Anita Jones is indicative of the fertile interplay of theory and practice in security research; her article was the outcome of a designer assessing the usefulness of the take-grant system which has been the subject of extensive theoretical analysis. In the final paper of this section, Naftaly Minsky addresses Peter Denning's principle of "Attenuation of Privilege" and presents an authorization scheme which satisfies the principle.

IV. Theoretical Models of Operating Systems Security

1. "On Classes of Protection Systems" by R. Lipton and T. Budd

2. "Information Transmission in Sequential Programs" by Ellis Cohen

3. "Monotonic Protection Systems" by Michael Harrison and Walter Ruzzo

4. "On Synchronization and Security" by Richard Lipton and L. Snyder

In this final section, Richard Lipton and Timothy Budd open the selection in theoretical contributions by showing us that there is an efficient way to decide safety for a wide variety of protection systems. The requirement is that the systems must be related in certain ways. Ellis Cohen notes that the various possibilities for information flow in sequential programs and gives an elegant form of treatment of his ideas. Michael Harrison and Walter Ruzzo extend their well-known investigation into a particular security model by giving a characterization of the relative "power" of different operations allowed in the model. In the final paper, Richard Lipton and Larry Snyder proved the surprising equivalent of a well studied security model with an apparently unrelated model for synchronizing parallel processes.

The papers described above and the edited text of the panel discussions and informal discussions appear in a volume entitled "Foundations of Secure Computation" edited by Richard DeMillo, David Dobkin, Anita Jones and Richard Lipton which was published in late 1978 by Academic Press.

The attendees and other reviewers of the book have been enthusiastic about the outcome. Not only did we obtain a collection of first rate contributions to security research, but upon reviewing the contents of the contributions we found an unexpectedly large number of survey papers. Therefore, with minimal supplement by an instructor, the book could make an excellent text for a graduate course in security.

Meetings of this sort are rare. We had an advantage in that security was being covered rather heavily by the National Press at the time of our meeting and this lent an air of excitement to the gathering, but a meeting of active researchers in an area in which there is growing interest clearly can have beneficial impact upon the future development of the area. Therefore, as a final personal note I should like to add not only my thanks to the Office of Naval Research and the U.S. Army Research Office for their generaous support of our meeting but would like to strongly recommend that similar projects be funded in the future. As Michael Rabin told me at the close of our meeting, such gatherings can be a "great service to science."

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Final Report for
ONR Grant N00014-77-G-0030

5. TYPE OF REPORT & PERIOD COVERED
Final

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Richard A. DeMillo

8. CONTRACT OR GRANT NUMBER(s)
N00014-77-G-0030

9. PERFORMING ORGANIZATION NAME AND ADDRESS
School of Information and Computer Science ✓
Georgia Tech
Atlanta, Georgia 30332

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
U.S. Army Research Office
Box 12211
Research Triangle Park, NC 27709

12. REPORT DATE
December 1, 1978

13. NUMBER OF PAGES
4

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for Public Release

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES
The findings of this report are not to be construed as an official department of the Navy opinion.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Computer security, databases, operating systems, cryptography

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report summarizes the workshop on "Foundations of Secure Computation" held October 3, 4, 5, 1978 in Atlanta, Georgia.