IFIP Transactions A: Computer Science and Technology

International Federation for Information Processing

Technical Committees:

Software: Theory and Practice (TC2)
Education (TC3)
System Modelling and Optimization (TC7)
Information Systems (TC8)
Relationship between Computers and Society (TC9)
Computer Systems Technology (TC10)
Security and Protection in Information Processing Systems (TC11)
Artificial Intelligence (TC12)
Human-Computer Interaction (TC13)
Foundations of Computer Science (SG14)

IFIP Transactions Editorial Policy Board

The IFIP Transactions Editorial Policy Board is responsible for the overall scientific quality of the IFIP Transactions through a stringent review and selection process.

Chairman
G.J. Morris, UK
Members
D. Khakhar, Sweden
Lee Poh Aun, Malaysia
M. Tienari, Finland
P.C. Poole (TC2)
P. Bollerslev (TC3)
T. Mikami (TC5)
O. Spaniol (TC6)
P. Thoft-Christensen (TC7)
G.B. Davis (TC8)
K. Brunnstein (TC9)
E. Hörbst (TC10)
W.J. Caelli (TC11)
R. Meersman (TC12)
B. Shackel (TC13)
J. Gruska (SG14)

IFIP Transactions Abstracted/Indexed in:
INSPEC Information Services
Index to Scientific & Technical Proceedings®

A-37

COMPUTER SECURITY

Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec'93
Toronto, Canada, 12-14 May, 1993

Edited by

E. GRAHAM DOUGALL
ManuLife Financial
Toronto, Ontario, Canada

1993

NORTH-HOLLAND

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Library of Congress Cataloging-in-Publication Data

IFIP TC11 International Conference on Information Security (9th : 1993 : Toronto, Ont.)
Computer security : proceedings of the IFIP TC11 Ninth International Conference on Information Security, Toronto, Canada, 12-14 May, 1993 / edited by E. Graham Dougall.
p. cm. -- (IFIP transactions. A, Computer science and technology ; A-37)
Includes bibliographical references.
ISBN 0-444-81748-4
1. Computer security--Congresses. I. Dougall, E. Graham.
II. Title. III. Series.
QA76.9.A25I45 1993
005.8--dc20 93-34965
CIP

Keywords are chosen from the ACM Computing Reviews Classification System, ©1991, with permission.
Details of the full classification system are available from
ACM, 11 West 42nd St., New York, NY 10036, USA.

ISBN: 0 444 81748 4
ISSN: 0926-5473

This book is printed on acid-free paper.

Preface

This volume contains the papers presented at IFIP/Sec'93 at Deerhurst Inn, Huntsville, Ontario ,Canada from May 12 to 14 1993. This conference was second one to be hosted by Canada, the first was IFIP/Sec'84. As I was involved in the 84 conference it was a pleasure renewing old friends and forming new ones.

The theme of the conference was *Discovering Tomorrow*. We were fortunate in having Patrick Gallagher, the Director of the United States Government's National Computer Security Center which is part of the National Security Agency as the opening keynote speaker. He addressed the changing outlook of his Center.

IFIP/Sec'93 was honoured in having the first presentation of the Kristian Beckman Award. This award recognizes the contribution Kristian made in the organization of the first conference in Stockholm in 1983 and subsequent founding of TC11. It will be presented annually at the TC11 conferences to an individual who has made an outstanding contribution to computer security internationally. The acceptance speech of this year's recipient, Dr. Harold J. Highland is included in this volume.

I would like to thank all those involved in making IFIP/Sec'93 a success and look forward to meeting in Aruba in 1994.

E. Graham Dougall

IFIP/Sec'93

IFIP/Sec'93 was organized under the auspices of IFIP TC 11 by the National Security SIG of the Canadian Information Processing Society (CIPS) and the Toronto Chapter of the Information Systems Security Association (ISSA).

Organizing Committee

David Batchelor, Chair (Canada)
Dan Eng
David Gamey
Tim Haist
Beth Kendall
Peter Kingston
June S. Morrison

Program Committee

Graham Dougall, Co Chair

Jim Finch, Co Chair (Canada)
John Beatson, (New Zealand)
Bertil Fortie (Netherlands)
Darren Jones (Canada)
Rick Koenig (USA)
Hal Tipton (USA)

Sponsors

IFIP/Sec'93 would like to thank the following organizations for their support..

Computer Associates
Concord - Eracom Computer Ltd.
The Kingston Group
Nabisco Brands Ltd.
Sussex Systems Ltd.

IFIP/Sec'93
Table of Contents

Computer Security (A-37)
E.G. Dougall (Editor)
Elsevier Science Publishers B.V. (North-Holland)

A VIEW OF INFORMATION SECURITY TOMORROW

Dr. Harold Joseph Highland, FICS [1]

Mr. Chairman, Members of IFIP TC 11, Ladies and Gentlemen:

By naming me the first recipient of the Kristian Beckman Award, IFIP TC 11 has paid me the highest complement of my career, that thus far has spanned 55 years. For that honor we are most thankful. I say *we* because I must share this coveted Award with my wife, Esther Harris Highland.

Over a decade ago, when both of us retired from our respective universities, I conceived and we planned a new professional journal, *Computers & Security*. She served as Managing Editor of the Journal for years before her name ever appeared on its masthead. Our then publisher could not envision placing a woman's name on the masthead of any professional journal, especially one in information security.

For almost a decade we worked as a team producing the Journal just as we had for many years earlier worked together in industry and at our universities. It was she who did the final editing [even rewrote many submitted papers, naturally with the author's permission] before those papers were sent to our Editorial Review Board for final judgment. Furthermore, she did all the abstracting and wrote all the copy that appeared in "*Abstracts of Current Literature.*" I often humorously said that she was the best read individual in infosec, reading through more than 120 publications each month.

I must hasten to add that she has never edited my column, "*Random Bits & Bytes*". Nor did she edit this paper. Our experience in having her edit my many books and technical papers precluded her from editing my column or this paper; neither of us wish to get a divorce after 53 years of marriage.

Those who know me are aware that I can prepare a professional, technical paper replete with footnotes. My speech today is less formal -- personal observations and predictions.

Kristian Beckman

Before I continue with my paper I must pay tribute to Kristian Beckman, the first chairman of TC 11. He was a gentle man, a scholar and a visionary. I first met him in Stockholm in 1983, at the birth of TC 11, and we quickly became friends. I was honored to have the Journal I fathered become the official Journal of TC 11.

In the short time we were friends before his untimely death, I was buoyed by his enthusiasm and foresight in information security. He was a great man who should always be remembered for his contribution to information security not only in his country but in the world.

How We Got Here

I fondly recall my early days in computing some 35 years ago, first with an IBM 650 and soon afterwards with an IBM 1620 Model 1. Security was simple -- only authorized users with a key could enter the room that housed the computer to use it. The first signs of security came soon after. Each of us with a key to the computer center could protect his/her programs and data. Each had a large metal card file and there was only one key held by the file's owner.

More than two decades ago I helped build the SITRA computer network in Finland, linking computers in universities as far north as Oulu [near the Arctic Circle] and as far west as Turku [on the coast near Sweden]. The main computer, a Univac 1108, was located in Helsinki. No one bothered with security aside from a simple user ID and password system which was not enforced.

However, today we live in an age of computer insecurity. Today we live in an age in which too many people lie about the status of information security in their organization. Although aware of the shortcomings, they rationalize their lies. Some unfortunately, I have found, even believe their own lies. If you are confused and disturbed about the current state of information security, you are not alone.

It was the use of computers by the military and intelligence agencies in many countries that prompted the growth of information security as we know it today. As computers became more widely used in industry, the computer manufacturers who installed the systems for the military transferred those "security features" to the commercial environment. Few people in industry had any idea of what was needed and relied heavily on the computer manufacturer's specialists to guide them. [I believe that there are some today who have never progressed beyond that era.]

For years information security has been an after-thought, an add-on after a system was designed and installed. Most systems used today in the business world were never designed with security in mind. The failure to develop meaningful computer security measures has to be shared by three communities.

- First there is the academic community. It has always been lax in its acceptance of information security. In the early days we freely exchanged both programs and data. We were an elite community of computer scientists who shared in our effort to promote the use of computers among scholars. Today many feel that even the low level of computer security impinges on their freedom.

I use one of the newer UNIX systems with "advanced security" at one of our local universities. The system will not permit me to use a "weak" password -- my family name or that of the university. But I can use my first name, my home address or the name of my community in which I live. The system prohibits my reuse of a password for 10 times. But the university does not require any user to change his/her password periodically.

- Secondly, the business community, even when it recognized the need for computer security, was unable to really specify its needs. Instead it blindly continued to accept the military model created by the computer manufacturers. It is only within the past decade that the existing model has been seriously challenged. But all there has been is a challenge, *not* a change.

Since I am a network freak, I have access to a very large multi-national company's computer system. The security director prides himself that he requires all users to change passwords on the first Monday of every month. I comply but on Tuesday I, like many others, change the password back to the one I used earlier. There is nothing in the system to prevent the reuse of a recent password nor does the security director make a random check on the reuse of old passwords.

- Thirdly, the military too has been guilty of developing a security model, necessary for them, but unsuitable for the real world. Of course it is not their fault that business has followed blindly. However, their models have been designed as if there is an endless supply of money to build them and then later change or discard them. The problems of human compliance have been overlooked because military protocol and procedure make it easy to overlook human compliance in the outside world.

Although the military network on which I am on generates an eight-character password for me to remember and use, the security director is powerless to prevent anyone from embedding his/her password in a telecommunications program, using macros or sign-on scripts to avoid keyboard entry. Those macros or scripts are *not* protected; they remain in cleartext, readable by anyone who can get to the computer terminal.

Where We're At

Possibly more disturbing to me is the false sense of security in which too many information security directors have wrapped themselves. Today we operate in an environment in which many information security directors feel that they have done their job by issuing a written set of security guidelines and by installing a security package on their systems. Too often the guidelines are not enforced. The security software packages are often installed without a real understanding of the options.

A few years ago I discussed aspects of the password segment of the security packages with a number of infosec directors. Few knew the minimum size password a user can really use. They had been sold a package noting that a six- or eight-character password is used by the system. What they are not told is that many of these systems will accept shorter passwords, even as little as *one* character.

I have also encountered security directors who disclaimed any responsibility for microcomputer security. None of them had any knowledge about microcomputing and had no interest in those "game machines." They left security to the individual user, often people with no professional training or any understanding of the problems involved. Some users did not even make backups. As one user explained, he did not make backups of his stereo tape recordings, so why was it necessary to make backups of his disks.

I often think of a security director of a very large international organization based in Europe who bemoaned the fact that he could not control any microcomputers because those units were purchased by department funds; therefore, they were not part of his corporate responsibility. I also encountered a security director of a major U.S. government agency who would not assume any responsibility for microcomputer security; there were over 2,000 units in his agency. To him those machines were not real computers; he just walked away from the problem.

Even today with the rapid growth of LANs there are too many security directors who are willing to accept the security that is part of the network communications package. They neither recognize nor care that the software developer is a communications specialist with no real understanding of security. How else can one explain a popular LAN package where the default option is set for unlimited attempts to sign-on to the system. It is possible to set a limit but that requires overt action during installation.

Although comprehensive industry data are not readily available, I believe that the turn-over rate for computer security specialists is higher than for any other group of computer specialists.

- A Deloitte-Touche study in 1990 indicated that directors of information security in the U.S. have an average tenure of three years. And a third of these did not leave *voluntarily*.

- Several years ago Bob Courtney, the *dean* of computer security who served for many years as IBM's interface with U.S. government agencies, noted that the average tenure of computer security specialists in these agencies is about *seven months*. I doubt that it has changed much since then.

There appears to be a constant stream of new entrants into this field. Unfortunately from a technical viewpoint, the average member of the infosec community has only, what I call, *catalogue knowledge*. Their knowledge is based on [1] literature they receive from vendors, [2] information (often incomplete and at times inaccurate) they receive from colleagues, and [3] a smattering they remember from reading articles in computer publications or attending computer security conferences. Too many do not have the time, and some unfortunately do not have the backgrounds, to learn much beyond the security buzzwords.

Generally they know about risk analysis, contingency planning, access control, audit trails. Some have heard about the *Clark-Wilson Integrity Model* and its superiority over *The Orange Book* or even *ITSEC*. Some have somewhere heard about baseline security concepts. Others read about the utopia promised by biometrics. Some might know the difference between FIPS and IFIPS, between TCSEC and ITSEC, and even between CHIPS and CHAPS. Some probably even know the details about the *Bell La Pudula* model. Others are even versed in DES transposition and substitution along with P-boxes and S-boxes.

Even in the best of times, information security has never been more than temporary. The more one studies attempted solutions to security, the more one has the impression of well-meaning, often gifted, people wearing out their ingenuity at an impossible task. They are trying to get information security in neat and permanent packages without regard to their interaction with the human element.

It's Time for a Change

For more than a decade since my retirement from the university, I have meet hundred, perhaps thousands, of security directors and consultants in business, industry, government and even the military/intelligences agencies from all parts of the world. Over the years some of them have become close friends. All of them have a difficult, and often frustrating, administrative jobs. Some are capable, knowledgeable, dedicated administrators.

The information technology explosion of the past several years makes it necessary to radically change our concepts, principles and implementation of information security. There is a new base of infosec knowledge.

As we are all aware, information security has concentrated on hardware and software over the past few decades. The results have been far from heartening. There are some who can point to great advances during that time frame. Yes, we have advanced somewhat, but as a pessimist, I find that it has been too little and too slow.

All of us have heard top management blamed for our inability to implement a meaningful infosec program. Top management too often looks at infosec as a necessary encumbrance, something akin to paying taxes or insurance premiums. They see many of the proposed infosec measures as procedures that reduce worker productivity. Too many infosec directors are living in the past embracing mainframe concepts and procedures which cannot work in today's workplace where old ethics and values have been eroded.

Blame is also placed on the lack of adequate infosec background of some working in this field. Many of our early infosec directors had military or police experience. Most organizations have inadequate guidelines for selecting anyone in information security. When an organization wishes to hire a programmer they seek someone with programming training and/or experience. Few schools in the past have offered any courses in computer security.

Some 20 years ago when I introduced a course in computer security and cryptography, my course graduates were easily placed in infosec positions in the aerospace and electronics industries on Long Island. But they had something *extra* in their education. All advanced courses in our department emphasized interaction with others. We used our students to assist in teaching elements of computing to business, engineering, science and health services majors.

There is a move in the U.S. and Canada to introduce certification of infosec specialists. It is not the first such attempt and it may not be the last. What is ? Is it possible to produce a common core of information security that is meaningfully worded? Consider an element that states that "there should be an adequate password system in place." What is *adequate*? About a decade ago a European commission attempted to produce a dictionary of infosec terms in three languages. There were many definitions in English, but German and French translations could not be agreed upon. The section on privacy was most interesting. There were German and French definitions but none in English.

I have been involved with various certification programs [accreditation of colleges, approval of new courses in computing, certification of nurses and other health

professionals, certification of data processing teachers at two-year colleges] for more than 30 years. I have seen accreditation in several so-called professional fields where it is nothing more than self aggrandizement. Too often it reflect the action of a small group with similar interests who feel that holding a certificate of accreditation proclaims them as specialists. I have seen accreditation used to support commercial companies who conduct conferences make money because certified members have to keep up to date.

A certification program is effective in an area where there is a true body of scientific knowledge. Information security today, I feel, is more an art than a science. If we are going to experiment in this area, I would be happier if an accreditation program were requested by a group of Fortune 1000 companies and government agencies. Furthermore, the program should be organized and controlled by *all* the *major*, large-membership computing organizations and not by a self-appointed committee of a few sponsored by smaller organizations.

As chairman of IFIP WG11.8 on infosec education, I am aware of an increasing number of universities that are offering courses in information security. Some are offering even graduate degrees in the field. Chances are that these graduates will join professional computer societies. They will see little need for certification; they knowledgeable base will be greater and better than many who hold certificates.

Where We Are Going

We are living in an age of *universal computing* -- a world in which a personal computer - one used by a single individual, whether it be a terminal, a micro, a laptop or a notebook computer - will be ubiquitous. Practically all of the users will have no formal computer education or training. Their terminals/microcomputers will replace their typewriters, adding machines, and record books, just as the computer replaced the engineer's slide rule.

We may not reach the *paperless office*, if ever, but certain changes will impact on the infosec director's duties and responsibilities. Although politicians and government officials are reluctant to acknowledge it, the ratio of the number of people employed in office work to the volume of work performed will be greatly reduced. An efficient review of document handling is long overdue. Those companies that have done so have been amazed to discover how many unnecessary places and hands these documents pass through.

Added to this change is the growing awareness among the public, users, attorneys and infosec specialists, of a number of key issues and/or problems. These include privacy, confidentiality and property rights, data integrity and computer user responsibility. It also includes computer ethics, hacking and computer viruses.

If we are to succeed in developing effective infosec programs, we can no longer overlook today's most important component in information security -- *wetware*. This is the term used for about a decade to refer to the human brain, possibly because it is moist when removed from the cranium. It is the term used by neuroscientists to differentiate the working of the human mind from the software used by computers. It is one factor that must play a greater role in the future.

In the past, and even today, infosec specialists ignore the individuals except for their interaction with security software and hardware. Today we try to solve the problems of human interaction with icons and pull-down screens -- gimmicks that really do not address the problem. Human compliance with infosec rules requires an understanding of how people work and think. The old ethics of the workplace are gone. Maybe we need communications specialists and psychologists in place of infosec directors.

The World To Come

We are in the midst of a great transformation in the role of the infosec director. This transition started several years ago, unnoticed by some, resisted by others. We are in a user environment and to perform the information security task, we will have to redefine the infosec director's role.

Aeons ago I made my living as an analyst and forecaster. In 1945 I wrote about the future of the aircraft industry and the airlines. My forecast of larger planes and the manyfold increase in air traffic to carry passengers and freight was derided by many airline officials. In the mid 1950s my forecast of the role of television and audio visual equipment in schools was considered utopian, but we surpassed my predictions more than a decade ago.

I stuck my neck out many times before and will do so again now. This time there is a difference -- I am on safer ground. At the age of 76, I won't be around in twenty years from now for anyone to tell me that I was wrong.

1. The InfoSec Director's Role Will Be Different

- The infosec director will *share* his/her duties, and to some extent responsibilities, with others -- the many LAN managers, the telecommunications manager, head of main- and/or mini-computer operations, director of programming, input data manager, etc. Yet, despite the sharing he/she will have final responsibility.

- The infosec director will be both a supervisor and a coordinator. It may be difficult to get the technical heads of computer personnel in operations and the heads of telecommunications not only to understand the need for security but to carry out the security policies and practices. It will be even more difficult to get LAN managers, many without any professional computer training or knowledge of security, to do the same.

- The infosec director will also be a teacher. As the team leader he/she will have to provide leadership, guidance and education of his team members. Unlike the military where orders can be issued from the top down, the security director will have to cajole, to entreat, to play father and mother to assist the members of his team in the education of their users.

- Much more attention will be paid to the human side of security management. We must recognize that we are dealing with a new generation of users and must adapt our educational programs. Most current and new users have a *Sesame Street approach* to learning -- snapshot capsules that change frequently; their attention span is short. There will be a greater and better supply of security awareness training aids to assist the infosec director. These aids -- with more emphasis on multimedia material for the PC -- will be far better than the pap available today. Some of the current material reminds me of the military films shown to troops during World War II to warn them about venereal disease.

2. Some Current Security Problems Will May Disappear

Changes in technology will reduce and may even eliminate some of the problems faced today. At the same time new problems will emerge.

- Data transmitted within an organization, whether over LANs or telecommunications networks, will be automatically and transparently *encrypted*, but key management problems will not go away. Newer solutions will have to be developed.

- The possible threats to cellular communications and wireless LAN transmission will still remain, albeit not as great as today.

- The proposed U.S. Capstone encryption algorithm does not appear to offer an acceptable solution. Within days of its announcement our bulletin boards have been filled with suggested ways to attack the keys. The response from the professional and business communities to the proposed chip has been greater and faster than it was years ago when the DES was proposed. There are many more encryption "specialists" today than in 1977 and they are more critical.

- The backup of data files will be automated and will be transparent to the user. We have the technology today but not widely used. It will be improved and more readily

used in the future. Currently, every data file I close on my Compaq 486/66M is automatically written to a floptical disk drive attached externally to my system. It could easily be located in another room or sent to a site many miles away.

3. Some Security Problems Will Not Go Away

- Computer viruses will not go away. Virus writers have perfected their skills and even now produce viruses that cannot be detected by most anti-virus scanners on the market. The attempt to include anti-virus software in MS DOS 6.0 is a disaster; it appears to be an earlier version of that used by Central Point. Some virus writers have already produce viruses targeted to penetrate that software, which wasn't so great in the first place.

- More companies will establish definitive policies and procedures to reduce the threat of a virus attack. Their success will depend on their enforcing sanctions against policy and procedure violators. Also in the future there will be more reliance on integrity programs in order to combat viruses.

- Hackers will never die! They will always remain a threat. They will always be challenged to attack newer methods of access control. But they will be less likely to succeed. I recently tested a product that keeps any unauthorized machine from accessing a LAN server. Any attempt to access a server with an *unauthorized* machine makes it impossible for the attacker to obtain a sign-on screen.

- Because the law fails to keep up with technology we will still be faced by the many problems of individual privacy rights in the workplace. Even though safeguards to protect privacy of data files will be improved, that threat will continue.

4. InfoSec Will Be Part of Corporate Risk Management

- The security director will be part of a risk team head by the corporate risk director, who will be responsible for financial, environmental, occupational safety, operational disaster, insurance, etc. The corporate risk director most likely will have a legal and/or insurance background and "selling" that director will probably require the greater use of models, more detailed statistical analysis and a reliance on mathematical cost-benefit analysis, something which is foreign to most infosec directors today.

Postscript

For those who feel that some of the changes I noted are unattainable or unrealistic, I must note that I was around decades ago when we tried to get top management to accept modern mathematical analysis. These techniques were made possible by the computer -- break-even analysis, linear programming, modeling and simulation, non-parametric sampling, game theory. Over the years as the older top managers retired or died, the newer ones, trained in these areas, readily accepted them. By the year 2013 top management in business and government will not only readily accept integrated information security but will *insist* on it.

Dr. Harold Joseph Highland retired in 1980 from the State University of New York's Technical College at Farmingdale with the rank of Distinguished Professor Emeritus. He created and acted as Editor-in-Chief of *Computers & Security*, the official journal of IFIP TC 11 until 1990 when he became Editor-in-Chief Emeritus. Professor Highland also serves as Managing Director of Comuplit, Inc. and is head of its Microcomputer Security Laboratory. His mail address is 562 Croydon Road, Elmont, NY 11003-2814. He can be reached by electronic mail at: Highland@dockmaster.ncsc.mil or Highland@ACM.org.

Dr. Highland was named a Fellow of the Irish Computer Society in 1985. As a member of the Association for Computing Machinery [ACM] for well almost 30 years, he had been active in SIGSIM, SIGMETRICS and SIGSAC. He is also a member of the New York Academy of Science [NYAS], the Institute for Electrical and Electronic Engineer's Computer Society [IEEE/CS], the Information Systems Security Association [ISSA], the international Computer Anti-Virus Research Organization [CARO], the American Association for the Advancement of Science [AAAS], Computer Professionals for Social Responsibility [CPSR], and the Society for Basic Irreproducible Research.

Additional biographical data are available in *Who's Who in America*, *Who's Who in Science and Technology*, and *Who's Who in Education*.