Computer and Communications

Security Reviews

Volume 3 Number 1 (March 1994) ISSN 1352-6278

CONTENTS

This journal reviews research in computer and communications security. Work published in major journals and conferences is covered automatically; local publications (such as research reports) should be sent to the editor, care of the University Computer Laboratory, Pembroke Street, Cambridge CB2 3QG, United Kingdom.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 28 February 1994; and books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Crypto 93: 22-26/8/93, Santa Barbara, California; *proceedings are v 773, Lecture Notes in Computer Science*; we review two papers which were not covered in volume 2 number 4

NCSC 93: 16th National Computer Security Conference, 20-23/9/93, Baltimore, *proceedings published by NIST*

SITA 93: 16th Symposium on Information Theory and Its Applications, 19-22/10/93, Kanazawa, Japan, *Proceedings published by IEEE Tokyo Chapter*

Fairfax 93: 1st ACM Conference on Computer and Communications Security, 3-5/11/93, Fairfax, Virginia *Proceedings published by the ACM - ISBN 0-89791-629-8*

Security Applications 93: Ninth Annual Computer Security Applications Conference, 6-10/12/93, Orlando, Florida *Proceedings published by the IEEE - ISBN 0-8186-4330-7*

SCIS 94: 1994 Symposium on Cryptography and Information Security, 27-29/1/94 Lake Biwa, Japan; *proceedings published by the Institute of Electronics, Information and Communication Engineers*; not all papers had been abstracted by press time

We regret that copyright laws prevent us from supplying copies of articles reviewed in this journal.

Statutory Information

'Computer and Communications Security Reviews' is published quarterly by, and is copyright of Northgate Consultants Ltd, whose registered office is:

Northgate Consultants Ltd
Ivy Dene, Lode Fen
Lode, Cambridgeshire,
United Kingdom CB5 9HF

Subscription rates, conditions and ordering details are on the inside back cover.

1 Applications and Engineering

031101 'Banks resist signature option'
NR Achs, *Cards International no 102 (21/1/94) p 2*

A row is developing among MasterCard members over whether banks which use PINs with debit cards should have to accept signatures as well, especially from other banks' customers. This dispute arose out of the MasterCard/Europay alliance because there are very few PIN pads in UK eftpos locations. VISA, on the other hand, differentiates its PIN and signature based products.

031102 'A Methodology for the Use of Single Level RDBMS Software in a Multi-level Secured System'
MO Aldritch, *Security Applications 93 pp 11 - 20*

The US military's Reserve Component Automation System uses a single level database running on a multilevel platform; this is a common enough design due to the lack of multilevel software products. It is also large, with over 10,000 systems running Unix on both Intel and MIPS based CPUs, and providing office automation as well as the military application. The designers set out to reduce the amount of trusted code, and exclude it altogether from the application; it ended up as application support software, where it mediates between the item granularity of the RDBMS and the file granularity of the compartmented mode workstations which access it. It also shields application programmers from having to know SQL or X-windows in detail.

031103 'Why Cryptosystems Fail'
RJ Anderson, *Fairfax 93 pp 215 - 227*

The author presents a survey of how cryptographic systems used in retail banking have been defeated by criminals. This information was gathered in the context of court cases in the UK; it showed that the conventional crypto threat model was wrong. The actual attacks were not really technical in nature, even although plenty loopholes existed; they were rather the result of the banks' own blunders in implementing and operating their ATMs and supporting systems; dozens of examples are given. The evaluated product list approach to security engineering is criticised for being largely irrelevant to real needs, and it is suggested that security practitioners' first priority should be better software engineering practices; in particular, many lessons can be learned from the safety critical systems community.

031104 'Fake's Progress'
D Austin, *Banking Technology (Dec 93/Jan 94) pp 25 - 26*

Counterfeiting accounted for 5% of UK card losses last year, and the problem is growing. Card verification values are being introduced worldwide, starting in the UK; customs officers have been supplied with card readers to check whether suspects' card magnetic strip and embossed details are the same.

031105 'Pointing the finger'
D Austin, *Banking Technology (Dec 93/Jan 94) pp 20 - 24*

Card fraud losses have recently fallen in the UK; the most important factor was an increase in online authorisation, although secure card delivery also plays a role. At 0.15%, losses are close to the international average, but above the levels achieved in the US, in Spain (which has fully online authorisation), and in France (which uses smartcards). Watermark cards are being tried out by two banks in Northampton.

031106 'Fighting the war against fraud'
Banking World v 12 no 3 (Mar 94) pp 28 - 30

Card fraud losses were down slightly last year in the UK. In the medium term, a national hot card list will be in place by 1996; and tamper resistant magnetic strip technologies are being considered, together with biometrics and smartcards, for a long term solution.

031107 'SWIFT rolls out security package'
Banking World v 12 no 3 (Mar 94) pp 31 - 33

During 1994, four thousand banks will be installing smart card readers to upgrade the security of SWIFT. The cards will control user logon and manage the authentication keys.

031108 'A Prototype Distributed Audit System'
D Banning, *NCSC 93 pp 146 - 154*

A prototype distributed audit system was developed for networks of heterogeneous systems. It is based on the ISO network management standard CMIS/CMIP, and creates an auditing Management Information Base (MIB) to extend the MIB used for general network management. While the need to protect audit data in transit and authentication between hosts was recognized, neither the architecture nor the prototype built to demonstrate the architecture includes any mechanism yet to secure the audit data. The prototype supports Unix systems only, and includes a graphical user interface for use by the audit administrator. Audit data is gathered exclusively from existing system databases on client machines.

031109 'Administration of Access Rights in a Multi-Vendor System - A Case History'
LJ Becker, CA LaBarge, WS Buonanni, *NCSC 93 pp 129-136*

The US Defense Mapping Agency buys equipment from a number of vendors, each of whom proposes access control methods that are sometimes subtly, and sometimes greatly, different from their competitors'. This leads to problems for the customer, whose experience building a distributed multi-vendor system is described.

031110 'A Cryptographic File System for Unix'
M Blaze, *Fairfax 93 pp 9 - 16*

AT&T Bell Labs has developed software to do transparent encryption of Unix files. It operates at the file system interface, and uses DES in a novel combination of OFB and ECB modes to allow random access. The effect is a virtual file system, which, once activated by a directory key, is transparent to applications. Performance data for an NFS implementation are given.

031111 'Modelling Constructs for Describing a Complex System-of-Systems'
DJ Bodeau, FN Chase, *Security Applications 93 pp 140 - 148*

This article describes a tool developed by Mitre called Analysis of Networked Systems Security Risks (ANSSR), which has been extended to cover multiple systems connected via a common backbone.

031112 'Integration of Security Services into the NORAD/USSPACECOM Technical Infrastructure: A Case Study'
DJ Bodeau, V Swarup, *Security Applications 93 pp 1 - 10*

This system, N/U TI, provides a structure for military application developers which defines application programming interfaces and system services ranging from CASE through transaction processing, and access management to audit, and defines interfaces to hardware security functions. Its goal is to simplify the replacement of legacy systems by providing a reference model from which the needed services can be selected, with some hope that different applications' security services will then be compatible.

031113 'Special Report - GSM Security'
C Brookson, *Information Security Monitor v 9 no 1 (Dec 93) pp 5 - 6*

The GSM security measures were designed to make the radio path as secure as the fixed network, to prevent billing fraud, and to stop operators compromising each others' security. There are two encryption algorithms in use, A5/1 for COCOM countries and A5/2 elsewhere; their secrecy is considered important, but some of the other technical security measures are outlined.

031114 'Cryptographic Application Programming Interfaces'
W Caelli, I Graham, L O'Connor, *Computers and Security v 12 no 7 (Nov 93) pp 640 - 645*

Current crypto interfaces are vendor dependent, and the authors argue that it is premature to start standardising them yet; the main problem lies in key management, and in particular how one imports, exports, labels, addresses and describes keys. The security properties of these operations are very complex, and interact with host security mechanisms such as reference monitors and object managers in unexpected ways.

031115 'Representation of Mental Health Application Access Policy in a Monotonic Mode'

C Calvelli, V Varadharajan, *Security Applications 93 pp 195 - 209*

The authors describe and model the access rules needed to control patient records in a psychiatric hospital. They show how to implement them using revocation tickets, which give the holder the right to revoke another party's access. The issues involved in managing these, together with conditional and temporary access rights, are explored; there are some problems where the requirements are non-monotonic.

031116 'MasterCard set to combat fraud'

Cards International no 103 (3/2/94) p 6

This article describes MasterCard's new security features, which are supposed to reduce counterfeiting losses by $35m a year. They include a tamper-evident signature panel containing the account number, and two cryptographically derived check values of which one is encoded in the magnetic strip and the other printed on the signature panel.

031117 'Northern lights shine brightly'

Cards International no 103 (3/2/94) pp 12 - 15

This survey of the bank card industry in Scandinavia covers a smart card system which is about to be moved from pilot applications to production in Finland, and another which is in use for small payments in Denmark.

031118 'Labeled Quadtrees: Security and Geographical Information Systems'

ME Carson, M Ranganathan, *NCSC 93 pp 377 - 384*

The authors describe how multilevel security mechanisms can be integrated into geographical databases, so that, for example, detailed road maps of military areas are only available to cleared users. They describe an IBM prototype which uses quadtrees to organise spatial information in such a way that classification levels can operate with different granularity in different places.

031119 'Special Report - PBX Trunk Fraud'

JB Condat, *Information Security Monitor v 9 no 3 (Feb 94) pp 5 - 7*

Toll fraud now costs French companies $220 million a year; villains get access codes for commercial PBXs and sell long-distance calls through them. In order to prevent this, companies should restrict facilities to those which they really need and monitor their usage carefully.

031120 'A Practical Application of Commercial-Off-The-Shelf Products to the Automated Information Systems Security of the NASA Johnson Space Center Control Center Complex'

JW Coyne, *NCSC 93 pp 210 - 215*

This paper describes practical experience in the composition of evaluated components. One aim was to minimise the amount of custom-written software, using commercial products instead. The work described was a proof of concept; as this resulted in a favourable report it seems likely that NASA will adopt the products tested.

031121 'Button Up Your LAN Security'

Datamation 1/2/94 pp 59 - 60

This article describes a Dallas Semiconductor access token called SignOn which can be used with NetWare. Token readers are attached to the PC's parallel port.

031122 'BApasswd: A New Proactive Password Checker'

C Davies, R Ganesan, *NCSC 93 pp 1 - 15*

Most Unix systems are vulnerable to password guessing attacks, so it is advisable to check that user password choices are not in the dictionary or otherwise easily guessable. Previous password checkers used a lot of storage for dictionaries; BApasswd gets round this problem by modelling language as a Markov process on trigrams. Empirical trials are reported; as the system explains why passwords are rejected, users quickly learn to choose good ones.

031123 'C2 Auditing in the X Display Manager'
J DeMeester, *Security Applications 93 pp 265 - 271*

Sun's C2 enhancement of SunOS greatly improves audit functions, but is not completely compatible with X Display Manager. Integrating the two involves modifying the login procedures.

031124 'User Interface for a High Assurance Windowing System'
J Epstein, R Pascale, *Security Applications 93 pp 256 - 264*

The authors describe TRW's Trusted X prototype secure windowing system and discuss the design decisions which led to it. It runs one instance of X Windows per sensitivity label, and, apart from a TMach shell, its trusted code is essentially limited to the input and display managers and the property escalator (which allows users to cut and paste from a lower level to a higher one). The trusted code is only 8K statements - much less than in a typical compartmented mode workstation. Trusted path functions are described in some detail, as is window management, which presents some novel covert (and overt) channel problems.

031125 'Securing your money - a focus on money transmission'
G Edwards, *Financial Technology Insight (Jan 94) pp 5 - 11*

Real frauds against high-value payment systems such as SWIFT and CHAPS have involved either counterfeit input paperwork or manipulation of the feeder system which passes payment messages to and from the trusted network; a number of variants on these themes are described. Best industry practice involves a number of controls, which include mechanisms (such as MACs on feeder system messages) and management (such as putting the system administrator in a different department from the one which carries out payments).

031126 'Smart Card Tutorial - Part 18'
D Everett, *Smart Card News v 3 no 2 (Feb 94) pp 34 - 38*

The author provides an overview of the security mechanisms used in smart card payment systems to pass value from the purse provider, to the purse holder, to the service provider, and back to the purse provider. He describes the challenges, responses, payment and accounting messages in a hypothetical system.

031127 'EDI and Payment Risk'
Financial Technology Insight (Jan 94) pp 17 - 19

This article provides statistics of interbank payments in the US and the UK; fraud or system failure could strike in a number of ways, including indirectly through industry netting arrangements such as that operated by London insurance firms.

031128 'Banks roll out multimedia pilot'
Financial Technology International Bulletin v 11 no 5 (Jan 94) p 1 and p 12

Barclays in the UK has teamed up with Sao Paolo Bank from Italy to develop multimedia retailing kiosks, at which customers will be able to use smartcards to buy cars, furniture and other goods as well as financial products.

031129 'Post office automates benefit payments'
Financial Technology International Bulletin v 11 no 4 pp 5 - 6

The UK post office is spending $20m on installing 8000 terminals which can read smartcards. One goal is to cut social security benefit fraud; another is to capture data from customer payments to utilities, which will be invited to issue compatible cards to their customers.

031130 'Post office puts automatic signature verification on public trial'
Financial Technology International Bulletin v 11 no 5 (Jan 94) p 6

The UK post office is conducting a field trial in Southampton of an automatic signature verification system developed by the University of Kent. Its novel feature is that it is used to screen signatures and support human decisions rather than to take decisions itself; this means that instead of being set for a low insult rate, with a correspondingly high fraud rate, it has fraud and insult rates approximately equal; and when a signature is rejected, this merely tells the staff to look more closely.

031131 'Security Conscious'
J Goodman, *Computer Weekly 3 February 1994 pp 36 - 37*

This article describes the system used by the British prison service to record the names, offences and release dates of all inmates. It runs on Unix processors situated in the prisons, with a central server. Despite various security measures, no prisoner is released without reference to a paper warrant.

031132 'Message Handling Systems (X.400) Threats, Vulnerabilities, and Countermeasures'
MJ Gosselin, *NCSC 93 pp 226 - 235*

The introduction of standards such as X.400 aids interoperability between disparate systems but may introduce new security threats. The paper explains some of the deficiencies in X.400.

031133 'Security and Auditability of Electronic Vote Tabulation Systems: One Vendor's Perspective'
GL Greenhaigh, *NCSC 93 pp 483 - 489*

The US market for automated voting systems is both conservative and small, with sales usually less than $10m per annum. The Federal Election Commission has published standards, but these are voluntary and have some inadequacies which are described. It is suggested that an independent institute be set up to develop standards, certify equipment, keep software in escrow, and provide technical support to local officials.

031134 'Improving LAN security and auditing Novell NetWare Version 5.0'
WR Hampton, *Computer Security Journal v 9 no 2 (Fall 93) pp 37 - 47*

This paper presents an architectural overview of NetWare, describes traditional LAN security vulnerabilities, and discusses the alternatives offered by NetWare 5.0 controls as well as by other general technical and managerial control techniques.

031135 'Radio Intelligence and Communication Security'
J Halliyan, *Cryptologia v XVIII no 1 (Jan 94) pp 52 - 79*

This article contains declassified US Navy reports from circa 1930 on the crypto capability of other countries. These include a 1924 Swedish assessment of British naval signals during the first world war.

031136 'The Phantom Tollbooth'
P Harrop, *IEE Review v 20 no 1 (Jan 94) pp 31 - 34*

Over $500m per year is being spent worldwide on developing road toll collection systems. These are used to charge for transit, parking and congestion; most use microwave interrogation of a transponder in the vehicle window, and many use a smartcard to store user value. A number of fielded systems are described, and the various design tradeoffs are discussed.

031137 'A New Scheme on Efficient Scrambling for Color image'
R Hayun, *SCIS 94 paper 7B*

The author point out that for pay-TV applications it is enough to scramble the picture to the point where it is unacceptable for leisure viewing; it is not necessary to ensure that no residual picture is visible. He proposes scrambling either the luminance or colour signal of NTSC, by interchanging some subset of lines and some subset of pixels. The memory requirements and delay times are analysed.

031138 'I Worked with Murphy'
EB Heinlein, *Computers and Security v 12 no 7 (Nov 93) pp 627 - 628*

The author recalls working with the originator of Murphy's law on an early missile guidance system design. The experience highlighted the importance of covering 'don't care' conditions, which being ignored often lead to software problems, and of building contingency plans into systems to allow recovery from anticipated faults.

031139 'Windows NT: How good is the security of Microsoft's newest operating system?'
G Hyatt, *Computer Security Journal v 9 no 2 (Fall 93) pp 1 - 11*

In this article the authors discuss Microsoft's Windows NT operating system and the security it offers. It covers the C2 level evaluation that Microsoft seeks and the security features that involve object oriented security, access control, and domains.

031140 'Pink Death Strikes at US West Cellular'
Information Security Monitor v 9 no 2 (Jan 94) pp 1 - 2

Cellular phone fraud is now an industry costing $100 - 200m a year, and some of the techniques are described; some illegal phones even change their user ids every few minutes. US West Cellular is using pattern analysis techniques to pinpoint suspect calls.

031141 'Open systems needn't be'
M Johnson, *Computer Fraud and Security Bulletin (Mar 94) pp 8 - 19*

The author discusses the security implications of downsizing, and discusses a number of products used in high availability Unix clusters with mirrored disks and high availability communications. Many Unix systems can achieve the same C2 level as RACF, and have the advantage that corporate information security policies can be implemented more consistently on compatible platforms. CA-Unicenter and Oracle 7 are discussed in particular.

031142 'Japanese skills harnessed for Mondex'
D Jones, *Banking World v 12 no 3 (Mar 94) p 36*

This article describes the consortium of companies behind the new Mondex product; it includes Matsushita, Oki and Dainippon.

031143 'System for the recognition of human faces'
MS Kamel, HC Shen, AKC Wong, RI Campeanu, *IBM Systems Journal v 32 no 2 (1993) pp 307 - 320*

This article describes an experimental IBM system to match a face with a set stored on a database. It has algorithms to recognise gross features, work out head orientation, and encode the relative feature distances. These encoded representations are searched using knowledge refinement techniques; each time a new face is added, it is compared with all those in the existing database to tune the search algorithm. Test results show that the system works much better than holistic methods such as neural networks.

031144 'Heterogeneous Workstation to STU-III Prototype'
EM Kayden, LJ Schaefer, *Security Applications 93 pp 100 - 107*

The authors describe integrating trusted XENIX with a STU-III encryption device by providing a mapping between the two technologies' security attributes at various levels. They also discuss lessons learned during the project.

031145 'Securing a Global Village and its Resources: Baseline Security for Interconnected Signaling System # 7 Telecommunications Networks'
HM Kluepfel, *Fairfax 93 pp 195 - 212*

The author relates Bellcore's experience of the security weaknesses of SS7 switching systems, which use packetised out-of-band signals. He discusses a number of outages and concludes that most of the problems can be solved by exploiting existing security features and auditing known loopholes. He provides extremely extensive checklists for this. Enhanced user authentication techniques may be deployed in future.

031146 'Police Information Technology'
C Lewis, *GEC Review v 9 no 1 (93) pp 51 - 58*
The author describes how GEC adapted its military C^3I skills to build a business developing criminal intelligence systems for UK and overseas police forces.

031147 'Associations set smart standards'
R Martin, *Cards International no 99 (9/12/93) pp 1 - 2*
VISA, MasterCard and Europay have agreed to develop common standards for interoperable smartcards. Banks in Germany and Belgium have decided to use smartcards; other organisations may use them for specialised purposes.

031148 'Neural networks: the way forward?'
R Martin, *Cards International no 99 (9/12/93) p 9*
Neural networks are in use to detect abnormal card transactions in Mellon Bank and the Eurocard Netherlands network, and both claimed that the system would pay for itself in 1-2 years.

031149 'Banks ready to do business with smart cards'
H McKenzie, D Austin, *Banking Technology v 11 no 1 (Feb 94) p 4*
Smartcards are finally becoming an option in the world of finance outside France, with Mondex in the UK, an AT&T/Chemical Bank initiative in the USA, and various agreements between interbank organisations.

031150 'Threats to Suffrage Security'
R Mercuri, *NCSC 93 pp 474 - 477*
US voting systems are exempt from the Computer Security Act, despite known sources of potential error and abuse. The responsible local agencies have largely ignored the advice available from NIST and NCSC.

031151 'Vital Signs of Security'
B Miller, *IEEE Spectrum (Feb 94) pp 22 - 30*
The theory and practice of biometric identification is surveyed. This is now a $12m market, and a number of applications are described: fingerprint scanners are used in the Pentagon, and by Los Angeles county to identify welfare recipients; hand shape recognisers are used in 4000 locations, including by US immigration at some airports; voice recognition is used for access control and telephone services; face recognition is at the trials stage; and both signature dynamics and typing rhythms are already in use.

031152 'Smart card travels south'
F Mollett, *Cards International no 102 (21/1/94) pp 13 - 14*
Portuguese banks are overhauling their ATM/POS network in preparation for the introduction of smartcard-based electronic purses later this year. These will be targeted at young people, for whom conventional cards are considered inappropriate, and will be used to pay for school buses and lunches as well as ATM withdrawals. The cost will be paid by the banks out of the float generated.

031153 'Denial of Service'
RM Needham, *Fairfax 93 pp 151 - 153*
Denial of service attacks have received relatively little attention in the literature, yet burglar alarms provide a good example of a system to which they are the main threat: the central server must never think that the alarm is sending an 'all's well' signal when this is not the case. End-to-end protection is best, and messages in the network should be anonymous as far as possible; this keeps the network itself outside the trust envelope.

031154 'Security Criteria for Electronic Voting'
PG Neumann, *NCSC 93 pp 478 - 482*
The author sets out the technical requirements for electronic voting systems and discusses a number of the ways in which electronic elections can be subverted. Sometimes there seems to

be a conflict of requirements, such as between voter anonymity and end-to-end monitoring; and the mechanisms which could resolve such conflicts introduce new sources of complexity and thus of potential error. Even with honest developers and vigilant operators, some residual risks are inevitable.

031155 'A methodology for improving computer access security'
MS Obaidat, *Computers and Security v 12 no 7 (Nov 93) pp 657 - 662*

The author tested five pattern recognition algorithms on identifying users by their typing patterns. Each of 6 users typed 15 characters 40 times, and the interkey times were classified using k-means, Bayes' rule, Euclidean distance, cosine measure and potential functions. The best were potential functions and Bayes' rule in that order, but both of them took over 12 trials to converge.

031156 'EDIFACT security made simple - the EDIMED approach'
J Ølnes, *Computers and Security v 12 no 8 (Dec 93) pp 765 - 774*

Norwegian researchers have developed a secure EDI protocol to exchange health care information via X.400 electronic mail. It uses end-to-end DES encryption with manual key exchange; public key encryption was ruled out due to the number of doctors with elderly PCs.

031157 'Data-security, use misuse and abuse'
A Pauli, *De Vonk v 12 no 3 (Nov 93) pp 7 - 15 (in Dutch)*

This article, which introduces a one-day seminar held at the University of Twente in the Netherlands, reviews the debate over phantom withdrawals from autoteller machines. It presents the views of a number of experts, and the experiences of a number of victims of ATM fraud.

031158 'PC access products: how good are they?'
A Rodgers, HB Wolfe, *Computer Fraud and Security Bulletin (Feb 94) pp 10 - 13*

The authors report tests of 5 PC security products, which are unfortunately not named. Some could be trivially bypassed; others were hard to install or had suspect encryption mechanisms.

031159 'An Integrity Model is Needed for Computerised Voting and Similar Systems'
RG Saltman, *NCSC 93 pp 471 - 473*

The author describes the history and technology of automated voting in the USA: lever machines and other machine-readable ballots are being replaced with direct entry on touch-screen and other devices, but the lack of security standards causes some concern.

031160 'Migrating a Commercial-off-the-shelf Application to a Multilevel Secure System'
R Schultz, T Ehrsam, *Security Applications 93 pp 21 - 28*

The authors describe adapting a software product, C-Gate, to a multilevel operating system. The product is designed to facilitate the flow of engineering drawings, parts lists and the like among US defence suppliers; it must cope with very complex security inheritance properties, as there can be 'secret' parts in 'unclassified' systems. One lesson was that coping with the multilevel aspects can have a serious effect on portability.

031161 'OS/2: Open System to Everyone?'
SP Sims, *Info Security News v 5 no 1 (Jan 94) pp 19 - 22*

The authors discuss the security of the OS/2 operating system, and the improvements offered by two commercial security packages: OS/2 High Performance File System and Local Security, and Microsoft LAN Manager.

031162 'Contingency/Disaster Recovery Planning for Transmission Systems of the Defense Information Systems Network'
DR Smith, WJ Cybrowski, F Zawislan, D Arnstein, AD Dayton, TD Studwell, *IEEE Proceedings on Selected Areas in Communications v 12 no 1 (Jan 94) pp 13 - 22*

The authors describe the US Defense Information Systems Network (DISN), and consider the various hostile and other threats to the service it provides. The ability to set up networks quickly, such as in Desert Storm, has a lot in common with the ability to reconstitute a network after a failure. DISN's service level objectives are described, as are its management hierarchy, problem areas and current recovery strategies. Finally, the authors recommend various improvements.

031163 'A Particular Solution to Provide Secure Communications in an Ethernet Environment'
M Soriano, J Forné, F Recacha, JL Melús, *Fairfax 93 pp 17 - 25*
The authors describe an Ethernet encryption device, the 'Cryptonet', which was developed at the Polytechnic University of Catalonia. It provides a secure bridge, based on RSA and DES, between LANs; the construction and protocols are described, and performance figures are given.

031164 'Security Services for Multimedia Conferencing'
SG Stubblebine, *NCSC 93 pp 391 - 395*
The security requirements for multimedia conferences are not limited to the traditional ones of confidentiality, integrity and availability, but can entail much more complex properties. Examples are anonymous voting, and the ability to ensure that people from different companies should communicate only via the main conference rather than in private side conversations.

031165 'Specification Issues of Secure Systems'
MR Sweezey, *Security Applications 93 pp 36 - 45*
The author describes the system used by the US Space Defense Operations Center at Colorado Springs. This has a number of components using different operating systems and security policies, which conflicted in a number of interesting ways, particularly in that they used a number of different mechanisms for file and record level access.

031166 'Bonus or Bogey'
The Banker (Jan 94) pp 75 - 77
Smartcards could be either a big opportunity for the banks, if the application mix can be got right, or a serious threat if they allow other players into the retail payments market.

031167 'Business Code'
The Banker (Dec 93) p 69
Banks have a privileged and in some cases monopoly position in information security; they have the expertise, the customer base and dominance of EFT. Thus they might be natural suppliers of services such as secure networking and trusted third parties.

031168 'Certification and Accreditation Approach for the WWMCCS Guard'
B Tretick, *NCSC 93 pp 245 - 252*
This paper explains the evaluation procedure used for the US World-Wide Military Command and Control System (WWMCCS) and for many of the components of its underlying network. The approach used here is due to be repeated for other defence projects.

031169 'Operational Requirements for Multilevel Security'
B Tretick, *Security Applications 93 pp 30 - 35*
This article surveys the US military use of multilevel systems and describes some of the problems. In particular, the effort involved in manually downgrading data can inhibit effective operations. One example is given by the WWMCCS; this is a top secret communications system, but it provides feeds to many lower level systems, as do a number of intelligence gathering systems whose output must be bowdlerised. The proposed long term solution is to extend multilevel features to all command, communications, processing and simulation systems.

031170 'Security Issues on Distributed System Applications'
CR Tsai, *NCSC 93 pp 385 - 390*
The author describes a distributed security management prototype developed for IBM; this is based on a tool called SMIT which manages distributed access control lists across AIX systems.

031171 'Networks and security: the role of the session manager'
A Webb, *Computer Audit Update (Dec 93) pp 10 - 13*

Session managers such as TUBES on MVS are explained; they introduce a new set of audit concerns. Although they can cut down on access control administration, any failure in administering them properly can have serious effects.

031172 'Dreams Come True with Password Genie'
CC Wood, *Information Management and Computer Security v 1 no 5 (93) pp 37 - 41*

The author describes a password generator program called Password Genie. This gives users a choice of one out of five randomly generated passwords, and is implemented for Novell systems.

031173 'Principles of secure information systems design with groupware examples'
CC Wood, *Computers and Security v 12 no 7 (Nov 93) pp 663 - 678*

Most groupware security controls will have to be built in by application developers, for whom an overview is provided of what makes controls effective (such as compartmentalisation, sustainability, auditability, and user acceptability) and how these properties affect each other. These points are illustrated by discussing the features of a number of products, from Lotus Notes to Higgins. Groupware complexity is at odds with the requirement that controls be simple to administer; on the other hand, it provides an opportunity to get away from single control points, which can also be points of failure.

2 Operating System and Database Security

031201 'Renewed Understanding of Access Control Policies'
MD Abrams, *NCSC 93 pp 87-96*

Existing access control policies may be incompatible with modern evaluation criteria such as TCSEC. Classification of policies as discretionary or mandatory is too inflexible to describe certain policies. The authors conclude that TCSEC may have to be extended to take account of existing and future systems.

031202 'Report of an integrity research study group'
MD Abrams, EG Amoroso, LJ LaPadula, TF Lunt, JG Williams, *Computers and Security v 12 no 7 (Nov 93) pp 679 - 689*

The authors study the practicalities of implementing the Clark-Wilson integrity model, and provide a framework for discussing the trust objectives, the internal and external interfaces, the functional design and the rules of operation. Where these focus on dual control and external consistency, Clark-Wilson has the drawback that implementing dual control system administration requires trusted hardware. In the context of secure databases, there are significant difficulties in implementing an integrity TCB.

031203 'NDU(C): A Mandatory Denial of Service Model'
E Amoroso, *NCSC 93 pp 31 - 38*

The author proposes a level-based non-denial of service model, NDU(C), which is based on Millen's resource allocation model. It ensures that low priority subjects cannot interfere with (deny service to) high priority subjects, just as the Biba model guarantees that low integrity subjects cannot interfere with high integrity subjects and objects. Comparisons show how NDU(C) relates to the Bell-LaPadula and Biba models, the System Z problem, and the trusted process problem.

031204 'Real-time Trust with "System Build": Lessons Learned'
MM Bernstein, TC Vickers Benzel, *Security Applications 93 pp 130 - 136*

The conflict between security and real-time operation can often be simplified by noting that highly classified information, such as mission intelligence, is present only during clearly defined operations (such as aircraft flights) during which low level operatives such as ground crew have no access. Thus a 'system build' phase prior to takeoff can be well worth while; and practical experience shows that it also means a less complex operating system, as no security objects are created dynamically, and all access relationships can be compiled into capabilities.

031205 'Authorisations in Relational Database Management Systems'
E Bertino, P Samarati, S Jajodia, *Fairfax 93 pp 130 - 139*

In relational database systems, one important issue is whether revocations should cascade. Many previous writers had assumed that they would, but most revocations are due to promotions or other staff moves rather than sackings, and so cascading can be quite inappropriate. Algorithms are presented for dealing with both positive and negative privileges, with and without cascading.

031206 'High Assurance Discretionary Access Control for Object Bases'
E Bertino, P Samarati, S Jajodia, *Fairfax 93 pp 140 - 150*

Discretionary access control systems may be vulnerable to Trojans, but this can be ameliorated by data filtering, especially in object-oriented systems where we can take advantage of the encapsulation. A filtering algorithm is proposed which acts on the objects' access control lists.

031207 'Multilevel Model for Object-Oriented Database'
M Boulahia-Cuppens, F Cuppens, A Gabillon, K Yazdanian, *Security Applications 93 pp 222 - 231*

The authors tackle the construction of multilevel object bases by combining one system for each level. They present a formalism of the object oriented model and show how it can be extended to multilevel systems. In particular, the proposal will support cover stories without the usual difficulties of polyinstantiation; the cost is that while it allows read down, it prevents write up by low level users. High level users access low level data indirectly via pointers, and there is some discipline on the use of cover stories.

031208 'Effects of Multilevel Security on Real-Time Applications'
RK Clark, IB Greenberg, PK Boucher, TF Lunt, PG Neumann, DM Wells, ED Jensen, *Security Applications 93 pp 120 - 129*

The requirements of multilevel security and real-time computing clash over scheduling, and threads often have to be replicated in order to prevent covert channels. This thread fragmentation was studied in the context of airborne applications during the development of an operating system called Secure Alpha; each fragmented thread needs a trusted object to manage it. Implications for application development are discussed.

031209 'Database security: Features and considerations'
SK Cunningham, *Computer Security Journal v 9 no 2 (Fall 93) pp 13 - 25*

The authors examine database security from a general perspective, with the goal of teaching the reader how to analyze the security features of competing products during a selection process.

031210 'Secure Information Processing versus the Concept of Product Evaluation'
ECMA *Technical Report TR/64 (Dec 93)*

This is the report of an industry working group on the differences between ITSEC and TCSEC, and their implications for vendors. The success of TSSEC C2 as a commercial baseline has put pressure on suppliers, but problems are caused by the different provisions in ITSEC and the secrecy of the evaluation process. Since at present there is too much emphasis on the security of products at the expense of operations, the aim with products should be to get 90% of the TCSEC value at 10% of the cost; the proposal is that there should be a specifically commercial functionality class within ITSEC, which would be based on existing quality standards such as ISO 9000 and rely mostly on self certification.

031211 'A Rigorous Approach to Determining Objects'
DP Faigin, JJ Dondelinger, JR Jones, *Security Applications 93 pp 159 - 168*

The authors describe a way of systematically identifying all the trusted objects in a system by working outwards from the trusted computing base. This prevents designers from missing non-obvious objects, and carrying over assumptions wrongly from similar systems. This methodology, which is called RODA, is described in some detail; it is suitable for systems up to level B2.

031212 'Composing Trusted Systems Using Evaluated Products'
D Gambel, J Fowler, *NCSC 93 pp 200-209*

The authors suggest that the composition of evaluated components might invalidate the evaluations, and that this should be avoided if possible. They suggest composition procedures which preserve the result of previous evaluations.

031213 'Virus tests to maximise availability of software systems'
E Gelenbi, M Hernández, *Theoretical Computer Science v 125 no 1 pp 131 - 147*

Existing operating systems theory on the optimum interval between checkpoints has to be modified once we take viruses into account. The optimum dump interval is computed, as is the optimum number of failure tests between dumps, based on a Weibull density infection rate; and numerical methods for the solution of these equations are described.

031214 'An Open Security Architecture'
F Gluck, *NCSC 93 pp 117 - 128*

A 'workstation-centric' architecture is presented for use in personal computer environments, protecting data at workstations (including laptops and notebooks), servers, and in transit between the two. Data is protected when it is first created by storing access information with the file, and protecting the combination with encryption, thus ensuring that access control information is not lost when a file is emailed or sent across a network. The architecture is intended for overlay on existing networks at minimal cost.

031215 'Does Licensing Require New Access Control Techniques?'
R Hauser, *Fairfax 93 pp 1 - 8*

Licensing control systems increasingly determine how much money large users pay to software publishers. As trusted hardware is impractical in most applications, this function should ideally be integrated with the access control system. At the cost of maintaining some state, it could be integrated into operating systems (and even distributed file systems); it could then be used to license nonexecutables such as encyclopaedias as well.

031216 'A study of a security model for commercial uses'
N Hiroshi, E Gutierrez, S Hideki, *SITA 93 pp 515 - 518*

The military model of multilevel systems is inadequate for commercial users, who are more interested in integrity than secrecy, but still need to control conflicts of interest. The authors suggest that in addition to access control matrices which mediate between subjects and objects, further matrices are needed to control subject/subject and object/object relationships; and that transformation procedures on constrained data should also be supported.

031217 'Use of the Trusted Computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems'
HL Johnson, ML De Vilbiss, *NCSC 93 pp 137-145*

This paper summarises a proposal under consideration by the US Department of Defense for designing and evaluating systems composed of validated components. The aims are two-fold: to make evaluation easier, and hence more reliable; to help contain the cost of such evaluations.

031218 'A Pump for Rapid, Reliable, Secure Communications'
MH Kang, IS Moskowitz, *Fairfax 93 pp 118 - 129*

Existing techniques for dealing with covert channels in multilevel systems include blind write-ups and periodic read-downs. The authors propose instead a data pump with both low and high buffers, and discuss its capacity; this can be improved by judicious use of randomisation, and in practice there should be no performance penalty in benign situations.

031219 'Analysis of an Algorithm for Distributed Recognition and Accountability'
C Ko, DA Frincke, T Goan, LT Heberlein, K Levitz, B Mukherjee, C Wee, *Fairfax 93 pp 154 - 164*

Given that hackers often use one compromised machine as a base for attacking others, it is important to collate information about intrusion attempts right across a network. An algorithm is presented to do this; it first tries to associate suspicious activities with a single NID (assigned by entry point) and then works outwards.

031220 'Security Considerations in the Design of Multi-Level Secure (MLS) Database Applications'
F Kramer, D Nelson, S Heffern, J Studt, *NCSC 93 pp 185 - 192*

A multilevel secure (MLS) database product was used to replace an existing single level product, and the database application was modified to use its features. The unexpected consequences included the need to de-normalize the database, and some effects of polyinstantiation. The common practice of building applications for single level products and then substituting multilevel platforms when they become available has a bad impact on database application design.

031221 'A Taxonomy of Computer Program Security Flaws, with Examples'
CE Landwehr, AR Bull, JP McDermott, WS Choi, *US Navy Report NRL/FR/5542–93-9591 (19/11/93)*

The authors collate details of dozens of operating system security flaws from the computing literature of the last twenty years or so. These mostly concern loopholes in various versions of Unix, Multics, VM and MVS, though some viruses are also discussed. This collection is then classified from various points of view: where the flaw was located; the stage of the life cycle at which it was introduced; whether the introduction was malicious or accidental; and in the latter case, the type of programming error responsible.

031222 'Database Design & MLS DBMSs: An Unhappy Alliance?'
S Lewis, S Wiseman, *Security Applications 93 pp 232 - 243*

Given a multilevel database product, how should one actually design a database? Two examples are given which show how applications can be built under SWORD; the obvious way is to construct a multilevel table from the lowest level up, and arrange things so that lower level users see the null value 'not cleared' instead of high level entries. It is also possible to have a table per level. The trade-offs illustrate problems inherent in even simple integrity requirements.

031223 'Integration of DCE and Local Registries: Design Approaches'
P Lin, S Chandersekaran, *Fairfax 93 pp 165 - 170*

This paper provides an overview of OSF DCE security and looks at how it can be harmonised with local access control. Propagation is the main problem; as DCE supports both 'push' and 'pull' updates, maintaining consistency and manageability is not trivial. The proposal is to propagate the common information from DCE to local registries, and manage the rest locally. The idea is that less information is held centrally, and a fallback position is available to administrators when the network goes down.

031224 'A Distributed System Security Architecture: Applying the Transport Layer Security Protocol'
M Mirhakkak, *Computer Communication Review v 23 no 5 (Oct 93) pp 6 - 16*

The author reviews the OSI Transport Layer Security Protocol and discusses the services it can deliver. It is particularly important in mediating between the reference monitors of two separate multilevel systems; it uses confidentiality, integrity and authentication mechanisms to support access control functions.

031225 'Knowledge-based security control for on-line database transaction processing systems'
VK Murthy, EV Krishnamurthy, *ACM SIGSAC v 12 no 1 (Jan 94) pp 7 - 14*

Some online systems process transactions and simultaneously extract biometric or other pattern based information on users. This raises interesting questions about what happens when an intruder is detected and transactions have to be reversed out, and particularly about the tradeoffs between security and concurrency when cascaded aborts must be provided. Possible strategies include using finer granularity, shadow paging, two phase locking, two version configuration locking and timestamping.

031226 'The Deductive Filter Approach to MLS Database Prototyping'
G Pernul, W Winiwarter, AM Tjoa, *Security Applications 93 pp 244 - 253*

Prototyping can help to develop the classification scheme for a multilevel database, but may involve much trial and error. A security constraints language has been developed to make this activity more structured and productive. Details are given with examples of the rules for retrieving a security object.

031227 'Query Acceleration in Multilevel Secure Database Systems'
W Perrizo, B Panda, *NCSC 93 pp 53-62*

Some techniques for searching multilevel databases throw up results that, while technically correct, will be rejected because of the security policy and so are never shown to the user. Removing these answers after the event incurs a cost. Alternative data structures are proposed that do not return these false hits when searched, resulting in better performance.

031228 'BSD IPC Model and Policy'
S Romero, C Schaufler, N Bolyard, *NCSC 93 pp 97 - 106*

An informal model is presented for a TCSEC Class B1 implementation of Unix BSD Interprocess Communication. Both connectionless and connection oriented services are modeled. Access control policies for four operations (attribute read, attribute write, data read, and data write) are presented. For Unix domain sockets both mandatory (multi-level) and discretionary policies are included, while for Internet domain sockets only a mandatory policy is present. Formulating the policy helped the implementers understand how the system should be built.

031229 'Expressive Power of the Single-Object Types Access Matrix Model'
RS Sandhu, S Ganta, *Security Applications 93 pp 184 - 194*

The authors explain the typed access matrix model, describe a simplified version in which primitive operations may act on only one object at a time, and show that the former can be reduced to the latter.

031230 'Referential Integrity in Multilevel Secure Databases'
RS Sandhu, S Jajodia, *NCSC 93 pp 39-52*

Consider an employee employed on a classified project. What might his or her employment record contain? The authors consider methods of reducing, and in some cases eliminating, polyinstantiation and examine the descriptive power of the resulting system.

031231 'Modularity of Assembly-Language Implementations of Trusted Systems'
EJ Sebes, TC Vickers-Benzel, *NCSC 93 pp 173 - 184*

Modularity must be assessed in high assurance (TCSEC B2+, ITSEC E4+) systems. However, making statements about the modularity of assembly language programs is more difficult, as low level languages lack inherent program structuring, data typing, and data hiding capabilities. Mimicing high level language constructs by macros (enforced by convention and review) can help provide some structure; but systems written in low level languages still require greater documentation, both in the code and externally, to make their code comprehensible.

031232 'Regulating Processing Sequences via Object State'
DL Sherman, DF Sterne, *NCSC 93 pp 75 - 86*

By limiting the types of operation that may be applied to an object with state, we can restrict the sequences of operations that may be applied. Thus a user who could normally perform an operation might find that it is temporarily prohibited until some dependent operation has been performed, possibly by another party. The relationship with mandatory access controls is discussed.

031233 'MLS File Service for Network Data Sharing'
RE Smith, *Security Applications 93 pp 94 - 99*

NFS systems provide a natural platform for developing MLS systems; the main problem is whether to acknowledge messages from low to high clients. If one does, a covert channel opens up; if not, reliability may be compromised.

031234 'Discretionary Access Control in Object-Oriented Databases: Issues and Research Directions'
RK Thomas, RS Sandhu, *NCSC 93 pp 63 - 74*

The authors propose a framework within which to classify different techniques for implementing discretionary access control in databases.

031235 'Task-Based Authorisation: A Paradigm for Flexible and Adaptable Access Control in Distributed Applications'
RK Thomas, RS Sandhu, *NCSC 93 pp 409 - 415*

In many applications, it is natural to base access control on tasks rather than objects. Mainframe systems could support this by protecting transactions, but the move to distributed systems makes things more complex as multiple principals may be involved. The main design problems are capturing the failure semantics and the dependencies between subtasks.

031236 'A Framework for Distributed Authorisation'
TYC Woo, SS Lam, *Fairfax 93 pp 112 - 117*

The authors generalise access control lists to cope with defaults and inheritance conditions in distributed systems, and propose mechanisms by which authorisation can be delegated from one server to another. Authentication and authorisation may be handled by separate servers.

3 Security Management and Policy

031301 'Cracking the Code'
RJ Anderson, *Banking Technology v 11 no 2 (March 1994) pp 42 - 44*

In this simplified version of the material presented in 'Why Cryptosystems Fail' (031103 above), the author presents a management overview of the causes of automatic teller machine fraud. He discusses the lessons for bankers, and emphasises the need to get competent consultants.

031302 'The OECD Guidleines for the Security of Information Systems: A Look to the Future'
C Axsmith, *NCSC 93 pp 301 - 310*

This article describes the reasoning behind the recent OECD guidelines, and sets out the principles followed in drafting them. It also discusses the admissibility of digital signatures and computer evidence in general in the USA, and argues that adopting the standards quickly could give US firms a competitive advantage.

031303 'Information Systems Security Design Methods: Implications for Information Systems Development'
R Baskerville, *ACM Computing Surveys pp 375 - 414*

The author compares the methodologies used to develop security with those used overall systems design. First generation techniques were based on checklists, of which three are compared. From this emerged risk analysis methods, which led in turn to second generation security techniques focussed on the software life cycle; of these, Fisher, Parker, CRAMM, RISKPAC and BDSS are described. Third generation methods are considered to be those based on logical transformation of an attribute model; the interface between CRAMM and SSADM is an example. The conclusion is that security has consistently lagged behind the rest of the development environment.

031304 'The Rationale Behind the Canadian Criteria'
EM Bačić, A Robinson, *Security Applications 93 pp 170 - 179*

Two of the authors of Canada's TCPEC criteria describe its scope and goals. They assumed that all security can be described in terms of interaction between objects, and thus that mechanisms can be seen as isolation, mediation and audit. They discuss typing, discretionary and mandatory mediation, and the range of functionality that can be evaluated; this is not restricted to confidentiality but also covers integrity, availability and fault tolerance. Finally, trust levels are compared with those of TCSEC and ITSEC.

031305 'Contingency Planning'
K Bennett, *Financial Systems (Q3 93/NY 94) pp 44 - 46*

After the Bishopsgate bombing in London, there was poor crowd control; hundreds of souvenir hunters and opportunistic thieves went through the wreckage, and the streets were littered with documents for weeks. Salvaging hard disks from PCs is not trivial with dirt and glass everywhere, and with the emergency services pushing everyone to tidy up quickly. Finally, rebuilding is going so slowly that some recovery sites may be in use for as long as two years.

031306 'Insuring against exposure'
G Booth, *Banking Technology v 11 no 2 (Mar 94) pp 36 - 40*

Over the last ten years, many banks have centralised risk management, with one officer responsible for controlling credit, market, legal and operational risks. In the last category, worries about computer fraud are coming to dominate, and a series of claims has pushed up insurance premiums.

031307 'Digital signatures: can they be accepted as legal signatures in EDI?'
PW Brown, *Fairfax 93 pp 86 - 92*

Under US law, there is no reason why digital signatures should not be valid, as a signature can be any agreed mark or seal and industry standards and practice would guide the court. Nonetheless, they still have to be tested in court, and in the meantime they may be backed up by contractual guarantees (such as by a member of an exchange). There are also implications for fraud law.

031308 'Trusted Systems: Applying the Theory in a Commercial Firm'
EC Charles, DA Diodati, WJ Mozdzierz, *NCSC 93 pp 283 - 291*

This article describes the information security strategy adopted by Aetna, the US's largest insurance company. This is based on a C2 evaluated mainframe product, with a clearly defined trusted computing base extending to other machine architectures as well, and a policy that applications implement security by calling operating system features. This has brought considerable technical and management benefits, which are discussed.

031309 'Securing Your Business Process'
BS Collins, S Matthews, *Computers and Security v 12 no 7 (Nov 93) pp 629 - 633*

The main cause of new infosec threats will be the increasing computer literacy of the workforce, and the complexity of networks will exacerbate things. Just as matching packaged applications to business processes is the main problem for IT managers and makes productivity gains hard to realise, so the main problem for security managers is mapping security features to business responsibility structures, which may be department or task based.

031310 'Information systems: the 'meta' framework'
Computer Audit Update (Feb 94) pp 3 - 9

This article describes the many international initiatives under way to produce security guidelines, including those from the OECD, the US ISSA/GSSP, the UK DTI codes of practice for information security management, and others.

031311 'Why information systems security standards?'
Computer Audit Update (Jan 94) pp 3 - 9

International standards take a long time to establish, and for this and other reasons it is argued that national signals security agencies should play the pivotal role.

031312 'Illegal software'
T Corbitt, *Computer Fraud and Security Bulletin (Jan 94) pp 14 - 16*

This article describes the activities of two UK software vendors' associations in raiding and suing companies which copy software illegally.

031313 'The Computer Misuse Act'
T Corbitt, *Computer Fraud and Security Bulletin (Feb 94) pp 13 - 17*

This UK law makes unauthorised access to, or modification of, computer programs or data an offence. Its provisions and the requirements for proof are described, as are the measures a company should take to make prosecutions likely to succeed.

031314 'Safety-critical systems - legal liability'
D Davis, *Computing and Control Engineering Journal v 5 no 1 (Feb 94) pp 13 - 17*

The author examines the remedies available in English law to victims of errors in software and hardware. In addition to contract and tort, one may use product liability legislation and the European Community's Machine Safety Directive.

031315 'Improved Password Mechanisms through Expert System Technology'
WG de Ru, JHP Eloff, *Security Applications 93 pp 272 - 280*

It is important to make passwords simultaneously memorable and hard to guess. The authors report building an expert system which can help users construct passphrases with these properties.

031316 'Baseline security for networks'
C Dixon, *Computer Fraud and Security Bulletin (Jan 94) pp 16 - 19*

Most network security problems stem from poor management of existing facilities and so one should tighten up on administration before spending money on technical security measures.

031317 'How to Market the Information Systems Security Program'
D Eakin, *NCSC 93 pp 292 - 300*

A security program can fail if the security manager is a technical person without suitable interpersonal skills. It is particularly important for the security function to be seen as ‘part of the team’ rather than as an impediment to business operations.

031318 ‘Organisational Issues in IT Security’
P Fagin, *Computers and Security v 12 no 8 (Dec 93) pp 710 - 715*

Security management developed in bureaucratic organisations such as the military, but many companies are power-based (dominated by a strong willed individual) or task-based (organised into project teams) instead. In these cultures, standing is often based on recognised expertise, and should be exercised through persuasion; power derived from position or procedures may be negative. A devolved approach is suggested in which departments develop their own security polices, with advice and audit feedback from the centre.

031319 ‘An Examination of Federal and Commercial Access Control Policy Needs’
DF Ferraiolo, DM Gilbert, N Lynch, *NCSC 93 pp 107-116*

NIST surveyed various classes of computer user to determine possible security requirements. These users expressed dissatisfaction with existing security products, often believing their requirements to be unique. The authors discuss some access control policies that might be usefully applied in a number of the organisations surveyed.

031320 ‘Risk Analysis: Ten Years On’
KJ Fitzgerald, *Information Management and Computer Security v 1 no 5 (93) pp 23 - 31*

The author gives a history of the risk analysis methodologies proposed in computer security, and proposes a technique based on threat matrices, whose coefficients he derives from opinions expressed by clients in workshops.

031321 ‘The Computer Ethics of University Students: An International Exploratory Study’
KA Forcht, RG Brookshire, SP Stevens, R Clarke, *Information Management and Computer Security v 1 no 5 (93) pp 32 - 36*

The authors surveyed the attitudes of business students at an Australian university and compare the results with similar US research. The attitudes in the two countries were quite similar, but opinions were more strongly held in the USA.

031322 ‘Certification and Accreditation Approach’
KP Frederick, *NCSC 93 pp 260 - 273*

The author provides an overview of the process of certifying and accrediting large US military systems. This covers all stages from system requirements through final certification.

031323 ‘Commercial Accreditation of Information Security’
G Hardy, *Computers and Security v 12 no 8 (Dec 93) pp 716 - 729*

This is the final report on an EC project to examine the accreditation of commercial information systems. Over 200 organisations were consulted and their views compared with the ITSEC model; it was concluded that accreditation by independent examiners was a worthy goal and that standards should be harmonised internationally. An accreditation framework is proposed.

031324 ‘A View of Information Security Tomorrow’
HJ Highland, *Computers and Security v 12 no 7 (Nov 93) pp 634 - 639*

Poor computer security is blamed on the lax attitude of computing academics, the passive acceptance by business of the military model, and the military’s indifference to the problems of human compliance. Many security managers are complacent and learn little of the subject beyond what they pick up from sales material. However, in addition to more technical knowhow, security managers also need to deal with people better.

031325 ‘IFIP TC11 News’
HJ Highland, *Computers and Security v 12 no 8 (Dec 93) pp 735 - 739*

This describes the curriculum of a Master’s degree course in information security offered jointly by Queensland University of Technology and Stockholm University.

031326 'Recovery: The Uncharted Phase in Disaster Relief'
FPA Hooring, JGH Quint, *Disaster Management v 6 no 1 (94) pp 9 - 12*

This article reports a study of local government disaster preparedness in the Netherlands: it observes that in natural disasters, government policy will focus on immediate relief by emergency service personnel, and there is little planning for the subsequent recovery phase. Thus organisations should plan to supply the deficit; in particular they should be prepared to cope with post traumatic stress disorder and to restore their normal administrative structures as quickly as possible.

031327 'Tandem Threat Scenarios: A Risk Assessment Approach'
LM Jaworksi, *NCSC 93 pp 155-164*

Many systems have possible failure modes where a single attack might be detected but two or more simultaneous attacks might succeed. Such attacks might require deliberate collusion or an attacker might wait for a failure before mounting an attack. The author describes a risk assessment methodology aimed at detecting such 'tandem' threats.

031328 'Social Psychology and INFOSEC: Psycho-social Factors in the Implementation of Information Security Policy'
ME Kabay, *NCSC 93 pp 274 - 282*

The author discusses the lessons which social psychology can teach about making security training more effective. A number of points are made: for example, initial training is best conducted individually or in small groups, but norms have to be integrated into the community to be really effective. A variety of techniques are available to change behaviour patterns, which may need to be used in combination over a sustained period in order to be effective.

031329 'Information contingency planning: a public sector perspective'
D Kennedy, H Nicholson, *Computer Audit Update: part 1 Jan 94 pp 10 - 16; part 2 Feb 94 pp 9 - 15*

The authors, who are with the Australian Department of Social Security, argue that the existing disaster recovery literature does not distinguish between the private and public sector, and thus fails to cope with the diversity of government departments. Abuse statistics are discussed; unions and industrial unrest are a significant problem in the state sector, but the maximum permissible delay in service is often much greater than in private business.

031330 'IT-Security:- A Quality Aspect!'
K Keus, W Kurth, D Loevenich, *NCSC 93 pp 324 - 333*

The authors survey the dependencies between IT security standards and the quality assurance standards set out in the ISO 9000 series and related EN/DIN documents. They also describe the product evaluation process in Germany, and the adoption of process models by the German Information Security Agency.

031331 'The role of quality assurance in high integrity systems'
G Kirk, *High Integrity Systems v 1 no 1 (94) pp 79 - 82*

This article describes the quality assurance manager's job in projects with a security or safety element. Its main point is that she should focus on the process rather than the product.

031332 'System threats and vulnerabilities - the contrary principle'
F Koerner, *Computers and Security v 12 no 8 (Dec 93) pp 775 - 779*

The author objects to the standard definitions of threats and vulnerabilities, and proposes instead that one should assess vulnerability in terms of 'adversary mission objectives' and 'threat logic trees'.

031333 'Workflow software: the value for auditors'
V Lilley, *Computer Audit Update (Feb 94) pp 15 - 18*

Software which passes a task such as a mortgage application from one person to another in sequence has some tricky audit requirements, particularly of productivity and process timing; on the other hand, audit trails can be automated very easily.

031334 'Should you let your staff go online?'
K Lindup, *Computer Audit Update (Dec 93) pp 5 - 10*
The author discusses the benefits and risks of giving staff access to the Internet, and describes how the exposures can be controlled.

031335 'COMPUSEC, A Personal View'
HO Lubbes, *Security Applications 93 pp x - xviii*
In this award lecture, the author discusses the evolution of computer security concerns, goals, standards and practices in the US Navy over the last 25 years. The theme is how the labelling and segregation of information at different classification levels has evolved from physical document control to the current multilevel systems. Early systems were discredited by the repeated success of penetration testing; and once it was realised that penetrate-and-test was not a serviceable design methodology, the stage was set for TCSEC and the involvement os NSA. The current approach, based on an evaluated products list, is still nowhere near an adequate solution; it provides no assurance for composite systems, and the different levels lack operational meaning in any case.

031336 'Targeting Safety-Related Errors During Software Requirements Analysis'
RR Lutz, *ACM Software Engineering Notes v 18 no 5 (Dec 93) pp 99 - 106*
The author provides a checklist for ensuring that software interfaces are robust. This helps to make checks on ranges, timings and so on explicit.

031337 'Seven Strategies for Information Technology Protection in the 1990's'
TR Malarkey, *NCSC 93 pp 334 - 351*
The author observes that whatever the drawbacks of evaluated products, the NCSC program has been useful in raising awareness of security issues. Given that the end of the Cold War and the lack of major incidents are making security a harder sell, he argues for a partnership between public and private sectors which would extend national policy from classified information to other sensitive data such a medical records and trade secrets, and promote development of the necessary quality control, accountability and enforcement functions. In particular, this initiative should aim to make different vendors' security mechanisms interoperable.

031338 'On dependability, its measurement and its management'
JA McDermid, *High Integrity Systems v 1 no 1 (94) pp 17 - 26*
A uniform treatment of security, safety and availability is becoming more common as these properties share a number of features. Dependability can best be assessed from the actual failure record: statistical and modelling methods are often inefficient, and they are based on a large number of assumptions (such as whether we are engineering for worst-case or average-case conditions). The principal measures should be loss, and the associated risk per unit time.

031339 'Public Network Integrity - Avoiding a Crisis in Trust'
JC McDonald, *IEEE Proceedings on Selected Areas in Communications v 12 no 1 (Jan 94) pp 5 - 12*
A number of recent service failures in the USA have shown how dependent many businesses have become on their telephone; modern telecommunications are so cheap and effective that they squeeze out alternative business processes. However, technological advances such as fibre optics, large switches and software control have led to a concentration of network assets and thus of risks. There are possible technical countermeasures, and a measure of service loss is proposed; however prudent managers will design their businesses to limit the impact of network failures.

031340 'An introduction to security in distributed systems'
JD Moffett, JA Clark, *High Integrity Systems v 1 no 1 (94) pp 83 - 91*
The authors present an overview of distributed systems security, and discuss its advantages and disadvantages compared with centralised processing. They review the OSI security framework, and briefly describe the available mechanisms such as encryption and authentication.

031341 'Defending large networks - the key threats'
T Mulhall, *Computer Fraud and Security Bulletin (Jan 94) pp 10 - 14*

Telephone network weaknesses include manufacturers' online access to the switches, through cloning of cellular phones, to abuse of corporate DISA facilities designed to let salesmen call in from payphones using an 0800 number and a four-digit code, and then straight out to the public network; these can be compromised by phone phreaks using autodiallers.

031342 'Security Policy in a Complex Logistics Procurement'
MJ Nash, RJ Kennett, *Security Applications 93 pp 46 - 53*

The Royal Air Force has been engaged since 1989 in a ten year, £500 million project to build a single computer system for all its engineering and supply operations. This example is used to compare and contrast US and UK approaches to certification; the US focusses on products and the UK on systems. The evolution of the information security function in the RAF is described, as is the process for developing a system security policy and architecture. In this case, the architecture consists of two E2/E3 systems at 'restricted' and 'secret' levels, and a limited number of E4/E5 'guards' to pass information between them.

031343 'The prupose of application reviews'
C Nelson, *Computer Audit Update (Dec 93) pp 13 - 17*

Implemented systems should be audited from time to time to check that they still do what they are supposed to. This process is discussed and a checklist suggested.

031344 'Strategic Sample Size in Auditing'
ER Patterson, *Journal of Accounting Research v 31 no 2 (Autumn 93) pp 272 - 293*

The author presents a mathematical model of how the audit sample size affects the optimal strategies of both auditor and auditee. An analogue of the prisoners' dilemma is constructed to show that increasing the sample size does not necessarily cut the risk of defalcation, especially if the auditee gains much more from cheating than the auditor gains from catching him.

031345 'Towards a Comprehensive INFOSEC Certification Methodology'
CN Payne, JN Froscher, CE Landwehr, *NCSC 93 pp 165-172*

TCSEC, and similar evaluation criteria, address components rather than systems. The authors suggest some ways of examining systems rather than components. They hope to apply these techniques to a significant system.

031346 'Getting management buy-in to computer security'
M Plant, *Computers and Security v 12 no 7 (Nov 93) pp 623 - 626*

The author discusses how to sell security in organisations and how this was done at the Abbey National. There is no panacea; success depends on a number of cultural factors.

031347 'Prevalence Simulation of Computer Viruses in Networks'
Y Sengoku, M Mambo, E Okamoto, T Uyematsu, *SITA 93 pp 525 - 528 (in Japanese)*

The authors report computer simulations of virus spread in networks, and provide graphs showing the extermination rate needed to control a virus with a given infection rate. This turns out to be dependent on the network topology.

031348 'Identification and Authentication when Users have Multiple Accounts'
WR Shockley, *NCSC pp 416 - 425*

It is common for users to have multiple logons to distributed systems, and this may prejudice some security policies (such as separation of duties). Biometrics are suggested as a possible solution.

031349 'A brief history of PC virsuses'
A Solomon, *Computer Fraud and Security Bulletin (Dec 93) pp 9 - 19*

The author tracks the evolution of PC viruses from their early beginnings in 1986 with Brain and virdem, through the first encrypted viruses to the modern polymorphic and stealth varieties. He also describes the media and commercial developments which have occurred in parallel, and remarks that it is getting much harder to write antivirus software as the sheer number of viruses makes false alarms a problem.

031350 'The Draft Federal Criteria and the ITSEC: Progress Towards Alignment'
J Straw, *NCSC 93 pp 311 - 323*
The assurance classes of the draft US Federal Criteria are compared against those of TCSEC and ITSEC, and the detailed assurance requirements tabulated. The draft criteria are designed to provide functionality building blocks, rather than to assess monolithic operating systems as TCSEC does; but unlike ITSEC, they apply only to components and not to systems as well. One strong point is that they assess ease of use, and particularly of administration.

031351 'How Responsibility Modelling Leads to Security Requirements'
R Strens, J Dobson, *NCSC 93 pp 398 - 408*
Responsibilities are the natural interface between an organisation's structure and its security policy. Responsibility relationships are called into being by delegation, and in turn provide not only the basis for a need-to-know security policy, but functionality and audit requirements as well. Responsibility modelling was used to derive a security policy for use an a hospital.

031352 'Response to Mayday'
The Banker (Feb 94) pp 67 - 68
This article presents twenty lessons gleaned from the Bishopsgate bomb and discusses some general recovery problems.

031353 'A Concept for Certification of an Army MLS Management Information System'
VP Thompson, FS Wentz, *NCSC 93 pp 253 - 259*
The US military's usual NCSC component evaluation process was eliminated for reasons of speed in RCAS, an office automation system for the National Guard (see 031102 above). Instead, evaluation of both system and components was carried out under the auspices of the program office. This may be emulated elsewhere in the DoD.

031354 'Information security in the global village: Do you practice safe fax?'
JR Wenek, *Computer Security Journal v 9 no 2 (Fall 93) pp 49 - 55*
This article addresses the security concerns of facsimile communications; it discusses standalone machines, server systems, and PC-based fax-modems.

031355 'Wire Pirates'
P Wallich, *Scientific American v 270 no 3 (Mar 94) pp 72 - 80*
This article explains network security problems to the general reader. It covers abuse of telephone credit cards, PBX fraud through toll-free numbers, reprogramming of cellular phones, and the various problems on the Internet. Many problems persist because administrators are not told the risks. The main Internet services are described, together with some of the ways in which they can be subverted.

031356 'Bridging the gaps'
M Whybrow, *Banking Technology v 11 no 1 (Feb 94) pp 38 - 40*
The Bishopsgate bombing is now showing up medium-term post disaster concerns such as stress, low morale, inadequate temporary accommodation, and forced decentralisation. The problems of Mitsubishi and the Royal Bank of Canada are described in detail; these were particularly acute for the dealing room, and standby dealing room services are discussed.

031357 'Fight them on the breaches'
M Whybrow, *Banking Technology v 11 no 2 (Mar 94) p 14*
Distributed processing is making banking technology more complex. There is still a lack of standards; different approaches include moving security responsibility to project teams, and writing support software to provide a standard application programming interface.

4 Formal Methods and Protocols

031401 'Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise'
SM Bellovin, M Merritt, *Fairfax 93 pp 244 - 250*

The authors enhance their Oakland 92 protocol 'EKE' for discrete log based remote login, so that the authentication server can store passwords in hashed form rather than in the clear. The security of the new protocol is analysed, and possible variants are discussed.

031402 'Formal methods: epideictic or apodeictic?'
J Bowen, V Stavridou, *Software Engineering Journal v 9 no 1 (Jan 94) p 2*

Formal methods do not deliver $\alpha\pi\acute{o}\delta\epsilon\iota\xi\iota\varsigma$ (rigorous proof) so much as $\epsilon\pi\acute{\iota}\delta\epsilon\iota\xi\iota\varsigma$ (exhibition); their main value lies in increasing understanding of a system, especially in the early stages of the design process.

031403 'Security Planning for Personal Communications'
D Brown, *Fairfax 93 pp 107 - 111*

The author compares three candidate key setup and authentication protocols for personal communications - the Beller/Chang/Yacobi scheme, Europe's GSM and the US Electronic Industry Association's USDC standard. GSM uses end-to-end challenge-response, while in USDC the home network will send the user's secrets across to the visited network; GSM also gives the user a temporary alias to hide his identity, but, as a precaution against network failure, the system can always request his clear ID.

031404 'Safety-critical systems, formal methods and standards'
J Bowen, V Stavridou, *Software Engineering Journal v 8 no 4 (July 93) pp 189 - 209*

This massive survey of the use of formal methods has 179 references, and discusses applications in aerospace, railway systems, nuclear power, medical systems and ammunition control. It studies the cost of failures, and draws economic arguments for formal methods from the nuclear and medical industries in particular. A number of government and industrial initiatives are described, and there is extensive material on safety standards.

031405 'Using Logics to Detect Implementation-Dependent Flaws'
U Carlsen, *Security Applications 93 pp 64 - 73*

An attack is shown on a protocol of Neuman and Stubblebine which depends on confusing nonces and keys. Such attacks are implementation dependent, as they are thwarted by strong typing; this raises the question of whether they are in fact beyond logics of belief. A logic of Bieber and others is developed to answer this question, by tying assumptions about nonces to honest behaviour by means of the predicate 'X sends/receives the value V exactly once'.

031406 'Analysing High-Integrity Systems'
JA Clark, JA McDermid, A Burns, *Computing and Control Enginering Journal v 5 no 1 (Feb 1994) pp 18 - 23*

The authors discuss the formal techniques available to analyse system reliability, including timing analysis and software fault tree analysis.

031407 'Towards practical "proven secure" authenticated key distribution'
Y Desmedt, M Burmester, *Fairfax 93 pp 228 - 231*

Yacobi had produced a security proof for a key distribution protocol which turned out to have a flaw - it breaks if a session key becomes publicly known after the event. The flaw is explained, and provides an illustration of when history has to be taken into account in formal proofs.

031408 'On the Shortest Path to Network Security'
JA Fitch, LJ Hoffmann, *Security Applications 93 pp 149 - 158*

The authors argue that resource constrained shortest path techniques are the natural way to evaluate networks of composed systems. They illustrate this with respect to the cascade problem.

031409 'Authentication services in distributed systems'
D Gollmann, T Beth, F Damm, *Computers and Security v 12 no 8 (Dec 93) pp 753 - 764*
The authors discuss what an authentication server should do, and go on to describe the protocols used in MIT's Kerberos, DEC's SPX and EISS Karlsruhe's SELANE. The last of these is based on El-Gamal public key encryption and uses handshakes rather than timestamps to prevent replay attacks; third parties are thus only needed for user registration, but revocation becomes correspondingly more tricky.

031410 'Lower Bounds on Messages and Rounds for Network Authentication Protocols'
L Gong, *Fairfax 93 pp 26 - 37*
The author examines the number of messages and the number of rounds needed for authentication, depending on whether the protocol is time or challenge based, whether the server, one client or both clients choose the session key, and whether a handshake is required. He proves lower bounds and shows that these are tight by exhibiting protocols which meet them. He then goes on to consider a number of special scenarios such as the case with more than two clients.

031411 'Non-repudiation in Open Telecooperation'
R Grimm, *NCSC 93 pp 16 - 30*
The authors propose mechanisms by which two or more mutually suspicious parties may commit to contracts or financial transactions. They require that failure to agree will disadvantage all parties.

031412 'A Second Look at the SDNS Key Management Protocol'
WA Jansen, *Security Applications 93 pp 74 - 81*
The author provides an overview of NIST's proposed key management protocol for the Secure Data Network System (SDNS) program, including the hierarchy of service agents which stand in for the key management centre, and the mechanisms for revocation and rekeying.

031413 'Choosing Among Standards for Lower Layer Security Protocols'
WA Jansen, DL Walters, *NCSC 93 pp 216-225*
There are a number of competing standards for low level network protocols (OSI levels 2 to 4) with subtly different security characteristics. This paper examines a number of these protocols with the aim of helping system designers to choose between them.

031414 'The Security problem for Cryptographic Protocols - A Solution with Tree Automata'
Y Kaji, T Fujiwara, T Kasami, *SCIS 94 paper 1B*
The security of a cryptographic protocol depends on whether any combination of known data has an undesired effect, and can thus be expressed as a term rewriting problem - and in particular as a unification problem under restricted substitutions. It is shown how this approach can be used to break a faulty protocol, and how tree automata can provide an algorithm which has a sufficient condition for termination.

031415 'Security Protocol for Frame Relay'
P Katsavos, V Varadharajan, *Computer Communication Review v 39 no 5 (Sep 93) pp 17 - 35*
The authors consider how frame relay can be integrated with existing security structures, and suggest that an extra sublayer be inserted in the data link layer to provide end-to-end security. This would support a greater range of topologies than SDE; its proposed design is discussed in some detail.

031416 'Integrating Security in Inter-Domain Routing Protocols'
B Kumar, J Crowcroft, *Computer Communication Review v 39 no 5 (Sep 93) pp 36 - 51*
Routers which have been wrongly configured, whether accidentally or maliciously, can pose a serious threat to networks, and as most routing updates are propagated automatically, the threats can be subtle, persistent, and their source hard to detect. OSI's interdomain routing protocol

(IDRP) tackles the problem with a trusted route server in each domain, MACs on updates between adjacent routers, digital signatures on route setup packets, and timeout mechanisms. Nonetheless, there are still vulnerabilities, and some improvements are suggested to make manipulation still more difficult.

031417 'Toward a Calculus of Systems Dependability'
ZM Liu, EV Sørensen, AP Ravn, CC Zhou, *High Integrity Systems v 1 no 1 (94) pp 49 - 65*
The authors propose a probabilistic calculus to assess dependability, and in particular the likelihood that an automaton will remain in a desired set of states. It is especially suited for real-time systems where the component failure rates are known.

031418 'Technique for authentication, access control and resource management in open distributed systems'
MR Low, B Christiansen, *Electronics Letters v 30 no 2 (20 Jan 94) pp 124 - 125*
The authors propose a distributed security mechanism based on proxy tickets which use public key cryptography and have built-in certificates. These enable cross-domain verification when the relevant server is offline, and facilitate delegation and resource management in heterogeneous systems.

031419 'Integrating Specifications, Integrating Assurances'
J McLean, *NCSC 93 pp 355 - 357*
The author discusses some of the difficulties in dealing formally with the composition of security properties, and provides an example of a secure system which has an insecure subsystem.

031420 'NetCash: A design for practical electronic currency on the Internet'
G Medvinski, BC Neuman, *Fairfax 93 pp 102 - 106*
The authors propose protocols for exchanging value by email, which feature electronic cash and cheques, multiple banks, and operation while the issuing bank is offline. These are based on a number of currency servers which swap coins for new ones without keeping a record, and also exchange coins and non-anonymous instruments such as electronic cheques. Thus anonymity is based on trusting these devices rather than in the cryptographic security used in Chaum's schemes. The servers also detect double spending in a number of ways.

031421 'Applying Noninterference to Composition of Systems: A More Practical Approach'
Q Shi, JA McDermid, JD Moffett, *Security Applications 93 pp 210 - 200*
Imposing a composable property such as noninterference on all components of a system may be superfluous of not all of their outputs are available externally. The conditions on internal communications can be relaxed to rely and guarantee conditions, which merely prevent interference of components. This shows that it is possible for a system to have security properties which are provably stronger than those of its components.

031422 'Cryptanalysis and Protocol Failures'
GJ Simmons, *Fairfax 93 pp 213 - 214*
Cryptographic systems often fail at the protocol rather than the algorithm level, and preventing these failures requires a kind of paranoia: it depends on suspecting everything, and especially those things which are accepted implicitly.

031423 'Adding Time to a Logic of Authentication'
PF Syverson, *Fairfax 93 pp 97 - 101*
The author presents an extension of the Abadí-Tuttle logic to deal with attacks on protocols where nonces and keys can be confused (the so-called causal consistency attacks). This involves adding a number of temporal axioms.

031424 'On Simple and Secure Key Distribution'
G Tsudik, E Van Herreweghen, *Fairfax 93 pp 49 - 57*
The authors describe the thinking behind the design of IBM's KryptoKnight authentication

protocol. In particular, multiparty key distribution is constructed systematically using two party protocols as building blocks. The extension to n parties means that insider as well as outsider attacks have to be considered.

031425 'Extending Cryptographic Logics of Belief to Key Agreement Protocols'
P van Oorschot, *Fairfax 93 pp 232 - 243*

The author proposes an extension of the BAN logic to cope with Diffie-Hellman type protocols, the possible goals for which are formalised. A protocol of Diffie, van Oorschot and Wiener is analysed and shown to meet all these goals; two other protocols, by Goss and Günther, are shown to satisfy some of them.

031426 'Optimality of Multi-Domain Protocols'
R Yahalom, *Fairfax 93 pp 38 - 48*

The author examines the number of messages needed to set up an authenticated key between two clients linked by a chain of n key servers. He exhibits optimal protocols for this: where the server in the target client's domain generates the key, $n + 4$ messages are required, and this goes up to $n + 5$ if the other server generates it.

5 Secret Key Algorithms

031501 'Message collision in block ciphers with message authentication'
C Allinson, H Bergen, E Dawson, *Computers and Security v 12 no 8 (Dec 93) pp 781 - 787*

The authors report experimental verification of the birthday collisions expected when block ciphers are used to calculate 32-bit MACs. Collisions were counted for between 2^{16} and 2^{20} messages, and with the underlying algorithm being DES or FEAL-N for N = 4, 8, 16 and 32; the number of collisions found was not significantly different from that predicted by theory.

031502 'Weak Keys for IDEA'
J Daemen, R Govaerts, J Vandewalle, *Crypto 93 pp 224 - 231*

The authors exhibit a large number of weak keys for IDEA: where there are multiplicative subkeys of 1 or -1, we may be able to construct a linear factor or find a characteristic with probability 1; building on these observations, we can easily solve the 2^{51} keys which have nonzero values only in bits 26-40, 72-83 and 99-122. These attacks can be prevented if we exclusive or each subkey with a suitable constant.

031503 'Divide and conquer attacks on certain classes of stream ciphers'
E Dawson, A Clark, *Cryptologia v XVIII no 1 (Jan 94) pp 25 - 40*

The authors extend Anderson's collision attack on the multiplex generator to universal logic sequences, which they define as those generated by a multiplex generator which has added feedback from the output to the multiplexer address lines. Such generators include the summation generator as a special case. Various optimisations of these attacks are presented, together with the results of numerical investigations into their effectiveness.

031504 'Almost perfect nonlinear permutations'
D Feng, B Liu, *Electronics Letters v 38 no 3 (3/2/94) pp 208 - 209*

The authors show that $y^7 + 1 = \alpha^{-6}(y + 1)$ has three solutions in $GF(2^{13})$, thus disproving a conjecture of Beth and Ding that where $2^n - 1$ is a prime and $2 < m < n - 1$, x^{2m-1} is an almost perfect nonlinear permutation mod 2^n. However, they also show that there are many d for which x^d is a uniform differential permutation.

031505 'The Number of Nonlinear Shift Registers That Produce All Vectors of Weight $\leq t$'
H Fredericksen, *IEEE Transactions on Information Theory v 39 no 6 (Nov 93) pp 1980 - 1990*

Feedback shift registers whose truth tables contain the minimum possible density of ones are natural candidates for generating all vectors of a given weight. The number of such registers can be established by counting the spanning subtrees of a graph whose nodes are equivalence classes of these vectors under rotation.

031506 'Yet another matrix cryptosystem'
GR Greenfield, *Cryptologia v XVIII no 1 (Jan 94) pp 41 - 51*

The author considers encrypting messages by matrix multiplication over a finite field, and in particular by $C = K^{-1}MK$ where $K = X^r$.

031507 'An Improvement Scheme of DES against Differential Cryptanalysis'
S Hada, H Tanaka, *SCIS 94 paper 14A (in Japanese)*

The authors propose modifying DES by using addition mod 2^4 instead of exclusive-or to combine the output of the autoclave with the intermediate half-blocks. This brings the partial pairs xor table of this addition into play as well as that of the S-boxes; the best characteristics for 3, 4 and 13 rounds are discussed, and if the last of these gives the best differential attack on the full algorithm, then this is 2^{17} times harder than the corresponding attack on DES.

031508 'A note on the propagation characteristics and the strict avalanche criterion'
S Hirose, K Ikeda, *SCIS 94 paper 8B*

The authors study Boolean functions with various combinations of differential and avalanche properties, and show how to construct functions whose differential properties are tightly bounded except for a single characteristic.

031509 'An Iterated Cryptosystem Based in Translation Tables Dependent on Keys'
N Iwayama, R Akiyama, T Kaneko, *SCIS 94 paper 14C (in Japanese)*

The authors propose a block cipher which is similar to the Russian GOST-28147 in that its autoclave (f-function) has eight 4-bit keyed S-boxes to provide confusion and a shift to provide diffusion. Extra diffusion is provided by combining the 4-bit values together at various stages during the S-box operations.

031510 'Design of the commercial data masking facility data privacy algorithm'
DB Johnson, SM Matyas, AV Le, JD Wilkins, *Fairfax 93 pp 93 - 96*

IBM has developed a 40-bit variant of DES called CDMF for use in export products. It is derived from vanilla DES by hashing the key, and the algorithm used is described in this paper.

031511 'Strength evaluation of RDES against differential attack'
T Kaneko, S Morita, T Imamura, *SITA 93 pp 519 - 522 (in Japanese)*

The authors graph the strength of RDES keys against differential attack; 40% of them are easier to find than keys of 8-round DES, and some are as weak as 4-round DES.

031512 'Necessary Conditions to Strengthen DES S-boxes against Linear Cryptanalysis'
KJ Kim, SJ Lee, SJ Park, *SCIS 94 paper 15D*

The authors show that the security of DES against differential and linear attack can be improved by following five S-box design criteria. These ensure that iterative linear approximations for four and five rounds will not occur, that the maximum value in the linear distribution table is less than 16, that the nonlinearity is adequate, and that $S(x) \neq S(x \oplus 11ef10)$.

031513 'The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic'
A Klapper, *Journal of Cryptology v 7 no 1 (Winter 94) pp 33 - 51*

The author exhibits geometric sequences whose linear complexity is high over $GF(2)$ but low over some $GF(q)$. Thus testing over $GF(2)$ alone is not sufficient; and geometric sequences are not in general suitable as keystream generators, unless they possess certain properties which are described. An algorithm is given for attacking weak sequences.

031514 'Structure and Properties of Linear Recurring m-Arrays'
DD Lin, ML Liu, *IEEE Transactions on Information Theory v 39 no 5 (Sep 93) pp 1758 - 1762*

Every linear recurring array in which each nonzero m by n matrix occurs exactly once can be constructed by folding a maximal length linear shift register sequence. This fact is tied up with the translation/addition and crosscorrelation properties of these arrays.

031515 'Complementarity Attacks and Control Vectors'
D Longley, SM Matyas, *IBM Systems Journal v 32 no 2 (93) pp 321 - 325*

The first author describes how the DES complementation property could be used to attack cryptographic systems using IBM's concept of control vectors, and the second author then shows how previously undocumented features of the IBM implementation thwart such attacks.

031516 'Linear Cryptanalysis of DES Cipher (III)'
M Matsui, *SCIS 94 paper 4A (in Japanese)*

The author improves his linear attack on DES and makes the first report of a successful attack on a DES key. The improvement is mainly achieved by doing a best-first search after the data collection phase, and reduces the required material to about 2^{43} known plaintexts. From experiments with 8-round DES, the overall work factor was estimated at the equivalent of 1.13 x 2^{42} encryptions, and this was confirmed experimentally: from August to October 1993, a program of about 100 lines each of C and PA-RISC assembly language was run on 12 Mitsubishi ME/R 99MHz workstations. The data collection phase took 40 days; thereafter the analysis involved sorting and totalling operations, followed by a successful 2^{30} keysearch. The author concludes that further performance improvements are likely, and that even if an attacker has less than the 2^{43} texts, he can still use what he has to cut the keysearch effort.

031517 'Highly efficient exhaustive search algorithm for optimising canonical Reed-Muller expansion of Boolean functions'

JF Miller, P Thomson, *International Journal of Electronics v 76 no 1 pp 37 - 56*

The authors present a new way of finding fixed polarity Reed-Muller expansions which satisfy certain conditions, and this gives a particularly fast way of improving a suboptimal expansion.

031518 'Nonlinear Pseudorandom Number Generator with Dynamic Structure and Its Properties'

T Moriyasu, M Morii, M Kasahara, *SCIS 94 paper 8A*

The authors consider a generalised Geffe generator, in which the selector shift register does not merely choose a bit from one of two other shift registers but the output of one of two nonlinear filter functions of these registers. They prove a linear complexity bound but show that a small change on one of these functions can affect the actual linear complexity enormously.

031519 'A Weak Cipher that Generates the Symmetric Group'

S Murphy, K Paterson, P Wild, *Journal of Cryptology v 7 no 1 (Winter 94) pp 61 - 65*

The symmetric group is generated by a block cipher whose round functions consist of exclusive-or with the key and a simple permutation, yet this cipher is very weak.

031520 'Differential cryptanalysis of hash functions based on block ciphers'

B Preneel, R Govaerts, J Vandewalle, *Fairfax 93 pp 183 - 188*

The authors examine whether differential attacks on block ciphers can be used to find collisions in hash functions constructed from them. The basic idea is to look for characteristics for which input-output xors are the same, with the result that they cancel out giving two strings with the same hashcode. DES is not threatened, as no characteristics are known with an even number of rounds; but collisions are exhibited for FEAL-N with N up to 16.

031521 'The Blowfish Encryption Algorithm'

B Schneier, *Dr. Dobbs Journal v 20 no 4 (Apr 94) pp 38 - 40*

The author describes a new secret-key encryption algorithm. This has a 64-bit block, a key whose length is variable up to 448 bits, and is designed to encrypt data at a rate of 26 clock cycles per byte on a 32-bit microprocessor. C source code is included, and there is a cracking contest for the best attack submitted before April 1995.

031522 'The Cambridge Algorithms Workshop'

B Schneier, *Dr. Dobbs Journal v 20 no 4 (Apr 94) pp. 18 - 24*

A workshop on fast software encryption was held at Cambridge University in November 1993. At the workshop, a number of new secret-key encryption algorithms were presented, as well as a number of papers on the underlying theory. This article discusses the algorithms briefly, and provides descriptions for a general audience of differential and linear cryptanalysis and the possible problems which can arise when algorithms are cascaded one after another.

031523 'Systematic Generation of Cryptographically Robust S-boxes'

J Seberry, XM Zhang, YL Zheng, *Fairfax 93 pp 171 - 182*

The authors call an S-box robust if it resists both differential and linear cryptanalysis, and show that group Hadamard matrices can be used to generate S-boxes which are not only robust but which also possess good nonlinearity and avalanche properties. Bounds on the differential characteristics of these structures are shown, as is the fact that linear combinations of their component functions do not necessarily satisfy the strict avalanche criterion. 12 by 10 boxes are constructed as an example.

031524 'SHA: The Secure Hash Algorithm'

W Stallings, *Dr. Dobbs Journal v 20 no 4 (Apr 94) pp 32 - 34*

The author describes the U.S. government standard Secure Hash Algorithm for a general audience, with the help of diagrams to illustrate the processing steps involved.

031525 'Ciphertext Only Attack for One-way Function of the MAP by Using One Ciphertext'

Y Tsunoo, E Okamoto, T Uyematsu, *SCIS 94 paper 15B*

MAP is a supposedly one-way function based on 4-round FEAL with feedforward. The authors exhibit a 2^{32} attack on it; when implemented in C on a Sparcstation 2, this took 15.7 hours to compute three plaintexts hashing to a given value.

031526 'Generation of All Reed-Muller Expansions of a Switching Function'

B Vinnakota, VVB Rao, *IEEE Transactions on Computers v 43 no 1 (Jan 94) pp 122 - 123*

The authors present a matrix-based method for obtaining the canonical sum-of-products expansion of a Boolean function. This approach has the advantage of being able to cope with some of the input variables being inverted.

031527 'Permutation Binomials over Finite Fields'

DQ Wan, *Acta Mathematica Sinica v 10 (Special Issue 1994) pp 30 - 35*

The author proves a conjecture of Carlitz, namely that there are no permutation polynomials of the form $x^{1+(q-1)/3} + ax$ $(a \neq 0)$ in field of characteristic two, the case of odd characteristic having been proved in a previous paper. He also characterises those cases where $x^{m+(q-1)/2} + ax^m$ is a permutation polynomial.

031528 'A Table of Primitive Binary Polynomials'

M Živković, *Mathematics of Computation v 62 no 205 pp 385 - 386 and microfiche insert*

The author gives one primitive k-nomial of degree n for $k \in \{3,5,7\}$ and $2 \leq n \leq 5000$, where these exist and the factorisation of $2^n - 1$ is known.

6 Public Key Algorithms

031601 'Parameter Selection for Server-Aided RSA Computation Schemes'
J Burns, CJ Mitchell, *IEEE Transactions on Computers v 43 no 7 pp 163 - 174*
The authors explore various attacks on the two server aided protocols of Matsumoto, Kato and Imai. These have a number of effects: results must always be checked, and strategies are needed to cope with attempted frauds without disclosing secrets. The consequences for parameter selection are discussed.

031602 'A Note on Secure Multi-Party Protocols to Compute Multiplicative Inverses'
M Cerecedo, T Matsumoto, H Imai, *SCIS 94 paper 3B*
The authors consider how two players can solve $xa + yb = d$, where $\gcd(a, b) = d$, without revealing a or b to each other; and in general how a number of players can compute the multiplicative inverse of a shared secret. A gcd algorithm of Purdy provides a more efficient approach than previous proposals.

031603 'One-way Functions over Finite Near-Rings'
E Chida, H Shiyuza, T Nishizeki, *SCIS 94 paper 9B*
The authors ask whether there are one-way functions which are homomorphisms of structures other than groups, and answer in the affirmative: any group homomorphism can be extended to a near-ring (a ring without either the left or right distributive law). Furthermore, if we have an oracle for Diffie-Hellman but not for discrete log, we can construct a one-way homomorphism on the ring whose 'multiplication' maps g^x and g^y to g^{xy}, and derive a ring of operations mod N in which discrete log is equivalent to factoring.

031604 'Attacks on the Birational Permutation Signature Schemes'
D Coppersmith, J Stern, S Vaudenay, *Crypto 93 pp 435 - 443*
Shamir's birational permutation signature schemes are attacked in a number of ways. Symmetry can be exploited, and the trap door conditions lead to equations on the coefficients of the transformations. If enough if these can be gathered, they can be solved by gcd or Groebner basis methods.

031605 'A New RSA-type Scheme over Singular Elliptic Curves'
H Kuwakado, K Koyama, *SCIS 94 paper 10B*
The authors propose an encryption and signature scheme which uses the singular elliptic curve $y^2 = x^3 + bx^2$ over Z_N, where b is a quadratic residue mod N. This avoid the need to calculate the order of the curve, as in schemes like Demytko's based on nonsingular curves, but still appears to give some advantage over RSA: in particular, it appears to resist the low multiplier attack in broadcast applications.

031606 'Remarks on LUC public key system'
CS Laih, FK Tu, WC Tai, *Electronics Letters v 30 no 2 (20 Jan 94) pp 123 - 124*
The authors discuss a number of the Lucas function's properties, such as that the roots of its characteristic polynomial have order $p + 1$.

031607 'Identity-based conference key broadcast systems'
T Hwang, JL Chen, *IEE Proceedings on Computers and Digital Techniques v 141 no 1 (Jan 94) pp 57 - 60*
The authors propose an identity based key distribution scheme based on RSA and discrete log, which can be extended to conference groups by Lagrange interpolation.

031608 'Key Management for Decentralised Computer Network Services'
L Harn, HY Lin, *IEEE Transactions on Communications v 41 no 12 (Dec 93) pp 1777 - 1789*
The authors propose using a master key to generate access passwords for a number of membership services from a single secret stored on a smartcard.

031609 'A Note on Multisignatures'
M Mambo, E Okamoto, *SCIS 94 paper 2B*

The authors provide variants of Fiat-Shamir in which a recipient can check that the signature was produced by a number of groups of players in a specified order, and a fail-stop scheme in which a group of signers can prove a forgery.

031610 'How to Improve the Security of Efficient Secure Broadcast Communication'
M Mambo, E Okamoto, S Tsujii, *SITA 93 pp 447 - 450*

Combinatorial methods can be used to broadcast a message to n recipients out of a large population, while keeping the message length below $O(n)$; the cost is that certain combinations of unauthorised persons may also be able to receive it. The authors show how to cut this cost by arranging for each user to be positioned on more than one lattice simultaneously.

031611 'A New Signature Scheme Based on the DSA, Giving Message Recovery'
K Nyberg, RA Rueppel, *Fairfax 93 pp 58 - 61*

The authors present a variant of the Schnorr signature scheme as follows. If g generates Z_p^*, m is the message, x is the secret signing key, $y = g^x$ is the public key and k the message key, then the signature is (r, s) where $r = mg^{-k} \pmod p$ and $s = k + sr \pmod p$. The recipient can recover m as $g^s y^r r \pmod p$. As with RSA and other message recovery schemes, the message must contain some redundancy for the scheme to be secure; unlike them, however, it cannot be used for encryption.

031612 'Weaknesses in some recent key agreement protocols'
K Nyberg, RA Rueppel, *Electronics Letters v 30 no 1 (6 Jan 94) pp 26 - 27*

Key agreement schemes proposed by Arazi and by Alexandris, Burmester, Chrissikopoulos and Desmedt both have the property that if an opponent obtains one of the session keys, then she will be able to compute all other session keys generated by the same principals. This is because key generation depends on a single instance of the Diffie Hellman problem, namely $g^{x_A x_B}$ where x_I is I's secret key.

031613 'A New Scheme of Key-Sharing within Set'
N Oda, Y Murakami, M Kasahara, *SITA 93 pp 443 - 446 (in Japanese)*

The authors propose a new key-sharing scheme based on characters in the residue class group modulo N. They argue that it is as hard to break as the discrete logarithm problem.

031614 'Designated Confirmer Signatures Using Trapdoor Functions'
T Okamoto, K Ohta, *SCIS 94 paper 16B*

The authors formalise Chaum's idea of designated confirmer signatures - signatures which can only be checked by a specific person. They show that such schemes exist if public key encryption schemes do, and provide a practical construction which is faster than Chaum's and depends only on discrete log.

031615 'Observer Transaction Systems Based on Secret-Chain Zero Knowledge Proofs'
T Okamoto, K Ohta, E Fujisaki, *SCIS 94 paper 12B*

The authors show how to implement the multiple-prover model of Eng, Okamoto and Ohta (031805 below) using either discrete logs or factoring as the primitive. The suggested application is the observer in an electronic wallet; it would cooperate in a proof if and only if a coin was not being double spent.

031616 'Sorting Out Signature Schemes'
B Pfitzmann, *Fairfax 93 pp 74 - 85*

The author shows a way to deal systematically with most kinds of signatures, including the undeniable and fail-stop ones. The classification works back from the 'courtroom' in which the recipient is trying to prove a signature while the signer is trying to disavow it, and then uses temporal logic to sort out the available options while studying the system's interfaces to the various parties concerned.

031617 'New signature scheme with message recovery'
JM Piveteau, *Electronics Letters v 29 no 25 (9 Dec 93) p 2185*

The author proposes an El-Gamal variant which gives message recovery. If g is the generator, m the message, x the secret key, $y = g^x$ the public key and k the message key, then the signature is r, s with $r = mg^k \pmod p$ and $s = (1-kr)/x \pmod{p-1}$. To recover the message, the recipient computes $y^s r^r = gm^r \pmod p$.

031618 'Transparent Cosignatures for Electronic Documents'
S Russell, *Security Applications 93 pp 82 - 91*

The author provides some arguments for the use of threshold signature schemes. The main argument is that control can be improved by making a gateway a mandatory partner in the scheme.

031619 'New Schemes of Noninteractive ID-based Key Sharing Schemes'
R Sakai, M Kasahara, *SCIS 94 paper 3C*

The authors propose an id-based key distribution mechanism based on secret linear transformations of the user ids, to which random numbers are added in the hope of preventing collusion attacks. There is also a stronger version computed with respect to a composite modulus.

031620 'Notes on ID-based Common Key Generation Systems'
R Sakai, M Kasahara, *SITA 93 pp 439 - 442 (in Japanese)*

The authors prove the equivalence of two id-based key agreement systems, and propose a new scheme in which the keys are generated by linear combinations of the centre secrets.

031621 'On Group Signature Schemes'
K Sakano, CS Park, K Kurosawa, *SCIS 94 paper 13A*

The authors present a (k, n) threshold scheme with no trusted dealer, together with undeniable and fail-stop variants. These are based on Schnorr signatures; each player chooses public and private keys, the former are multiplied together to give a group public key, and the latter are shared using a polynomial scheme.

031622 'Comments on an Attribution-Analyzing Protocol'
K Sako, *SCIS 94 paper 3A*

The author considers mechanisms for use in anonymous surveys where the goal is to prevent respondents being identified by combinations of attributes. He proposes that one entity should be in charge of each column of data attributes, and that cross correlations should where authorised be calculated using a multiparty computation protocol, whose input data are blinded and processed using quadratic characters.

031623 'A Structural Comparison of the Complexity of Cryptosystems Based on Discrete Logarithms'
K Sakurai, H Shizuya, *SCIS 94 paper 15C*

The authors compare the complexity of Diffie Hellman, Bellare-Micali, El Gamal and Shamir's three pass key transmission scheme; they show that in general $3PASS \leq EG \leq BM \equiv DH$. Equality holds in Z_p if the factorisation of $p-1$ is known, and in elliptic curves over $Z-p$ if the order of the curve is p.

031624 'Subliminal channels in the Digital Signature Algorithm'
B Schneier, *Computer Security Journal v 9 no 2 (Fall 93) pp 57 - 63*

The Digital Signature Algorithm has several subliminal channels: these are covert communication channels that a signer can use to send a message to a specific receiver or observer. These channels are described and discussed in this article.

031625 'Bulk encryption algorithm for use with RSA'
RF Sewell, *Electronics Letters v 29 no 25 (9 December 93) pp 2183 - 2185*

The author shows how to use RSA is such a way that both encryption and decryption are carried out using small exponents. The idea is to use vanilla RSA to set up a message key K, and then encipher plaintext p_i to ciphertext c_i by $c_i = \{(c_{i-1} \oplus K)^e \bmod N\} \oplus p_i$.

031626 'On expanding the domain and the range of some public-key crypto-functions'
M Shimada, *SITA 93 pp 523 - 524 (in Japanese)*

The author proposes a variant of his previously suggested technique for scaling inputs to encryption functions such as RSA whose domain and range is not a neat power of two.

031627 'Cryptography Without Exponentiation'
P Smith, *Dr. Dobbs Journal v 20 no 4 (Apr 94) pp 26 - 30*

The LUC cryptosystem is a variant of RSA that uses Lucas functions instead of exponentiation. The author presents three similar variants to the El Gamal public-key system: one for encryption, one for key exchange, and one for digital signatures. He claims that due to the lack of subexponential attacks, a 420 bit modulus gives the same security as 512 bit RSA or El Gamal.

031628 'Identity-based Non-interactive Key Sharing Scheme and Its Application to Some Cryptographic Systems'
H Tanaka, *SCIS 94 paper 3D*

The author produces an id-based key distribution scheme based on doing Diffie Hellman modulo a composite number, but such that the centre's calculations are less onerous than with the Maurer-Yacobi scheme.

031629 'Mathematical Problems in Cryptology'
NP Varnovsky, AI Varchenko, EA Primenko, *Journal of Soviet Mathematics v 67 no 6 (Dec 93) pp 3373 - 3406*

The authors provide an overview of cryptology, and of public key systems in particular: they cover schemes based on coding theory and formal languages as well as on number theory; discuss protocols for voting, coin flipping, zero knowledge proof and pseudorandom number generation; and discuss the complexity aspects of these protocols.

7 Computational Number Theory

031701 'On Secure Elliptic Curves Against the "Reduction Attack" and their Design Strategy'
JH Chao, K Tanada, S Tsujii, *SCIS 94 paper 10A*

The authors show that if an elliptic curve over $GF(q)$ has order m, $q^2 \neq 1 \pmod{m}$, and $\phi(m)/2$ is B-smooth, the Menezes-Okamoto-Vanstone reduction will transform the elliptic logarithm problem to a discrete log problem in $GF(q^k)$ where $k > B$. This enables the Atkin-Morain algorithm to be used to construct curves for which the reduction attack will be arbitrarily difficult, and complex multiplication can stretch the technique to elliptic curves over extension fields as well.

031702 'Discrete Weighted Transforms and Large-Integer Arithmetic'
R Crandall, B Fagin, *Mathematics of Computation v 62 no 205 (Jan 94) pp 305 - 324*

The authors introduce a variant of FFT multiplication in which a weighted transform is used. This not only allows faster operation on sparse multiplicands, but also bounds convolutional errors, with the result that it can deal with integers with eight times as many bits as a comparable FFT multiply routine.

031703 'Solving Homogeneous Linear Equations Over $GF(2)$ via Block Wiedemann Algorithm'
D Coppersmith, *Mathematics of Computation v 62 no 205 (Jan 94) pp 333 - 350*

The author presents an improvement of an algorithm of Wiedemann for solving large sparse systems of linear equations over $GF(2)$. This algorithm has much smaller storage requirements than Gaussian elimination, but in its original form was rather slow. This problem can be solved by operating on blocks rather than bits. It involves a matrix version of the Massey-Berlekamp algorithm, and will succeed except in the usually rare case that the matrix has several nonzero eigenvalues of large multiplicity.

031704 'A fast algorithm for finding "small" solutions of $F(X,Y) = G(X,Y)$ over imaginary quadratic fields'
I Gaál, *Journal of Symbolic Computation v 16 no 4 (Oct 93) pp 321 - 328*

The author shows how to use lattice basis reduction to solve Thue equations in imaginary quadratic fields, and in particular $F(X,Y) \leq G(X,Y)$ where deg $F \geq 4 +$ deg G. He illustrates this by finding all Gaussian integers of norm less than 10^{200} satisfying $\mid X^8 + (1+i)X^2Y^6 + (2-i)XY^7 + (4+i)Y^8 \mid < 50 \mid X^2 + Y^2 \mid$.

031705 'Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field'
AJ Menezes, T Okamoto, SA Vanstone, *IEEE Transactions on Information theory v 39 no 5 (Sep 93) pp 1639 - 1646*

This is the journal version of the authors' STOC 91 paper showing how the Weil pairing can be used to reduce elliptic logarithms to logarithms in an extension of the ground field, and that this is practical for supersingular curves in particular.

031706 'Notes on Public Key Cryptosystems with Fast Algorithms'
K Satake, M Kasahara, *SITA 93 pp 451 - 454 (in Japanese)*

The authors present fast modular exponentiation techniques for use when the modulus is slightly less than 2^m and m is a multiple of the computer word size.

031707 'A Systolic Power-Sum Circuit for $GF(2^m)$'
SW Wei, *IEEE Transactions on Computers v 43 no 2 pp 226 - 229*

The author presents a systolic array processor design for calculating $AB^2 + C$ in $GF(2^m)$. It uses m^2 cells, but the design of each cell is very simple with only three gates and ten latches.

8 Theoretical Cryptology

031801 'Random Oracles are Practical: A Paradigm for Designing Efficient Protocols'
M Bellare, P Rogaway, *Fairfax 93 pp 62 - 73*
The authors propose that theoretical analysis of cryptosystems should be based on random oracles rather than on the specific properties of one-way functions, as this allows security proofs to be carried out in a more general setting. For example, if f is a trapdoor permutation and H is a random oracle, then the signature $f^{-1}(H(m))$ is secure against chosen message attack.

031802 'Verifiable Secret Sharing for Monotone Access Structures'
T Beth, HJ Knobloch, M Otten, *Fairfax 93 pp 189 - 194*
Verifiable secret sharing is carried out without a trusted dealer - several parties distribute partial shares which are then combined. This is extended to general monotone access structures using the Lagrange interpolation formula which it combines with standard geometric sharing schemes.

031803 'On the Structure of the Privacy Hierarchy'
B Chor, M Geréb-Graus, E Kushilevitz, *Journal of Cryptology v 7 no 1 (Winter 94) pp 53 - 60*
The authors explore how many of a function's inputs can be known without revealing any further information, except possibly its value. They show that there is a t-private function for exactly $\lceil (N+1)/2 \rceil$ values of t, namely $\lceil N/2 \rceil$ to $N-2$.

031804 'Privacy, Additional Information and Communication'
B Chor, E Kushilevitz, A Orlitzky, *IEEE Transactions on Information Theory v 39 no 6 (Nov 93) pp 1930 - 1943*
When two parties compute the value of a function for which they each possess one input, there is a certain privacy cost - a minimum amount of information which they must reveal. Three ways of measuring this cost are proposed, which take into account the combinatorial aspects, the information theoretic aspects, and a combination of both. Bounds are shown for these measures, as well as ways to link these results to zero knowledge.

031805 'Secret-Chain Zero-Knowledge Proof Models'
T Eng, T Okamoto, K Ohta, *SCIS 94 paper 12A*
The authors provide a formal setting to analyse what happens when multiple provers each know a share of a secret; they characterise such proofs and show how one can be provided for graph isomorphism.

031806 'Definition and Properties of Zero-Knowledge Proofs'
O Goldreich, Y Oren, *Journal of Cryptology v 7 no 1 (Winter 94) pp 1 - 32*
The authors sharpen up the definition of zero-knowledge; they show that all zero knowledge proofs of practical importance are of a kind they call 'auxilliary-input zero knowledge', and argue that for proofs to be nontrivial, both the prover and verifier must have random input.

031807 'Opaque and Transparent Bit Commitment Schemes and Their Application'
T Itoh, Y Ohta, H Shizuya, *SCIS 94 paper 12C*
Bit commitment schemes may have the property that $F(x,0,r)$ and $F(x,1,r)$ are indistinguishable precisely when x is in (or is not in) a certain language L. In the former case, L has a prover-practical statistical zero-knowledge proof; in the latter, it has a bounded round perfect zero-knowledge proof.

031808 'Checkers for Adaptive Programs'
T Itoh, M Takei, *SCIS 94 paper 6C*
The authors extend the work of Blum and others on checking programs which, if incorrect, may exhibit adaptive behaviour. The define two classes of adaptively checkable languages, and characterise them by the existence of competitive interactive proof systems.

031809 'Three Results on Interactive Communication'
M Naor, A Orlitsky, P Shor, *IEEE Transactions on Information Theory v 39 no 5 (Sep 93) pp 1608 - 1615*

The authors present three results on the number of bits which must pass between two parties in order to communicate some information, and how this decreases with the number of messages sent, especially in the case where some probability function of the information is known.

031810 'Authentication Codes Based on Combinatorial Designs'
YJ Song, K Kurosawa, S Tsujii, *SCIS 94 paper 13B*

The authors present an authentication scheme based on triangular graphs; the advantage of this is that for a given cheating probability there are many fewer encoding rules needed than for schemes based on balanced incomplete block designs.

031811 'Transmission Schedules to Prevent Traffic Analysis'
BR Venkataraman, RE Newman-Wolfe, *Security Applications 93 pp 108 - 118*

If we try to prevent traffic analysis by delaying packets randomly, then we introduce a covert channel whose bandwidth is inversely proportional to the flexibility of the scheduling policy. The key to reducing this exposure is keeping all transmission parameters constant over long periods of time.

9 Book Reviews

'CODE BREAKERS'
FH Hinsley, A Stripp *Oxford 1993, ISBN 0-19-820327-6*

This is the story of Bletchley Park, written by the people who worked there. Britain's legendary success in reading Axis signals during the second world war has been described in a number of books since Winterbotham broke the secret in 1974, but these have focussed either on the technical achievement of breaking Enigma or on assessing the military and political impact of the Ultra product.

Now at last the legend is stripped away, and we learn what it was actually like to work in Bletchley during the war. Twenty-eight alumni tell their stories and bring home the scale of the operation: wartime SIGINT is not just about cryptanalysis, but about industrial organisation. Tens of thousands of messages have to be intercepted, logged, deciphered, translated, and evaluated, and the intelligence product has to be distributed quickly and securely to commanders in the field. This operation is described from a number of viewpoints, including those of technical, clerical and military staff.

The book is not however devoid of new material of technical interest. The most significant article is probably one by Jack Good on how German teleprinter traffic was first cracked using a device called 'Heath Robinson', which performed a rudimentary correlation attack using paper tapes, and then using the Colossus, which did the necessary Boolean logic in thyratrons.

Other articles show that the high level cipher machine traffic was only part of the operation. A range of manual ciphers were used in the field by both Germans and Japanese, and a number of these are described. Bletchley also had its failures, and as these were mainly due to management rather than technical problems, the lessons are as relevant today as they were fifty years ago.

Given that all the contributors are now over sixty five years old, and some are in their 80's, this book comes none too soon. It is a very welcome addition to the literature on the subject; it certainly makes the history of the period come alive.

'APPLICATIONS OF FINITE FIELDS'
AJ Menezes, IF Blake, XH Gao, RC Mullin, SA Vanstone, T Yaghoobian
Kluwer 1993, ISBN 0-7923-9282-5

This book is the result of a 10-week seminar in finite fields held at the University of Waterloo. It does not attempt to compete with Lidl and Niederreiter's definitive textbook, but instead focusses on a number of areas of recent research, from self-dual bases through algebraic geometry codes.

The other topics are factoring polynomials over finite fields and the related problem of constructing irreducible polynomials; the characterisation of normal elements and the construction of normal bases; the recent Gao-Lenstra classification of optimal normal bases; a review of discrete log algorithms, including index calculus and its Gaussian integer variant; and elliptic curve cryptosystems.

Each chapter presents a corpus of recent research results, and the book as a whole provides a useful survey of current work in the field.

'ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS'

AJ Menezes

Kluwer 1993, ISBN 0-7923-9368-6

Since Miller and Koblitz introduced elliptic curve cryptosystems eight years ago, there have been about a hundred research publications on the subject, and a number of systems have been fielded. However, these systems use results from algebraic number theory and, more recently, algebraic geometry with which many working cryptologists are unfamiliar.

This book attempts to close the gap by providing a systematic exposition of the relevant results. It includes much material not easily available elsewhere; there is a good treatment of curve isomorphism classes, including an elementary proof of Waterhouse's theorem, and this treatment is especially detailed for the case of characteristic two (which being mainly a concern of cryptologists tends to get ignored in the more general mathematical texts).

There is also a clear exposition of the techniques available to reduce elliptic logarithms in the singular and supersingular cases, and a treatment of Schoof's algorithm which may make it more widely understood.

On the presentational side, the book falls somewhat between two stools: being written at the level of a research paper, it neither explains the basic concepts thoroughly enough to be an introductory text, nor contains enough detail to serve as a reference book for the working mathematician. Many proofs are omitted, and for some of these the reader is referred to an obscure technical report; and the uses of elliptic curves in factoring and primality proving are barely touched on.

Nonetheless, the author has put together a fairly complete compendium of the results which are of immediate relevance to anyone considering building an elliptic curve cryptosystem, and communicates some of the practical know-how which he and his colleagues have acquired while doing just this. The book should enable many working cryptologists to acquire a deeper understanding of this growing subject.

'TOWARDS SECURE OPEN SYSTEMS'

P Overbeek

Published by the author at PO Box 495, NL-2600 AL Delft, The Netherlands; ISBN 90-9005824-9

This book is the result of a project called SEDIS, for Security in Distributed Systems, which was undertaken at TNO (the Dutch organisation for applied scientific research). Its thesis is that technology will force a greater reliance on technical rather than organisational security measures; it explores a number of current standardisation initiatives by ISO, ECMA and CCITT, and concludes that none of them is adequate. In particular, the proposed mechanisms are weak at dealing with real organisational structures, and at coordinating the elements of an open system; and the interaction between networks, operating systems and applications is not always handled well.

The proposed solution is an architecture which integrates the network and operating system protocol stacks, and an intermediate Security Service layer at level 7, which takes over the traditional functions of an operating system TCB and implements an extended Clark-Wilson security policy model. The security mechanisms can be tailored according to the amount of trust placed in the various security domains involved; this involves combining the vertical (operating system) and horizontal (network) issues in intelligent ways. The project's main contribution is probably in that it provides the means to discuss these simultaneously, and to relate them to the underlying trust relationships.

‘FORMAL METHODS AND DIGITAL SYSTEMS VALIDATION FOR AIRBORNE SYSTEMS’
J Rushby
NASA Contractor Report 4551, NA81-18969 (Dec 1993)

This book studies the nature and efficacy of formal methods, particularly in airborne systems. The author explores the various levels of rigour available, and the effects of applying them at various stages of system development. There is a lot of material on the various formal tools available and on airborne system failures; but the actual experience of using formal methods, in tasks ranging from avionics to TCSEC evaluations, is mixed. There is slight evidence of increased assurance, and little documentation of the effects of quality methods on safety critical software. Since most actual faults are caused by poor communication between design teams, and particularly by poorly understood interfaces, and since skill shortages force formal methods to be reserved for the hardest problems. the author recommends that they should be focussed on clarifying design descriptions. He also recommends that systems which need high levels of assurance should not rely on software alone, but should buttress it with mechanisms depending on different technologies, such as control cables and hydraulics.

‘APPLIED CRYPTOGRAPHY’
B Schneier
Wiley 1994, ISBN 0-471-59756-2

This massive book brings together much of modern cryptography in a form which is accessible to the nonspecialist. It provides a very extensive and readable tutorial on the theoretical and practical background to modern cryptology.

It opens with a discussion of what cryptography can do, and shows that it is not limited to confidentiality; a large number of concepts such as blind signatures, fail-stop signatures, zero knowledge proofs, bit commitment, digital cash and secure multiparty computation are explained.

The core of the book is a series of chapters on cryptographic algorithms. They describe dozens of secret and public key systems, and cover most published algorithms of significant practical use. Once this foundation has been laid, and the various hashing and signature schemes have been explained, the author proceeds to show how to use the toolkit, and in particular how to implement protocols such as blind signatures and zero knowledge proof. He also covers advanced topics such as subliminal channels, secret sharing and quantum cryptography.

The final part of the book, entitled ‘The Real World’, firstly discusses how cryptography is used in computer networking, covering commercial protocols such as IBM’s key management scheme and Kryptoknight, the ISO authentication framework, and the competing email products PEM and PGP. It goes on to discuss the political issues - the controversy surrounding patents, export licensing and the US government’s key escrow initiative. Finally, a bibliography of 908 items points to much of the significant research material.

One can always nitpick: there could be more on stream ciphers, on the formal verification of cryptographic protocols, and on banking and military systems. However, the book is aimed at bringing the essentials of modern cryptography to the working computer programmer, and succeeds in its mission. It includes source code for algorithms such as DES, IDEA, MD5 and SHA, as well as for historical curiosities such as Lucifer and Enigma. This is supplied on diskette to readers in North America; US ‘national security’ considerations mean that the rest of us have to scan or type it in from listings in the appendix.

How to Subscribe

Subscription orders are accepted for complete volumes only, starting with the first issue of any year. Continuing orders can also be made, and cancellations are accepted prior to the first issue of the year to which they apply. Claims for replacement of issues lost or damaged in the post should be made within six months.

Subscription rates: Regular subscriptions cost £95, and individual subscriptions are available at the reduced rate of £60. Purchase orders are accepted for regular subscriptions only. US Dollar cheques are accepted at an exchange rate of US$1.50 = £1; credit card orders (VISA and MasterCard) are charged in sterling.

Back issues offer: Get a 1994 subscription plus a complete set of 1992 and 1993 back numbers at a price of £90 for individual subscribers and £145 for regular subscribers. This back number offer is only available while stocks last.

Individual subscription for v 3 (1994) - Please debit my VISA/MasterCard with £60 ☐ I enclose a cheque for £60 ☐ / US$90 ☐

Individual subscription for all issues to end 1994 (v 1, 2 and 3) - Please debit my VISA/MasterCard with £90 ☐ I enclose a cheque for £90 ☐ / US$135 ☐

Regular subscription for v 3 (1994) - Please debit my VISA/MasterCard with £95 ☐ I enclose a purchase order ☐ / cheque ☐ for £95 ☐ / US$142.50 ☐

Regular subscription for all issues to end 1994 (v 1, 2 and 3) - I enclose a purchase order ☐ / cheque ☐ for £145 ☐ / US$212.50 ☐

Name: ....

Card number: .... **Expiry Date:** ....

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

You can fax this order form to us on +44 223 334678, or mail it to us at:
Northgate Consultants Ltd., Ivy Dene, Lode Fen, Cambridge CB5 9HF, UK