Computer and Communications
Security Reviews

Volume 2 Number 4 (December 1993) ISSN 1352-6278

CONTENTS

This journal reviews research in computer and communications security. Work published in major journals and conferences will be 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 26 November 1993; and books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Laser Communications 93: Proceedings of Free Space Laser Communications Technologies V, 20-21/1/93 Los Angeles, *proceedings published by SPIE volume 1866*
Computer Arithmetic 93: 11th symposium, Los Alamitos, *proceedings published by IEEE Computer Society Press, 1993*
IFIP SEC 93: 9th IFIP International Conference on Computer Security, 12-14 May 93, Ontario, *published by North-Holland, Elsevier Science Publishers BV ISBN 0-444-81748-4*
COMPASS 93: proceedings of the Eighth Annual Conference on Computer Assurance, 14-17/6/93, NIST, Maryland *proceedings published by the IEEE, ISBN 0-7803-1251-1*
Crypto 93: 22-26/8/93, Santa Barbara, *proceedings to be published in Springer LNCS series; page numbers given here are for preproceedings*
SRIWIT 93: 6th Joint Swedish-Russian International Workshop on Information theory, 22 - 27/8/93, Mölle, Sweden, *proceedings published by Studentlitteratur, Lund 93, ISBN 90-7167-002-5*
SICON/ICIE 93: IEEE Singapore International Conference on Networks and Information Engineering, September 1993, *proceedings published by IEEE Press*
Usenix Security 93: UNIX Security Symposium IV, 4-6/10/93, Santa Clara, *proceedings (ISBN 1-880446-55-3) available from USENIX Association, Berkeley, CA, USA*

We regret that, due to the large number of conferences which take place toward the end of the year, we have had to hold over covering two of them (NCSC and the ACM Conference on Computer and Communications Security) until volume 3.

We also regret that UK 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

024101 'Strategy for the future'
NR Achs, *Cards International no. 90 (22/7/93) pp 10 - 11*
VISA's card security strategy is described in this article. Fraud will be fought by transaction monitoring at interbank switching centres, and smartcards will be used for value added functions rather than risk control.

024102 'Catching the phantoms'
D Austin, *Banking Technology (Sep 93) p 24*
This article covers the current UK dispute over phantom withdrawals from ATMs, and reports the positions of the banks and the solicitors representing the plaintiffs in a class action against them.

024103 'Report - SIBOS 93'
D Austin, *Financial Technology Insight (Oct 93) pp 6 - 8*
This article reports the annual SWIFT conference in Geneva, with policy statements from the CEO and major users. The live issue is that many large corporations are demanding direct access to the international banking network.

024104 'Netzwerksicherheit durch selektiven Pakettransport'
F Bauspieß, P Horster, S Stempel, *Universität Karklsruhe EISS report 93/1 (in German)*
The authors report a project at EISS in which the address resolution protocol in TCP/IP is manipulated by a gateway in order to isolate the local network from the Internet. The effect is that only those machines with direct outside access (such as mail and news servers) need to be fully secured against outside attack. This system is implemented and in service.

024105 'Privacy and Authentication on a Portable Communications System'
MJ Beller, LF Chang, Y Yacobi, *IEEE Transactions on Strategic Areas in Communications v 11 no 6 (Aug 1993) pp 821 - 829*
The authors propose three protocols for key distribution and authentication in cellular telephone networks and other systems where the computing power of the terminals is limited. These protocols are based on the Rabin and Diffie-Hellman schemes and are designed to provide privacy, prevent billing fraud, or both.

024106 'Packets Found on an Internet'
SM Bellovin, *Computer Communications Review v 23 no 3 (July 93) pp 26 - 31*
This describes the security and monitoring features implemented at Bell Labs' Internet gateway, and reports a number of strange packets which it has caught. Some of them were clearly security events, while others were probably software and network artefacts; a number of bugs seem to be masked by the resilience of the Internet.

024107 'Software Auditing: Effectively Combatting the Five Deadly Sins'
P Berner, *Information Management and Computer Security v 1 no 3 pp 11 - 12*
In the US there are 1.3 software products sold per cpu; in the UK the figure is 0.85. A monitoring product, called FPRINT, is described which uses checksumming to identify which products have been legally installed.

024108 'NREN security issues: policies and technologies'
DK Branstad, *Computer Security Journal v 9 no 1 (Spring 93) pp 61 - 71*
The National Research and Education Network (NREN) is part of a federal initiative to improve the U.S. government's information technology. The security issues of this network are discussed.

024109 'Winds of exchange'

G Booth, *Banking Technology (Oct 93) pp 40 - 44*

This article discusses EDI security problems, and reports an initiative from the UK banking industry to improve this. The development is based on digital signatures; secret keys can be kept on smartcards or on personal diskettes. Trusted third party services may be used, and there may be an effect on the EC's TEDIS project and on the international EDIFACT message standard.

024110 'UNIX Security Update'

JM Carlin, *Usenix Security 93 pp 119-130*

This is a fifth anniversary status report on the California-based telephone company Pacific Bell's security program - management support, standards, training, tools, and product reviews. The author describes today's major concerns, which focus on networked computing. Pac Bell logs a copious amount of activity, reduces it with software, and actually looks at 3-4 pages a day. Unauthorised access attempts such as finger and ftp attacks are identified and reported. Outside probes tend to use log_tcp and reverse fingers, and come from local universities, foreign countries, and now Internet pay services.

024111 'Fighting the infection'

A Campbell, *Financial Systems (Autumn 93) pp 25 - 26*

The author discusses problems with virus specific countermeasures such as scanners, and proposes instead to control an organisation's diskette population and thus get protection against all possible kinds of externally written malicious code. He suggests using disk authorisation programs to implement this.

024112 'The cryptographer who took a crack at "junk" DNA'

A Coghlan, *New Scientist (26 June 93) p 15*

Correlation analysis techniques suggest that the introns in DNA (the sequences which fill the gaps between the exons or genes) may act as a kind of error detecting or even error correcting code. Three quarters of the bits in an intron can be predicted from neighbouring exons.

024113 'High Confidence Visual Recognition of Persons by a Test of Statistical Independence'

JG Daugman, *IEEE Transactions on Pattern Analysis and Machine Intelligence v 15 no 11 (Nov 93) pp 1148 - 1161*

The author presents a new biometric technique - identifying individuals by analysing the pattern of fine lines in the iris. This separates individuals much better than other biometrics, for a number of reasons. Firstly, there are over 170 degrees of freedom in each eye's pattern, and with little genetic penetration into this feature, all eyes are quite different (even those of a single individual); secondly, the iris is easy to detect in a video picture, does not wear out, and has its own cleaning mechanism; and thirdly, a living eye can be distinguished from a picture of one by the fact that the diameter of the pupil is constantly fluctuating. The upshot is that individuals can be recognised with a probability of fraud of 10^{-20} and below.

024114 'Future pattern: chips with everything'

L de Rauglaudre, *Cards International no. 96 (27/10/93) debit card special p 9*

A smartcard manufacturer argues that in addition to security, these devices can offer new services such as loyalty programmes and low value prepayments.

024115 'Security for EDIFACT Messages'

BB Di Turi, *Computers and Security v 12 no 5 (Aug 93) pp 447 - 455*

This article describes the status of UN standards work on EDIFACT security. Documents on digital signature and the security framework have already been issued; confidentiality, key management and implementation standards are still in the pipeline. The basic mechanism consists of adding appropriate headers and trailers to standard message formats.

024116 'Getting it taped'

M Dorvill-Evans, *Financial Systems (Autumn 93) p 48*

This article surveys voice recording technology and applications. Open tape systems are still prevalent, but VHS and optical disk systems can provide greater volume and faster access repectively. Digital techniques will come into their own once compression technologies mature and are adopted.

024117 'Single sign-on technology streamlines network access'

J Edwards, *Software Magazine (Nov 93) pp 35 - 40*

Administrators need to balance security concerns with easy access to their networks. Single sign-on products may help to resolve the more obvious conflicts here, but lack of standards are a concern.

024118 'Electronic Trade Confirmation: A Review of Progress Made to Date'

J Essinger, *Financial Technology Insight (Sep 93) pp 11 - 14*

Electronic confirmation of financial trades made over the telephone is a fast growing application; its benefits lie not just in reducing risk, but in facilitating rapid portfolio reporting and management. A number of UK bodies, including the Inland Revenue and the Securities and Investments Board, now accept such electronic confirmations as binding.

024119 'An analysis of security issues in a DOS-based implementation of Kerberos'

A Feldman, S Kanungo, *Computer Security Journal v 9 no 1 (Spring 93) pp 15 - 25*

This paper deals with issues relating to "Kerberizing" DOS applications. It discusses the design criteria involved, the advantages and the pitfalls.

024120 'Encryption and error correction codes for reliable file storage'

J Fernández-González, GB Agnew, A Ribagorda, *Computers and Security v 12 no 5 (Aug 93) pp 501 - 510*

The authors discuss combining encryption, interleaving and error correction coding in file storage systems. They analyse the various combinations in terms of whether a message can be recovered after a burst error.

024121 'Accounting for EDI'

Financial Technology Insight (August 93) pp 16 - 19

Accounting standards vary across the EC, being especially structured and uniform in France, and much more adaptable to a company's trading practices in the UK. National accounting organisations have therefore set up EDIFICAS, a body whose task is to define standard accounting messages for EDI. They have run into problems with admissibility of computer records, especially as certain hard copy documents traditionally had to be signed, and have suggested that these signature requirements be abolished.

024122 'Anti-counterfeit trials begin with watermark technology'

Financial Technology International Bulletin v XI no 2 (Oct 93) pp 6 - 7

VISA is beginning trials of watermark magnetic strip technology with 30,000 cards in Nottingham, England. This technology embeds a unique serial number in the magnetic strip to make counterfeiting hard; it is already in use in Sweden.

024123 'Ten years of FTIB'

Financial Technology International Bulletin v XI no 1 (Sep 93) pp 3 - 4

Reviewing 10 years of banking technology, the success stories were ATM sharing, digital dealing rooms, card authorisation terminals, open systems, home and office banking via PCs, and customer based (rather than account based) ledger systems. The four non-starters were smartcards, interactive video, financial EDI and artificial intelligence.

024124 'UK banks explore fingerprint technology'
Financial Technology International Bulletin v XI no 3 (Nov 93) pp 3 - 4
This article reports a product demonstrator by EDS which compresses fingerprint features into 10 - 64 bytes, enabling storage on a magnetic strip card. The claim is a fraud rate of 5%, with an insult rate close to zero.

024125 'Taking Stock of LAN Security'
T Garon, *Info Security News v 4 no 5 (Sep 93) p 23*
Local area networks are growing in complexity and sophistication, making the task of securing them more dependent on the tools available, a number of which are described.

024126 'Magnetic stripe versus chip card"
G Gysels, *Cards International no. 96 (27/10/93) debit card special pp 8 - 9*
A senior Belgian banker argues that online checking, rather than a move from magnetic strips to smartcards, is the way forward; and that PINs can be used at the point of sale provided the terminals have a secure encryption module and one-time keys are used. Chip cards are too expensive, and he claims that the chip failure rate has been 3% where these cards have been used as real payment cards, as in France.

024127 'French thieves turn to ATM fraud'
Information Security Monitor v 8 no 11 (Oct 93) pp 3 - 4
Crooks in Paris attached false fronts to ATMs to capture cards and PINs; some banks there recommend that customers only use ATMs with sliding fronts.

024128 'US Chemical Bank ATM fraud netts $357,000'
Information Security Monitor v 8 no 10 (Sep 93) pp 1 - 2
The recent merger of Chemical Bank with Manufacturers Hanover meant that, from the 11th to the 30th May, their ATMs did not check account numbers and available balances. The result was the largest ATM loss ever admitted in the USA.

024129 'The Architecture and Implementation of Network Layer Security in UNIX'
J Ioannidis, M Blaze, *Usenix Security 93 pp 29-39*
The authors describe a software security product, swIPe, which secures the Internet Protocol layer and is available for SunOS, BSD, and Mach. Its building blocks are IP encapsulation, sequence numbering, MD5, and DES; it works on IP networks, is higher-layer transparent, and is decoupled from key management. Features include source authentication, data integrity, and confidentiality; it can be run from the firewall outward, end-to-end, or between firewalls. A throughput of 1000 packets/second was achieved on a SPARC-2, and the 28-44 byte overhead per packet was most noticeable using interactive protocols.

024130 'Laser communications for covert links'
JL Jaeger, RT Carlson, *Laser Communications 93 pp 95 - 106*
The authors describe a prototype laser communications system built by MITRE and others to replace military line-of-sight RF communications. The devices operate in the infrared; this not only increases the difficulty of detection, but also provides eye safety at all distances. The design is described, and extensive field tests reported: depending on the weather, the link operates at 1,024, 128 or 16Kbps, and at the lowest of these rates, the system can cope with all conditions except for heavy fog or rain. Excellent covertness is claimed.

024131 'Retrofitting Network Security to Third-Party Applications - The SecureBase Experience'
JI Kamens, *Usenix Security 93 pp 41-57*
This paper describes a Kerberos capable API for SYBASE. It can be difficult for users to retrofit security to object-code-only systems, such as commercial relational data bases; choices

may be severely limited by a shortage of software hooks. The solution described involves putting a software wrapper round the application, either embedded or at a lower protocol layer. Working at the application layer has the advantages of selectivity and platform independence, but may cause problems with performance or maintenance.

024132 'Komponenten informationstechnicher Authentifikationsdienste'
B Klein, F Damm, *Universität Karlsruhe EISS report 93/2 (in German)*
The authors compare the features of Kerberos, SPX and Selane from the point of view of administration and key management. They link this to the technical details of the authentication service provided, and show how design decisions affect the management aspects of such protocols.

024133 'Closing the Gaps in E-mail'
P Korzeniowski, *Info Security News v 4 no 5 (Sep 93) pp 20 - 21*
There are several security problems with current electronic mail systems; this article discusses the practical requirements for security in such systems.

024134 'Data security in X.25 networks'
F Labuschagne, J Roos, *Computers and Security v 12 no 5 (Aug 93) pp 469 - 475*
The authors discuss various options for securing X.25 traffic. The simplest is putting a sequence number and manipulation detection code in the user data field of each packet; encryption is better but involves more work, such as setting up session keys at the start of each virtual call.

024135 'CryptoLib: Cryptography in Software'
JB Lacy, DP Mitchell, WM Schnell, *Usenix Security 93 pp 1-17*
The authors describe a software encryption toolkit called CryptoLib. This provides secure hash functions and both secret and public key cryptographic algorithms. On a Sparc 2, DES performance is 1.2 Mbit/second, and 512 bit RSA decryption runs at 3.2 Kbit/second. The arithmetic routines implement addition chains, Montgomery transformation, Chinese remaindering, and Karatsuba's divide and conquer multiplication. Key generation is supported by two random number generation routines, plus 50 round Rabin testing for RSA keys.

024136 'The Encapsulated Security Services Interface'
P Lin, *IFIP SEC 93 pp 119 - 136*
The author describes a programming interface developed by IBM Canada to separate communications and security functions, and which is targeted at OSF/DCE applications. Its stated goal is to minimise development and upgrade complexity, and to maximise portability; to this end, it uses Kerberos primitives, on top of which another level of interface calls are defined.

024137 'A Generic Security Platform for Workstations'
B Lindberg, *IFIP SEC 93 pp 277 - 286*
Many Swedish government agencies were not allowed to use PCs as they were not considered secure enough to hold personal data. This created tension, and in 1991 a project was started to specify and build a security solution. The resulting device, called an 'Allterminal', consists of a PC with a smartcard reader for keys, and software to handle encryption and authentication.

024138 'A survey of intrusion detection techniques'
TF Lunt, *Computers and Security v 12 no 4 (June 93) pp 405 - 418*
This article surveys tools which trawl through audit data to try and find indications of wrongdoing, and discusses SRI's IDES in particular detail. Such systems may be online or after-the-fact; they may just monitor gross usage patterns, or go so far as to keep checking users' keystroke dynamics. Their effectiveness is hard to assess; one way forward may be to build products which monitor a system in several ways at once. This could have the added benefit of trapping intruders who are sophisticated enough to mask their activity; such activity may only be detected if we can compare audit data from the application, command line and system call levels.

024139 ‘A Smart Approach to Security’
B Miller, *Info Security News v 4 no 5 (Sep 93) pp 22 - 28*
This article discusses the applications of smart cards; technical refinements, new standards, and lower costs are all said to have helped the acceptance of this technology.

024140 ‘Credit Cards get high-tech security’
M Moeller, *Computer Fraud and Security Bulletin (Nov 93) p 7*
This reports credit card security plans: in VISA’s new CardShield programme, watermark and holomagnetic features will be introduced to credit card strips over a number of years; while Mastercard has started to require that all new cards contain a 3-digit cryptographic card validation code on the strip.

024141 ‘Italian ATM fraud’
S Ongetta, *Computer Fraud and Security Bulletin (Nov 93) p 3*
Three villains in Italy, plus a former bank employee, managed to intercept ATM data traffic on the local loop to the exchange. They harvested card and PIN data, and had planned to forge cards en masse and use them over the weekend, when the machines are offline; had they not been detected, the loss could have been of the order of $10m.

024142 ‘Cellular phones offer chip opportunity’
D Robinson, *Cards International no. 98 (24/11/93) p 10*
Many cellular phones have smartcard readers; cards are used as subscriber identity modules. VISA is investigating the possibility of introducing multifunction smartcards which can be used to deliver banking products as well as activating telephone services.

024143 ‘Paradigms for Verification of Authorisation at Source of Electronic Documents in an Integrated Environment’
S Russell, *Computers and Security v 12 no 6 (Oct 93) pp 542 - 549*
Many frauds are caused by employees exceeding their authorisation level in ordering goods and initiating other transactions. EDI gives an opportunity to automate checks, which could be carried out by either party to a transaction or even by a trusted third party. However, there is a conflict here: the receiver will want to perform the checks because of his legal duty to act with reasonable care, while the sender will want to control the checks for reasons of privacy, cost and standards.

024144 ‘A force to reckon with’
I Ryan, *Cards International no. 90 (22/7/93) pp 12 - 14*
In an interview, the chairman of Cartes Bancaires in France describes the success of smartcards in producing a fraud rate of 0.08% against Mastercard’s 0.2% and VISA’s 0.1% in 1992, and discusses various implementation and reliability problems.

024145 ‘Fraud remains a serious problem’
I Ryan, *Cards International no. 90 5 (7/10/93) p 12*
Speakers at the EFMA smartcard conference in Brussels in September gave fraud figures of 0.05% for France, 0.06% for Belgium, 0.1% for Italy (down from 0.9% in 1990) and 0.3% in the UK (up from 0.12% in 1988). British speakers described measures being taken to improve their position.

024146 ‘Secure RPC Authentication (SRA) for Telnet and FTP’
DR Safford, DK Hess, DL Schales, *Usenix Security 93 pp 63-67*
After a major series of intrusions, during which passwords were stolen from their network, Texas A&M University decided to authenticate Telnet and ftp. They used Sun’s secure RPC (a 192-bit Diffie-Hellman key exchange) before the Telnet and ftp authentication. The Diffie-Hellman result provides a DES key to encrypt the password sequence.

024147 'The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment'
DR Safford, DL Schales, DK Hess, *Usenix Security 93 pp 91-118*

The authors describe a Unix security system developed in response to massive and recurring intrusions at Texas A & M University: attackers had exploited backdoors and Trojan Horses; IP tunneling; vulnerabilities in NFS, rdisk, and rsh; and eavesdropping to gain passwords. The new system includes tools for packet filtering (Drawbridge), monitoring (Netlog), and host checking (Tiger). Drawbridge lets through only SMTP, DNS, and after passing tests, Telnet and ftp traffic, and nearly 100 attempted intrusions are now detected per month. Netlog tools collect three million bytes a day, from which an extractor eliminates routine records. Etherscan monitors service protocols like Telnet and ftp for suspicious logins, traffic that looks like tunneling, and UDP attacks on RPC. Statistics on protocols and ports are used to identify unusual activity. Tiger scripts are used to check host security: they constantly probe login access, anonymous ftp, NFS exports, inetd, .netrc, PATH for root, file permissions, hash sums of files and patches, embedded pathnames, e-mail aliases, cron files, group files, password files, printcap files, and .rhost files; and look for file system anomalies and evidence of break-ins.

024148 'Network Security: Unsafe at Any Node'
S Salamone, *Data Communications v 22 no 12 (Sep 93) pp 61 - 68*

This survey article describes the features of fourteen network security products.

024149 'Tearing up the rules'
P Sampson, *Banking Technology (Nov 93) pp 26 - 30*

Mellon Bank has installed a neural-net-based monitoring system which checks card transactions every two hours and looks for abnormal activity. It is claimed to be substantially more effective than rule-based systems.

024150 'Secure E-Mail Cheaply With Software Encryption'
P Strauss, *Datamation v 39 no 23 (1/12/93) pp 48 - 50*

This article reviews the use of encryption by email software packages and service providers. At present, none of the facilities offered are compatible with other suppliers' offerings, but this may change with the adoption of PEM in the next generation of products.

024151 'ATP - Anti-Tampering Program'
D Vincenzetti, M Cotrozzi, *Usenix Security 93 pp 79-89*

The authors describe a file integrity checker which is intended to detect a virus or Trojan Horse after an intrusion. Network attacks include using NIS to obtain the password file, NFS to mount one's own disk, DNS to gain information or trick daemons like rsh, and IP source routing to penetrate router protection. The damage may range from a mere nuisance to altered files, backdoors, and regenerating viruses. ATP keeps an encrypted table of attributes (owner, size, times, checksums) for each file in a Unix system; it works with NFS and handles symbolic links.

024152 'A Software-based Communication Security Facility for RHODOS and the Study of the Cost of Providing Secure Communications'
M Wang, A Goscinski, *SICON/ICIE '93 pp 409 - 415*

This paper describes the design and implementation of the RHODOS communication security facility which provides software message encryption. The facility is implemented at the transport layer, and supports both DES and LOKI. The cost of providing secure communication in RHODOS is studied.

024153 'Variable-length error-detecting codes'
HG Zhang, ZP Qin, *Chinese Journal of Computers v 16 no 7 (July 93) (in Chinese)*

The authors present variable-length error correcting codes, analyse their capabilities, and suggest that they be used to detect computer viruses.

2 Operating System and Database Security

024201 'UNIX Job Openings'
2600 Magazine (Autumn 93) pp 16 - 17
This is a beginner's guide to the ways in which Trojan horse programs can be constructed in UNIX using shell scripts which abuse the suid command.

024202 'Extending the ISO access control framework for multiple policies'
MD Abrams, MV Joyce, *IFIP SEC 93 pp 343 - 358*
Where multiple access control policies are imposed by different domain authorities, the reference monitor (access control enforcement function) may have to resolve input from a number of these authorities (probably using votes of the form 'allow', 'forbid' and 'don't care'). Nonetheless it can still separate the enforcement of the policy from the policy itself.

024203 'Sendmail without the Superuser'
ME Carson, *Usenix Security 93 pp 139-144*
IBM set out to apply the principle of least privilege to the UNIX sendmail command, and thus hope to limit the impact of any remaining security holes. Sendmail can be run in user mode, daemon mode for retries, or network daemon mode; it needs privilege to access users' mailboxes, change ownership of files, and bind to TCP port 25. IBM split the program into a larger, unprivileged part and a smaller part set to group mail rather than user root. It did not tackle multi-level secure mail, or systems in which mail triggers program execution.

024204 'Operating system protection through program evolution"
FB Cohen, *Computers and Security v 12 no 6 (Oct 93) pp 565 - 584*
One systematic problem in security is blocking a dynamic attack with a static defence. The author suggests that making some of the defences dynamic might drive up the cost of an attack; he suggests that defensive code should be obscured using techniques such as instruction reordering and garbage insertion.

024205 'The technology of safety and security'
J Cullyer, *The Computer Bulletin v 5 no 5 (Oct 93) pp 10 - 13*
The author compares safety and security kernels; the latter are widely researched (even if little implemented), while very little work has been done on the safety side at all because of the critical systems culture of minimising software risk by writing in assembler on a bare machine. Nonetheless there are a lot of common problems with specification, implementation and validation.

024206 'Designing Secure and Reliable Applications Using FRS: an Object-Oriented Approach'
JC Fabré, Y Deswarte, B Randell, *University of Newcastle upon Tyne Technical Report 438 (7/93)*
The use of fragmentation, redundancy and scattering can provide both confidentiality and fault tolerance in distributed processing; the idea is to chop up data and applications in such a way that the fragments are no longer sensitive. Examples of such decompositions are the medical and administrative parts of hospital records, name and salary information on payrolls, and key fragments in threshold signature schemes. The main practical difficulty lies in this decomposition, and it can usually be tackled by successive refinement. Finally, implementation issues are discussed; a sizeable test of the concept was carried out by implementing a distributed diary.

024207 'On security policy modelling'
JW Freeman, RB Neely, *COMPASS 93 pp 61 - 69*
Understanding security policy models is not trivial; there may easily be confusion about what a formal model represents. If it is not comprehensible, a model is unlikely to increase security. Experience of a number of projects is presented, and it is argued that a plain language model

which lies between the policy statement and the formal model is a good way to bridge the gap; it helps the modelling team to focus on important features, and enables the design to be reviewed by a wide audience.

024208 'Turning Multiple Evaluated Products into Trusted Systems with Assurance'
D Gambel, J Fowler, *IFIP SEC 93 pp 195 - 206*

The authors discuss some of the problems of developing trusted systems from evaluated components. Many developers adopt a strategy of selecting products and modifying them to resolve feature conflicts, with the result that the system architecture ends up tied to external dependencies.

024209 'The Monday Morning Syndrome'
Information Security Monitor v 8 no 12 (Nov 93) pp 5 - 7

This article gives the technical background to a recent hacking case, in which Paul Bedworth was acquitted but two other men were convicted after an attack on JANET. A trap was set: Sun's x25trace program was renamed 'screenblank' and its output directed to overwrite a dummy file. This showed the attackers making probes against 122 machines at 70 different sites, and of these 68 (on 40 sites) were penetrated. The modus operandi was to gain superuser access using a known weakness in BSD, and then replace login with a trojan.

024210 'SUID and SGID based attacks on UNIX: A look at one form of the use and abuse of privileges'
R Kaplan, *Computer Security Journal v 9 no 1 (Spring 93) pp 73 - 77*

This paper discusses a set of security problems with the Unix operating system, which are based on abusing the suid and sgid commands.

024211 'Mainframe Controls in a Decentralized Environment'
R Kay, *Info Security News v 4 no 4 (Jul 93) pp 16 - 17*

There are problems in applying the traditional security techniques from the mainframe world to a client-server environment. The solutions proposed by different mainframe security product vendors are discussed.

024212 'Monitoring File System Integrity on UNIX Platforms'
G Kim, G Spafford, *Info Security News v 4 no 4 (Jul 93) pp 21 - 22*

There are several Unix products that check file integrity. This article discusses the technology of integrity checking, existing Unix products, and desirable features for future products.

024213 'Historical Labels in Open Distributed IT Systems: an ITSEC/ECMA Specification'
S Kowalski, *IFIP SEC 93 pp 207 - 226*

This article reports a Swedish military project on the incorporation of historical clearance information in systems. Many real world clearance procedures involve 'historical labels' such as passports and cv's, and constantly validating these can be inefficient. This motivates the use of history certificates which can be attached to objects; such certificates are also useful when a user is revoked for treachery, as they limit the scope of the subsequent 'disinfect' operation. A model for historical label servers is presented; these track which objects are initiators, and which targets, of changes. Finally, the author discusses the relationship of this work to ITSEC and the ECMA model, and the related management, audit and enforcement mechamisms.

024214 'System data ownership in IBM MVS systems'
LG Lawrence, *Computer Fraud and Security Bulletin (Aug 93) pp 10 - 15*

MVS has complex data structures, with naming conventions which vary from one site to another. Ownership assignment would be rather complex, and instead a scheme is proposed where each dataset has an owner (a user or the whole organisation), an agent (typically one or more systems programmers) and a custodian (the operations staff).

024215 'Toward a model of security for a network of computers'
WH Murray, P Farrell, *Computer Security Journal v 9 no 1 (Spring 93) pp 1 - 13*

This paper proposes a model for evaluating the security of networks of computers: it focusses on the security of a collection of composed systems, rather than on the security of the connecting infrastructure.

024216 'Knowledge-based Key-hole Monitoring of Users for Security Control in Transaction Processing Systems'
VK Murthy, EV Krishnamurthy *SICON/ICIE'93 pp 416 - 420*

This paper considers the interrelationships between knowledge-based security, concurrency and recoverability in on-line database transaction processing systems (OLTP). It describes how OLTP can permit a user to carry out the desired actions, and concurrently activate scrutinizing transactions that identify the user with respect to his/her biometric or other characteristics.

024217 'Approximating Clark-Wilson Access Triples with Basic UNIX Commands'
WT Polk, *Usenix Security 93 pp 145-154*

Clark and Wilson developed an integrity framework based on triples (x can modify y with program z) that required complex access control rules: it described constrained and unconstrained objects, and derived integrity requirements for constrained objects. Clark-Wilson triples turned out to be hard to implement; but this paper constructs a method of using the Unix set user and set group mechanisms, together with ownership and access permission bits, to simulate them. The construction contains an error due to the way set user implements groups.

024218 'Superseding Manual Generation of Access Control Specification - From Policies to Profiles'
D Pottas, SH von Solms, *IFIP SEC 93 pp 327 - 342*

The authors report a project to generate access profiles for mainframe access control systems automatically, and discuss the experience with their prototype. Problems mostly had to do with redundancy and consistency, although the unorthodox authorisations needed by some applications were also a nuisance.

024219 'Open Systems Security Standards'
M Reitenspiess, *Computers and Security v 12 no 4 (June 93) pp 341 - 361*

This article discusses the historical evolution and scope of TCSEC and ITSEC, and their application to compartmented mode workstations by X/Open. The Commercial IP Security Option (CIPSO) is briefly described, as are the trusted session management functions and the SDNS protocols for secure LAN and email; although these are military products, a commercial version may be produced. Security is starting to affect all the standards in distributed computing, and the activities of the various standards committees are described.

024220 'Assigning probabilities for assurance in MLS database design'
L Russell, *COMPASS 93 pp 99 - 109*

It is extremely hard to eliminate aggregation and inference problems completely in multilevel secure databases, and the author had previously proposed a probabilistic model to make this problem more tractable. Here he elaborates the theoretical basis of this work; assigning probabilities is somewhat like assigning security levels, and is handled by a functional data model.

024221 'Lattice-Based Access Control Models'
RS Sandhu, *IEEE Computer v 26 no 11 (Nov 93) pp 9 - 19*

The author provides and introduction to computer security theory, covering access matrices, discretionary and mandatory access control, the Bell-LaPadula and Biba models, Denning's axoims for a lattice, the lattices of Smith and Lipner, and the Chinese Wall model (which he shows can also be expressed in lattice form).

024222 'Added-on security for MVS: weaknesses and measures'
C Schramm, *Computers and Security v 12 no 4 (June 93) pp 379 - 388*
This article describes the interface between MVS and RACF in some detail, and highlights a number of vulnerabilities in the path between the two. Audit points are summarised: the MVS and RACF router tables must be in synch; the MVS router exit and the CICS Program Control Tables must be in order; and there are a number of other places where system programmers frequently put routines which may have an adverse effect on security. Just looking at the RACF dataset, as many auditors do, is quite inadequate.

024223 'Developing Secure Systems in a Modular Way'
Q Shi, JA McDermid, JD Moffett, *COMPASS 93 pp 111 - 121*
The authors argue that one should define security in terms of module interactions. This approach is natural when considering composable trusted systems, and has the added benefit that knowing which components actually need which security properties enables designers to avoid overspecification, and facilitates maintenance and upgrade. They develop a formal apparatus of state machines, traces and matrices which relate events; security properties become problems of matrix matching.

024224 'Integrity in object-oriented database systems'
JM Slack, EA Unger, *Computers and Security v 12 no 4 (June 93) pp 389 - 404*
Deciding where to put integrity constraints in an object-oriented database is nontrivial. A variety of constraints are considered, especially those involving relations between objects; the author suggests that, in order to avoid breaking encapsulation, security should be provided by an upper layer which acts on the results of methods.

024225 'Towards Secure, Optimistic, Distributed Open Systems'
JF Snook, *University of Hertfordshire Division of Computer Science Technical Report no 151*
This report describes a distributed office document architecture whose security properties are based on a trusted visibility server. This server contains the names and hashcodes of all authorised documents in the system, and provides them to users on demand; it also enforces agreed rules on which combinations of users need to sign an update of an authorised document. This architecture can deliver a very wide range of integrity functions, and the amount of code that must be trusted is small enough to be verified by each participant if he wishes to. The report also has an extensive literature survey of integrity in distributed operating systems.

024226 'Context-Dependent Access Control in Distributed Systems'
H Strack, KY Lam, *IFIP SEC 93 pp 137 - 156*
The authors report the development of a prototype to tackle this problem: this completely replaces the UNIX security system with an algorithm which makes a user's access rights a function of the access program and time as well as of his user id and group. Programs accessing data carry labels called 'context prescriptors'; a wide range of objects can be used as prescriptors, including pathnames and email addresses, and so prescriptors can be either discretionary or mandatory. This approach helps to manage process dependencies such as nesting and delegation.

024227 'Design of a secure operating system s-unix"
T Yang, FJ Chen, CX Sheng, *Chinese Journal of Computers v 16 no 6 (June 93) (in Chinese)*
The authors describe the design of a secure unix system whose target was a level of assurance at least as good as B2.

024228 'Controlling VM with ACF2'
A Webb, *Computer Audit Update (July 93) pp 8 - 12*
This article provides an introduction to VM security, and discusses the better known back doors which arise when using ACF2 as the main security product. It describes how to close these doors by a suitable choice of installation options.

3 Security Management and Policy

024301 'The 1992 Profile of Computer Abuse in Australia: part 2'
T Adams, *Information Management and Computer Security v 1 no 2 (1993) pp 21 - 28*
This article presents statistics of 184 crimes investigated in 1990-91 in Australia, and compares them with cumulative figures based on 313 claims in previous years. Analyses are given by industry, perpetrator and value of loss.

024301 'Controversy Clouds New Clipper Chip'
M Alexander, *Info Security News v 4 no 4 (Jul 93) pp 40 - 42*
The author discusses the controversy surrounding the U.S. government's Clipper chip initiative, and gives a technical summary of how the key escrowing system works.

024303 'The Risk Data Repository: a novel approach to security risk modelling'
AM Anderson, D Longley, AB Tickle, *IFIP SEC 93 pp 185 - 194*
The authors propose that risk analysis could be improved by creating a registry of information to be used during system development and upgrade. This registry would function as a blackboard to facilitate communication, and in particular to eliminate assumption mismatch between different development teams.

024304 'KGB Foreign Intelligence from Brezhnev to the Coup'
C Andrew, *Intelligence and National Security v 8 no 3 (July 93) pp 52 - 67*
Documents supplied by the defector Gordievski show that although the KGB's foreign intelligence directorate recruited many of the Soviet Union's brightest graduates, it wasted much of its effort in bureaucracy and in inventing reports to please the leadership. Its best foreign agents ceased to be ideologically motivated high flyers, and instead were petty criminals and misfits such as Walker at the NSA and Prime at GCHQ. This explains why an approach from Bettaney at MI5 was turned down as a provocation.

024305 'Computer Crime: ignorance or apathy?'
J Austen, *The Computer Bulletin v 5 no 5 (Oct 93) pp 23 - 24*
The head of Scotland Yard's computer crime squad discusses Britain's Computer Misuse Act, and describes a number of recent cases which have clarified its applicability.

024306 'Dial-In Security Firewall Software'
R Baldwin, J Kubon, *Usenix Security 93 pp 59-62*
Increasing demand for remote access and ubiquitously available modems make dial-in security at large institutions difficult to enforce. Tools include dialback hardware or software and one-time password tokens. The secured terminal server can provide per-user destination control and an extendable front-end. The authors also recommend making administration simple, providing local host protection with rlogin or Kerberos, and using logging and auditing tools.

024307 'Security Architecture in the Third Generation Networks'
A Barba, F Recacha, JL Melús, *SICON/ICIE'93 pp 421 - 425*
This paper compares the security features of the Universal Mobile Telecommunication System with those of the future Public Land Mobile Telecommunication System.

024308 'Teaching Computer Security'
M Bishop, *IFIP SEC 93 pp 65 - 74*
The author describes three 9-week courses taught at Dartmouth College in New Hampshire: an introductory course, and courses on mathematical cryptography and computer security. He presents the syllabi, lists the course books and discusses his teaching experience.

024309 'The Digital Signature Standard: Overview and Current Status'
DK Black, *Computers and Security v 12 no 5 (Aug 93) pp 437 - 446*

This article describes the digital signature algorithm, and some of the controversy surrounding it. In particular, there are many more citations of the RSA paper than the ElGamal one, which indicates that the former is better studied. There remain problems with administrative matters, such as the legal standing of digital sugnatures, but the main benefit of digital signatures may lie in cutting paperwork in low-security applications. The US Army. for example, has saved a lot of money by electronic processing of routine purchase orders.

024310 'International Standards and Organisational Security Needs: Bridging the Gap'
CJ Bosch, JHP Eloff, JM Carroll, *IFIP SEC 93 pp 171 - 184*

The authors present diagrams of the assurance given by the various TCSEC levels in respect of various assurance, documentation and policy features; these features are contrasted in turn with the requirements of the banking sector.

024311 'Licencing embedded programs'
G Bull, *Computer Law and Security Report (Sep/Oct 93) pp 206 - 213*

Where software is embedded in ROM, there is no act of copying from one storage medium to another, and so (at least under English law) it appears that copyright does not apply. Nonetheless there are a number of open questions with embedded software, including rights of repair, implied licence terms, and the consequences of resale or rental of goods containing the software.

024312 'Computers trusted, and found wanting'
S Castell, *Computer Law and Security Report (Jul/Aug 93) pp 155 - 156*

The author challenged computer printouts in a UK criminal case on the grounds that they contained no header information such as their provenance, the user id, and the date and time. The case also highlighted problems with the distinction between knowledge and belief in computer industry practice, and the lack of a paradigm of what constituted a legally reliable computer system. It is suggested that write-only audit trails could provide such a paradigm.

024313 'Data protection Registrar's annual report, June 1993'
Computer Fraud and Security Bulletin (Sep 93) pp 5 - 6

In this summary, the DP registrar is reported as pointing out a major loophole in UK law: if information is passed to someone who is registered as a receiver of data (such as a private detective), then the law cannot control any use to which the information is subsequently put.

024314 'International legal protection for software'
Computer Law and Security Report (Nov/Dec 93) pp 262 - 273

This article tabulates the status of software protection, whether under patent or copyright, in a large number of countries, and discusses the effect of NAFTA, GATT and various other conventions.

024315 'Ruling reduces cardholder liability'
J Doherty, *Cards International no. 98 (24/11/93) p 6*

The Bamberg regional court in Germany has ruled that there is no obligation on a customer to check regularly that he is still in possession of a card; the case concerned a customer whose card was stolen while he was in holiday in Spain, and who only discovered the theft after a month had passed and DM8,600 had been spent.

024316 'A Model for Organising Information Security Documentation'
LM du Toit, SH von Solms, *IFIP SEC 93 pp 227 - 242*

The authors propose a document hierarchy for commercial organisations in which a policy document stands at the apex, driving goal documents and finally application guidelines.

024317 'Electronic Data Interchange (EDI) Security and Audit - a practical approach'
I Ekebrink, *IFIP SEC 93 pp 267 - 276*
This paper reports a Swedish project on EDI security and summarises its findings. The model is an EDI handler sitting between the communications layers and the application layer; the author distinguishes the internal from the inter-organisational security issues and discusses audit requirements.

024318 'A comparative framework for risk analysis methods'
JHP Eloff, L Labuschagne, KP Badenhorst, *Computers and Security v 12 no 6 (Oct 93) pp 597 - 603*
The authors compare and contrast the risk management techniques incorporated in three systems: CRAMM (UK government), LAVA (Los Alamos National Laboratory) and Melissa (French government).

024319 'The FTI Interview"
J Essigner, *Financial technology Insight (Oct 93) pp 15 - 18*
In an interview, the MD of Sligos (a UK ATM switching company) discusses the company's operations; he predicts that the growth areas in the industry will be in third parties providing cheque imaging and card authorisation services.

024320 'Mapping hidden depths'
D Evans, *Computer Weekly (9/9/93) p 36*
The author describes how relationship mapping software can be used to analyse transaction records and find out which individuals are doing business with each other. This has been useful in police work, and could make a contribution to fighting insider trading.

024321 'Business Continuity Planning in a Distributed Decentralized Environment'
KT Fitzgerald, *Information Management and Computer Security v 1 no 2 (1993) pp 34 - 39*
Distributed systems have more, and more complex, dependencies than mainframes, and resilience needs to be designed in. This design should include business strategies for local stand-in processing where this is feasible.

024322 'The EDP Auditor: Disappearing or Adapting?'
GG Gable, GB Davies, *IFIP SEC 93 pp 253 - 266*
Decentralisation of information processing will force general auditors to cope without specialist EDP auditor support, while greater skills will be required for complex systems. EDP auditors must therefore specialise further, or rejoin the ranks of the audit generalists.

024323 'Information Security in the Small Systems Context: A Framework for Understanding'
GG Gable, HJ Highland, *IFIP SEC 93 pp 37 - 52*
The authors discuss the factors which make it harder to secure small systems than large ones, and compare the security management problems in small firms with those encountered by big businesses downsizing to distributed systems and by end user computing departments of large corporations. They provide a large number of references on these topics.

024324 'The Evolution of IT Security Convergence'
PR Gallagher, *IFIP SEC 93 pp 13 - 22*
The author describes the historical role of the NCSC in promoting IT security and in security evaluation. Current trends are the development of new criteria for network-oriented products and the convergence of various national standards towards a single international standard.

024325 ‘The MSc in Information Security at Royal Holloway’
D Gollmann, *IFIP SEC 93 pp 31 - 36*

This article describes the curriculum of a one-year postgraduate course which covers security management, computer security and cryptography; it also provides background information on the institution, its staff and their research interests.

024326 ‘The KGB after The Coup’
O Gordievski, *Intelligence and National Security v 8 no 3 (July 93) pp 68 - 71*

Although the KGB’s troops have been transferred to the Ministry of Defence and its ideological departments abolished or cut back, it still retains hundreds of thousands of domestic informers; meanwhile its external network has been reincorporated as the Russian Foreign Intelligence Service. Despite a shortage of foreign currency, this is unlikely to shrink much; but it is likely to be less dangerous now that the ideological mission is gone.

024327 ‘Random thoughts on problems with new technology’
D Grover, *Computer Law and Security Report (Jul/Aug 93) pp 152 - 154*

The author raises the question of how a court could determine whether the software in a tamper-proof cryptographic module violated a complainant’s patent or copyright. His suggestion is to incorporate a secret key which would be used (on production of a court order) to dump the memory.

024328 ‘Computer Security as a Liability Control Tool’
D Hains, *Information Management and Computer Security v 1 no 4 pp 15 - 16*

This article reports card thefts by a bank employee from accounts of recently deceased customers, and emphasises that technical security measures must be supplemented by a suitable corporate culture.

024329 ‘Recovery Management’
EB Heinlein, *Computers and Security v 12 no 4 (June 93) pp 334 - 337*

Making users put a price on the availability of computer services is a useful management tool for negotiating service levels and for planning recovery in a systematic way. This was illustrated by a consultancy assignment in the banking sector which is reported here.

024330 ‘World Trade Center - A Retrospective’
EB Heinlein, *Computers and Security v 12 no 5 (Aug 93) pp 435 - 436*

Few mainframe computers were housed in the World Trade Center building because of previous incidents, including a fire and two telecommunications failures. Nonetheless a number of disaster recovery plans were exercised, and workplace issues such as relocation and travel costs turned out to be the most troublesome. The moral is that recovery planning should focus on business functions rather than technical issues.

024331 ‘A View of Information Security Tomorrow’
HJ Highland, *IFIP SEC 93 pp 1 - 11*

This is Harold Highland’s address on receiving the Kristian Beckman Award. It gives his assessment of the current state of information security and his prediction for future developments (particularly in the rôle of information security managers).

024332 ‘Secret Service’
C Hipwell, *Computer Weekly 2 Dec 93 pp 44 - 48*

This article gives a brief history of Bletchley Park, the UK codebreaking centre from 1938 - 1946, and reports a campaign to establish a museum on the site which would cover the history of computing, cryptology, the intelligence services, and radar.

024333 'Viewpoint - Clipping Clipper'
LJ Hoffmann, *Communications of the ACM v 36 no 9 (September 1993) pp 15 - 17*

This article describes the US government's recent Clipper initiative and criticises it as a constitutionally suspect measure which erodes the power of Congress. It further describes the possible outlawing of non-escrowed encryption as a 'Digital Volstead Act', and points out that cryptographic products are readily available, both in the US and overseas. It claims that the NSA has clearly wrested control of civilian policy from NIST, and that US business will be harmed.

024334 'Teaching security basics: The importance of when and how'
A Hunstad, *IFIP SEC 93 pp 23 - 30*

Basic knowledge of computer security would be spread more widely if it were taught as part of general employee training, rather than as a specialist course; indeed, security should be integrated in all levels of computer education, from novice through graduate computer science, rather than left as a bolt-on optional extra.

024335 'IT Security Procedures'
Information Security Monitor v 8 no 10 (Sep 93) pp 5 - 7

According to surveys by the UK National Computer Centre in 1991 and 1993, many physical and most logical breaches of IT security were due to lack of procedures and poor training.

024336 'Corporate Security: An Australian Ostrich'
H James, RA Caldwell, *Information Management and Computer Security v 1 no 4 (1993) pp 10 - 12*

Most large companies in Australia describe their implementation level and priorities for security policies, planning and training as low; the same holds for quality assurance.

024337 'Fighting fraud with chips and cards'
D Jones, *Banking World v 11 no 12 (Dec 93) p 42*

Recent reports that the smartcards used in satellite TV systems have been reverse engineered may dissuade bankers from using these devices in retail payment systems.

024338 'Caller Identification System in the Internet Environment'
HT Jung, HL Kim, YM Seo, G Choe, SL Min, CS Kim, K Koh, *Usenix Security 93 pp 69-78*

Seoul National University started using TCP/IP in 1982 but only connected to the Internet in 1992. They soon afterwards observed many hostile attacks, which they have tried to track. A number of difficulties with this are reported.

024339 'The OECD guidelines for the security of information systems'
M Kirby, *Computer Law and Security Report (Jul/Aug 93) pp 190 - 193*

The recent OECD guidelines are summarised, and a history of their development is given by one of the participants.

024340 'Congratulations, You're the New Infosecurity Officer!'
GL Kovacich, *Info Security News v 4 no 4 (Jul 93) pp 25 - 26*

Becoming an information security officer is a difficult task. However, there are several general principles that a new officer can follow to make his job easier, and these are discussed in this article; it also offers suggestions on developing a strategic and tactical plan.

024341 'Internal Control by Objectives: The Functional Control Matrix'
KH Krueger, *IFIP SEC 93 pp 157 - 170*

The author describes the procedures used to keep control when the World Bank's accounting functions were decentralised to its operating divisions. Matrices were constructed of risks versus controls, and used to review procedures. The whole exercise is presented as a model in documenting control procedures.

024342 'Computer Viruses - Towards Better Solutions'
MF Kunsey, *Computers and Security v 12 no 6 (Oct 93) pp 536 - 541*

Most viruses effectively only exist in the laboratory; and the appetite of virus researchers for new specimens may be the main cause of their spread. In any case, the scanners which these researchers sell spend 90% of their time looking for code which has never harmed a real user.

024343 'The requirements for a methodology to test secure open systems'
R Lampard, *NPL Report DITC 222/93 (Sep 93)*

The author proposes that when evaluating secure open systems, conformance testing should be carried out first to reduce the cost and provide an opt out for the client. He discusses test implementations, test suites and the impact on testing of composition and dispersed functionality.

024344 'Fighting the Viruses: Practical Anti-Virus Training'
M Larsson, *IFIP SEC 93 pp 301 - 312*

The author discusses how to set up anti-virus training, and how to set up and manage controlled environments in which viruses can be contained for pedagogic and research purposes.

024345 'IT Security and the User'
W List, *The Computer Bulletin v 5 no 5 (Oct 93) pp 8 - 9*

This article gives a brief introduction to the theory of internal controls in an organisation, and its relevance to access control and disaster recovery. In practice, common problems include an inability to print out security data such as access control lists in a form accessible to management, and a lack of selectivity in backing up data, leading to a recovery choice of all or nothing.

024346 'The Inslaw Affair'
W Madsen, *Computer Fraud and Security Bulletin (Sep 93) pp 12 - 15*

This article attacks the US Department of Justice report into the Inslaw affair as a cover-up. In this matter, the department is supposed to have pirated police software and sold versions with trapdoors to the domestic intelligence agencies of a number of foreign countries; a journalist attempting to investigate it died in circumstances which the author claims were suspicious.

024347 'NCIC criticised for open security and privacy doors'
W Madsen, *Computer Fraud and Security Bulletin (Oct 93) pp 6 - 8*

The FBI has been criticised by the GAO for failing to keep US criminal records and intelligence secure. Their system can be accessed by about half a million people, almost all of whom come in through local systems which are often completely open. As a result, private investigators and illegal information brokers have been getting routine unauthorised access, and criminal records have been used on several occasions to discredit political opponents or troublemakers.

024348 'Reducing the Price of Convenience'
B Masuda, *International Security Review no 82 (Autumn 93) pp 45 - 48*

The author reports a successful project to cut credit card fraud at an electrical goods chain in the New York area. He observed was that offender profiling (by age, sex, race etc) was ineffective, and used puchase profiling instead. This involved not just being suspicious of high value purchases, but training staff to be careful when customers were careless about purchases and spent less than the usual amount of time discussing options and features. Employee rewarding was crucial; with a $50 reward per bad card captured, some staff were regularly earning $150 or $200 each week. The result was a decrease of 82% in fraud over the previous year.

024349 'Covert local area network surveillance'
K McLeod, *Computer Audit Update (Oct 93) pp 13 - 15*

A growing number of network tools allow villains to eavesdrop on LANs and harvest sensitive data such as passwords. This can not only facilitate penetration, but frustrate attempts to prosecute employees who commit crimes.

024350 'Banks angry at consumer attacks over client liability issue'
F Mollett, *Cards International no. 90 (22/7/93) p 4*

Portuguese banks are under attack from the press and from a consumer body for holding customers liable for transactions for 24 hours after a card loss has been reported (the largest bank imposes a delay of 48 hours). This appears to contravene an EC ruling limiting customer liability.

024351 'BMS CAT in Action: Electronic/Communications Security Recovery at the World Trade Center, New York'
DW Moore, *Information Management and Computer Security v 1 no 4 (1993) pp 13 - 14*

This article describes the recovery operation at a bank in the World Trade Center. Tests were used to quantify soot corrosion; these facilitated a quick decision to refurbish rather than replace the exposed equipment.

024352 'A Beginner's Guide to Auditing Unix'
C Nelus, *Computer Audit Update: part 1 in Sep 93 pp 6 - 9 and part 2 in Oct 93 pp 8 - 12*

This article provides a reasonably thorough introduction to unix security and lists all the main system auditing actions, from technical measures such as checking setuid programs to assessing the effectiveness of the system administrator.

024353 'Information Loss Rarely Recovered'
T Newman, *Information Management and Computer Security v 1 no v (1993) pp 17 - 18*

This article contains a number of anecdotes about industrial espionage, including printouts recovered from trash and a company which displayed confidential sales information on a wallchart in a public area.

024354 'Computer crime: why should we still care?'
DF Nigri, *Computer Law and Security Report (Nov/Dec 93) pp 274 - 280*

A government review of Britain's Computer Misuse Act shows that few companies see any point in prosecuting people, as it imposes potentially large costs but brings few benefits. The market for expert advice about computer crime is non-existent due to lack of demand from business.

024355 'A Quantitative Accreditation Model - Assessing the Value of Assurance"
M Ohlin, *IFIP SEC 93 pp 313 - 325*

The author presents a quantitative assurance model which tries to link the appropriate ITSEC assurance level of an IT system to the expected loss accrued over the system's lifetime.

024356 'Network Security Model'
T Ohta, T Chikaraishi, *SICON/ICIE'93 pp 507 - 511*

This paper proposes a reference model for network security in which network security issues can be treated integrally.

024357 'Corporate Network Security'
R Oppliger, D Hogrefe, *SICON/ICIE'93 pp 426 - 430*

This paper deals with security of corporate networks. Passive and active attacks in such networks are outlined. Countermeasures to prevent corporate networks from being attacked are discussed.

024358 'The State of Security in Cyberspace'
D Parker, *Computer Fraud and Security Bulletin (Aug 93) pp 15 - 18*

This article reports SRI research on hacking. The main vulnerabilities are not specifically technical, but the ease with which outsiders can get critical technical information, and poor systems administration and maintenance.

024359 'The Green Book on the security of information systems'
GR Price, *Computer Audit Update (Nov 93) pp 3 - 9*

The author discusses the EC programme on information security, and reports on a workshop held on 16/17 September 1993 in Brussels to consider the latest draft of the green book.

024360 'The Persistent Hacker'
E Rodriguez, *Usenix Security 93 pp 131-137*

Universidad de Chile have been connected to uucp since 1985, X.25 and Bitnet since 1986, and Internet since January, 1992. Intruders soon discovered a trivial password, quickly became superuser, and installed bogus Telnet and login software. Countermeasures included warnings and tracking, which resulted in a journey across four continents.

024361 'Legal Response to a Computer Crime - Retrospect of a "Mere Chance" Case'
J Saari, *IFIP SEC 93 pp 369 - 374*

The author considers what the legal position would be if an electronic payment between two companies were diverted by chance to a third party who made off with the money, and how the legal arguments would be likely to evolve.

024362 'An Electronic John Hancock?'
B Schneier, *Info Security News v 4 no 5 (Sep 93) pp 54 - 55*

This article provides a brief overview of digital signatures, including how they can be used to authenticate documents and how they are seen by the US legal system.

024363 'Developing Awareness, Training and Education: A Cost Effective Tool for Maintaining System Integrity'
CD Schou, WV Maconachy, J Frost, *IFIP SEC 93 pp 53 - 64*

This paper discusses the US government approach to security education, which is explained in terms of a 3-dimensional model whose axes are information states (transmission, storage, processing), information characteristics (availability, integrity, confidentiality) and security measures (policy, technology and training). It goes over the practicalities of curriculum design and implementation, and reports experimental use of groupware to facilitate the committee work involved.

024364 'Information security professionalism for the 1990s'
CD Schou, WV Maconachy, FL McNulty, A Chantker, *Computer Security Journal v 9 no 1 (Spring 93) pp 27 - 37*

This paper deals with the importance of the protection of information assets, and the trend toward the professionalisation of individuals charged with managing this protection.

024365 'The Filter Model of Information Security: A Conceptual Model for Education and Training'
AR Smith, *IFIP SEC 93 pp 75 - 90*

The author presents a model of security management, in which different organisational measures are seen as filters which reduce the company's exposure to some subset of the possible threats. The idea is to work forward from a threat model to specify the relevant control measures using a dependency matrix, the values of which were determined from a survey.

024366 'Lessons learned from the bombings at Willis Corroon Group'
P Smith, *Computer Fraud and Security Bulletin (Oct 93) pp 8 - 11*

One of this insurance company's London sites was knocked out by the Bishopsgate bomb. The experience is described, and the lessons learned are discussed.

024367 'Computer Aided Industrial Espionage'
P Sommer, *Computer Fraud and Security Bulletin (Nov 93) pp 10 - 17*

This article provides a detailed overview of industrial espionage in the UK; a number of cases are reported, and the relevant laws are discussed. Prosecution is difficult, and prevention the only real remedy; computers are often involved, and the ease with which data can be copied to diskettes or removable disks is becoming increasingly significant.

024368 'Software forensics - can we track code to its authors?'
EH Spafford, SA Weeber, *Computers and Security v 12 no 6 (Oct 93) pp 585 - 595*

The authors ask whether programming styles can be traced to authors using statistical techniques? It is a standard technique to establish the authorship of prose by looking at word and sentence length, choice of words, and the number of adjectives per noun. In software, the job is harder, as many features get lost in compilation; but there is still a lot of evidence left, such as choice of programming environment, use of library and system calls, programming skill, characteristic errors, and the ratio of local to global variables.

024369 'Information Systems Security and Fraud Prevention in Office Automation'
PM Stanley, *IFIP SEC 93 pp 375 - 384*

The author argues that auditors must extend their range of interest from control of money to control of documents, and outlines the principles of managing electronic document security.

024370 'Evolution of IT Security in India - Implementation Issues'
K Subramanian, *IFIP SEC 93 pp 359 - 368*

The author discusses the IT strategy of the government of India and the control issues it raises. Encryption and security competence are still largely concentrated in the Defence Department; but a start on civil standards has been forced by foreign banks' use of security and by dial access. Government policy is to build a network of security administrators in government departments and big corporations; the country also needs computer evidence laws, EDP auditor certification, and an insurance market.

024371 'Controlling Network Security in a Multivendor Environment'
N Swain, *Computer Fraud and Security Bulletin (Aug 93) pp 6 - 10*

This article provides a management overview of security in networks; it covers the X.400 security model, digital signatures and the supporting framework, and the architectural issues. The need for simple manageable designs is stressed.

024372 'Microcomputer Based CAAT in the 90's'
CE Thiel, *Computer Audit Update: part 1 in Oct 93 pp 3 - 8, and part 2 in Nov 93 pp 9 - 14*

The author discusses computer aided audit techniques, and particularly the use of microcomputers to extract and analyse data from larger systems. The technical obstacles to data transfer and conversion are more than outweighed by the lower cost and greater control: the auditor can write his own software and control his own computing environment, rather than having to rely on the staff and facilities of the system under investigation.

024373 'A Model for Information Security Management'
R von Solms, SH von Solms, WJ Caelli, *Information Management and Computer Security v 1 no 3 (1993) pp 12 - 17*

A common failing in security management is not considering the operating security environment in detail. There are typically a number of such environments, ranging from the ideal one down to that prescribed by insurers, to that accepted by management, to the current environment, and finally to the survival environment which would exist during an emergency. The gaps between these layers are a matter for self insurance and risk management.

024374 ‘A Process Approach to Information Security Management’
R von Solms, SH von Solms, JH Carroll, *IFIP SEC 93 pp 385 - 400*
This paper discusses managing information security from the points of view of research, policy, education, contingency planning, reporting and operations management.

024375 ‘Come hell or high water’
M Warwick, *Communications International v 20 no 10 (Oct 93) pp 33 - 40*
This article presents a number of anecdotes of computer disasters, reports recent surveys, provides statistics on reported causes of disasters, and gives a checklist for establishing contingency procedures.

024376 ‘Data Integrity and Security: Who’s in Charge Here Anyway?’
KP Weiss, *Information Management and Computer Security v 1 no 4 (1993) pp 4 - 9*
Most commercial security standards are set by banks, and are geared to denying responsibility when things go wrong; their uncritical acceptance by other industries is at best dubious. Outside the financial world, the main threat is not so much embezzlement as loss of trade secrets and whistle-blowers; the use of computers has swept away the old paper document based controls without offering any viable replacement.

024377 ‘Duress Terminations and Information Security’
CC Wood, *Computers and Security v 12 no 6 (Oct 93) pp 527 - 535*
Firing senior or otherwise trusted employees can have very wide ramifications; at the very least, organisations should have a plan of how, to whom and by whom the status change will be communicated. A skeleton for such a plan is presented in this article; it can also be applied to routine privilege changes.

024378 ‘The Easy Approach to Information Security’
CC Wood, *Computer Fraud and Security Bulletin (Oct 93) pp 11 - 12*
It is especially important in the commercial world to avoid negligence about computer security, and the most effective way to improve matters is often to look for additional low-cost controls. Unfortunately, this is often overlooked, and people plan expensive overall solutions which end up not being implemented.

024379 ‘Regulating US Cryptography’
MA Wright, *Computer Fraud and Security Bulletin (Sep 93) pp 10 - 12*
This article provides an overview of the US government’s involvement in civilian cryptology, including DES, DSS, Clipper and Capstone; and reports the controversy over the key escrow system.

024380 ‘Evaluation of an academic programme in IT security 1985-1990’
L Yngström, *IFIP SEC 93 pp 287 - 300*
Stockholm University set up a ‘security informatics’ programme in 1985. The results of evaluation since then are discussed, including the views of former students and their career performance as assessed by their employers.

4 Formal Methods and Protocols

024401 'Authentication and delegation with smartcards'
M Abadí, M Burrows, C Kaufman, B Lampson, *Science of Computer Programming v21 no 2 (Oct 93) pp 93 - 114*

As current smartcards do not have their own keyboards or clocks, the trust relationships between card, user, workstation and security server can be quite complex in realistic systems. This is explored by a number of protocols: in the basic scheme, the card validates the workstation, then solicits the user PIN, and finally generates a delegation key with which the workstation can access files on the user's behalf. Variants take account of the smartcard not knowing the time, and of a security server which is not completely trustworthy. The authors analyse these protocols using a variant of the BAN logic to highlight the assumptions about trust which have to be made.

024402 'Entity Authentication and Key Distribution'
M Bellare, P Rogaway, *Crypto 93 pp 21.1 - 21.13*

A formal model of entity authentication and authenticated key distribution in a distributed environment is proposed. It is assumed that all the communications are under enemy control, and that the enemy can simultaneously read, modify, delay and replay many messages. Secure mutual authentication and authenticated key exchange are defined from a standpoint of complexity theory, and, in each case, an example of a protocol with provable security is given. The proofs assume the existence of pseudorandom functions.

024403 'Scheme for secure digital mobile communications based on symmetric key cryptography'
T Hwang, *Information Processing Letters v 48 no 1 (29/10/93) pp 35 - 38*

The author proposes a variant of the wide-mouthed frog protocol for use in digital mobile communications.

024404 'Long Running Jobs in an Authenticated Environment'
AD Rubin, P Honeyman, *Usenix Security 93 pp 19-28*

Khat (Kerberized at) is a Kerberos Version 4 authenticated job scheduler designed to be robust against active attacks and to provide notification in case of denial of service. Kerberos tickets have short, fixed lifetimes and replay detection, which are unable to deal with delayed execution; Khat makes available a server that can "run a job three weeks from now" without storing passwords in shell scripts.

024405 'Nonmonotonic Cryptographic Protocols'
AD Rubin, *University of Michigan CITI Technical Report 93-9*

New methods are presented for handling cryptographic protocols which rely on the deletion of information. These techniques are tested against the standard examples such as Needham-Schroder, and then used to display a flaw in the Khat protocol for securing delayed-execution jobs. This has the effect that intruders can use replays to delay a job's execution until the ticket runs out; the fix is to set up fresh nonces before a restart.

024406 'Formal Methods for the Analysis of Authentication Protocols'
AD Rubin, P Honeyman, *University of Michigan CITI Technical Report 93-7*

This report surveys the formal techniques available to analyse and verify cryptographic protocols. They use Meadows' classification, according to whether the method is based on general specification languages, expert systems, doxastic logics or term-rewriting; techniques proposed by twenty seven authors are classified, and the main ones described. About half the report is devoted to the BAN logic and its derivatives; the bibliography has 67 entries.

024407 'Planning For The EDI of Tomorrow Using Electronic Document Authorisation'

S Russell, *IFIP SEC 93 pp 243 - 252*

The author makes three criticisms of Fischer's model of electronic document authorisation, in which a company publishes the rules according to which it will be bound by various combinations of its officers and managers. Firstly, publishing the signing powers of officers may have been the practice in banking, but in general EDI applications it gives far too much information to both real and potential suppliers; secondly, real world delegation is complex (an engineer may have great power to buy instruments, but little for stationery and none for vehicles); thirdly, it is the sender rather than the receiver of commercial messages who is liable in law for the contents. For all these reasons, protocols for EDI should assume that authorisation functions will be performed internally to the sending company, which need only publish the classes of authorisable documents and the keys or other mechanisms needed to authorise them.

5 Secret Key Algorithms

024501 'Guaranteeing the period of linear recurring sequences (mod 2^n)'
AD Barnard, JR Silvester, WG Chambers, *IEE Proceedings-E - Computers and Digital Techniques v 140 no 5 (Sep 93) pp 243 - 246*

A linear sequence of degree n over GF(2^e) can have period of up to $(2^n - 1)2^{e-1}$. For this maximum to be achieved, it is not sufficient for the polynomial to be primitive; there is an extra condition which must be satisfied modulo 4. The authors provide four equivalent forms of this, which make it possible to find large families of satisfactory trinomials and pentanomials, and to check many other polynomials by inspection.

024502 'Differential Cryptanalysis of Lucifer'
I Ben-Aroya, E Biham, *Crypto 93 pp 18.1 - 18.13*

The authors introduce the notion of a conditional characteristic to break several variants of Lucifer. The probability of a conditional characteristic depends on one or more key bits, rather than just on the series of differences predicted by the characteristic as in previous differential attacks. This technique is made necessary by the key-dependent substitutions in Lucifer, and succeeds to the extent that about 55% of all possible Lucifer keys are insecure: in such cases an attack requires only about 2^{36} plaintexts. The authors also show that the order of the S-boxes in Lucifer is important, and that RDES, a recently proposed variant of DES, is in fact weaker than DES.

024503 'Cryptanalysis on Schwartz graphical encryption method'
YC Chin, PC Wang, JJ Huang, *Cryptologia v XVII no 3 (July 93) pp 301 - 304*

The authors point out that a method proposed by Schwartz for encrypting graphics is a disguised additive stream cipher and thus vulnerable to a known plaintext attack.

024504 'The Shrinking Generator'
D Coppersmith, H Krawczyk, V Mansour, *Crypto 93 pp 3.1 - 3.11*

The authors propose a keystream generator which combines two shift register sequences: a bit of keystream is taken from the output of the first shift register whenever the output of the second is equal to 1. They show that the resulting keystream has almost maximal period and linear complexity, that its out-of-phase autocorrelation is low, and that the distribution of bit patterns is almost uniform.

024505 'A Product for Twelve Hadamard Matrices'
W de Launey, *Australasian Journal of Combinatorics v 7 (93) pp 123 - 127*

The author shows how to obtain Hadamard matrices of exponent nine; given Hadamard matrices of orders 4a, 4b, ..., 4k, 4l, he constructs one of order 512ab...kl by generalising the Craigen-Seberry-Zhang product.

024506 'Correlation properties of extended m-sequences'
UC Fiebig, M Schnell, *Electronics Letters v 29 no 20 (30 Sep 93) pp 1753 - 1755*

In some applications, it is desirable to extend an m-sequence into a de Bruijn sequence by adding an extra elements. The authors here show that the autocorrelation properties are not unduly disturbed by this modification.

024507 'Automated cryptanalysis of substitution ciphers'
WS Forsyth, R Safavi-Naini, *Cryptologia v XVII no 4 (Oct 93) pp 407 - 418*

The authors show how breaking substitution ciphers can be recast as a problem in combinatorial optimisation, and tackle it with a simulated annealing algorithm which they describe in some detail. The automated solution of 5000 character texts is straightforward; whether it works on shorter texts depends on the nature of the plaintext.

024508 'Backforward Generation of Binary Bent Sequences'
BA Guo, CN Cai, *Acta Electronica Sinica v 21 no 1 (Jan 93) (in Chinese)*

The authors present a method to generate bent sequences using a feedforward network. This technique is claimed to be simple and fast.

024509 'Data encryption and decryption system using multiple-valued logic array'
S Han, *Chinese Journal of Computers v 16 no 6 (June 1993) (in Chinese)*

The author proposes a data encryption algorithm based on a generalised m-valued planar logic array, and discusses its realisation in hardware and software.

024510 'Security of Iterated Hash Functions Based on Block Ciphers'
W Hohl, XJ Lai, T Meier, C Waldvogel, *Crypto 93 pp 32.1 - 32.11*

The authors examine hash functions built from block ciphers whose output length is twice the length of the block, and in particular their security against free start attacks. Upper bounds for security against such attacks are derived, and a hash function is presented which achieves these, despite requiring only half the number of encryptions used by the Meier-Schilling scheme.

024511 'Selbstmodifizierende Verbindungsnetzwerke'
P Horster, *Universität Karlsruhe EISS report 93/3 (in German)*

The author discusses the use of switching techniques to implement keyed substitutions for use in block ciphers and hash functions. Benes networks are used to construct self-modifying substitutions; the modification may be made to depend on previous ciphertext or plaintext, depending on the error propagation characteristics required. A number of modification schemes are discussed. It is claimed that these make possible much simpler cipher designs than are required with fixed substitutions, and a trial hardware implementation is discussed.

024512 'On the de Bruijn Torus Problem'
G Hurlbert, *Journal of Combinatorial Theory series A v 64 (Sep 93) pp 50 - 62*

The author defines a de Bruijn torus as the 2-dimensional analogue of a de Bruijn sequence, and proves that these tori exist for a number of parameters.

024513 'A construction for Hadamard matrices'
H Kharaghani, *Discrete Mathematics v 120 (Sep 93) pp 115 - 120*

Given a Hadamard matrix of order $2^n m$, Golay codes of length r can be used to construct a large number of such matrices of order $(r + 4^n + 1)4^{n+1}m^2$.

024514 'New Approaches to Secret-Key Exchange'
T Leighton, S Micali, *Crypto 93 pp 38.1 - 38.11*

The authors present key distribution schemes which are based on hashing plus either secure hardware or a trusted third party. In the latter case, user U_i gets a secret key $K_i = H(K \mid i)$ where K is the third party's secret; the matrix $P_{ij} = H(K_j \mid i) \oplus H(K_i \mid j)$ is then made public (or available for online enquiry). When U_i wishes to communicate with U_j, he can use $H(K_J \mid i)$ as a key. Hardware versions can be adapted to security hierarchies, and to withstand the compromise of a certain number of chips.

024515 'Edit Distance Coding of Information Sources'
H Morita, K Kobayashi, *SRIWIT 93 pp 245 - 249*

The authors define the edit distance between two strings as the number of insertions and deletions needed to transform one into the other, and the edit script as the list of these operations. They then show how to construct codes of minimum edit distance by building dictionaries of edit scripts.

024516 ‘On the distribution of characteristic in composite permutations’
L O’Connor, *Crypto 93 pp 34.1 - 34.12*

The author defines a composite permutation as a mapping that consists of several concatenated permutations, as in the S-boxes of DES. He shows that their XOR tables approach the best possible as the size of the permutations is increased. The exact distribution for an entry on the XOR table is derived, including the largest entry and the density of zero entries.

024517 ‘Differential attack on message authentication codes’
K Ohta, M Matsui, *Crypto 93 pp 19.1 - 19.11*

The authors consider a differential attack on message authentication codes (MACs) produced by block ciphers, such as DES and FEAL, by encrypting a message in CBC mode and then keeping the left 32 bits of the ciphertext as the MAC. They show that MACs produced from DES restricted to 8-rounds are insecure while MACs from 12-round DES are secure. For FEAL, both 8-round and 12-round MACs are insecure.

024518 ‘String Editing under a Combination of Constraints’
SV Petrovič, JD Golič, *Information Sciences v 74 (Oct 93) pp 151 - 164*

The authors consider how to calculate the edit distance between two strings, and generalise the work presented at Eurocrypt 90 to different constraints; by allowing insertions and substitutions as well as deletions, they get an algorithm which is less affected by noise. Where the two string lengths are n and m, it takes time $O(n^2m)$ and space $O(nm)$.

024519 ‘More efficient software implementations of (generalised) DES’
A Pftizmann, R Aßmann, *Computers and Security v 12 no 5 (Aug 93) pp 477 - 500*

The authors explain the techniques for implementing DES quickly in software, such as pre-computing large key-specific lookup tables, and discuss the various trade-offs. They point out that these techniques also apply to ‘generalised’ DES with arbitrary S-boxes and key schedules, but that the expansion tables have an effect on speed.

024520 ‘Cryptanalysis of DES in the CFB mode’
B Preneel, M Nuttin, V Rijmen, J Buelens, *Crypto 93 pp 20.1 - 20.11*

The authors consider the cryptanalysis of DES when used in CFB mode, and obtain a ‘meet-in-the-middle’ attack that is faster than exhaustive search by a factor of 2^{20} when DES is restricted to 3 rounds. Also, a modified differential attack is presented for m-bit feedback, where $m \geq 3$. This attack is faster than exhaustive search for DES restricted to 10 or less rounds.

024521 ‘Hash functions based on block ciphers: a synthetic approach’
B Preneel, R Govaerts, J Vandewalle, *Crypto 93 pp 31.1 - 31.11*

The authors present a systematic analysis of all the ways in which block ciphers can be chained to give hash functions and MACs. Out of the 64 possibilities, only 12 are secure; these are examined and discussed. Finally, they show how to overcome Merkle’s ‘fix’ of Rabin’s hash function.

024522 ‘A taxonomy of encryption algorithms’
B Schneier, *Computer Security Journal v 9 no 1 (Spring 93) pp 39 - 59*

This paper describes and classifies many of the better-known cryptographic algorithms, including secret-key algorithms, public-key algorithms, and one-way hash functions.

024523 ‘The IDEA Encryption Algorithm’
B Schneier, *Dr. Dobbs Journal v 18 no 13 (Dec 93) pp 50 - 56*

This article describes the IDEA encryption algorithm in detail, and provides source code of an implementation in C.

024524 'Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics'

J Seberry, XM Zhang, YL Zheng, *Crypto 93 pp 6.1 - 6.12*

By concatenating and recursively modifying the rows of Hadamard matrices, one can generate sequences which are balanced and which have higher nonlinearity than sequences obtained by concatenating bent sequences. One can also construct balanced sequences which satisfy a high order propagation criterion almost everywhere.

024525 'Some Orthogonal Matrices Constructed by Strong Kronecker Multiplication'

J Seberry, XM Zhang, *Australasian Journal of Combinatorics v 7 (93) pp 213 - 224*

Given Hadamard matrices of order 4a and 4b, the authors show how to construct one of order 4ab by combining Kronecker products and disjoint weighting.

024526 'An Integrity Check Value Algorithm for Stream Ciphers'

R Taylor, *Crypto 93 pp 5.1 - 5.8*

The author proposes combining a keystream with a message, several bits at a time, by using a polynomial over a suitable finite field. The idea is that this can be used to calculate message authentication codes as well as to provide secrecy. If the b message bits are m_i and the keystream word is Z, the suggested polynomial is $f(m_i, Z) = \sum_0^{b-1} m_i Z^{b-i} \pmod{p}$, where p is just larger than 2^b.

024527 'Correlation Resistant Combining Functions for Stream Ciphers'

R Taylor, *Telecom Australia Research Laboratories Report 8280 (1993)*

This report presents an elaboration of Rueppel's summation generator; the idea is to make correlation attacks harder by adding quadratic terms. The outputs of n shift registers are fed into an adder, whose sum bit and carry bit are s_j and c_j respectively; the keystream is then formed as $k_j = m_j + m_{j-1}m_{j-2} + m_{j-3}m_{j-5} + m_{j-6}m_{j-9} + \ldots + m_{j-k(k-1)/2}m_{j-k(k-3)/2} + c_{j-k(k-3)/2}$. This pattern of delays in the quadratic terms is chosen to maximise the difficulty of finding a function of a small number of keystream bits which is correlated to any underlying register by more than $\frac{1}{2} + \frac{1}{2^{k+1}}$.

024528 'Approximate String Matching with Suffix Automata'

E Ukkonen, D Wood, *Algorithmica v 10 (Nov 92) pp 353 - 364*

Finding a substring of a string of length n which is at edit distance at most k from a given pattern can be done in $O(kn)$ operations using a suffix automaton and a suitable edit distance table.

024529 'Value sets of polynomials over finite fields'

DQ Wan, PJS Shue, CS Chen, *Proc AMS v 119 no 3 (Nov 93) pp 711 - 717*

The authors establish lower and upper bounds on the number of values assumed by various types of polynomial over a finite field, which improve on previous results.

024530 'Triple correlation analysis of m-sequences'

ES Warner, B Mulgrew, PM Grant, *Electronics Letters v 29 no 20 (30 Sep 93) pp 1755 - 1756*

The triple correlation $1/L \sum s(t)s(t+\tau_1)a(t+\tau_2)$ of an m-sequence takes values $-1/L$ or 1; the latter is assumed quite frequently in the plane with axes τ_1, τ_2. Observing these peaks allows the period and the feedback polynomial to be determined in the presence of noise with shorter sequence lengths than previously.

024531 'Efficient DES Key Search'

MJ Wiener, *Crypto 93 rump session*

The author presents a design for a DES key search machine, which was carried as far as a detailed design, which is described in very considerable detail. It uses a custom chip which is highly pipelined, with separate silicon for each round of the encryption; this chip will allow 50m keys to be tested every second, is built from 0.8μ CMOS and would cost \$10.50. One million dollars would buy enough chips (and supporting hardware) to find a DES key in an average of 3.5 hours.

024532 'Balanced Source Coding and its Application in Stream Ciphers'
CK Wu, XM Wang, *Acta Electronica Sinica v 21 no 7 (July 93) (in Chinese)*
The authors present a coding technique which results in balanced codewords and which is optimal for codes based on Huffmann coding. They discuss its application to stream ciphers.

6 Public Key Algorithms

024601 'Decomposition of Weakly Invertible Finite Automata'
F Bao, *Fifth Asian Logic Conference, Signapore, 1993*
The author investigates the conditions under which a weakly invertible finite automaton can be decomposed. Some automata with delay 2 cannot be decomposed into automata with delay 1; a primary automaton with delay 1 can be decomposed into a delay free machine and a delay unit if and only if it is strongly connected; and over GF(2), an automaton can be decomposed into a delay free machine and k delay units if and only if all the states have delay k.

024602 'The Increasing Ranks of Linear Finite Automata and the Complexity of FA Public Key Cryptosystem'
F Bao, *Science in China v 37 no 4 (April 94) (in Chinese)*
If the public key of a finite automaton based cryptosystem consists of a linear automaton of delay τ and a nonlinear automaton with delay 0, then the resulting system has many of the properties of the linear component, and this opens it up to an attack whose complexity is analysed.

024603 'Two results about the decomposition of delay step of weakly invertible finite automata'
F Bao, *Chinese Journal of Computers v 16 no 6 (Aug 93) (in Chinese)*
Not all weakly invertible finite automata can be decomposed; in particular, the author shows that there exists an n-ary weakly invertible finite automaton with delay 2 which cannot be equivalent to the serial composition of any two automata with delay 1. A 2-ary automaton with delay 2 can be decomposed if its states have the same delay.

024604 'Privacy-protecting offline electronic cash systems'
S Brands, *Crypto 93 pp 26.1 - 26.15*
This is the conference paper version of the author's technical report (reviewed in **022603**) on basing digital cash schemes on the representation problem and on restricted blind signatures. Its advantages over previous schemes are more provable security, modularity, extendability, and the fact that the bank cannot frame a user.

024605 'The Number of Distinct Subset Sums of a Finite Set of Vectors'
EF Brickell, M Saaks, *Journal of Combinatorial Theory series A v 63 no 2 (July 93) pp 234 - 256*
The authors count the minimum number of vectors which can be obtained as a linear combination of R^n-spanning subsets of a finite set of vectors in R^n, and use this to count the number of distinct subset sums.

024606 'Attacking Two Birational Permutation Signature Schemes'
D Coppersmith, *Crypto 93 rump session*
The author shows that the 3 variable version of Shamir's proposed birational signature scheme can be broken by reduction to Ong-Schnorr-Shamir, and other cases by a number of further tricks.

024607 'Shamir's Scheme Says It All'
E Dawson, D Donovan, *IFIP SEC 93 pp 91 - 102*
The authors show how Shamir's secret sharing scheme can be extended to cope with arbitrary access structures by choosing suitable sets of polynomials. The simplest construction for this is a tree of s-out-of-s threshold schemes covering the structure's minimal sets; similar constructions can be used to cope with multipart and multilevel schemes, and to create shares in the absence of a trusted dealer. They also suggest dealing with disenrollment by prepositioning blinded schemes, which can be activated without the need for a secure channel.

024608 'Extensions of Single-Term Coins'
N Ferguson, *Crypto 93 pp 25.1 - 25.11*

The author extends his RSA-based digital cash scheme, proposed at Eurocrypt 93, with a secret sharing feature. This allows coins to be spent up to n times without losing anonymity, and to incorporate observers which prevent double spending. The scheme still avoids the need for a cut-and-choose protocol at coin issue.

024609 'Randomising the Public Key for Improving Performances of Public-Key Cryptosystems'
EM Gabidulin, O Kjelsen, *SRIWIT 93 pp 297 - 301*

The authors propose strengthening public key cryptosystems based on coding theory, and particularly McEliece's and Niederreiter's, by adding a hiding matrix to the public encryption matrix. They show how this hiding matrix can be constructed from a leader of any of the code's cosets in such a way that the number of errors corrected by the secret decryption matrix is only reduced by one. This technique foils the Sidelnikov-Shestakov attack on Niederreiter's system.

024610 'User Impersonation in Key Certification Schemes'
AK Lenstra, Y Yacobi, *Journal of Cryptology v 6 no 4 (1993) pp 225 - 232*

The authors dicuss features of some signature schemes which make hashing essential. A scheme of Cylink's in which user A with public key y_A and id I_A receives a certificate which is an ElGamal signature of $y_A^{I_A}$ is vulnerable in that A can display certificates for multiples of I_A; and a scheme of Beller, Chang and Yacobi which was based on Rabin signatures can also be broken if the hash function is not chosen carefully.

024611 'Cryptanalysis on the threshold RSA signature scheme'
CM Li, TNL Hwang, NY Lee, *Crypto 93 pp 35.1 - 35.9*

The authors make the trivial remark that $k+1$ users can recover $\phi(n)$ in the Desmedt-Frankel threshold signature scheme.

024612 'On the Security of the Niederreiter's Publickey Algebraic-Code cryptosystem and the Optimisation of Parameters'
YX Li, XM Wang, *Acta Electronica Sinica v 21 no 7 (July 93) (in Chinese)*

The authors present a new attack on Niederreiter's public key cryptosystem based on linear algebra. They show that its security is equivalent to that of McEliece's and discuss the optimal choice of parameters.

024613 'Another method for attaining security against adaptively chosen ciphertext attacks'
CH Lim, PJ Lee, *Crypto 93 pp 36.1 - 36.12*

Some public key cryptosystems are vulnerable to chosen-ciphertext attacks, where the attacker can obtain the decryption of ciphertexts related in some way to the target ciphertext; Zheng and Seberry proposed securing systems against such attacks by checking redundancy in the plaintext. The authors point out that ciphertext redundancy can also be used, and propose new constructions to immunise the RSA and El Gamal systems.

024614 'Elliptic Curve Cryptosystems and Their Implementation'
AJ Menezes, SA Vanstone, *Journal of Cryptology v 6 no 4 (1993) pp 209 - 224*

This article provided an up-to-date survey of elliptic curve cryptosystems. The authors introduce elliptic curves and discuss the elliptic logarithm problem, with particular reference to the many things that can go wrong in characteristic two; they then show how to choose curves if the goal is a system with a short key, and discuss some implementation issues.

024615 'Improved algorithms for the permuted kernel problem'
J Patarin, P Chauvaud, *Crypto 93 pp 33.1 - 33.11*

The permuted kernel problem was suggested by Shamir in 1989 as a new basis for zero-knowledge proofs of identity. Several algorithms have been proposed for solving this problem, all of which are faster than exhaustive methods but still require unrealistic amounts of time and space when applied to the cases originally suggested by Shamir. The authors combine and extend the previous algorithms, and show that the smallest of Shamir's cases may be solved in time about 2^{52}, and could thus be insecure.

024616 'Realising digital signatures with one-way hash functions'
C Ruland, *Cryptologia v XVII no 3 (July 93) pp 285 - 300*

The author explains Winternitz's and Merkle's methods for producing one-time signatures using hash functions, and analyses their performance.

024617 'Efficient Signature Schemes Based on Birational Permutations'
A Shamir, *Crypto 93 pp 1.1 - 1.10*

The author proposes signature schemes, which were broken by Coppersmith and others before the paper was presented. He generalised the Ong-Schnorr-Shamir scheme to several variables by using a birational function f, chosen so that both f and f^{-1} were low degree rational functions; the secret key was an algebraic basis which made them tractable.

024618 'The quadratic residue cipher and some notes on implementation'
SJ Shepherd, PW Sanders, CT Stockel, *Cryptologia v XVII no 3 (July 93) pp 264 - 282*

The authors explain Rabin encryption and algorithms for extracting modular square roots with the help of worked examples; they discuss its use as a keystream generator in the manner of Blum, Blum and Shub, and compare it with RSA.

024619 'On the Insecurity of Cryptosystems based on generalised Reed-Solomon Codes'
VM Sidelnikov, SO Shestakov, *Discrete Mathematics v 1 no 4 (92) pp 439 - 444 (in Russian)*

The Niederreiter public key cryptosystem can be attacked by searching for an equivalent matrix, that is, one which defines the same Reed-Solomon code. In order to do this, we need to guess three columns of the matrix; the rest can then be reconstructed from the known relationships. The attack has complexity $O(n^3)$.

024620 'LUC: A New Public Key System'
PJ Smith, MJJ Lennon, *IFIP SEC 93 pp 103 - 118*

The authors propose a public key system based on using Lucas functions, rather than exponentiation, with respect to a composite modulus. The basic facts about these functions, and the Lehmer totient function, are presented, and the details of how to use them for encryption and decryption are developed. Like RSA, this system can be broken if the modulus is factored; unlike RSA, it has no straightforward homomorphic property. In effect, one is operating in the corational groups of $GF(p^2)$ and $GF(q^2)$, rather than the multiplicative groups of $GF(p)$ and $GF(q)$; and the technique is a special case of Müller and Nöbauer's proposal to use Dickson polynomials.

024621 'Cryptanalysis of knapsack ciphers using genetic algorithms'
R Spillman, *Cryptologia v XVII no 4 (Oct 93) pp 367 - 377*

The author describes the design and use of a genetic algorithm to attack small trapdoor knapsacks and gives performance data to show that it functions 50 - 100 times faster than exhaustive search.

024622 'A new identification scheme based on syndrome decoding'
J Stern, *Crypto 93 pp 2.1 - 2.10*

The author proposes an identification scheme based on the NP-hard problem of decoding a linear code. The code's parity check matrix H is made public, and the identity of user I is determined as $i = H(s)$ for a random s of a fixed Hamming weight known only to I. He gives a zero-knowledge protocol that I can use to demonstrate possession of s, which can only be impersonated with a vanishingly small probability. This protocol is proposed as an alternative to Shamir's permuted kernel scheme.

024623 'Cryptosystem for Selectively Broadcasting Separate Secrets'
TC Wu, YS Yeh, *J of Computer Systems, Science and Engineering, April 1993*

This paper proposes a cryptosystem for selectively broadcasting secrets over broadcast links. The computational complexity of the proposed system is analysed.

024624 'Common-multiplicand multiplication and its applications to public key cryptography'
SM Yen, CS Laih, *Electronics Letters v 29 no 17 (19 Aug 93) pp 1583 - 1584*

The authors point out that where we have to compute XY_1 and XY_2, we can speed things up slightly by calculating $X(Y_1$ AND $Y_2)$ in advance.

7 Computational Number Theory

024701 'MRA: A Computational Technique for Security in High-Performance Systems'
M Abdelguerfi, A Dunham, W Patterson, *IFIP SEC 93 pp 401 - 417*

The authors propose that modular arithmetic routines can be parallelised by using multiple radices. In this scheme, one chooses a smooth base B which is the product of enough distinct small primes that $B > n^2$, where n is the modulus. The separate processors then each perform calculations modulo one of the primes dividing B; the algorithm for modular reduction is described in some detail.

024702 'A subexponential algorithm for discrete logarithms over all finite fields'
L Adleman, J DeMarrias, *Crypto 93 pp 14.1 - 14.12*

The main contribution of the paper is to give subexponential algorithms for determining logarithms in any finite field. The first author's index calculus method for $GF(p)$ is extended to $GF(p^n)$ in two ways; one for $n < p$ and one for $n > p$. The first models $GF(p^n)$ as $\mathcal{O}/(p)$ for the integer ring $\mathcal{O}$ of a suitable extension of the rationals, while the second is a generalisation of Coppersmith's method for characteristic two.

024703 'Properties of Zech's Logarithms over Fermat Prime Fields'
LI Alfredsson, *SRIWIT 93 pp 310 - 314*

Zech's logarithms to base 3 have a number of nice properties, and in particular can be used to work out discrete logarithms quickly in fields with $2^n + 1$ elements.

024704 'Factor Refinement'
E Bach, J Driscoll, J Shallit, *Journal of Algorithms v 15 no 2 (Sep 93)*

Given an algorithm which splits composite numbers into two or more factors, we can apply it repeatedly to factor a number m completely in about $O(log^3 m)$ bit operations. The authors show that this can be reduced to $O(log^2 m)$ by ordering each successive factor list so that only adjacent pairs have a nontrivial gcd. This simple idea can also be applied to the distributed factorisation of polynomials, recognising units in number fields and solving linear equations with respect to a composite modulus.

024705 'Fast Exponentiation Based on Lempel-Ziv Algorithm'
IE Bocharova, BD Kudryashov, *SRIWIT 93 259 - 263*

In rings where squaring is cheaper than multiplication, the number of multiplications needed to perform an exponentiation can be reduced by applying Lempel-Ziv compression to the binary form of the exponent. This delivers a speedup of about 50% over naïve square-and-multiply.

024706 'Comparison of three modular reduction routines'
A Bosselaers, R Govaerts, J Vandewalle, *Crypto 93 pp 17.1 - 17.11*

The authors discuss three algorithms for performing modular reductions on large integers: the 'classical' method, which uses division, and the algorithms due to Barrett and Montgomery, which enable division to be done using a power of the base. They conclude that for general exponentiation Montgomery's algorithm is the best, but show cases where each of the others is superior.

024707 'An implementation of the general number field sieve'
J Buchmann, J Loho, J Zayer, *Crypto 93 pp 15.1 - 15.7*

The general number field sieve is asymptotically the fastest known factoring algorithm, under reasonable assumptions. The authors describe a trial implementation of this algorithm, which was used to factor several numbers of about 50 decimal digits. The only outstanding problem is that of finding a good polynomial, and the empirical results emphasise that this has a huge effect on the algorithm's running time.

024708 'Modification to the Number Field Sieve'
D Coppersmith, *Journal of Cryptology v 6 no 3 (1993) pp 169 - 180*

The running time of the number field sieve can be cut from L($\frac{1}{3}$, 1.923) to L($\frac{1}{3}$, 1.902) by choosing a series of polynomials such that the large sparse matrix which results from the sieving is zero in certain predictable places. Furthermore, an opponent able to make a huge precomputation could further reduce the complexity to L($\frac{1}{3}$, 1.639) by finding optimal bases for all numbers of a given size range.

024709 'On the factorization of RSA-120'
T Denny, B Dodson, AK Lenstra, MS Manasse, *Crypto 93 pp 16.1 - 16.10*

The authors used the quadratic sieve to find the two 60-digit prime factors of RSA-120, the smallest unfactored number on the RSA challenge list. The factorization was achieved by combining the output of 4 separate sites, with a total running time of 825 MIPS years, or 2.6 x 10^{16} instructions, over a period of 82 days. This generated 1.2 Gb of data, of which 160 Mb were useful, and resulted in a sparse matrix of 250,000 rows and columns. It was estimated that to factor a similar size number using the number field sieve would require about 1200 MIPS years.

024710 'A Modified Massey-Omura Parallel Multiplier for a Class of Finite Fields'
MA Hasan, MZ Wang, VK Bhargava, *IEEE Transactions on Computers v 42 no 10 (Oct 93) pp 1278 - 1280*

Some polynomials give rise to redundancy in the Massey-Omura multiplier, in that a number of the product terms are just shifted versions of each other. This enables the circuit complexity to be further reduced.

024711 'On strong pseudoprimes to several bases'
G Jaeschke, *Mathematics of Computation v 61 no 204 (Oct 93) pp 915 - 926*

The author provides an algorithm for constructing a pseudoprime which will pass the Miller-Rabin test with respect to any given set of bases, and produces numbers which pass where the bases are the first n primes for n up to 11. He also shows the smallest such pseudoprimes for $n =$ 5, 6, 7 and 8.

024712 'High-radix modular multiplication for cryptosystems'
P Kornerup, *Computer Arithmetic 93 pp 277-283*

This paper analyzes two algorithms for modular multiplication of very large integers, and concentrates on their applicability for high-radix case. They both use interleaved modulo addition and reductions, but differ in the way the numbers are represented. Application to modular exponentiation with very large operands is also discussed.

024713 'A Parallel Galois Field Multilier with Low Complexity Based on Composite Fields'
C Paar, *SRIWIT 93 pp 320 - 324*

Previous designs for parallel multipliers over $GF(2^k)$ used $O(k^2)$ gates; a new design is presented using $O(k^{log 3})$ for any even k. This is based on a divide-and-conquer algorithm in $GF((2^m)^n)$, where $k = mn$. Gate numbers and primitive polynomials used for k up to 32 are listed.

024714 'A Design of a Fast Pipelined Modular Multiplier Based on a Diminished-Radix Algorithm'
G Orton, L Peppard, S Tavares, *Journal of Cryptology v 6 no 4 (1993) pp 183 - 208*

The authors argue that diminished radix representations offer a faster way to do modular multiplication. If the modulus is n, then this means finding a w such that $wn = 2^k - v$ where v is small (and certainly less than n). They survey previous hardware multiplier designs and performance, develop the design for a diminished radix alternative, and discuss the various pipelining and other tradeoffs; they calculate that a 1.5μ CMOS chip with about 250,000 transistors and a 20MHz clock could do 512 bit RSA decryption with a throughput as high as 650Kbit/sec.

024715 'Some Primality Testing Algorithms'

RGE Pinch, *Notices of the AMS v 40 no 9 (Nov 93) pp 1203 - 1210*

The author reviews primality testing algorithms, discusses pseudoprimes with respect to the Fermat test and its refinements, and explains the Lucas test. He then looks at how primality testing is implemented in four popular computer algebra packages (Mathematica, Maple V, Pari/GP and Axiom); all but Pari/GP declare at least one composite integer to be prime.

024716 'Simultaneous reduction of a lattice basis and its reciprocal basis"

M Seysen, *Combinatorica v 15 no 3 (1993) pp 363 - 376*

The author shows that by reducing the bases of a lattice and its reciprocal at the same time, the Håstad-Lagarias bound on reduced bases can be improved from $\exp(c_1, n^{1/3})$ to $\exp(c_2, ln^2(n))$ where c_1 and c_2 are independent of n. He also discusses a number of possible variants.

024717 'Fast implementation of RSA cryptography'

M Shand, J Vuillemin, *Computer Arithmetic 93 pp 252 - 259*

This paper gives detailed descriptions of many of the techniques applicable in hardware implementations of the RSA algorithm. These include Chinese remaindering, star chains, Hensel's odd division (a special case of the Montgomery method), carry save addition, quotient pipelining, and asynchronous carry completion adders. A programmable gate array implementation is described, achieving RSA decryption rate of 600 Kb/s for 512-bit keys, and 165 Kb/s for 1024-bit keys. The paper also provides a short discussion of methods to speed up software implementations.

024718 'A modular multiplication algorithm with triangle additions'

N Takagi, *Computer Arithmetic 93 pp 272-276*

A new algorithm for multi-precision modular multiplication is presented. The algorithm first adds up the upper half triangle of the partial products, and then computes the residue of the sum. It then proceeds to do the same with the lower half triangle of the partial products. Furthermore, a new method of modular reduction which speeds up the algorithm is described. The proposed techniques are especially applicable to smart cards.

024719 'Addition chains - an erratic sequence'

EG Thurker, *Discrete Mathematics v 122 (93) pp 287 - 305*

The author studies the number of minimal addition chains for a number n, and tabulates this function for a number of values. It seems at first to be highly erratic, but a number of patterns emerge and results are proved which give an explicit formula for $n = 2^k + 2^m$ and bounds for many other numbers.

024720 'On squaring and multiplying large integers'

D Zuras, *Computer Arithmetic 93 pp 260-271*

This paper introduces novel techniques for squaring large integers, which can be generalized for multiplication, and turn out to be faster than the FFT methods. Two new algorithms requiring $O(n^{1.465})$ and $O(n^{1.404})$ are presented. The time required to multiply is upper-bounded by twice the time required to square.

8 Theoretical Cryptology

024801 'One Message Proof Systems with Known Space Verifiers'
Y Aumann, U Feige, *Crypto 93 pp 9.1 - 9.11*
The paper describes a single message proof of knowledge system for any NP statement. It is shown that, assuming the verifier needs at least space S_{min} to verify the proof and space available to him/her is upper-bounded by S_{max}, for any polynomial ratio $k = S_{max}/S_{min}$, there exists a proof which is statistically witness indistinguishable with tolerance k.

024802 'Interaction in Key Distribution Schemes'
A Beimel, B Chor, *Crypto 93 pp 37.1 - 37.11*
Where we want g good guys to be able to construct any number of conference keys despite the presence of b bad guys, then they will need pieces of size $\mid S \mid (g + b - 1)!/b!(g - 1)!$, where $\mid S \mid$ is the size of the key space - this is the same as for an interactive scheme. However, a one time scheme will need pieces of size only $\mid S \mid^2 (g + b + 1)/b$. Thus interaction can improve the space efficiency of such schemes, but only if the number of keys to be generated is limited.

024803 'On Families of Hash Functions via Geometric Codes and Concatenation'
J Bierbrauer, T Johansson, G Kabatiaskii, *Crypto 93 pp 28.1 - 28.10*
An analysis of the Wegman and Carter construction of universal hash functions and authentication codes is performed using coding theory. Applying this theory allows new constructions of such functions with smaller key size. It is shown that good candidate functions can also be obtained from algebraic geometry codes.

024804 'Cryptographic Primitives Based on Hard Learning Problems'
A Blum, M Kearns, M Furst, RJ Lipton, *Crypto 93 pp 24.1 - 24.10*
The authors modify the standard learning definitions so as to get a strong correspondence between hardness for learning and cryptography. The main results are the construction of secure pseudorandom bit generators and private key cryptosystems from any class of functions that is hard to 'weakly predict', and a construction of one-way functions from any class of functions that is hard to 'strongly predict'.

024805 'Fully Dynamic Secret Sharing Schemes'
C Blundo, A Cresti, A De Santis, U Vaccaro, *Crypto 93 pp 11.1 - 11.10*
Secret sharing schemes with a number of access structures are considered. The dealer activates a particular access structure, for a given secret, by broadcasting a message to all the participants. Bounds on the size of shares and broadcast messages are derived, and ideal secret sharing schemes (with broadcast) that satisfy these bounds are defined and analysed. Fully dynamic schemes, which are a generalisation of threshold schemes with disenrollment, are introduced, and a bound on the size of shares is derived.

024806 'Concatenation of Error Correcting Codes and Cryptology'
M Bossert, C Mahr, M Heilig, *SRIWIT 93 pp 292 - 296*
The authors consider the problem of encrypting a signal which has already been encoded in such a way that the code's error correcting properties are retained. They propose a new mode of DES, in which the algorithm's output drives a bit permutation on 64 bit blocks. The performance of this permutation mode is analysed when used in conjuction with various Reed-Muller codes.

024807 'On the Communication Complexity of Zero-Knowledge Proofs'
J Boyar, C Lund, R Peralta, *Journal of Cryptology v 6 no 2 (1993) pp 65 - 85*
In this paper the communication cost of zero-knowledge proofs is investigated. Circuit based methods are established which can be applied to either zero-knowledge arguments (the Brassard-Chaum-Crepeau model) or zero-knowledge proofs (the Goldwasser-Micali-Rackoff model). Several

new techniques are used which greatly reduce the communication cost. The authors show that these techniques also lead to zero-knowledge proofs of knowledge (the Feige-Fiat-Shamir model).

024808 'On the Size of Shares for Secret Sharing Schemes'
RM Capocelli, A De Santis, L Gargano, U Vaccaro, *Journal of Cryptology v 6 no 3 (1993) pp 157 - 167*

The authors analyze the relationship between the size of the shares in a perfect secret sharing scheme and the size of the secret. They show that there exist access structures with four participants for which any scheme must assign shares with average size at least 1.5 times the size of the secret. Particular participants can do better: it is shown that, given any participant X in any access structure, there exist schemes for which the size of X's share is the same as that of the secret. Finally it is shown that there are access structures with $n \geq 5$ participants for which the size of the average share in any scheme is at least 1.5 times the size of the secret.

024809 'Performance of q-ary convolutional codes on jamming channels'
V Chepyzhov, S Popov, K Zigangirov, *SRIWIT 93 pp 38 - 41*

The authors find a bound on the error probability on a channel where the transmitter uses a convolutional code and the jammer, being ignorant of the details of this, just chooses a random jamming character not equal to the transmitted character. They present a decoding algorithm which is similar to Viterbi decoding but keeps only survivor paths, and analyse its performance for both convolutional and trellis codes.

024810 'Secret Sharing Over Infinite Domains'
B Chor, E Kushilevitz, *Journal of Cryptology v 6 no 2 (1993) pp 87 - 95*

The main result in this paper is that there do not exist monotone perfect secret sharing schemes for which the secret and the shares are taken from a countably infinite set. As a consequence, no perfect private-key encryption scheme over the set of all binary strings, exists. This is contrasted with what happens when the shares and the secret are real numbers: for this case, perfect secret sharing schemes and encryption schemes are presented.

024811 'Discreet Solitary Games'
C Crépeau, J Kilian, *Crypto 93 pp 27.1 - 27.12*

The authors show how one may shuffle a deck of cards in such a way as to make a random choice of permutations with particular characteristics, such as having no fixed points or no short cycles. They also show how to copy bits and evaluate gates in this model. Applications may include playing games such as patience (solitaire).

024812 'Interactive Hashing can Simplify Zero-Knowledge Protocol Design Without Computational Assumptions'
IB Damgård, *Crypto 93 pp 10.1 - 10.10*

The paper describes a method of transforming a bounded round public-coin protocol, which is zero-knowledge against an honest verifier, to one that is zero-knowledge against any verifier. The transformation is based on interactive hashing, and does not require any computational assumptions. The transformation preserves the proving properties of the original protocol, as well as any statistical zero-knowledge properties.

024813 'On the Existence of Statistically Hiding Bit Commitment Schemes and Fail-Stop Signatures'
IB Damgård, TP Pedersen, B Pfitzmann, *Crypto 93 pp 22.1 - 22.11*

The relation between fail-stop signatures and bit commitment protocols is studied. It is proved that the existence of a statistically hiding bit commitment protocol with non-interactive opening and public verification implies that fail-stop signatures exist. However the converse is true only if they have 'almost unique secret keys'. As a consequence, one may construct them from one-way permutations and collision free hash functions.

024814 'Secret Sharing and Perfect Zero Knowledge'
A De Santis, G Di Crescendo, G Persiano, *Crypto 93 pp 8.1 - 8.10*

The relation between secret sharing and perfect zero-knowledge in the non-interactive model is studied. Perfect zero-knowledge proof systems for the languages BL, of Blum integers, and OR, of logical or of quadratic residuosity, are given and yield in turn a non-interactive perfect zero-knowledge for threshold statements. This language, denoted by $T(k,m)$, consists of pairs $(x,\vec{y})$ where $\vec{y}=(y_1,y_2,\cdots,y_m)$ and less than k elements of $\vec{y}$ are quadratic nonresidues modulo x. The proof system is generalised to monotone access structures.

024815 'Broadcast Encryption'
A Fiat, M Naor, *Crypto 93 pp 39.1 - 39.10*

Previous schemes to broadcast a secret to n users with resilience against coalitions of up to k cheaters needed memory exponential in k. The proposal is to use a mass of 1-resilient schemes; each user belongs to several of these. The result is that security is almost free, in the sense of being almost independent of the security parameter; even with $n = 10^9$ and $k = 10^5$, each user needs only 20 keys.

024816 'Joint Encryption and Message-Efficient Secure Computation'
M Franklin, S Haber, *Crypto 93 pp 23.1 - 23.10*

This paper applies group-oriented cryptography to secure distributed computation. A probabilistic public key encryption scheme is proposed which is blindable and 'compact', and allows any subset of parties to encrypt a message such that efficient decryption is only possible if all the parties who were involved in encryption cooperate. One consequence is to reduce the message complexity of secure computation, as passive adversaries can be tolerated. In particular, a Boolean circuit of size C can be computed by n participants communicating only $O(nC)$ bits. This improves over previous results by a factor of n.

024817 'Statistical techniques for language recognition: an introduction and guide for cryptanalysts'
R Ganesan, AT Sherman, *Cryptologia v XVII no 4 (Oct 93) pp 321 - 366*

This paper provides a theoretical basis for the various techniques used to distinguish both known and unknown languages from noise. The authors review existing techniques, such as the index of coincidence and Sinkov's statistic; they then model language as a Markov process, and apply the theory of inference on Markov chains to develop likelihood ratio tests. Finally, there is an extensive survey of related work in statistics, and a bibliography of over 100 items.

024818 'Sequential Cryptographic Codes providing Secrecy and Authentication'
C Gehrmann, *SRIWIT 93 pp 280 - 284*

The author defines a cipher to be secrecy optimal if it provides perfect secrecy with the minimum necessary number of keys, and also authentication optimal if the deception probabilities are equal and all key information is used to give either secrecy or authenticity. He provides lower bounds on key size for combining secrecy, authentication and source coding in a block cipher.

024819 'Codes for Interactive Authentication'
P Gemmell, M Naor, *Crypto 93 pp 30.1 - 30.11*

The authors consider authentication with interaction between transmitter and receiver, but where an intruder may inject, delete or modify messages. It is shown that, for a single round protocol, authenticating n bits with cheating probability of at most p requires $log(n) + log(1/p)$ secret bits and for k round protocols the number reduces to $log^k(n) + 5log(1/p)$. Thus the size of secret required decreases with the number of rounds.

024820 'A Perfect Zero-Knowledge Proof System for a Problem Equivalent to The Discrete Logarithm'

O Goldreich, E Kushilevitz, *Journal of Cryptology v 6 no 2 (1993) pp 97 - 116*

The authors present a perfect zero-knowledge proof for the decision problem DLP_ε, which is computationally equivalent to the discrete logarithm problem. For a prime modulus p and generator g, given $y \equiv g^x \bmod p$, DLP_ε is the 'promise problem' that the exponent x lies in the interval $[(p-1)/2+1,\ p-1]$, if it is guaranteed that it lies either in $[1,\ \varepsilon(n)\cdot p]$ or in $[(p-1)/2+1,\ (p-1)/2+\varepsilon(n)\cdot p]$. Here $n^{-O(1)} < \varepsilon(n) < \frac{1}{2}$ and $n = \log_2 p$. The result is then extended from Z_p^* to any Abelian group.

024821 'The Discrete Logarithm Modulo a Composite Hides O(n) Bits'

J Håstad, AW Schrift, A Shamir, *Journal of Computer and System Sciences v 47 no 3 (Dec 93) pp 376 - 404*

This is the journal version of the authors' STOC 90 paper on this topic; provided it is hard to factor a Blum integer N, then inverting $y = g^x \pmod N$ is equally hard in all its bits.

024822 'A Low Communication Competitive Interactive Proof System for Promised Quadratic Residuosity'

T Itoh, M Hoshi, S Tsujii, *Crypto 93 pp 7.1 - 7.11*

The paper describes a proof system for quadratic residuosity. The protocol is compared with the Bellare-Goldwasser protocol, and is shown to be both more efficient in terms of communication complexity and less restrictive in terms of the condition on N - namely that k, the number of prime factors of N, is $O(log|N|)$. Provided this holds, the communication complexities of the prover and verifier are $k(|N|+4)$ and $4|N|$ respectively.

024823 'Multisecret Threshold Schemes'

WA Jackson, KM Martin, CM O'Keefe, *Crypto 93 pp 12.1 - 12.10*

The authors extend threshold schemes, by considering systems in which participants can construct a number of secrets. They define w-secure (t,k,n)-multithreshold secret sharing schemes to be such that each subset of k (out of n) participants holds a secret in a (t,k) threshold system and any subset of at most w, $0 \le w \le n-k+t-1$, participants cannot learn anything about any secret with which they are not associated. Bounds on the size of participants' shares are derived, and examples of systems satisfying the bounds are given.

024824 'On the Construction of Perfect Authentication Codes that Permit Arbitration'

T Johansson, *Crypto 93 pp 29.1 - 29.11*

The author considers authentication with arbitration; codes for which all types of deception are equally hard are called equitable. Previous constructions for equitable authentication codes had been very inefficient; the author presents a scheme which is perfect in the sense that it requires the minimum number of encoding rules for both transmitter and receiver.

024825 'Secret Sharing Made Short'

H Krawczyk, *Crypto 93 pp 13.1 - 13.10*

This paper considers secret sharing systems in a computational model of secrecy. Computationally secure (n,m)-secret sharing schemes are defined and a construction is given which uses information dispersal, encryption functions and hashing. It is shown that the size of shares is $1/m$ times the size of the secret, plus a short piece of information whose length only depends on the security parameter.

024826 'Some Aspects of Anonymity of Communications'

IN Landgev, *SRIWIT 93 pp 287 - 291*

The author shows how to increase the data rate of Chaum's dining cryptographers protocol using an (n, k, d) linear code; it can then be used to transmit up to $\lfloor \frac{d-1}{2} \rfloor$ messages simultaneously, and the collision probability can be calculated from n and the number of messages.

024827 'Minimal Codewords and Secret Sharing'
JL Massey, *SRIWIT 93 pp 276 - 279*
The author shows that where a secret sharing scheme of the kind proposed by McEliece and Sarwate is based on a linear code, the access structure determines, and is determined by, the set of minimal codewords in the dual code.

024828 'Applications of finite geometries to information security'
CM O'Keefe, *Australasian Journal of Combinatorics v 7 (93) pp 195 - 212*
The author gives an overview of the use of finite geometries in secret sharing and key distribution schemes, and the properties of Legendre planes; she then shows how these structures can be used to construct key distribution patterns.

024829 'A Lower Bound on Authentication After Having Observed a Sequence of Messages'
U Rosenbaum, *Journal of Cryptology v 6 no 3 (1993) pp 135 - 156*
Lower bounds for unconditionally secure authentication systems are obtained. There are two main results. First, a lower bound is obtained for the probability p_i that an opponent succeeds in generating an authenticated message after having observed i messages encoded under the same encoding rule. Then a lower bound is obtained for the probability P_ℓ that an opponent can be successful if he can choose up to ℓ messages encoded with the same encoding rule. Both results apply to general authentication systems, thus extending the results of Brickell, Simmons, and Walker. Furthermore, necessary and sufficient conditions are obtained for authentication systems that meet these lower bounds, which extend earlier results by Fåk, Gilbert and others. Finally, authentication systems that are ℓ–fold secure against spoofing are investigated.

024830 'Universal Test for Nonuniform Distributions'
AW Schrift, A Shamir, *Journal of Cryptology v 6 no 3 (1993) pp 119 - 133*
The authors show how to modify universal randomness tests to deal with sources which have a bias b (the probability of a 1 is b). Here the problem is to check that the sequence has no other property, such as intersymbol dependency; and there turn out to be a number of equivalent tests. These include the predict-or-pass test (it is impossible to predict the output bit on any nonnegligible fraction of the output strings with probability of success greater than b) and that the weighted success rate (namely prob$\{1$ is correctly predicted$\}/b$ + prob$\{0$ is correctly predicted$\}/(1-b)$) should be not greater than 2. The results are then generalised to the case where we wish to know whether our source can be distinguished from an arbitrary model.

024831 'Source encoding and cryptography'
YM Shtarkov, *SRIWIT 93 pp 250 - 253*
The author discusses the information theoretic aspects of combining coding and cryptography, with particular reference to the Witten-Cleary proposal to use adaptive compression of text with a secret prefix for privacy purposes.

024832 'Two Round ZKIP of Knowledge for SAT and its Applications'
HK Yang, JW Jung, DH Won, *SICON/ICIE'93 pp 512 - 517*
This paper proposes an optimal 4-move zero-knowledge interactive proof system for SAT and its applications. The new system is based on the trapdoor bit-commitment scheme and the witness indistinguishable and witness hiding properties.

9 Book Reviews

'DIFFERENTIAL CRYPTANALYSIS OF THE DATA ENCRYPTION STANDARD'
E Biham, A Shamir, *Springer (1993) ISBN 0-387-97930-1*

One of the most exciting developments of the 1990's has been the development of differential cryptanalysis. In its basic form, this studies the evolution of differences through successive rounds of a block cipher when two related plaintexts are encrypted using the same key; it has demolished most of the block cipher designs which had been proposed in the research literature, and led to a coherent theory of what makes a block cipher good.

The technique was invented by Eli Biham and Adi Shamir to attack the Japanese block cipher FEAL. However, their main achievement has been developing it to the point where it can break DES significantly more quickly than exhaustive keysearch; and so a textbook on this subject by these authors has particular authority.

The central concept is that of an n-round characteristic. This is a pattern of input bit changes which leads to a known pattern of output bit changes after n rounds with a certain probability. The characteristics of highest probability are thus the best signalling channels through the rounds of an algorithm; and given a high enough signal to noise ratio, we can use them to get information about certain subkey bits. Examples are given of how relevant characteristics can be found and used for DES with 4, 6, 8 and 9 rounds.

Having explained the basic technique, the authors show that modifying the P permutation could make the algorithm much weaker, and that the same holds for changing the E expansion or the binary functions within the autoclave. The significance of the S-boxes is shown; replacing them with random ones, changing their order, or even using boxes with uniform difference distributions (as some writers had suggested) all weaken the algorithm. Next, they show that even with independent subkeys, the attack complexity is only increased by a few bits.

Having thus shown that DES is in some sense optimal for designs of its type and size, the authors then go on to explain in detail how a differential attack can be used to break it using about 2^{47} chosen plaintexts, from which 2^{36} are easily selected for further scrutiny. Subsequent analysis costs the equivalent of 2^{37} DES operations and has a probability of success of 58%. The attack processes batches of 2^{14} plaintexts at a time, and does not require that the same key be retained from one batch to the next; thus whenever a system lets an opponent encrypt 2^{14} chosen plaintexts, its key can be broken with probability 2^{-33}.

Subsequent chapters go into detail on the analysis of FEAL, Khafre, REDOC-II, LOKI and Lucifer (only the eight-round attack is presented, not the full sixteen round attack reported in abstract 024502 above); and finally, the hash functions SNEFRU and N-hash are dealt with.

This work was originally published in a number of conference papers and journal articles, and although a special issue of the Journal of Cryptology in 1991 carried a snapshot of the art at that time, it did not give as much detail. The book also gives details of the attacks on algorithms other than DES which have not appeared before; it also ties the whole basic theory of this subject together in a form which makes it accessible enough to be used for teaching as well as reference. It is thus a timely and welcome addition to the literature, and should be required reading for research students starting work in cryptology.

'THE DEVELOPMENT OF THE NUMBER FIELD SIEVE'

AK Lenstra, HW Lenstra (editors), *Springer Lecture Notes in Mathematics no 1554, 1993, ISBN 0-387-57013-6*

Many fielded computer and communications security systems depend on the difficulty of factoring, and the number field sieve is asymptotically the fastest known factoring algorithm; yet many of the key papers on the topic had only circulated as manuscripts. The lack of published material made it rather difficult for many workers to understand what was going on. This sad state of affairs has now been rectified by the appearance of this book, which covers the number field sieve from its invention in 1988 through to recent implementations.

The book opens with Pollard's original manuscript 'Factoring with cubic integers' which proposed the basic technique and even speculated that F_9 would eventually be factored by it (which it was, in 1990). There follows a reprint of the 1990 STOC paper by Lenstra, Lenstra, Manasse and Pollard in which the number field sieve was introduced to the wider public.

The next two papers extend the theory further: an unpublished Pollard manuscript entitled 'The Lattice Field Sieve' shows how the machinery can be extended to two dimensions, and a paper by Buhler, Lenstra and Pomerance entitled 'Factoring Integers with the Number Field Sieve' introduces the general number field sieve, which tackles numbers which are not of any special form.

The two final papers discuss implementation issues. Couveignes shows a better way to compute square roots of algebraic integers, while in the last paper Bernstein and Lenstra describe a full implementation of the number field sieve on a massively parallel computer (Bellcore's 16K MasPar). They discuss a number of optimisations, and describe a number of factorisations leading up to that of $2^{523} - 1$, which at 158 digits set a new record in 1992.

For many students of number theory and cryptology, this will be the book which unlocks this complex and fascinating new subject. It should also be on the reading list of graduate students who are starting work in the area.

'A COURSE IN COMPUTATIONAL ALGEBRAIC NUMBER THEORY'

H Cohen, *Graduate Texts in Mathematics 138, Springer, 1993, ISBN 0-387-55640-0*

The stated goals of this book are that it should be introductory and emphasise practicality. First, basic number-theoretic algorithms are discussed in detail, followed by the computational problems of algebraic number theory. Elliptic curves are introduced, and finally the problems of primality testing and factorisation are tackled; there is an approximate historical progression from Fermat to the Number Field Sieve.

The first chapter discusses the most fundamental number-theoretic algorithms, such as Euclid's algorithm, in some detail. These algorithms are used frequently, so even minor improvements are valuable. The general pattern of presentation is to recall the theory behind a computational problem, and then give a simple algorithm to show that the problem can be solved. Then improvements are made, and alternative approaches considered, so that one is sometimes presented with three or four algorithms. Often the optimal algorithm will be situation-dependent, and the author discusses the circumstances when a particular choice of algorithm might be preferable. Asymptotic running times are often left as exercises.

Chapter 2 considers algorithms for linear algebra and lattices, notably normal forms and lattice basis reduction, with applications. Problems of numerical stability are mentioned, but not covered -

the emphasis is on algorithms rather than numerical analysis. Clarity of exposition takes precedence over implementational detail: the author intends us to actually understand the algorithms, not just to be able to program them, and the best way to do this is often to work out the details for oneself. As many proofs are left to the exercises, the trusting reader can progress quickly, whilst the conscientious student will find plenty of worthwhile problems to stimulate his learning.

The meat of Chapter 3 concerns factorisation of polynomials over prime fields, the integers and the complex numbers. Chapters 4 to 6 treat algebraic number fields: chapter 4 begins with definitions and problems of representing algebraic numbers, followed by a summary of the relevant algebraic number theory, leading to a list of the main computational tasks associated with algebraic number fields. Chapter 5 considers the important special case of quadratic fields; there is a careful exposition of the theory, and a detailed discussion of algorithms for computing the class number and class group of a quadratic field. Chapter 6 deals more briefly with number fields of higher degree, with a particularly interesting treatment of cubic fields.

The latter part of the book is devoted to primality testing and factorisation algorithms. By way of preparation, Chapter 7 gives a summary of the theory of elliptic curves, without proofs, and a collection of algorithms, also mostly without proof. As a concise exposition of the key results concerning elliptic curves, it is a useful chapter, and gives an excellent impression of the richness of this area of mathematics. Chapter 8 gives a careful description of exponential factoring algorithms, notably Pollard's ρ-method, Shanks's SQUFOF, and Pollard's $p-1$ method (in preparation for the Elliptic Curve Method). Chapter 9 covers two important modern primality tests: the Jacobi Sum test and the Elliptic Curve test. The final chapter gives an overview of the fastest known factoring methods, concluding with the Number Field Sieve. Here the treatment is necessarily brief, but gives a good introduction to the methods.

There are two appendices. The first discusses various computer packages which might interest number-theorists. The second contains tables of class numbers and units for some 700 quadratic and cubic fields, and a table of all modular elliptic curves over the rationals with conductor below 45. There is an extensive, and useful, bibliography.

In conclusion, this is not only an excellent book from which to learn, but is also sufficiently comprehensive to be a splendid reference. The algorithms presented are both beautiful and practical, and the clear exposition of the mathematics makes it an ideal introduction to computational algebraic number theory.

THE ANALYSIS AND DESIGN OF HASH FUNCTIONS'

B Preneel, *Katholieke Universiteit Leuven UDC 621.391.7 (1993)*

This thesis is a comprehensive guide to the state of the art of making and breaking hash functions. It introduces the application requirements for cryptographic hashing, the various possible attacks from the birthday problem through to differential cryptanalysis, and the information theoretic and complexity theoretic approaches, including collision freedom.

The core of the book, however, is the author's classification of hash functions based on block ciphers. Most of the early constructions were broken sooner or later, and the author shows why; the majority of possible schemes fall to one attack or another. The exhaustive analysis of which schemes break in which ways shows precisely which are secure, at least for the case where the hashcode is the same length as the cipher block, and one round of encryption is used per iteration. A substantial start is also made on the case where the hashcode is twice the cipher block length, and two encryptions are used per iteration.

Later chapters review attempts to base hash functions on number theory, the various Boolean function properties currently considered important in the design of dedicated hash functions and block ciphers, and the dozen or so systems in actual use, including BCA (a Belgian banking standard, in which a weakness is shown) and the decimal-shift-and-add system used by German banks (for which a practical attack is presented).

A number of other new attacks, or improvements of known attacks, are scattered throughout the book. Quite apart from this, and the classification of chaining modes, it is a useful reference, and should be reissued by one of the commercial publishing houses.

'DIGITAL WOES'
LR Wiener, *Addison-Wesley (1993) ISBN 0-201-62609-8*

Most actual computer security failures are not due to technical attacks on cryptographic algorithms or protocols, or to the exploitation of covert channels in operating systems, but to outright blunders in system design and implementation. Security professionals thus have to educate their clients about how systems fail, and communicate at least the basics of software engineering.

A common problem is that staff with the power to make a difference, such as the client's directors and senior managers, usually come from a background such as marketing or finance, and are hard to educate on technical matters. It is therefore most welcome to find in this book a well written and well researched investigation of system failures, produced by a journalist for a general audience rather than by an engineer for his peer group.

Using case histories drawn from sources as diverse as the research literature, local newspapers and the usenet newsgroup comp.risks, the author explores the many ways in which software projects fail, and in which even those which succeed end up with subtle and persistent bugs. She manages to get across the basic software engineering ideas, such as the waterfall and spiral models, without using jargon; she provides a number of insights into the nature of resilience; and, importantly, sets the problems in their organisational and political context.

Her conclusions are unexceptional: large systems cannot be made reliable, so we had better make safety critical systems small and simple; and software bugs are an inescapable fact of life which had better learn to live with. However the presentation is compelling, and reading this book would almost certainly make a corporate manager more receptive to security concerns. It also contains a fair amount of material of interest to security professionals and other people involved with dependable systems.

'INFORMATION SECURITY'
JE Ettinger (editor)
Unicom Series in Applied Information Technology v 16 (Chapman and Hall), 1993

This book is a collection of sixteen articles on various computer security topics. They are mostly fairly routine, but three of them provide insights into the UK government's information security programme. 'The current status of CRAMM', by Robin Moses, describes the risk analysis methodology in use; 'Licensed security evaluation', by Tom Farr, describes the process of evaluating products under ITSEC; and 'Distributed secure system technology demonstrator programme', by Andy Bates, describes the use of Trusted Network Interface Units and how they implement GOSIP, the Government OSI Profile.

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