Computer and Communications

Security Reviews

Volume 3 Number 3 (September 1994) ISSN 1352-6278

CONTENTS

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

'Computer and Communications Security Reviews' is published quarterly by, and is copyright, of Northgate Consultants Ltd, whose registered office is Ivy Dene, Lode Fen, Lode, Cambridgeshire, United Kingdom CB5 9HF. Subscription rates, conditions and ordering details are on the inside back cover.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 31 August 1994; and books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Canadian Info Theory 93: 30/5 - 2/6/93; Third Canadian Workshop on Information Theory and Applications, Rockland, Ontario; *Proceedings published by Springer Verlag, LNCS 793, 1994*

OOPSLA 93: 28 - 30/9/93; Eighth Annual Conference on Object-Oriented Programming Systems, Languages and Applications; *Proceedings published as v 28 no 10 of ACM SIGPLAN*

JW-ISC 93: 24-26/10/1993; Korea-Japan Joint Workshop on Information Security and Cryptology, Seoul, Korea

Fast Software Encryption 93: 9-11/12/1993; Cambridge Security Workshop; *Proceedings published by Springer Verlag, LNCS 809, 1994*

Dependable Computing 94: January 1994; IFIP Conference on Dependable Computing, San Diego, California

IFIP SEC 94: 24 - 27/5/94, Curaçao, Netherlands Antilles; *Proceedings to be published by Elsevier-North Holland: paper numbers here refer to preproceedings*

Securicomm 94: 1-2/6/94, Paris; *Proceedings published by MCI, 6 rue l'Isly, 75008 Paris*

Franconia 94: 14-16/6/94; Proceedings of the Computer Security Foundations Workshop VII, Franconia, USA; *Proceedings published by the IEEE CS press*

Salomaa Colloquium: June 1994; Results and Trends in Theoretical Computer Science - Colloquium in Honor of Arto Salomaa, Graz, Austria; *Proceedings published by Springer Verlag, LNCS 812, 1994*

Finite Fields 94: 5-6/7/94, IMA Conference on Applications of Finite Fields, Royal Holloway, University of London; *Proceedings to be published by Oxford University Press*

Singapore 94: 20-22/7/94; The 2nd Singapore Computer Security Conference: New Challenges, New Approaches

Database Security 94: 23-26/8/1994; IFIP WG 11.3 8th Annual Working Conference on Database Security, Bad Salzdefurth, Germany *Preproceedings published by University of Hildesheim; proceedings to appear*

Corrigendum: In volume 3 number 2 we carried a number of abstracts from SAC 94. This referred to the workshop on Selected Areas in Cryptography held at Queen's University, Kingston, Ontario on May 5-6, 1994; proceedings published by Queen's University.

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

1 Applications and Engineering

033101 'EasyCard will pay customer for using card'
NR Achs, *Cards International ni 111 (13/6/94) p III*
A chip card being introduced in the Czech Republic has the incentive that cardholders will receive a refund of 1% of their purchases for the first seven months.

033102 'Why Cryptosystems Fail'
RJ Anderson, *Securicomm 94 pp 47 - 60*
This is a shortened and updated version of **031103**, and describes a number of attacks on retail banking systems. The great majority of security failures were caused by blunders rather than by high-tech attacks; it follows that security designers should pay much more attention to robustness. The nature of robustness is discussed briefly.

033103 'The Truth About Biometric Verification'
J Ashbourn, *Security Surveyor v 25 no 2 (July 1994) pp 13 - 17*
The author surveys a number of biometric verification technologies, and suggests that his hand geometry systems are the best. This claim is backed by a trial at Sandia which achieved a single try error rate of 0.3%. A number of actual and hypothetical applications are discussed.

033104 'Rocking the cheque world'
D Austin, *Banking Technology (July/August 94) p 16*
This article reports an interview with the chief executive of Mondex, who claims that his system is the only properly transferable form of electronic money.

033105 'TETRA - A Standard for Police Communications'
H Azemard, *Electrical Communication Q2 94 pp 111 - 117*
The author describes a police communications system, which is based on GSM components but has extra data services and mobile switching centres.

033106 'Deposing cash as king'
Banking World (July 1994) p 36
This article describes moves in a number of countries to market electronic purses for low value payments. Operators will mainly benefit from increased float, but there may be charges for retailers and cardholders as well. European central bankers want only banks allowed to issue such purses, in order to keep control of the money supply.

033107 'A survey of current and possible future uses of X.500 directory services'
P Barker, T Johannsen, C Robbins, *Journal of Information Networking v 1 no 3 (94) pp 204 - 226*
The authors survey the X.500 email directory standard, and discuss the extent of its penetration in the various user communities and application areas. In addition to the security aspects, they discuss routing, mailing list management, bibliographic uses and future trends, and mention a number of current research projects.

033108 'Personal computer viruses'
J Bates, *Information Security Monitor v 9 no 8 (July 94) pp 5 - 8*
The author describes the main types of computer virus and exposes a number of myths.

033109 'Security Systems Based on Exponentiation Primitives TESS - The Exponential Security System'

T Beth, D Gollmann, *IFIP SEC 94 paper B3*

The European Institute for System Security at Karslruhe has developed some authentication and key-exchange protocols based on the fact that discrete exponentiation gives a one-way function which is also a homomorphism. The software is distributed free of charge; this paper describes the techniques that it employs and some of the network services that use it.

033110 'Digital Payment Systems in the ESPRIT Project CAFE'

JP Boly, A Bosselaers, R Cramer, R Michelsen, S Mjølsnes, F Muller, T Pedersen, B Pfitzmann, P de Rooij, B Schoenmakers, M Schunter, L Vallée, M Waidner, *Securicomm 94 pp 35 - 45*

The authors discuss the electronic wallet system being developed for the CAFE project. This supports multiple currencies, unconditional anonymity and loss tolerance; although it is a prepaid system, the wallet contents can be backed up regularly and so lost coins can be refunded. The project is currently being implemented.

033111 'Anatomy of the latest generation computer viruses'

VV Bontchev, *IFIP SEC 94 paper I6*

The formerly exponential growth in the number of computer viruses has now levelled off, but there are still 1000 new specimens per year to add to the current stock of 4,300; this means that new firms cannot economically enter the anti-virus software market. A number of the latest virus writers' tricks are explained; some means of stripping off encryption or dealing with polymorphism in other ways would be useful progress from the anti-virus point of view.

033112 'Evaluation de la Sécurité des Cartes à Microprocesseur selon les ITSEC: le Projet SPECS'

JP Boulé, P Brégant-Belin, JL Roussel, *Securicomm 94 pp 99 - 108 (in French)*

The first phase of a European project to evaluate the security of smartcard systems studied the applicability of ITSEC to telephone and bank card applications; it was restricted to application features and did not look at either the tamper resistance or the cryptographic algorithms. It considered the use of semi-formal methods, as required for an evaluation of E4.

033113 'A General Introduction to C3I Systems and their Application to Security Forces'

E Bourchin, *Electrical Communication Q2 94 pp 106 - 110*

The author gives an overview of C3I systems, particularly as applied to police forces, and describes the Alcatel architecture for such systems.

033114 'Caught in the act?'

J Burne, *The Times Magazine (16 July 1994) pp 14 - 17*

The author reports VIAS, the Video Identity Assessment System, whose purpose is to match suspects' faces against security video recordings. The idea is to measure the relative size of over 50 features such as interocular distance and nose width. Previously, expert evidence of identifcation had been disallowed due to the lack of statistical data on its reliability; it is hoped that this system will fill the gap.

033115 'Software Roundup: Virus-Prevention NLMs'

Byte v 19 no 8 (Aug 1994) pp 129 - 136

This article contains evaluations of seven anti-virus products which were designed for use with Novell NetWare.

033116 'ALCIDE - The Alcatel C3I Devlopment and Execution Platform'
D Carcagno, P Suslenschi, *Electrical Communications Q2 94 pp 111 - 117*

The authors describe an Alcatel software platform for C3I systems. This is designed to integrate a wide range of functions from air defence through cartography to intelligence, forces location and criminal records.

033117 'Dark horse in lead for fingerprint ID card'
Card World Independent (May 94) p 2

The UK government plans to issue driving licences with a photo, and appears to have an ID card with fingerprints as a long term goal. Thorn Secure Systems and EDS are thought to be front runners for the contract; meanwhile, an EDS system which uses fingerprints to prevent welfare fraud in Los Angeles is only 95% effective.

033118 'Phantom withdrawals raise security questions in UK'
Card World Independent (Apr 94) p 1

This article reports a case in which a policeman was convicted of attempted fraud after disputing ATM transactions; the branch manager insisted that he was guilty as their computer system did not make mistakes.

033119 'CaberNet (Computing Architectures for Basic European Research): the ESPRIT Basic Research-Funded Network of Excellence in distributed computing systems architectures'
N Cook, *Distributed Systems Engineering v 1 no 3 (Mar 94) pp 173 - 176*

The author describes CaberNet, an EC initiative to bring together the 43 main players in distributed systems research from both academia and industry. One of the research themes is dependability.

033120 'Canada sees rise in counterfeit cards'
D Cowan, *Cards International no 109 (12/5/94) p 7*

Fraud is now costing C$2.50 per cardholder in Canada, with lost and stolen cards accounting for over half of this and counterfeiting for a quarter.

033121 'Un example concret de sécurisation de réseaux locaux interconnectés'
A Denis, *Securicomm 94 pp 297 - 306 (in French)*

The author reports his experience in securing a multimedia system consisting of a number of interconnected LANs and about 3,000 workstations for a large corporation. The access control structure consisted of workgroups in a lattice of sites and divisions; the system had both unclassified and confidential servers. Most of the secrets were industrial in nature, with some defence material; techniques were largely physical, with fibre optic cable used for sensitive LANs and some TEMPEST equipment. Encryption was used to protect the hard disks of portable computers, and access control systems could use mutual authentication.

033122 'EDI security in TEDIS'
M De Soete, *Securicomm 94 pp 177 - 179*

The author describes the EC's TEDIS project for the development of EDI systems. The first phase of this project involved studying the use of digital signatures and the second phase will consider how to integrate them and provide the necessary legal foundation. Certification authorities will be piloted in 1994 and 1995.

033123 'Security in EDIFACT Systems'
T Dosdale, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 532 - 537*
This paper examines the requirements for EDI Security, and how these requirements are being met.

033124 'ATM fraud and the customer'

J Essinger, *Financial Technology Insight (June 1994) pp 12 - 14*

The author discusses recent bad publicity experienced by UK banks over phantom withdrawals from ATMs.

033125 'Multi-Application Smart Cards'

D Everett, *Smart Card News v 3 no 5 (May 94) p 95; v 3 no 6 (June 94) pp 116 - 119; and v 3 no 7 (July 94) pp 137 - 139*

The author discusses the problems in developing a proper operating system for smartcards, which would allow one card to share multiple applications. Some of these are still not tackled by the relevant standards, and manufacturers offer proprietary solutions, such as access control matrices fixed at manufacture. However a proposed ISO file structure has been used to guide the development of a system of application identifiers which is now in use in Denmark.

033126 'The Hedge End Experiment'

M Fairhurst, *International Security review no 85 (Summer 94) p 20*

The author reports a trial of the University of Kent's 'KAPPA' signature verification system at a post office near Southampton in January 1994. 8500 samples were taken from 343 customers, and 98.2% were verified correctly at the first attempt, rising to 99.15% after three attempts. 214 of the customers later participated in a survey and 97% said they would welcome the general introduction of the system.

033127 'Nomadic IT'

H Gliss, *Securicomm 94 pp 233 - 245*

The proliferation of laptop computers introduces new problems. The author provides a checklist for risk evaluation, and recounts a number of cases in which laptops with sensitive information were lost or stolen, or a virus propagated throughout the sales force. The main requirement is a cryptographically based access control system, and some desirable properties of this are discussed.

033128 'Security aspects in IT systems based on portable micro computers'

H Gliss, *Computer Fraud and Security Bulletin (July 1994) pp 13 - 19*

The author describes the design rationale behind his mobile PC security product, which offers access control, file and communications encryption, and virus protection.

033129 'The Story of the Hagelin Cryptos'

BCW Hagelin, *Cryptologia v XVIII no 3 (July 94) pp 204 - 242*

In this technical autobiography, the founder of Crypto AG tells the story of the series of rotor machines named after him and marketed by the firm be built up. He traces their development from the early prototype machines through the B-21, which was adopted by Sweden from 1925, and the related B-211, which was adopted by France from 1932 and copied by the Russians as well. His largest commercial success was the five rotor C-35 which the Americans bought from 1940 and renamed the M-209. A number of improved versions were produced after the war: these ranged from pocket machines for police use, through diplomatic machines with more rotors and irregular stepping, to devices for encrypting teleprinter traffic.

033130 'Authentication: A Prominent Issue for Data Communications'

D Hains, *Information Management and Computer Security v 2 no 1 (94) pp 25 - 27*

The author discusses authentication in EDI and describes a DES/RSA toolkit called SCORE from Eracom which helps users implement this.

033131 'Issues and problems in Secure Remote Access'
WM Hancock, *Network Security (June 94) pp 14 - 18*

The author describes a software system for securing dial access; users must authenticate themselves to a gateway server.

033132 'Security, Authentication and Policy Management in Open Distributed Systems'
R Hauser, S Zatti, *IFIP SEC 94 paper C6*

The authors describe a prototype security management system called SAMSON which uses Motif to enforce system-wide security policies and in particular to maintain coherent records about large numbers of users. Its goal is to make security management independent of the particular access control method in use at any local node.

033133 'Exploiting client-server computing to meet the needs of retail banking organisations'
M Haynes, G Ibbett, D Walker, *Ingenuity (formerly ICL Technical Journal) v 9 no 1 (May 1994) pp 47 - 66*

The authors describe an ICL client server system which supports retail banking, including ATMs, teller terminals and links to networks such as VISA. It is based on a hierarchy of servers (in branches and in central sites) running TUXEDO.

033134 'Banksys names smartcard due for trial'
G Hennessy, *Cards International no 114 (10/8/94) p IV*

The Belgian national payments system, Banksys, will be starting trials of an electronic purse in Leuven and Wavre during December.

033135 'How Secure is Data over the Internet'
HJ Highland, *Network Security (June 94) pp 9 - 11*

The author describes some of the threats to Internet security, and reproduces the checklist from Cheswick and Bellovin's book.

033136 'Security in Virtual Reality: Virtual Security'
A Hunstad, *IFIP SEC 94 paper I2*

Virtual reality introduces a whole new set of security problems, and workers in this field make the same elementary mistakes over and over again. One problem is that the higher the fidelity of the virtual world, the more we may be fooled by it; the opportunities may include face recognition and fast encryption.

033137 'AT&T Scientist claims "Clipper doesn't work" '
Information Security Monitor v 9 no 8 (July 94) pp 1 - 2

This article reports Blaze's false leaf attack on the Clipper protocol, and suggests that the NSA will have to withdraw the product for redesign.

033138 'New England shopping mall ATM scam copied in UK'
Information Security Monitor v 9 no 7 (June 94) pp 1 - 2

Thieves installed an ATM, which may have been stolen, in a bogus home loans shop in Roman Road, Bethnal Green, London; customers who used it had their cards copied, and £250,000 may have been taken through the Link network, which is more vulnerable to duplicate cards as transactions are processed overnight. Three men and a woman have been detained.

033139 'Barclays links with Mercury for trial'
A Jarman, *Cards International no 114 (10/8/94) p III*

Barclays is offering banking services via the subscriber identity modules of Mercury mobile phones, and hopes to sign up 10,000 customers in 1994.

033140 **'Privacy Enhanced Electronic Mail System for KREONet'**
Y Jeong, J Kim, C Lim, O Byeon, *JW-ISC 93 pp 160 - 168*
This paper discusses a trial implementation of PEM in a Korean network.

033141 **'New moves in EFTPOS'**
D Jones, *The Banker (Sep 94) p 41*
The author describes a new terminal product, Solve/SE, which can upgrade existing POS networks to full EFTPOS.

033142 **'Ramex: a prototype expert system for computer security risk analysis and management'**
M Kailay, P Jarrratt, *IFIP SEC 94 paper F6*
The authors describe an expert system developed to assist with risk management in small to medium sized firms. It uses production rules to work through from assets through threats to countermeasures.

033143 **'A Biologically Inspired Immune System for Computers'**
JO Kephardt, *in Artificial Life IV, MIT Press 1994*
The author discusses the workings of IBM's anti-virus lab. When a scanner spots unauthorised code, which does not correspond to a known virus signature, it sends it to this lab, which tries to 'culture' it by repeatedly invoking a suite of decoy programs. If these become infected, the new virus is analysed to separate code and data. Candidate signatures from the former are then compared with 500MB of innocuous applications software, and those with the lowest false positive rates are released to customers. The goal is to delegate these features from the lab to the fielded antivirus products, thus providing personal computers with full immune systems.

033144 **'Are You Who You Say You Are?'**
B Kett, *International Security Review no 85 (Summer 94) p 19 - 21*
The author describes the use of biometrics in access control, and a new smartcard based voice recognition system in particular.

033145 **'A High-speed Modular Multiplication Method for the RSA Cryptosystem'**
J Kim, H Lee, D Lee, *JW-ISC 93 pp 91 - 98*
This paper describes the architecture and design of a multiplier for a public-key encryption processor which implements the RSA algorithm with key lengths of 512 bits. The algorithm is based on a parallel multiplier, which has been implemented with 71,680 transistors using a 0.8 micron CMOS gate array process.

033146 **'The Postal Service Fails to Deliver the Goods'**
L Kruh, *Cryptologia v XVIII no 3 (July 94) pp 250 - 252*
The photograph of a German Enigma machine in a 1992 US postal service album is mistakenly identified there as a Japanese purple machine.

033147 **'Growing Pains'**
A Lawrence, *Computer Business review v 2 no 6 (June 94) pp 5 - 10*
This article discusses the strains which the Internet is suffering as it starts to accommodate commercial users. Proposals to put cash on the net have come from a number of parties, including Digicash, the IETF and CommerceNet; and various problems with encryption will have to be tackled.

033148 **'Smart moves down under'**
M Lawson, *Cards International no 113 (12/7/94) p IV*
This article reports three smartcard initiatives in Australia - a ticketing system in Melbourne, an electronic purse in Sydney, and a promotional system.

033149 'Encrypting Network Traffic'
M Lomas, *Fast Software Encryption 93 pp 64 - 70*

The author considers the engineering aspects of using software encryption in a LAN. As most network traffic is bursty, a considerable speed improvement can be achieved by using idle cycles to precompute keystream using DES in OFB mode. With Ethernet, performance also depends on packet size to the extent that tuning this can often make up the residual cost of software encryption. Thus, even with DES, well-designed encryption software can often be almost free of performance costs.

033150 'US vendor pushes international clipper chip scheme'
W Madsen, *Computer Fraud and Security Bulletin (June 94) pp 8 - 9*

Hewlett-Packard has proposed an alternative to Clipper which would allow each country to enforce a national crypto control policy, which could range from complete prohibition through key escrow to unrestricted use. France, for example, will require escrow, while Singapore insists that all traffic be decrypted to cleartext at its border.

033151 'High-level language computer viruses - a new threat?'
S Magruder, *Computers and Security v 13 no 3 (May 94) pp 263 - 269*

Companion viruses can be written in high level languages, which would make them hard for scanners to detect and open up the possibility of quite subtle effects. Some experiments with such viruses are reported.

033152 'Beating the counterfeiters'
R Martin, *Cards International no 113 (12/7/94) pp 7 - 9*

This article reviews a Scotland Yard report on organised plastic counterfeiting and presents a lot of fraud figures. A small subset of merchants appears to be responsible for a disproportionate number of bad transactions.

033153 'Paving the way for the Café society'
R Martin, *Cards International no 109 (12/5/94) p III*

This article reports the EC Café project to provide a multicurrency electronic wallet and describes how the devices would work.

033154 'The New Age in Security Communications'
R McCrie, *International Security Review no 84 (Spring 94) pp 45 - 46*

The author describes the options available in the USA for alarm signalling and for communications with static guards. Most of these have no specific security features such as regular interrogation, and only two networks cover the whole country.

033155 'From the archives - Arvid Damm makes an offer'
CG McKay, *Cryptologia v XVIII no 3 (July 94) pp 243 - 249*

The author reproduces two letters of October 1914 in which rotor machine pioneer Arvid Damm offers to license his inventions to the Swedish government, and makes passing reference to a Scottish partner (GL Craig) and to offers in 1913 and 1914 to the British government. He also relates a number of encryption mishaps, and stresses the need for automatic key management as a guard against treason.

033156 'Data Security related to Telework'
M Mergeay, *Securicomm 94 pp 225 - 231*

The author considers the risks involved in teleworking, and in particular the likelihood that the worker's PC will be used by other family members. Forbidding such use is unlikely to work; so he argues instead for the installation of systems to provide access control and secure communications.

033157 'Electronic purse trial goes early'
F Mollett, *Cards International no 114 (10/8/94) p II*

Portugal's banks are launching an electronic purse trial in Cascais during the third quarter of 1994. The cards will operate vending machines and public transport as well as ATMs and POS terminals.

033158 'The Structure and Functioning of the COST Privacy Enhanced Mail (PEM) System'
S Muftic, N Kapidzic, A Davidson, *IFIP SEC 94 paper B4*

COST-PEM is an implementation of a Privacy Enhanced Mail system that follows the appropriate Internet PEM proposals. It consists of an X.509 based certificate system and user functions for dealing with signed or encrypted e-mail. The COST-PEM implementation includes support for smart cards to hold signature keys.

033159 'A Holder Verification Protocol Using Fingerprints'
S Ozaki, T Matsumoto, H Imai, *JW-ISC 93 pp. 1-9*

The authors provide a protocol whereby a personal portable intelligent device with a built-in fingerprint sensor can prove the proper holder's identity to an external verifier without revealing the actual fingerprint.

033160 'An Introduction to Citadel - A Secure Crypto Coprocessor for Workstations'
ER Palmer, *IFIP SEC 94 paper E3*

IBM's Citadel co-processor adds hardware DES encryption and secure non-volatile key storage to existing PS/2 computers. A Mach based microkernel provides an interface between the host machine and the co-processor. The goal is to create a full-custom replacement for this prototype device and install it on other devices such as network interfaces or disc controllers so that the main processor need not be concerned with the encryption and decryption processes.

033161 'Integrity checking for anti-viral purposes - theory and practice'
Y Radai, *IFIP SEC 94 paper I7*

The author discusses the effectiveness of checksumming mechanisms against computer viruses, and in particular whether cryptographic techniques such as MACs and digital signatures give any advantage over simple CRCs. He shows that in many cases they do not; the answer depends on whether we are protecting files in one machine or many. CRCs are adequate for single machines where the checksummer is inaccessible, such as on a boot diskette used at regular intervals. A number of practical points for checksum implementers are also given.

033162 'Les Différentes Formes de Télétravail et les Besoins de Sécurité Associés'
T Raes, H Pinsard, *Securicomm 94 pp 213 - 224 (in French)*

Teleworking introduces a number of new risks. Information makes up an increasing proportion of an enterprise's capital, and simultaneously becomes more dispersed. How can professional and family information be segregated? How can one guard against burglary? How should one deal with information in which there is a public interest, such as classified military information, or the personal data of third parties? Technical solutions exist, but will have to be applied using rigorous risk analysis.

033163 'Money, money, money'
S Rainey, *Security Gazette (Jan 94) pp 14 - 15*

ATM disputes have inspired the development of a number of monitoring systems. Some of these capture, compress and store a picture of the cardholder, but in the USA only film or video evidence has so far been accepted by the courts.

033164 'Intag's smartcard set to incorporate biometrics'
F Rees, *Financial Technology Insight (Aug 94) p 5*

This announces a contactless smartcard from Australia which can operate at a distance of up to 15cm and incorporate biometrics.

033165 'Europe's central bankers tighten electronic purse strings'
M Rowe, *Financial Technology Insight (Aug 94) pp 6 - 7*

The council of the newly formed European Monetary Institute considers that money in an electronic purse is a bank deposit for monetary policy purposes, and that these devices should therefore be subject to central bank oversight.

033166 'Market diversity points way forward'
I Ryan, *Cards International no 111 (13/6/94) p III*

French manufacturer Solais shipped 53m microprocessor cards in 1993 and estimates total world sales of all manufacturers at 250 - 280 million. This should grow to 600m by 1997, with applications including health cards, phonecards and electronic purses. Some markets will shrink as products consolidate, as with France Telecom's decision to let customers use their bank cards in public telephones.

033167 'Microchip halves French card fraud'
I Ryan, *Cards International no 109 (12/5/94) p II*

Bank card fraud was halves to 0.04% of turnover in 1993, and this drop is attributed to the fact that 75% of transactions now involve validating a PIN.

033168 'Signal Detection Games with Power Constraints'
DW Saunder, E Geraniotis, *IEEE Transactions on Information Theory v 40 no 3 (May 94) pp 795 - 807*

The authors formulate and solve optimisation problems for jamming situations where the jammer has constraints on signal amplitude, time-averaged power or expected power. These are derived by applying Bayesian techniques to the game between the jammer and the receiver, and supported by simulation results.

033169 'An open architecture for security functions in workstations'
S Santesson, *IFIP SEC 94 paper E4*

This paper describes the Swedish Allterminal project, whose goal is to secure networked PCs for use in civil government. The system uses smartcards for key management, and provides a standard API for PC protection, authentication, encryption and integrity functions. A number of layers and interfaces have been developed and are described in some detail.

033170 'Passerelles Internet Sécurisées'
H Schauer, *Securicomm 94 pp 181 - 210 (in French)*

The author discusses the principles of IP filtering, and gives a review of a number of products which are designed (or can be adapted) to provide a secure Internet gateway or firewall. He also mentions some alternative solutions such as password generators.

033171 'CardTech/SecureTech 94'
Smart Card News v 3 no 5 (May 94) pp 86 - 89

This article describes a number of projects reported at a US smartcard conference. The military want to give their troops cards to control pay, medical treatment and casualty evacuation, while civilian projects include cutting welfare fraud.

033172 'German Motorway Toll Trial is GSM-based'
Smart Card News v 3 no 3 (Mar 94) pp 41 - 44

A system called SAGEM will enable motorway tolls to be collected from GSM SIM cards and will be tested on the motorway from Cologne to Bonn.

033173 'A Study on the Development of Real-time Intrusion Detection Expert System (IDES)'
DH Song, YJ Ko, JT Shin, MS Jun, CH Lee, *JW-ISC 93 pp 215 - 225*

IDES detects intrusions by comparing users' historical behaviour patterns with their current behaviour; deviations may indicate any one of a number of possible intrusions and violations of security policy.

033174 'Pass-sentence - a new approach to computer code'
Y Spector, J Ginzburg, *Computers and Security v 13 no 2 (Apr 94) pp 145 - 160*

The authors report a prototype access control system which replaces passwords with sentences, and can allow partial access if the sentence is partially right.

033175 'Securenet: a network-oriented intelligent intrusion prevention and detection system'
P Sprirakis, S Katsikas, D Gritzalis, F Allegre, D Androutsopoulos, J Darzentas, C Gigante, D Karagiannis, H Putkonen, T Spyrou, *IFIP SEC 94 paper E2*

This paper describes SECURENET, an intrusion detection system being built as an EC RACE project to protect integrated broadband communications. It uses a number of technologies, such as neural networks and secure distributed computation, to detect and classify attacks in real time.

033176 'Pretty Good Privacy'
W Stallings, *Byte v 19 no 7 (July 1994) pp 193 - 196*

The author explores the authentication, confidentiality and email compatibility features of Pretty Good Privacy.

033177 'The Need for Decentralisation and Privacy in Mobile Communication Networks'
F Stoll, *IFIP SEC 94 paper C2*

Existing mobile telephones and other communication services follow design concepts developed when communication networks were controlled by a few organisations in each country. The author suggests that a new approach be taken in that we dissociate billing information from identity to improve privacy. In general, many assumptions about networks are historical rather than necessary.

033178 'SAFARI - An Advanced C3I Approach to Crisis Management'
P Suslenschi, E Bourdin, *Electrical Communication Q2 94 pp 148 - 152*

The authors describe a C3I system designed for the French rapid reaction forces to support operations such as those in Somalia. The information provided includes maps, forces location and intelligence; the architecture is fully object oriented.

033179 'Smartcards - A Security Assessment'
J Svigals, *Computers and Security v 13 no 2 (Apr 94) pp 107 - 114*

The author discusses some security features of smartcards and notes the success of attacks on TV scrambling systems.

033180 'Biometrics ready to combat fraud'
The Banker (July 94) pp 38 - 39

This article recounts some recent developments in biometrics, and predicts that they will be fielded once smartcards can manage user templates offline.

033181 'Security in EDI between bank and its client'
P Vahtera, H Salmi, *IFIP SEC 94 paper H2*

The authors describe a Finnish financial EDI system which has been making bank payments without vouchers since 1992. A number of controls are discussed; message authentication codes are about to be introduced.

033182 'SMART: Structured Multidimensional Approach to Risk Taking for Operational Information Systems'
AM van der Veen, DP de Jong, JF Bautz, N Yousef Yengej, AMJ van Kempen, PPA van Dam, *IFIP SEC 94 paper F8*

The authors survey and criticise existing risk management models, and then present a new system aimed at the oil, chemical and construction industries.

022183 'New Products To Shore Up The Net'
M Wayner, *Open Systems Today no 156 (August 15 1994) p 8*

One company introduced a product which supports encryption of credit card numbers over the World Wide Web using Pretty Good Privacy (PGP); another is offering consulting services and equipment for Internet firewalls.

033184 'Electronic Eavesdropping: Are Defenses Adequate?'
G Whidden, *Journal of Security Administration v 16 no 2 (Dec 93) pp 11 - 16*

Eavesdropping systems can be made harder to detect in a number of ways, including turning the bug on and off by remote control, reducing the radiated power, and using store-and-forward. The latest technology to be introduced is spread-spectrum radio.

033185 'Identifying Faces Using Multiple Retrievals'
JK Wu, AD Narasimhalu, *IEEE Multimedia v 1 no 2 (Summer 94) pp 27 - 38*

The authors report a mugshot identification database developed in Singapore to assist police work. Classification is based on 17 features to which users assign weights; these assignments are normalised against standard faces. Faces can be composed from features and used to key a search; records are stored in an iconic index tree; and the prototype system works with several hundred faces. Work is afoot on automatic ageing, but this is turning out to be hard.

033186 'IT Security in a Large Distributed Trading System'
M Zickwolff, *Securicomm 94 pp 309 - 318*

The author describes the information security architecture at the Deutsche Terminenbörse (the German financial futures exchange), which is claimed to be the world's highest volume automated trading system. It is largely implemented on VAX/VMS systems, with a number of local communication servers front-ending two hosts which perform the clearing function; the communication servers act as firewalls and are permanently monitored.

2 Operating System and Database Security

033201 'One-Representative Safety Analysis in the Non-Monotonic Transform Model'
PE Ammann, RS Sandhu, *Franconia 94 pp 138 - 149*

The authors analyse the safety question for the Sandhu-Suri formal access control model called Non-Monotonic Transform, and identify a class of schemes for which safety is computationally tractable.

033202 'Degree of isolation, concurrency control protocols, and commit protocols'
V Atluri, E Bertino, S Jajodia, *Database Security 94*

This paper deals with the problem of transaction management in multilevel secure distributed databases. A secure locking protocol that provides different degrees of isolation and a secure early prepare commit protocol are presented, and the authors illustrate how the two protocols can be integrated without violating security. The costs of the proposed commit protocol are determined in terms of the number of messages exchanged for different degrees of isolation.

033203 'Extensible Access Control for a Hierarchy of Servers'
J Bacon, R Hayton, SL Lo, K Moody, *Operating Systems Review v 28 no 3 (July 94) pp 16 - 23*

The authors describe the access control system implemented in MSSA whose goal is to control access via value adding clients or network servers to distributed file servers. Access control lists are used to express policy, and are checked once for each set of accesses; thereafter a transient identity-based capability is generated which allows efficient runtime access with delegation as required.

033204 'A new authorization model for object-oriented databases'
E Bertino, F Origgi, P Samarati, *Database Security 94*

The paper presents an authorisation model for object-oriented database systems which supports both positive/negative and strong/weak authorisation. Starting from authorisations specified by the users, new authorisations are derived by the system using rules. The model is an evolution of the ORION authorisation model, but differs from it in many respects; in particular, the semantics of subject groups and of negative authorisations on sets of objects are different. These differences result in different derivation rules.

033205 'La Sécurité en environment client/serveur (authentification des documents dans le travail en groupe)'
A Bestougeff, *Securicomm 94 pp 273 - 283 (in French)*

The author reports a prototype secure groupware system. Any member of a group may fetch a document over the network and make it locally available, provided she signs it; further endorsements tell whether a document is shared by a number of group members, and its level of validation. This provides a lightweight but robust scheme for enforcing responsibility and reducing the administrative costs of access control.

033206 'A State-Based Approach to Noninterference'
WR Bevier, WD Young, *Franconia 94 pp 11 - 21*

The authors discuss an approach to using state machines to look at non-interference type problems.

033207 'Security in Open and Distributed Systems'
WJ Caelli, *Information Management and Computer Security v 2 no 1 (94) pp 18 - 24*

The author describes how interprocess protection mechanisms developed historically from Multics through VAX 11/780 to the Intel and Alpha processors. He goes on to describe OSF DCE security services and the Mach and TMach kernels.

033208 'Providing consistent views in a polyinstantiated database'
L Cholvy, F Cuppens, *Database Security 94*

This paper discusses the problem of polyinstantiation, on the assumption that this is always used to provide cover stories. The author presents an approach to eliminate, in the view at a given level, lower level information which represent a cover story for information visible at that level; this assumes that information at higher levels is more reliable that information at lower levels. In presence of a partial order, where information at incomparable levels may exist, the partial order is reduced to a total order by specifying some preference relationship among incomparable levels.

033209 'The SINTRA data model: structure and operations'
O Costich, MH Kang, JN Froscher, *Database Security 94*

The paper presents the SINTRA multilevel relational database. Each attribute value in a relation is given a security level, as is each tuple; the tuple's level represents the level at which it originated, and may be greater than the least upper bound of the level of its attributes. Constraints on the classification of elements in a relation are presented. Finally, the execution of insert, update, and delete operations on multilevel relations is illustrated.

033210 'Confidentiality in a Replicated Architecture Trusted Database System: A Formal Model'
O Costich, J McLean, J McDermott, *Franconia 94 pp 60 - 65*

SINTRA is an MLS secure database project at the US Naval Research Laboratory. Its key idea is that data on a low level back end database is replicated on the higher back end databases. This paper puts that idea, along with BLP, into a formal model.

033211 'Current trends in database technology and their impact on security concepts'
KR Dittrich, *Database Security 94*

The paper discusses the emerging technologies in the area of database systems, such as object-oriented, active, and federated DBMSs, and their likely impact on security. Finally, security design issues are explored, with particular reference to design methodologies and tools for helping security administrators to formulate security requirements and for mapping these requirements to control mechanisms.

033212 'A High Assurance Window System Prototype'
J Epstein, H Orman, J McHugh, R Pascale, M Branstad, A Marmor-Squires, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 159 -190*

This paper describes the security policy, architecture, and operation of Trusted X (TX), a prototype multilevel secure windowing system based on the X Window System. TX is an application, not a complete system, and uses the TMach 2.5 prototype as an operating system platform. Although TX does not satisfy all of the TCSEC's certification requirements for B3, the architecture was designed to satisfy the B3 structuring and minimization criteria.

033213 'User group structures in object-oriented database authorizations'
EB Fernandez, J Wu, MH Fernandez, *Database Security 94*

This paper presents an approach to structuring user groups. Groups can be defined on other groups by means of generalisation, composition, and relation structures. Generalisation allows one to define a group as a subgroup (specialisation) of another group. Composition allows one to partition a group into different subgroups. Relation allows one to gather together groups necessary to perform some tasks. Authorisations specified for a group are passed to its subgroups in the generalisation and composition structure and to groups defined on it in the relation structure. An algorithm for access control in this scenario is presented.

033214 'A Taxonomy of Trace-based Security Properties for CCS'
R Focardi, R Gorrieri, *Franconia 94 pp 126 - 136*

The authors look at noninterference-like properties by using CCS. This is done to incorporate both nondeterminism and asynchronous behaviour. They contrast their work with some of the other work in the field.

033215 'Reasoning About Confidentiality Requirements'
SN Foley, *Franconia 94*

Reflexive flow policies are used to analyze multilevel confidentiality requirements. In particular, multilevel relational databases are considered.

033216 'On Inter-Realm Authentication in Large Distributed Systems'
V Gligor, SW Luan, J Pato, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 137 - 157*

This paper propounds a policy for propagating authentication trust across realm boundaries; it is analogous to the procedures for identity and signature authentication in national and international law. The design helps limit the global exposures that may result from a realm authentication server being penetrated, it can either operate transparently with respect to inter-realm path selection and acceptance, or allow clients to choose paths from a set offered by a server. As an example, the paper presents a simple protocol that selects inter-realm authentication paths.

033217 'Making UNIX Systems Meet Existing Corporate Security Standards'
P Goldis, *Singapore 94*
The paper discusses the limitations of UNIX systems when measured against typical corporate mainframe standards, and distinguished between the perception and reality of UNIX systems.

033218 'A Naming and Trading Facility for a Distributed System'
A Goscinski, A Haddock, *Australian Computer Journal v 26 no 2 (May 1994) pp 50 - 65*

The authors describe the object management facilities of the RHODOS operating system. Objects are sharable, and can be imported from one domain to another; the mechanisms for this are described. As users want to preserve autonomy for security reasons, dynamic binding is needed and this is provided by a name server cum resource manager, which is called a trader and can be distributed in various ways.

033219 'Creating abstract dictionary modification policies with reconfigurable data objects'
T Gross, *Database Security 94*

This paper proposes a data abstraction, called reconfigurable data objects, for specifying authorizations. These objects are defined by functions whose body is an SQL query, similarly to views; each function has parameters which appear in the WHERE clause of the SQL query, and for each possible value of the function parameters, the reconfigurable object takes the value returned by the function. Authorizations are specified for users to access reconfigurable objects, and in particular write authorizations are considered. The problem of mapping changes made on reconfigurable data objects to the data in the underlying tables is discussed.

033220 'Oriented Scenario Dynamics in Information Systems Safety'
D Guinier, *ACM SIGSAC v 12 no 3 (July 94) pp 6 - 11*

The author presents a risk-driven model of safety dynamics which proposes certain relations between safety and security.

033221 'A practical formalism for imprecise inference control'
J Hale, J Threet, S Shenoi, *Database Security 94*

This paper proposes a formal approach for modeling and controlling imprecise inference in relational database systems. Imprecise refers to the situations where users restrict their uncertainty about possible values for an attribute without knowing the exact real value. To model this, the database, together with some additional relations representing imprecise a priori knowledge, is transformed into an imprecise database. Possible ways to secure systems from imprecise inference attacks are discussed.

033222 'Anonymous and Verifiable Databases: Towards a Practical Solution'
T Hardjono, YL Zheng, J Seberry, *IFIP SEC 94 paper B9*

The authors consider the misuse of information in databases, and suggest that users should have different pseudonyms in different databases so that it is harder to associate data from different sources. Given suitable authority, such as court order, somebody would be allowed to perform this association.

033223 'Program Structure for Secure Information Flow'
JS He, *IFIP SEC 94 paper E1*

Structuring a program correctly can simplify information flow analysis with respect to the lattice model, and indeed all secure programs have a form which requires only a trivial flow analysis. However, translating an arbitrary secure program into this form is an NP-complete problem. On a practical level, flow analysis can be simplified by taking program structure into account.

033224 'Sécurité des réseaux locaux Ethernet'
P Herbrard, *Securicomm 94 pp 251 - 260 (in French)*

The author gives an overview of the threats to Ethernet systems, including poor configuration, active and passive tapping and RFI. He reviews the various types of security product available and mentions some of the applicable security standards.

033225 'Providing a More Complete Security in Heterogeneous Environments'
NB Idris, WA Gray, RF Churchhouse, *Securicomm 94 pp 261 - 271*

The authors present a scheme for realising multilevel security in heterogeneous networks of servers. This is based on a common intermediate schema representation, with Shamir's secret sharing scheme as the underlying control mechanism. In order to overcome the blocks caused by local/global conflicts, there is provision for users to be assigned higher clearances on a temporary basis. A pilot implementation is reported.

033226 'Security Protection for Parts of a Data Structure'
P Kaijser, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 476 - 482*

This paper looks at protecting parts of a data structure such as a document. The author describes what protection can be achieved and what properties a data structure must possess for protection to be possible.

033227 'A Secure Two-Phase Locking Protocol for Multilevel-Secure Databases: S2PL'
AK Kang, AC Moon, *Technical report, Korea Advanced Institute of Science and Technology*

Conventional locking protocols introduce covert channels if used in MLS databases, and the authors therefore propose a system in which locks are queued by a trusted scheduler. Deadlocks are resolved securely by examining a waits-for graph.

033228 'A Method of Dynamic Discretionary Access Control'
HS Kang, T Matsumoto, H Imai, *JW-ISC 93 pp 207 - 214*

This paper proposes a dynamic discretionary access control mechanism providing both high confidentiality and high efficiency. To manage information flows the mechanism uses dynamic restrictions on group access permissions.

033229 'Reconciling Objects and Multilevel Security'
TF Keefe, *OOPSLA 93 p 308*

The author provides an overview of SODA, a multilevel object security model. This provides an abstraction of what objects are modifiable by a subject, and has a reference monitor which mediates method invocations. However, atomicity and security cannot both be ensured when a transaction fails.

033230 'A Security Model for Store and Forward Message Handling System'
SW Kim, DK Kim, *JW-ISC 93 pp 169 - 176*

The authors present a security model for message processing and message transfer. The message agent is designed to prevent unauthorized access, unauthorized information flow between messages, and unintended message transfer.

033231 'Security Constraints on Inheritance Hierarchy in Object-oriented Data Model'
Y Kim, B Noh, *JW-ISC 93 pp 235 - 244*

This paper develops security properties which conform to the semantics of an inheritance hierarchy, and then defines a variety of security constraints in accordance with this hierarchy.

033232 'A Decentralised Approach for Authorization'
B Lau, W Gerhardt, *IFIP SEC 94 paper B7*

The author proposes an access control system that broadly follows the hierarchical structure of the organisation that it serves but provides facilities for overriding the structure in certain circumstances. Allowing both permission and prohibition can lead to conflicts; these are resolved by a predetermined ordering.

033233 'Security in a Client Server Environment'
LG Lawrance, *Network Security (July 94) pp 5 - 15*

The author provides an introduction to client server architectures and describes a number of the risk points. He discusses the ISO-OSI security standards, OSF/DCE and Kerberos, and some of the certification issues.

033234 'SAMSON: Management of Security in Open Systems'
S Lechner, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 538 - 543*

This paper describes the EC's research project SAMSON, which aims to unify security management for network administrators.

033235 'Generic Interface to Security Services'
J Linn, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 483 - 491*
This paper describes the features of a Generic Security Service Application Program Interface (GSS-API), examines its underlying assumptions, and evaluates lessons learnt during its evolution. The GSS-API is designed to support architects of distributed protocols by providing them with a toolkit for integration of security features into those protocols.

033236 'Auditing for Database Integrity'
D Little, S Misra, *Journal of Systems Management (Aug 94) pp 6 - 11*
Integrity is the hardest of attributes to audit, but is still important: a recent MIT survey showed that over half of all chief information officers felt that data inaccuracy was a limiting factor, yet only 56% had systems in place to detect errors. A number of practical testing strategies are discussed.

033237 'Security Considerations of Content and Context Based Access Controls'
DG Marks, LJ Binns, PJ Sell, JR Campbell, *IFIP SEC 94 paper E8*
It is often desirable to base access control on the context of an access request as well as on the content of the requested record; this enables dynamic reclassification as circumstances change, based on a small set of rules. However, it can give rise to substantial problems if users are allowed to write as well as read data.

033238 'Hypersemantic data modeling for inference analysis'
DG Marks, LJ Binns, BM Thuraisingham, *Database Security 94*
The paper proposes a model, called the Multilevel Knowledge Data Model (MKDM) for the specification of security constraints of multilevel database applications. A language for the specification of security constraints is presented together with a graphical representation scheme for their visualization. A discussion of some inference problems and their resolution in the proposed model is presented.

033239 'The b2/c3 problem: how big buffers overcome covert channel cynicism in trusted database systems'
J McDermott, *Database Security 94*
The paper proposes an approach to supporting write-up operations in multilevel databases, in order to maintain mutual consistency between low level information and its higher level replicas. The proposed write-up service depends upon trusted software, which provides a set of write-up ports to the low processes (the writers) and a set of receive ports to the high processes (the readers); it maintains a stable storage buffer to store the messages. The problems of buffer management and of recoverability from failures are discussed.

033240 'A Resource Allocation Model for Denial of Service Protection'
J Millen, *Journal of Computer Security, v 2 , no 2 - 3 (1993) pp 89 - 106*
The author introduces the concept of a denial-of-service protection base, which is similar to a reference monitor, but whose function is to guarantee, rather than deny, access. It is made up of a resource monitor, a waiting time policy, and a user agreement; it ensures that each benign process will make progress in accordance with the waiting time policy, and that no non-CPU resource is revoked from a benign process until its time requirement is zero. He presents a formal model of a resource monitor, and gives an example of one that enforces a maximum waiting time policy.

033241 'Unwinding Forward Correctability'
JK Millen, *Franconia 94 pp 2 - 10*
The author shows that any event system can be represented by a state machine.

From this the concept of forward correctability is put into a state machine formulation and unwinding theorems are discussed.

033242 'Security Architecture for ODP Systems'
S Muftic, *Journal of Computer Networks and ISDN Systems v 26 no 11 (Aug 1994) pp 1343 - 1349*
This paper contains the description of the final results of the COST-11 "Security" project, which are mainly the concept, evaluation, and prototype implementations of the Comprehensive Integrated Security Systems (CISS).

033243 'Security Architecture for Distributed Systems'
S Muftic, M Sloman, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 492 - 500*
This paper describes a security architecture for open distributed systems, which may be used by applications which support a variety of security policies.

033244 'Security Planning in Data Processing System'
H Nagase, H Shina, G. Edmundo, *JW-ISC 93 pp 226 - 234*
This paper proposes a specification language for confidentiality, integrity, and availability requirements, using an entity/relationship model. Using this language, it is possible to evaluate the secrecy and integrity of computer systems.

033245 'Access right administration in role-based security systems'
M Nyanchama, S Osborn, *Database Security 94*
This paper proposes an authorization model based on rôles, which represent sets of authorizations to access objects. Users may impersonate rôles, and rôles may access objects; rôles are organized into a lattice, where higher rôles correspond to greater privilege and a rôle inherits the authorization of all rôles below it in the lattice. Constraints are added to ensure the absence of redundant authorizations (a rôle should not be given authorizations which already exist below it in the lattice) and arcs (a rôle should not be both directly and indirectly connected to any other rôle). Operations for adding, removing, and partitioning rôles are defined.

033246 'Trusted RUBIX: a multilevel secure client-server DBMS'
JP O'Connor, *Database Security 94*
The paper presents the design and implementation of a multilevel secure client-server architecture intended to evaluate at B2. The author reports on the migration of the existing standalone version of the Trusted RUBIX DBMS to a client-server architecture. The design issues that arise in developing a multilevel secure client-server DBMS architecture to satisfy high assurance levels are discussed. The design of client-server extensions to Trusted RUBIX in terms of its module structure, internal layering, and its process structure are presented. Finally, the relationships between critical client-server DBMS design choices and assurance issues are discussed.

033247 'A multilevel secure federated database'
MS Olivier, *Database Security 94*
This paper presents a model for a multilevel secure federated database. The assumptions are that participating sites are homogeneous and use the same data model and classification lattice; that each site is autonomous in that it defines the security classification of objects residing there; that each site can define the sites with which it is willing to share information; and that information in objects stored at a given site can be transmitted only to sites trusted by it. When information is transmitted to another site, the access restrictions at the original sites are propagated. The problems of object relocation and replication are also discussed.

033248 'Towards Secure Open Systems'
PL Overbeek, *IFIP SEC 94 paper C3*
The author summarises the work described in his book (reviewed in v 3 no 1 p 41).

033249 'Security guidelines for database system development'
G Pangalos, *Database Security 94*
This paper presents developers of secure database systems with a set of guidelines which may help to ensure the satisfaction of predefined security principles, as defined in the high level security policy. The proposed guidelines are classified into three main categories: database development guidelines, control of database software guidelines, and database operational and organizational guidelines.

033250 'Formal Specification of Information Flow Security Policies and Their Enforcement in Security Critical Systems'
RV Peri, WA Wulf, *Franconia 94 pp 118 - 125*
The authors give a trace based specification for a security critical system by placing restrictions on the functional behaviour of entities.

033251 'Evaluation of Policies, State-of-the-Art, and Future Research Directions in Database Security'
G Pernul, AM Tjoa, *IFIP SEC 94 paper E9*
The authors provide an overview of database security and discuss their Adapted Mandatory Access Control (AMAC) model.

033252 'A fine grained access control model for object-oriented DBMS'
A Rosenthal, J Williams, W Herndon, B Thuraisingham, *Database Security 94*
This paper presents a multilevel security model for object-oriented databases that supports element level classification but does not allow polyinstantiation; this is prevented by not allowing low users to assign values to an attribute if the attribute already has a value at a higher level. Thus, users may be informed of the existence of high level information, which they can neither see nor modify. The model includes operations to change an element's security level.

033253 'Security for OODBMS'
R Sandhu, *OOPSLA 93 p 307*
Object-oriented techniques can be helpful in solving a number of data security problems, especially those concerning integrity. Their implications for availability and for protecting intellectual property are likely topics for future research.

033254 'Object Oriented Approach to MLS Database Application Design'
PJ Sell, *OOPSLA 93 p 306*
The complex task of designing a multilevel database application can be simplified using object modeling techniques, and the NSA has developed a multilevel object modeling technique (MOMT) for this purpose.

033255 'Tightly Secure Transaction Scheduler in Multi-Level Secure Database Management Systems: TS^2'
YL Sohn, SC Moon, *Technical report, Korea Advanced Institute of Science and Technology*
Existing covert channel elimination techniques can cause significant performance deterioration; the authors propose instead a transaction scheduler based on concealing uncommitted data. Multiple versions of data are available to higher level users, who are guaranteed to be able to see the newest data. Conditions for the multiversion data to be one-copy serialisable are derived.

033256 'Formal Semantics of Rights and Confidentiality in Definite Deductive Databases'
A Spalka, *Franconia 94 pp 47 - 58*

This paper is a partial summary of a University of Bonn technical report. The author gives four formal definitions of confidentiality that attempt to capture real-life informal answers. A helpful review of similar literature is included.

033257 'Secure logic databases allowed to reveal indefinite information on secrets'
A Spalka, *Database Security 94*

This paper presents an approach for the protection of information in databases. Four definitions of confidentiality are proposed: at the highest level, the existence of information not visible to a user is hidden from that user, while at the lowest level the user is informed about the existence of information he cannot see, although it is not disclosed to him. The enforcement of integrity constraints in the application of the lowest form of confidentiality is discussed.

033258 'Redrawing the Security Perimeter of a Trusted System'
DF Sterne, GS Benson, H Tajalli, *Franconia 94 pp 162 - 174*

This paper was the introduction for a panel discussion on reconsidering the rôle of the reference monitor. It discusses the idea of including a controlled application set (CAS) with the trusted computing base.

033259 'On the Security Model Based on Lattice-Ordered Groups'
M Tetsuya, T Shigeo, *JW-ISC 93 pp 235 - 252*

The authors present a new security model based on lattice-ordered groups to solve a problem with the Bell and LaPadula security model. The problem is that the *-property can stop users transmitting information from lower to higher levels.

033260 'A Kernelized Architecture for Multilevel Secure Object-Oriented Databases Supporting Write-Up'
R Thomas, R Sandhu, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 231 - 275*

The object-oriented model for database management systems is attractive for a number of reasons. It is argued that it offers a good match between real-world objects and their system counterparts, making labelling policies easier to understand and implement. Write-up operations are a challenge, however, in a distributed system where integrity must be supported without creating covert channels.

033261 'Conceptual Foundation for a Model of Task-based Authorizations'
RK Thomas, RS Sandhu, *Franconia 94 pp 66 - 79*

The authors take a pre-formal methods approach to analyzing the integrity aspects of a paperless business enterprise. They lay the foundations for a task-based authorization model.

033262 'Integrating Object-oriented Technology and Security Technology: A Panel Discussion'
B Thuraisingham, *OOPSLA 93 p 304*

In this position paper, the author provides a brief survey of research into multilevel secure object-oriented systems, and the opportunities for using object-oriented modeling techniques to analyse more conventional security systems.

033263 'Modeling Security Requirements for Applications'
TC Ting, *OOPSLA 93 p 305*

Confidentiality properties are complex to specify in real applications, as there may be both organisational and personal privacy aspects. Developing a conventional discretionary access control policy into an application with proper logging and strict 'need-to-know' is nontrivial. Object-oriented techniques can help to elucidate application security semantics.

033264 'The integration of security and integrity constraints in MOKUM'
RP van de Riet, J Beukering, *Database Security 94*

The paper presents an approach to enforcing integrity and security constraints in an active object-oriented knowledge-base system. Integrity constraints can be static (properties which must always hold) or dynamic (properties which regulate the changes to objects). Security constraints allow us to restrict the execution of operations on objects to specific users. Constraints are expressed by Prolog predicates in the form of scripts associated with the objects which enforce integrity and security checks.

033265 'MOSS II: A Model for Open System Security'
PWJ van Zyl, MS Olivier, SH von Solms, *IFIP SEC 94 paper H6*

The authors present a security model for open systems which is based on access paths, security agents and security profiles. It elaborates Boshoff's path context model.

033266 'Multidomain Security'
J Vázquez-Gómez, *Computers and Security v 13 no 2 (Apr 94) pp 161 - 184*

The author describes the various approaches to multidomain security, including ECMA-138, Hosmer's multipolicy model, LaPadula's unified access control, Glasgow's security logic, MsLean's security algebra, McCullough's restrictiveness and Sutherland's deducibility. The interactions which these tools can control are tabulated.

033267 'Field level classification and SQL'
S Wiseman, *Database Security 94*

The paper presents the query language of SWORD, a multilevel relational database which supports element level classification. Polyinstantiation is avoided by making visible to users the existence of values even when the values themselves are hidden. The query language of SWORD, called SSQL (Secure SQL) extends SQL with the ability to use row labels in query expressions, and provides for classification of both rows retrieved by queries as well as their fields. The evaluation of expressions involving values which the subject executing the query is not cleared to see is discussed.

033268 'Authorization in Distributed Systems: A Formal Approach'
T Woo, S Lam, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 107 - 136*

This paper presents a formal language with a precise semantics for specifying access control policies independently of their implementations. The generality of the language, which allows it to capture a wide variety of authorization policies, stems from its ability to capture three structural properties inherent in an authorization policy: closure properties, default properties, and inheritance properties. The authors show that the specifications within the language can be translated into extended logic programs to assist in policy evaluation.

3 Security Management and Policy

033301 'Corporate computer crime management: a research perspective'
J Backhouse, G Dhillon, *IFIP SEC 94 paper H8*

The authors discuss the criminological aspects of computer abuse; corporate culture is very important, and nearly 40% of firms report no problems at all. Better management is the key to crime prevention.

033302 'Special care needed for the heart of medical information systems'
AR Bakker, *Database Security 94*

The paper discusses the security requirements of medical information systems, and in particular their audit requirements. Audit plays a special role where the actions of hospital employees may need to be analyzed to determine whether they have acted in a responsible way. Possible access control policies are discussed and a categorization of data generally stored in a medical information systems is provided.

033303 'Méthodes propriétaires: avantages et inconvénients'
V Balouet, *Securicomm 94 pp 121 - 133 (in French)*

The author compares and contrasts five risk management techniques - MARION, MELISSA, CRAMM, MEHARI and MEDESSI. Some of these are driven by causes, others by consequences, and yet others by both; they can be made more viable by special purpose analysis tools. These methodologies can mostly be adapted to distributed systems and incorporate different levels of aversion to particular risks.

033304 'Infohighway Security Viewpoints'
DS Bernstein, *INFO Security News v 5 no 4 (July 94) pp 17 - 19*

This article presents interviews with various people regarding the future security of the proposed US National Information Infrastructure (NII).

033305 'Voice Encryption for the Masses'
DS Bernstein, *INFO Security News v 5 no 4 (July 94) pp 23 - 24*

In this article the author presents a brief survey of commercially available voice encryption hardware.

033306 'The Future Information System'
CW Blatchford, *Computer Fraud and Security Bulletin (Aug 94) pp 9 - 13*

The author discusses the convergence between the methodologies used for quality assurance and security product evaluation.

033307 'A Comparison of International Information Security Standards Based on Documentary Micro-Analysis'
WJ Caelli, JM Carroll, *IFIP SEC 94 paper A8*

Several security standards - TCSEC, ITSEC, USFC, CTCPEC, and AS 3563.1 - were analysed to find those features they have in common and ways in which they differ. This analysis could be useful to people who have a choice between these standards.

033308 'Cryptography Policy Needs Another Look'
LJ Camp, *IEEE Spectrum (June 1994) pp 15 - 16*

The U.S. Government's proposed Clipper encryption standard is technologically suspect, relying on security through obscurity. The government controlled key escrow system adds additional risks and is not as flexible as alternative key escrow schemes developed in the private sector. Finally, U.S. export controls on products including cryptography are limiting the ability of U.S. businesses to compete in the international market, especially with DES-based products.

033309 'Risk Analysis in Distributed Systems'

R Clark, *Securicomm 94 pp 113 - 120*

The author describes the risk assessment technology used by BUPA. This involves the analysis of questionnaires sent to users. Users were more concerned about losing file servers than mainframe services, and the latter are indeed better protected.

033310 'Toll fraud on French PBX systems'

JB Condat, *Computer Law and Security Report v 10 no 2 (Mar/April 94) pp 89 - 91*

Toll fraud against PBXs cost French corporations $220m last year; hackers find their access codes and then sell long distance calls to the public.

033311 'Preventing fraud'

T Corbitt, *Security Gazette (Mar 94) pp 17 - 18*

Computer fraud is not limited to attacks on payment systems; it has included adding ghost employees to the payroll, passing invoices from accomplices and falsifying stock records.

033312 'Security in Electronic Messaging Systems'

DM D'Angelo, B McNair, JE Wilkes, *AT&T Technical Journal v 73 no 3 (May/June 94) pp 7 - 13*

The authors provide an overview of encryption techniques and discuss their application to messaging systems. Security functionality and design assurance are particularly important.

033313 'Security Evaluation Criteria - Position Paper'

J den Engelsman, M de Graaf, P Overbeek, H Schoone, L Strous, *IFIP SEC 94 paper C4*

This paper summarises the views of the Dutch Computer Society Special Interest Group on Information Security on Security Evaluation Criteria.

033314 'A methodology for the design of security plans'

F de Koning, *IFIP SEC 94 paper F9*

The author describes a security planning methodology developed for local governments in the Netherlands. This tackles privacy issues as well as the protection of blank passports and other 'assets'.

033315 'The US Key Escrow Encryption Technology'

DE Denning, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 453 - 457*

This paper discusses the SKIPJACK algorithm, the escrowed encryption chip, how this chip is used, law enforcement access, and an enhanced chip that includes algorithms for computing digital signatures and negotiating session keys.

033316 'Computer Access Control: What is Hacking?'

P Dunsterville, *Security Gazette (mar 94) pp 14 - 15*

Hackers' motivations vary widely, from curiosity through theft to revenge. Silent alarms are very important in combatting them, and good audit trails are needed too.

033317 'A Cost Model for Managing Information Security Hazards'

L Ekenberg, S Oberoi, I Orci, *IFIP SEC 94 paper F2*

The authors describe the risk management procedures used by Telia (formerly Swedish Telecom) and outline the kind of loss which concern them.

033318 'Is lack of quality software a password to information security problems?'
PFJ Fillery, AN Chandler, *IFIP SEC 94 paper C8*

The authors report empirical research on 50 institutions which concludes that the incidence of security problems is in inverse proportion to the level of quality assurance in place. The data are analysed by the cause of the incident and correlated with specific quality safeguards.

033319 'The Importance of a Network Disaster Recovery Plan'
KJ Fitzgerald, *Information Management and Computer Security v 22 no 1 (94) pp 41 - 43*

The author reviews the desiderata of disaster recovery plans for networks.

033320 'The Risk-based Information System Design Paradigm'
S Fletcher, *IFIP SEC 94 paper C7*

The author discusses the desiderata of a risk management system: it should be comprehensive, specific, tractable and assist with design decisions.

033321 'Information Compilation and Disbursement: Moral, Legal and Ethical Considerations'
KA Forcht, DS Thomas, *Information Management and Computer Security v 2 no 2 (94) pp 23 - 28*

The authors describe a number of the common data protection abuses in the USA.

033322 'Executive Liability for Computer Crime and How to Prevent It'
JM Geary, *Information Management and Computer Security v 2 no 2 (94) pp 29 - 31*

In the USA, executives can be held personally liable for fraud against their company, but this can be mitigated by a 'good faith effort' which should include security policies, awareness programmes, disciplinary standards, auditing systems and prompt reporting of incidents to law enforcement.

033323 'Evaluation de la Période d'Essai des ITSEC'
S Geyres, *Securicomm 94 pp 67 - 78 (in French)*

The author describes the results of surveys carried out in 1991 and 1993 on security industry attitudes towards ITSEC; both interest and confidence increased in all EC member states. A number of further recommendations are made.

033324 'Protection of Electronic Mail and Electronic Messages: Challenges and Solutions'
FB Gluck, *Information Management and Computer Security v 2 no 1 (94) pp 28 - 40*

The author reviews email security issues and basic encryption techniques.

033325 'Technology enables crime; shifting paradigms for the year 2000'
S Gordon, *IFIP SEC 94 paper I3*

The author discusses how viruses and hacking tools are propagated through bulletin boards, usenet and other mechanisms. The ultimate solution, she argues, will be a change to more mature user attitudes.

033326 'Sniffing in the Sun: History of a Disaster'
S Gordon, I Nedelchev, *Network Security (July 94) pp 16 - 19*

The authors describe the /dev/nit password sniffing incident which hit in February 1994 and could have compromised a quarter of the American Internet. The problem is not completely solved yet, as there are sniffers which evade CERT's detector.

033327 'Directories: the legal issues'
R Graham, *Computer Law and Security Report v 10 no 3 (May/June 94) pp 127 - 130*
The author points out some legal problems with directories of public keys. In Britain, the copyright will go to the compiler of the directory, and data protection law means that the operator might need to inform the subject whenever someone accessed his key. However, the operator might escape liability for errors. The situation in other EC countries is quite different, but the only help available from EC law is that if the operator abused his monopoly, he could be challenged in the European Court.

033328 'A High Level Security Policy for Health Care Establishments'
D Gritzalis, S Katsikas, J Darzentas, *IFIP SEC 94 paper E6*
The authors discuss the rôle of high level security policies in securing health care data, and advance some principles which might be incorporated in such a policy.

033329 'A very simple fraud'
P Harverson, *Banking Technology (July/August 94) pp 35 - 37*
The author describes the mechanics of the recent $350m bond stripping fraud at Kidder Peabody; this is ascribed to weaknesses in the accounting systems and to a culture of chasing profit at any cost. Managers should look carefully at staff who appear to be extraordinarily successful, not just at the failures.

033330 'Notes of caution'
VB Head, *Banking Technology (July/August 94) pp 42 - 43*
This article describes the history and technology of Australia's plastic banknotes. These cost only a little more than paper notes, but they last much longer and none have so far been successfully forged.

033331 'Security is a Dog from Hell'
KJ Higgins, *UniForum Monthly v XIV no 6 (June 1994) pp 20 - 23*
Security in distributed environment is difficult because of the lack of central controls. Bugs in UNIX systems are a common cause of security breaches, as is the wide-open nature of MS-DOS. Commercial and shareware products (such as Kerberos) can be used to close many of the holes.

033332 'The need for a new approach to information security'
J Hitchings, *IFIP SEC 94 paper C9*
The author reports empirical research on 132 organisations into human aspects of computer security. Most security breaches are opportunistic and are carried out by employees; yet personnel management was poor, the uptake of security technology was low, and only half the respondents enforced checks on password syntax.

033333 'Cryptography Policy'
LJ Hoffman, FA Ali, SL Heckler, A Huybrechts, *Communications of the ACM v 37 no 9 (Sep 94) pp 109 - 117*
The authors report a number of estimates of the size of the market for cryptographic products, and discuss the likely effect of the US government's key escrow initiative on this market.

033334 'Secure information exchange in organisations'
R Holbein, *IFIP SEC 94 paper H7*
The author discusses information exchange within organisations, and suggests that in addition to the usual goals such as confidentiality and integrity, one needs to add goal conformity as a primitive.

033335 'Do You Know Where the Briefcase Is?'
JE Hurd, *Journal of Systems Management (Aug 94) pp 16 - 27*

The author discusses why contingency plans are often less effective than hoped. Planners must must take business processes into account, not just the computerised aspect of them.

033336 'A framework for information system security management'
HJ James, PJ Forde, *IFIP SEC 93 paper H3*

The authors propose a new framework for security management and claim that a survey showed many security managers in agreement with it.

033337 'A Boom for Computer Security: Fears on the Internet Prompt Industry's Rise'
A Jenks, *Washington Technology, June 23 1994*

The rapid growth of the Internet (and the security problems coming to light as a result of that growth) is turning the market for security technologies from a niche market into a growth market, after a long period in which the only way to make money was by selling products to the government.

033338 'Business recovery planning - the Oracle approach'
M Johnson, *Computer Fraud and Security Bulletin (July 94) pp 8 - 12*

The author discusses the disaster recovery philosophy and strategy of Oracle UK.

033339 'The Future Looks Safe for Security Jobs'
J Johnson, *UniForum Monthly v XIV no 6 (June 1994) pp 34 - 35*

Data Security Administrators with 3-5 years experience typically earn $30,000 to $40,000/year in the USA. Among skills sought by hirers are OSF's DCE and Microsoft's OLE.

033340 'Ethical and Cultural Considerations for Effective Computer Security'
V Kamay, *Singapore 94*
This paper addresses some of the ethical and cultural considerations that underpin the development and implementation of effective computer security.

033341 'A Security Officer's Workbench'
FK Lam, D Longley, *IFIP SEC 94*

The authors describe a model based on a risk data repository which is intended to help managers understand the current status of security in their firms.

033341 'Deux Ans en Arrière, Deux Ans en Avant....'
JM LaMère, *Securicomm 94 pp 159 - 162 (in French)*

There are several tens of losses in excess of Ffr 10 million in Europe each year; potential losses are much greater and could reach Ffr 500 million for a single corporation. The frequency and amplitude of losses depend less on the available security mechanisms than on deficiencies in crisis management. In addition, errors caused by poor specification are on the increase; and a number of factors drive the increase in crime, including the globalisation of more and more industries, which constantly increases the stakes. Security weaknesses will increasingly be found in application and procedural detail; the riposte will involve both education and European legislation.

033343 'Codes, Keys and Conflicts: Issues in U.S. Crypto Policy'
S Landau, S Kent, C Brooks, S Charney, D Denning, W Diffie, A Lauck, D Miller, P Neumann, D Sobel, *Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM), June 1994*

This report puts forward a number of different perspectives on cryptography policy. These include the views of law enforcement and national security organizations, who describe how encryption may interfere with officially sanctioned electronic eavesdropping; the legal background to privacy expectations; the Computer Security Act of 1987; and the civil liberties interests. The focus of the report is an explanation of the Escrowed Encryption Standard (EES), also known as Clipper. As has been widely reported, this allows lawmen to listen in to secure communications. The technical and business tradeoffs in such a scheme are explored.

033344 'New Research on Systems Auditability and Control'
CH Le Grand, *Securicomm 94 pp 319 - 331*

The author reports a number of initiatives by the US Institute of Internal Auditors, and lists a number of audit points for new technologies such as object-oriented and document management systems.

033345 'The Computer Misuse Act'
SK Lee, *Singapore 94*

This paper provides the IT professional with an understanding of the nature and scope of the Singapore Computer Misuse Act.

033346 'Legal aspects of computer crime - general theory of computer crimes and the proposed bill to modify the Brazilian penal code'
OB Licks, JM De Araujo, *Computer Law and Security Report v 10 no 4 (Jul/Aug 94) pp 176 - 184*

Problems with computer crime arise from the fact that the information in a system is less well protected by law than the physical system itself. A number of legal theories are described, as is some legislation under discussion in Brazil's National Congress.

033347 'Legal Issues in Computer Security'
KT Lim, *Singapore 94*

The author highlights some legal issues and problems which have not been addressed by the Singapore Computer Misuse Act, and proposes some practical measures to resolve them.

033348 'Towards Operational Measures of Computer Security'
B Littlewood, S Brockelhurst, N Fenton, P Mellor, S Page, D Wright, J Dobson, J McDermid, D Gollmann, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 211 - 229*

The question of attacker effort is considered explicitly in this paper. It asks whether the kind of quantitative approach taken in the field of software reliability can be carried over to security. Certain fundamental parameters would have to be different; in particular, the paper proposes that time-to-failure would be replaced by effort-to-breach. It calls attention to the assumptions underlying the use of probability distributions.

033349 'US Adopts a Disputed Coding Standard'
J Markoff, *New York Times (23rd May 1994) pp C1, C10*

The author reports the adoption of the digital signature algorithm by the US government, and the fact that this is contested by a number of large suppliers who favour RSA instead. The Clipper issue is also aired.

033350 'Euro-Encryption Fears Grow'
C Mendler, *Communications Week International (27 June 1994) pp 1 & 38*

A recent meeting of national representatives in Brussels was due to decide on a crypto control policy for the European Union. When published, this is expected to feature key escrow along the lines of the US model.

033351 'The New Importance of "Business Continuity" in Data Processing Disaster Recovery Planning'
B Menkus, *Computers and Security v 13 no 2 (Apr 94) pp 115 - 118*

After a roof in New Jersey collapsed and buried a mainframe under snow, 5200 ATMs - 6% of the US total - were out of action for two weeks. These included machines as far afield as Texas and California.

033352 'The Security process'
J Ohlsson, *IFIP SEC 94 paper F1*

The author describes the procedures used by the Swedish defence materiel administration for developing, evaluating and accrediting secure systems.

033353 'Development of Security Policies'
J Ølnes, *IFIP SEC paper F3*

The author discusses how to go about developing a security policy and ensuring that it is a good fit with the organisation.

033354 'Security concepts for corporate networks'
R Oppliger, D Hogrefe, *IFIP SEC 94 paper F4*

The authors review network security threats and possible countermeasures.

033355 'Investigation of factors affecting the decision to report occurrences of computer abuse in Western Australian organisations'
JA Palmer, ASW Lee, *IFIP SEC 94 paper H4*

The authors investigated which computer abuses went unreported and why. Viruses and hardware theft were not sensitive, and would not be covered up; fraud was very sensitive; and unauthorised access, data theft and sabotage lay in between.

033356 'Avoid Encryption Anarchy'
DP Parker, *INFO Security News v 5 no 3 (May 94) pp 29-32*

The author argues that widespread use of cryptography, and use of strong cryptography without key escrowing, runs counter to the interests of business.

033357 'Security Management for OSI Networks'
A Patel, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 544 - 553*

This paper gives an overview of security management. The author examines two aspects of security management – management of user security services and provision of security to network management systems.

033358 'Issues in designing and implementing a practical enterprise security architecture'
R Paul, *IFIP SEC 94 paper H1*

The author describes the security architecture developed for, and implemented by, the World Bank. It consists of a number of 'mutually suspicious' domains, between which data transfer is mediated by security mechanisms.

033359 'Gaining confidence in IT systems through IT security testing'
D Pullen, *Information Security Monitor v 9 no 6 (May 94) pp 5 - 8*

While testing the security of an installed system is not trivial, such an exercise can bring many indirect benefits such as increased confidence, reduced errors and better availability. Some testing strategies are discussed.

033360 'Following the Flow of Funds'
R Ruffin, *Security Management (July 1994) pp 46 - 52*

Detecting and investigating fraud often means analysing transactions such as utility bills, credit card statements and even public records. The author, who is a special agent with the US Internal Revenue Service, discusses what to look for; a $25 utility bill may reveal a $250,000 second house hidden behind a nominee; safe deposit logs and loan collateral can help to strip away asset anonymity; and various patterns of bookkeeping and payment activity should be considered suspicious. However, observing a suspect's income and expenditure is still an extremely powerful tool.

033361 'Une Méthode d'Evaluation Numérique de la Sécurité des Systèmes d'Information'
B Saverio, *Securicomm 94 pp 83 - 95 (in French)*

The author tackles the problem of auditing EDI systems and describes a methodology developed at Italsiel. This involves a matrix of mechanisms and threats.

033362 'An Introduction to information Warfare'
W Schwartau, *IFIP SEC 94 paper K1*

The author argues that competition between the big three economic blocs will result in a sharper struggle for control of information, which will erode personal privacy and corporate security.

033363 'Briefing paper: business continuity'
J Shellingford, *Computer Business Review v 2 no 3 (May 94) pp 22 - 25*

This article surveys the US disaster recovery industry and the makers of uninterruptible power supplies and RAID storage products.

033364 'Computer Crimes in the Region: Nature and Investigations'
S Singh, S Leung, *Singapore 94*

This paper discusses the nature of computer (or computer-related) crimes handled by the Singapore Police Force and the Royal Hong Kong Police. Some cases, including theft from ATMs and cheating at banks, are described.

033365 'When is a computer not a computer?'
GJH Smith, *Computer Law and Security Report v 10 no 2 (Mar/April 94) pp 84 - 85*

Recent UK precedents suggest that computer evidence law does not apply to certain applications, and that a word processor (for example) might be considered to be just a glorified typewriter.

033366 'The law commisssion's report on the reform of the hearsay rule: its impact upon the reception of computer output'
C Tapper, *Computer Law and Security Report v 10 no 2 (Mar/April 94) pp 86 - 88*

Recent cases have raised doubts about when UK computer evidence law applies, but the Law Commission now proposes that computer generated documents should be treated no differently from any other documents, and that evidence should not be excluded from civil and magistrates' courts on the grounds of hearsay.

033367 'Viruses: what can we really do?'
HB Wolfe, *IFIP SEC 94 paper I4*

The author gives an overview of the virus world - their history, technology and the effectiveness of countermeasures.

033368 'An architecture for secure dial-up'
CC Wood, *Information Security Monitor v 9 no 9 (Aug 94) pp 5 - 8*
The author discusses the options available when securing dialup access to corporate systems, and how an intelligent choice of options can be made.

033369 'New European Software Copyright'
U Wuermeling, *Securicomm 94 pp 139 - 155*
The author discusses the effects of recent European Council directives on copyright law. These vest copyright in the creator; exceptions are that there is no protection for ideas, and that acquirers are allowed to make a backup, correct errors, and decompile the software. There are a number of risks as well as advantages for IT managers.

033370 'US Encryption Policy - "The Clipper Chip Controversy" '
BP Zajac, *Computer Law and Security report v 10 no 3 (May/June 94) pp 138 - 139*
The author mentions some of the possible legal problems of the Clipper programme.

033371 'US Encryption Policy (part II) - "Pretty Good Privacy" '
BP Zajac, *Computer Law and Security report v 10 no 3 (July/Aug 94) pp 201 - 202*
The author discusses PGP and the current legal proceedings against its author.

4 Formal Methods and Protocols

033401 'Secure Communication in LANs Using a Hybrid Encryption Scheme'
HK Aslan, MT El-Hadidi, NH Hegazi, *IFIP SEC 94 paper B6*

The authors have developed software for use on a network of personal computers, which provides authentication, integrity, non-repudiation, and confidentiality services. The RSA cryptosystem provides the first three services; Diffie-Hellman key exchange is used to establish DES session keys which are then used to ensure confidentiality. The protocols are presented.

033402 'TESS: A Security System Based on Discrete Exponentiation'
T Beth, F Bauspiess, H-J Knobloch, S Stempel, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp466 - 475*

This paper describes the basic mechanisms and functions of TESS, demonstrating their suitability to applications in network security and electronic signature. An overview of the implementation is given.

033403 'Cryptographic Protocol Flaws'
U Carlsen, *Franconia 94 pp 192 - 200*

Different types of flaws in cryptographic protocols are discussed and analyzed. Countermeasures are included in the discussion.

033404 'Optimal Privacy and Authentication on a Portable Communications System'
U Carlsen, *Operating Systems Review v 28 no 3 (July 94) pp 16 - 23*

The author proposes improved versions of the Beller-Chang-Yacobi protocols for setting up private links in mobile networks. He also argues that capacity constraints prevent the use of public key techniques to protect destination identity in such systems, and discusses some of the tradeoffs between end-to-end and link level protection.

033405 'An Interactive Tool for Design, Simulation, Verification and Synthesis of Protocols'
DY Chao, DT Wang, *Software - Practice and Experience v 24 no 8 (Aug 94) pp 747 - 783*

The authors describe a new CAD tool they have developed for the design, verification, synthesis and animation of protocols using Petri net and state diagram techniques.

033406 'Combining Components and Policies'
GW Dinolt, LA Benzinger, MG Yatabe, *Franconia 94 pp 22 - 33*

The authors propose a new model of security policies and properties. This is done with an eye towards system composition.

033407 'Une solution de sécurité pour la migration vers les architectures client/serveur'
C Garnier, *Securicomm 94 pp 285 - 296 (in French)*

The author argues that security protocol development should aim at providing federated tools which enable users to establish end-to-end security through a large number of existing mechanisms. It is inevitable that many diverse authentication and access control mechanisms will continue to be used, and thus rather than trying to supplant them with some wonderful new standard or product, we should build bridges between them. At the level of architecture, something like SESAME's application programming interfaces may be a better way forward than DCE's approach of hiding everything in RPCs.

033408 'Normalisation / Evaluation / Certification'
MA Hasbrouck, *Securicomm 94 pp 167 - 174 (in French)*

The author describes the security mechanisms of X.411 and X.435, and discusses how they can be used together with the X.500 series standards to provide secure EDI services.

033409 'On the Security Effeciveness of Cryptographic Protocols'
R Kailar, VD Gligor, L Gong, *Dependable Computing 94*

The authors argue that current cryptographic protocol logics are unable to deal with attacks involving cumulative properties of the underlying algorithms, such as if knowledge of a large quantity of corresponding plaintext and ciphertext allows an attacker to derive a key. Kerberos, Needham-Schroder and the Andrew secure RPC handshake are discussed as examples. They suggest using a property dependency graph instead.

033410 'Reasoning about Message Integrity'
R Kailar, VD Gligor, L Gong, *Dependable Computing 94*

The authors propose a formal method to assess the probability with which an opponent can guess a message which will be accepted by an authentication scheme. The object is to deal with key size, confounders and the like, and to obtain lifetime constraints on keys; measures to prevent message replay are not considered. Their method picks up one of the bugs in Kerberos V4, and they show that both Kerberos V5 and PEM could be improved by the use of confounders.

033411 'SESAME: The Solution to Security for Open Distributed Systems'
P Kaijser, T Parker, D Pinkas, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 501 - 518*

This paper describes SESAME, a security architecture for open distributed systems developed by Bull, ICL and Siemens Nixdorf. it presents the concepts behind the architecture, as well as the system's properties and features.

033412 'Identity authentication in heterogeneous computing environments: a comparative study for an integrated framework'
S Kanungo, *Computers and Security v 13 no 3 (May 94) pp 231 - 253*

The author discusses a number of authentication protocols including Kerberos, Sphinx, Zephyr, the Andrew authentication handshake and the HP/Apollo secure RPC.

033413 'AUTLOG - An advanced logic of authentication'
V Kessler, G Wedel, *Franconia 94 pp 90 - 99*

The authors present a modification of the BAN logic, implemented in Prolog, and a formal model of it. They discuss certain protocol flaws that this logic picks up.

033414 'Compositional Specification and Verification of Distributed Systems'
B Jonsson, *ACM Transactions on Programming Languages and Systems v 16 no 2 (Mar 94) pp 259 - 303*

The author presents a new technique for specifying and verifying both safety and liveness properties in composed distributed systems; verifying an implementation reduces to proving fairness, simulation and termination conditions. The method is illustrated by applying it to a voting protocol for concurrency control in replicated databases.

033415 'Development of Authentication Protocols: Some Misconceptions and a New Approach'
WB Mao, C Boyd, *Franconia 94 pp 178 - 186*

This paper looks at misconceptions in various secret-key algorithms and protocols. A common problem is identified and a method for dealing with it is proposed.

033416 'Exploring Minimal BAN Logic Proofs of Authentication Protocols'
A Mathuria, R Safavi-Naini, P Nickolas, *IFIP SEC 94*

This paper presents an improved version of the second author's Prolog program for BAN analysis. It searches for minimal proofs of a statement using forward chaining techniques; some technical aspects, such as loop avoidance and proof explanation, are described, as is its application to the Needham-Schroder protocol.

033417 'A Model of Computation for the NRL Protocol Analyzer'
C Meadows, *Franconia 94 pp 84 - 89*

In this paper the author constructs a model of computation for the NRL Protocol Analyzer, a formal methods tool for verifying security properties of cryptographic protocols. This model is a modification of that developed by Abadi and Tuttle for a version of BAN logic. It is compared with Abadi and Tuttle's model from the point of view of possible integration of BAN logic and the NRL Protocol Analyzer.

033418 'Formal Methods for the Informal World'
CK Muehrke, *Franconia 94 pp 36 - 46*

The author does a formal analysis, using the Z language, to examine how the environment interacts with a secure system.

033419 'Cryptographic protocols and voting'
V Niemi, A Renvall, *Salomaa Colloquium pp 307 - 316*

The authors describe a protocol for all-or-nothing disclosure of secrets, and two protocols for secret ballot elections with reduced likelihood of buying and selling of votes. However, it is noted the voting protocols are impractical for large-scale elections.

033420 'Cryptographic protocols for auctions and bargaining'
H Nurmi, *Salomaa Colloquium pp 317 - 324*

The article presents protocols for auctions, bargaining and arbitration. The protocols are intended to eliminate specific types of behavior which might undermine the desirable properties of the institutions.

033421 'Prohibiting the Exchange Attack calls for Hardware Signature'
W Mayerwieser, R Posch, *IFIP SEC 94 paper B8*

The "exchange attack" is the replacement of equipment with new equipment that appears superficially similar but performs additional functions not intended by the user. The author proposes that tamper-proof devices should contain a secret allowing users to determine if it has been replaced.

033422 'Nonmonotonic Cryptographic Protocols'
AD Rubin, P Honeyman, *Franconia 94 pp 100 - 116*

The authors analyze cryptographic protocols. Their techniques allow reasoning about nonmonotonic protocols and pick up the known flaws in the Needham Shroeder protocol. Their techniques also pick up an undiscovered flaw in their own khat protocol. The paper is especially readable by non-experts in the field.

033423 'Secure Network Management'
B Studer, *IFIP SEC 94 paper F7*

The author considers how security information could be embedded in the OSI Common Management Information Protocol (CMIP), using X.400, FTAM and SNMP as examples, and suggests an enhancement of CMIP.

033424 'A Taxonomy of Replay Attacks'
P Syverson, *Franconia pp 187 - 191*

This paper presents a taxonomy of all known replay attacks on cryptographic protocols in terms of message origin and destination. Some specific attacks are discussed, as are protocol analysis methods and replay countermeasures.

033425 'A Lesson on Authentication Protocol Design'
TYC Woo, SS Lam, *Operating Systems Review v 28 no 3 (July 94) pp 24 - 37*

The authors discuss a flaw discovered by Abadi in a key translation protocol they invented, and show that it can be repaired by inserting the parties' names sufficiently often in the encrypted messages. From this they derive the 'principle of full information': this is that each player should include, in every encrypted message which she sends, all the information she has gathered so far in the current protocol run.

033426 'Optimality of Asynchronous 2-Party Security Data-Exchange Protocols'
R Yahalom, *Journal of Computer Security v 2 no 2 - 3 (1993) pp 191 - 209*

Automated cryptographic key distribution in a network generally requires a protocol consisting of several steps, in order to protect against eavesdropping and message modification attacks. It is an inconvenience for a user to wait longer than necessary for these exchanges to take place, so it is of interest to minimize the number of messages in the key distribution protocol. This paper shows that five messages are necessary and sufficient under certain conditions, using a symmetric encryption system.

5 Secret Key Algorithms

033501 'A Modern Rotor Machine'
RJ Anderson, *Fast Software Encryption 1993 pp 47 - 50*

The author proposes a stream cipher in which a shift register turns three rotors, each of which is a 256-byte permutation. Ho points out that the classical attacks on both rotor and shift register systems fail against this combination, and sets a challenge in cryptanalysis.

033502 'On Modes of Operation'
E Biham, *Fast Software Encryption 93 pp 116 - 120*

The author investigates various nonstandard modes of DES. He shows, for example, that using intermediate values in feedback weakens the cipher, and that a number of triple encryption modes such as CBC | CBC | ECB and CBC | ECB | CBC are no stronger than single DES. The main idea is that an opponent can concentrate his attack on the shortest path through any mode of operation, and the moral is that one should use a single CBC (or other relevant) mode of triple DES.

033503 'Increasing the rate of output of m-sequences'
SR Blackburn, *Information Processing Letters v 51 no 2 (26/7/94) pp 73 - 78*

The author generalises a result of Robshaw to show that one may interleave k m-sequences and get an m-sequence of increased rate, provided k is coprime to their period; however, the resulting sequence will only be a shift of the component sequences if k is a power of 2. In some cases, more than one component sequence may be drawn from a single shift register.

033504 'Fish: A Fast Software Stream Cipher'
U Blöcher, M Dichtl, *Fast Software Encryption 93 pp 41 - 44*

The authors describe a keystream generator which shrinks a nonlinear combination of two Fibonacci generators, of lengths 52 and 55, which use arithmetic modulo 2^{32}.

033505 'On the periods of generalised Fibonacci recurrences'
RP Brent, *Mathematics of Computation v 63 no 207 (July 94) pp 389 - 401*

The author provides a new set of conditions under which a recurrence of degree r mod 2^n will have period $2^{n-1}(2^r - 1)$; these hold for primitive trinomials of degree greater than two.

033506 'Comments on "Generating and Counting Binary Bent Sequences"'
C Carlet, J Seberry, XM Zhang, *IEEE Transactions on Information Theory v 40 no 2 (Mar 94) p 600*

The authors disprove a conjecture of Adams and Tavares that any bent sequence is either bent-based or linear-based by showing that this would imply that all bent sequences were quadratic.

033507 'Weak Keys and Weak Data: Foiling the Two Nemeses'
JM Carroll, S Nuridati, *Cryptologia v XVIII no 3 (July 94) pp 253 - 280*

The authors consider the effect which censoring highly patterned subsequences would have on the complexity of the output of a keystream generator.

033508 'Two Stream Ciphers'
WG Chambers, *Fast Software Encryption 93 pp 51 - 55*

The author presents two keystream generators; one is a cascade of clock controlled registers with S-boxes between successive stages, and the other is a nonlinear linking of two shift registers over $GF(2^n)$ from which the k most significant bits ($k < n$) are selected for the keystream. Both of these generators can be equivalently represented as cascades of coupled binary shift registers, and have longish periods.

033509 'On Quadratic m-Sequences'
AH Chan, RA Games, JJ Rushanan, *Fast Software Encryption 93 pp 166 - 173*

The authors investigate the effect of introducing quadratic terms into a shift register; the quadratic span of a sequence is the shortest such register which generates it. They prove some new results on the number of patterns of a given length, enumerate all quadratic sequences of span less than 7, and look at a number of larger registers which have exactly one quadratic term.

033510 'On the Distance Properties of the S-Box Internal Mapping'
H Chung, *JW-ISC 93 pp 272 - 281*

In this paper, some lower bounds are derived on the maximum distances to the affine mappings over the Boolean vector functions and balanced Boolean vector functions from $GF(2^n)$ to $GF(2^m)$ for the case when $n \geq 2m$. The distances of the internal mappings of the 32 4-bit to 4-bit component permutations in the DES S-boxes are also evaluated.

033511 'A New Approach to Block Cipher Design'
J Daemen, R Govaerts, J Vandewalle, *Fast Software Encryption 93 pp 18 - 32*

The authors present a block cipher called 3-Way, which is designed to run reasonably quickly in both hardware and software and to resist both differential and linear attacks; they also provide an implementation of it in C. With a 12 byte block and key length, its core is a nonlinear operation on three bits, which is combined with bit permutations and expansions to provide a nonlinear round function. Bounds can be obtained on its m-round propagation characteristics.

033512 'Some Statistical Properties of Feedforward Sequences (I)'
ZD Dai, XN Feng, ML Liu, ZX Wan, *Scientia Sinica (Series A) v 37 no 1 (Jan 1994) pp 34 - 41*

The authors discuss the statistical properties of non-linear feedforward sequences of m-sequences. They exhibit the weights of non-linear feedforward sequences, and calculate the correlation functions of two of them.

033513 'Some Statistical Properties of Feedforward Sequences (II)'
ZD Dai, XN Feng, ML Liu, ZX Wan, *Scientia Sinica (Series A) v 37 no 2 (Feb 1994) pp 129 - 136*

The authors continue their discussion of the statistical properties of non-linear feedforward sequences. In this paper, they give the number of 0-runs and 1-runs of the non-linear feedforward sequences associated with a quadratic monomial.

033514 'VINO: A Block Cipher Including Variable Permutations'
A Di Porto, W Wolfowicz, *Fast Software Encryption 93 pp 205 - 210*

The authors present a cipher with 64-bit data blocks and a 128-bit key. It uses a keyed permutation due to Vinogradov, which is generated by decimating a regularly ascending and descending sequence of integers; four of these permutations are combined with xor's and additions to make up a round of the cipher, and four rounds are suggested in use.

033515 'The Differential Cryptanalysis and Design and Natural Stream Ciphers'
CS Ding, *Fast Software Encryption 93 pp 101 - 115*

The author considers sequence generators in which a counter is filtered through a nonlinear function. Certain patterns in the output leak more information than others about the counter state, and this can be the basis of an attack. There turn out to be relationships between the information leakage, the nonlinearity of the function, and the autocorrelation of the keystream.

033516 'On generalised inversive congruential generators'
J Eichenauer-Herrmann, *Mathematics of Computation v 63 no 207 (July 94) pp 293 - 300*

The author extends some of his results on inversive congruential generators from prime to composite moduli and provides discrepancy bounds in terms of the square roots of the prime factors of the modulus.

033517 'Maximal length sequences over the Gaussian integers'
PZ Fan, M Darnell, *Electronics Letters v 30 no 16 (4/8/94) pp 1286 - 1287*

The authors show that maximal length sequences can be constructed over the Gaussian integers $a + bi$ where $i^2 = -1$. They have the usual properties, except that each period of the sequence can be partitioned into four parts $(a, ia, -a, -ia)$ and the autocorrelation therefore has four peaks - at the phases $(0, L/4, L/2, 3L/4)$, where L is the sequence length.

033518 'On the security of shift register based keystream generators'
JD Golić, *Fast Software Encryption 93 pp 90 - 100*

The author presents an extended survey of the art of breaking shift register based stream ciphers. He considers both the divide-and-conquer and the correlation attacks, and classifies stream ciphers according to whether the registers are regularly clocked, and whether the combining function has memory. Some new ideas for divide-and-conquer attacks on combiners with memory are presented, which are exponential in the number of memory bits eliminated; at present, irregularly clocked systems are preferable, due to the lack of fast correlation attacks.

033519 'Cryptanalysis of Clock Controlled Shift Registers'
D Gollmann, *Fast Software Encryption 93 pp 121 - 126*

The author provides a survey of the cryptanalytic techniques available for attacking clock controlled shift registers. These vary from automata theoretic methods through string matching techniques to correlation attacks on stop-and-go systems. He also discusses a freak result for registers of length 3.

033520 'To Decode Short Cryptograms'
GW Hart, *Communications of the ACM v 37 no 9 (Sep 94) pp 102 - 108*

The author develops techniques for solving monoalphabetic substitutions given only a short ciphertext. He uses the most common 135 English words together with a number of heuristics based on maximum likelihood and tree pruning techniques.

033521 'A successful attack against the DES'
F Hendessi, MR Aref, *Canadian Info Theory 93 pp 78 - 90*

The authors describe a pipelining computer for exhaustive key search of DES, and claim that DES could be broken easily and cheaply using it.

033522 'Fast Block Cipher Proposal'
BS Kaliski, MJB Robshaw, *Fast Software Encryption 93 pp 33 - 40*

The authors sketch the design of a cipher operating on 256-byte blocks which draws on the experience of designing fast has functions for 32-bit processors. Each round is in effect 64 successive applications of an MD5 half round, with the message in the has function being replaced by the key in the cipher, and the hash function buffer words being replaced by plaintext. The key material is a 256-byte permutation and 2048 32-bit subkeys.

033523 'Dynamic Swapping Schemes and Differential Cryptanalysis'
T Kaneko, K Koyama, R Terada, *JW-ISC 93 pp 292 - 301*

The authors propose a dynamically randomized version of DES (called RDES) in which a probabilistic swapping of the left and right halves is added at each round. The authors claim that this variant is more secure against differential cryptanalysis because the best characteristic probability is decreased.

033524 'Reconstruction of s^2DES S-boxes and their Immunity to Differential Cryptanalysis'
K Kim, S Park, S Lee, *JW-ISC 93 pp 282 - 291*

The authors present a replacement set of S-boxes for DES. The variant algorithm, called s^3DES, is more resistant to differential cryptanalysis than DES.

033525 '2-adic Shift Registers'
A Klapper, M Goresky, *Fast Software Encryption 93 pp 174 - 178*

The authors present a deep and novel attack on the summation generator. They show that its output sequence has a short linear span when considered over the 2-adic numbers, and can thus be synthesised using Mandelbaum's algorithm. The effect is that one can emulate the summation generator using a feedback-with-carry shift register - one in which 'normal' addition with carry is used instead of exclusive-or to combine the feedback bits.

033526 'Partial Period Autocorrelation of Geometric Sequences'
AM Klapper, M Goresky, *IEEE Transactions on Information Theory v 40 no 2 (March 94) pp 494 - 502*

The authors consider the autocorrelation of part of a pseudorandom sequence generated by correlating two windows. If this varies over all start positions, then its expected value is equal to the full period autocorrelation; and for sequences which can be generated by filtering an m-sequence over GF(q) through some function f:GF(q)$\rightarrow$GF(2), the expected partial period autocorrelation can be given explicitly, as can bounds on its variance. These results bound the length of sequence needed by a computationally unlimited opponent to recover the generator's phase.

033527 'The Weight Distribution of Cosets'
T Kløve, *IEEE Transactions on Information Theory v 40 no 3 (May 94) pp 911 - 913*

The author generalises Sullivan's bound on the weight distribution of the cosets of a binary linear code to codes over GF(q), and derives an expression for the probability of an undetected error.

033528 'Practically secure Feistel ciphers'
LR Knudsen, *Fast Software Encryption 93 pp 211 - 221*

The author discusses the techniques available to make block ciphers secure against linear and differential attacks, and shows how to get a practical lower bound on the effort required for these attacks where round subkeys are independent. This leads to the principle that the strength of key schedules should be comparable to that of the overall cipher. Finally, he suggests how differentially uniform functions can be used to construct a round function.

033529 'The Shrinking Generator: some practical considerations'
H Krawczyk, *Fast Software Encryption 93 pp 45 - 46*

A C implementation of the shrinking generator runs at 2.5 Mbit/sec on a 33MHz IBM workstation. With shift register lengths of 61-64 bits, this gives an effective key length of about 110 bits. The bottleneck is updating the shift registers' state; as their feedback polynomials form part of the key, matrix multiplication was used.

033530 'Attacks on Double Block Length Hash Functions'
XJ Lai, LR Knudsen, *Fast Software Encryption 93 pp 157 - 165*

The authors review the various types of attack on hash functions, and show that a class of functions whose outputs are twice the length of the underlying block function have both target and free-start attacks which take only twice as much effort as the attacks on the best single-length hash function based on the same block cipher. They also tabulate the costs of attacking a number of proposed systems.

033531 'Cryptographic Pseudo-random Numbers in Simulation'
N Maclaren, *Fast Software Encryption 93 pp 185 - 190*

The author surveys the uses of pseudorandom numbers in statistical simulation and contrasts the requirements there with those of stream ciphers and other cryptographic applications. The two research communities could gain from talking with each other in areas such as randomness properties. Three areas of common research interest are the relationship between local and global randomness in sequences, practical complexity results, and the independence of parallel generators.

033532 'SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm'
JL Massey, *Fast Software Encryption 93 pp 1 - 17*

The author describes a block cipher designed for, and made public domain by, Cylink corporation, and provides an implementation of it in Pascal. Designed to run quickly on 8-bit processors; it has 8 byte data and key blocks, and can have between 6 and 10 rounds. Each round consists of a new linear transform (called the pseudo Hadamard transform) to provide diffusion, and a number of exponentiation and discrete log operations in the field $GF(257)$ to provide confusion. Weak keys are eliminated by the use of additive biases in the key schedule.

033533 'The Breaking of The Japanese Army Administrative Code'
D Mead, *Cryptologia v XVIII no 3 (July 94) pp 193 - 203*

The author recounts how in April 1943 he solved a Japanese enciphered code system. He describes the coding blunder which allowed the initial break, and the stereotypes practices which made the subsequent codebook reconstruction possible.

033534 'Intrinsic weakness of variable-memory keystream generators'
R Menicocci, *Electronics Letters v 30 no 11 (26/5/94) pp 850 - 851*

The author shows a correlation attack on the McLaren-Marsaglia generator and on other generators which use a small memory to combine two or more shift register sequences.

033535 'Cryptanalysis of tree-structured ciphers'
W Millan, EP Dawson, LJ O'Connor, *Electronics Letters v 30 no 12 (9/6/94) pp 941 - 942*

Anderson's attack on ciphers which can be represented as an m-ary tree of Boolean functions can be speeded up where the nonlinear structure of each cell is known. In the particular case of the Kühn cipher, the fact that cells are unchanged when the first four bits are simultaneously complemented enables the subkeys to be found quickly and reduces the cost of the attack from $O(2^m m^{R-1})$ to $O(m^R)$.

033536 'Using a genetic algorithm for optimizing fixed polarity Reed-Muller expansions of Boolean functions'
JF Miller, H Luchian, PVG Bradbeer, PJ Barclay, *International Journal of Electronics v 76 no 4 (Apr 94) pp 601 - 610*

The authors report a genetic algorithm which gets good sub-optimum Reed-Muller expansions of Boolean functions more quickly than previous techniques.

033537 'New Bent Mappings Suitable for Fast Implementation'
K Nyberg, *Fast Software Encryption 93 pp 179 - 184*

The author shows a quick way to generate an n-bit to m-bit bent mapping. The input is divided into two halves; one is loaded into a shift register; and the output bits are calculated as the dot products of the shift register's successive states with the other half of the input. She also provides another family of bent functions based on a construction of Carlet.

033538 'Design Principles for Hash Functions'
B Preneel, *Fast Software Encryption 93 pp 71 - 82*

This paper discusses the techniques used to design hash functions. Collision resistance and one-wayness reduce to similar properties of the underlying compression functions. However, some bijectivity in round functions helps to maintain state, and the author explains how this tradeoff is managed in a number of specific designs. Some systems use the message to 'encrypt' some constants; the key schedule here may be an error correcting code (as in SHA). Finally, performance figures for a number of algorithms are given.

033539 'Performance of Symmetric Ciphers and One-way Hash Functions'
M Roe, *Fast Software Encryption 93 pp 83 - 89*

The author tested the speed of MD2, MD4, MD5, SHA, RIPE-MD, DES, GOST-28147 and SAFER on both Sparc and Alpha processors, and for both short and long messages. He also tested five possible triple encryption modes of DES. He suggests ways in which such algorithms can be strengthened with no performance penalty.

033540 'A Software-Optimised Encryption Algorithm'
P Rogaway, D Coppersmith, *Fast Software Encryption 93 pp 56 - 63*

The authors describe a very fast stream cipher called SEAL (for Software Encryption ALgorithm) which takes about 5 machine instructions per byte and is closely optimised for the Intel and PowerPC architectures. It uses just over 3 Kbytes of table, which are generated from the key using SHA and are then used to calculate up to 64 Kbytes of keystream by repeated combination of table lookup and register operations on 192 bits of register state. Speeds of megabytes per second have been achieved.

033541 'Description of a New Variable-length Key, 64-bit Block Cipher (Blowfish)'
B Schneier, *Fast Software Encryption 93 pp 191 - 204*

The author presents a block cipher with 8 byte data blocks and a key of up to 256 bits. It has a Feistel structure, and its autoclave function has four 8 bit to 32 bit S-boxes, which are key dependent and whose output is mixed using both exclusive or and addition modulo 2^{32}; additive key biases are also used to prevent weak keys. There is a reward of $1000 for the best attack found by April 1995.

033542 'Encryption's Bright IDEA'
B Schneier, *INFO Security News v 5 n 4 (July 94) p 79*

In this article, the author gives an overview of the IDEA encryption algorithm.

033543 'Parallel FFT-Hashing'
CP Schnorr, S Vaudenay, *Fast Software Encryption 93 pp 149 - 156*

The authors describe improved versions of the FFT hashing algorithm, one of which can be implemented in a highly parallel way. Rather than using a traditional compression function it allows multiple fan-in: many words can enter at each round and compression is only applied at the end.

033544 'Fast Construction of Irreducible Polynomials over Finite Fields'
V Shoup, *Journal of Symbolic Computation v 17 no 5 (May 94) pp 371 - 392*

The author introduces a new algorithm for constructing primitive polynomials of degree n over $GF(q)$. Where n is prime, the polynomial is $X^n - \xi$ where ξ is a nonresidue in a field defined by a suitable cyclotomic polynomial. Having given new algorithms for factoring cyclotomic polynomials and checking irreducibility, he shows that his construction takes about $O(L(n)(n^2 \log n + n \log q))$ field operations.

033545 'On finite automaton one-key cryptosystems'
RJ Tao, *Fast Software Encryption 93 pp 135 - 148*

The author shows how automata theory can be used to classify secret key cryptosystems according to their error propagation properties. He also discusses the merits of Latin squares as nonlinear filters in stream ciphers, and proves a number of results including for the period of such systems.

033546 'Analytical Known Plain-Test Attack for FEAL-6 Based on Bit-by-Bit Comparisons'
Y Tsunoo, E Okamoto, T Uyematsu, M Mambo, *JW-ISC 93 pp 253 - 261*

This paper extends a byte-by-byte attack on FEAL to a bit-by-bit attack. This uses an inverse round function and key-independent intermediate messages.

033547 'A Bulk Data Encryption Algorithm'
DJ Wheeler, *Fast Software Encryption 93 pp 127 - 134*

The author describes a very fast algorithm, WAKE, which takes only about 20 machine instructions per 20-bit word. It is based on a 256 byte permutation which serves as the key and is used with register operations and 128 bits of internal state to encrypt the data. A number of modes are possible, from an arbitrary length block cipher to a keyed hash function. C source code is included in the paper.

033548 'A divisionless form of the Schur Berlekamp-Massey algorithm'
CJ Zarowski, *Canadian Info Theory 93 pp 38 - 44*

By mapping the Berlekamp-Massey algorithm into Schur form, a divisionless algorithm is developed, which can also be parallelised.

033549 'Tables of primitive binary polynomials, II'
M Živković, *Mathematics of Computation v 63 no 207 (July 94) pp 301 - 306*

The author updates his list of primitive polynomials (**031528**) to take account of the factorisation of further numbers of the form $2^k + 1$.

6 Public Key Algorithms

033601 'Fortifying key negotiation schemes with poorly chosen passwords'
RJ Anderson, TMA Lomas, *Electronics Letters v 30 no 12 (23/6/94) pp 1040 - 1041*

Key negotiation schemes of the Diffie-Hellman type are vulnerable to middleperson attacks, and passwords remembered by users are vulnerable to guessing attacks. The authors provide a new way of using even guessable passwords to detect a middleperson attack; the technique uses hash functions which are designed so as to have a controlled number of collisions.

033602 'Normal and self-dual bases from factorisation of $cx^{q+1}+dx^q-ax-b$'
IF Blake, SH Gao, RC Mullin, *SIAM Journal of Discrete Mathematics v 7 no 3 (Aug 94) pp 499 - 512*

Sidel'nikov introduced normal bases for finite fields which could be generated from a single element by repeatedly applying the transform $x \to (ax+b)/(cx+d)$. The authors show that every such basis can be constructed from roots of $cx^{q+1}+dx^q-ax-b$, and that this enables us to construct bases for $GF(q^n)$ of low complexity which have explicit multiplication tables.

033603 'A remote password authentication scheme based upon ElGamal's signature scheme'
CC Chang, WY Liao, *Computers and Security v 13 no 2 (Apr 94) pp 137 - 144*

The authors propose a public key based authentication scheme in which the 'passwords' issued to users are in effect secret keys with which they sign a timestamp.

033604 'On the cryptosystem using elliptic curve'
YJ Choie, HS Hwoang, *JW-ISC 93 pp 105 - 113*

The authors discuss a Diffie-Hellman-type encryption algorithm over the elliptic curves using a modified polynomial basis.

033605 'Anonymous payment schemes'
D Everett, *Smart Card news v 3 no 3 (Mar 94) pp 55 - 58*

The author provides a tutorial on Chaum's anonymous electronic cash scheme.

033606 'Smart cards and key management'
D Everett, *Smart Card news v 3 no 4 (Apr 94) pp 75 - 78*

This article describes key management using both secure devices and public key schemes, and discusses the problem of certifying public keys generated in a smartcard after issue.

033607 'What are Today's Alternatives for a Digital Signature Scheme?'
W Fumy, E Hess, *Securicomm 94 pp 25 - 34*

The authors compare and contrast a number of signature schemes, and suggest that elliptic curve based systems may be the best. This depends on the assumption that 128-bit elliptic curve schemes are comparable in strength with 660-bit RSA.

033608 'Transport des Clefs au Moyen d'Algorithmes Asymmetriques'
M Girault, D Guerin, *Securicomm 94 pp 9 - 20 (in French)*

The authors discuss techniques for key transport using asymmetric algorithms, and give an overview of the banking standard ISO 11166, in which the session key is first encrypted and then signed. This standard is now in competition with ISO CD 11770-3, and is opposed by ISO committee JTC1/SC27, which recommends signature before encryption. A number of implementation issues are discussed.

033609 'Public key cryptosystem design based on factoring and discrete logarithms'
L Harn, *IEE Proceedings on Computers and Digital Techniques v 141 no 3 (1994) pp 193 - 195*

The author proposes public key schemes which are based on the Diffie-Hellman and factoring problems; key distribution is essentially Diffie-Hellman mod p followed by RSA mod $p-1$.

033610 'Enhancing the security of ElGamal's signature scheme'
J He, T Kiesler, *IEE Proceedings on Computers and Digital Techniques v 141 no 4 (1994) pp 249 - 252*

The authors propose two variants of ElGamal which depend on factoring as well as discrete log. Their modulus p has two large prime factors, which are secret; with secret key x, a user has public key g^{x^2} and signs m as (r, s) where $r = g^{k^2} \bmod p$ and $s = (m - xr)/k \bmod (p-1)$.

033611 'Authenticated encryption schemes with low communication costs'
P Horster, M Michels, H Petersen, *Electronics Letters v 30 no 15 (21 July 94) pp 1212 - 1213*

The authors extend the Nyberg-Rueppel variant of the digital signature algorithm to provide authenticated encryption which uses the DSA key infrastructure and signature primitives. Furthermore, the ciphertext is shorter, and the computational overhead lower, than with the Nyberg-Rueppel scheme.

033612 'Fast RNS division algorithms for fixed divisors with application to RSA encryption'
CY Hung, B Parhami, *Information Processing Letters v 51 no 4 (24/8/94) pp 163 - 170*

The authors present two residue number system division algorithms for use in modular exponentiation: they are based on precomputing reciprocals and on the Chinese Remainder Theorem.

033613 'A Multipurpose Membership Proof System based on Discrete Logarithms'
S Kim, BS Um, *JW-ISC 93 pp 177 - 183*

The authors propose a proof-of-membership scheme. In this system, a prover who holds one piece of secret information can convince a verifier of his membership in a group.

033614 'A New RSA-type Cryptosystem over Singular Elliptic Curves'
H Kuwakado, K Koyama, *Finite Fields 94*

This article describes an RSA-type cryptosystem over the non-singular part of a singular elliptic curve. Encryption/decryption is about the same speed as for RSA-type cryptosystems over non-singular elliptic curves, and it is claimed that breaking this system is no easier than breaking the corresponding RSA cryptosystem.

033615 'A Practical Electronic Cash System for Smart Cards'
CH Lin, PJ Lee, *JW-ISC 93 pp 34 - 47*

This paper presents a practical electronic cash system which is suitable for smart card implementation in both computation time and storage requirements. A trusted authority makes it possible to trace monetary transactions given a court order.

033616 'An Attack on an ID-Based Key Sharing System'
V Luchangco, K Koyama, *JW-ISC 93 pp 262 - 271*

This paper gives a collusion attack on a non-interactive ID-based key sharing system proposed by Tsujii, Araki, and Sekine.

033617 'On a New Approach to Key Sharing Problem'
T Matsumoto, H Imai, *JW-ISC 93 pp 81 - 89*

This paper develops a new class of key sharing schemes. In a very large network, Alice can compute a common key shared with Bob, using her secret algorithm, Bob's identity, and a public algorithm generated by a protocol conducted by her and the managing organization.

033618 'On the Selection of Public Modulus for RSA Cipher'
H Nagase, N Takeda, *Finite Fields 94*

The authors propose a "lattice point search" factorization algorithm. Although it is not as fast as the quadratic sieve and other fast factorization algorithms, it is claimed to be a useful new constraint for the selection of strong RSA moduli.

033619 'A Generalization of Public Key Residue Cryptosystem'
SJ Park, DH Won, *JW-ISC 93 pp 202 - 206*

This paper describes a generalized public-key cryptosystem whose security is based on the Yth-residuosity assumption. The paper also gives a proof that the proposed scheme is polynomially secure.

033620 'Comment: New Signature Scheme with Message Recovery'
RGE Pinch, *Electronics Letters v 30 no 11 (26/5/94) p 852*

The author points out that in Piveteau's signature scheme (**031617**), the proposed means of message recovery is not feasible, but that there is another approach which works.

033621 'Modern Key Agreement Techniques'
RA Rueppel, PC van Oorschot, *Journal of Computer Communications v 17 no 7 (Jul 1994) pp 458 - 465*

The authors present a survey of modern key agreement techniques, and discuss distinguishing characteristics, including entity and key authentication, key confirmation and key freshness.

033622 '(k, n) Threshold Undeniable Signature Scheme'
K Sakano, C Park, K Kurosawa, *JW-ISC 93 pp 184 - 193*

This paper describes a new (k, n) threshold undeniable signature scheme.

033623 'A new scheme of non interactive ID-based key sharing with explosively high degree of separability'
S Tsujii, K Araki, T Sekine, K Tanada, *JW-ISC 93 pp. 49 - 58*

The authors propose a new non-interactive ID-based key sharing scheme based on the concept of the degree of separability and iterative cancellation of random numbers. The newly introduced concept called "the degree of seperability" in both the key generating process and the form of shared key seems to play a role in clarifying the collusion threshold explicitly.

033624 'Bit-level Systolic Array for Fast Exponentiation in GF(2^m)'
CL Wang, *IEEE Transactions on Computers v 43 no 7 (July 94) pp 838 - 841*

The author describes a new design for a GF(2^m) exponentiator which uses many fewer gates than previous designs. It consists of a systolic array of multipliers, multiplexers and delay elements.

033625 'Practical Protocols for Electronic Cash'

HY Youm, SL Lee, MY Rhee, *JW-ISC 93 pp 10 - 22*

This paper proposes a practical electronic cash system using blind digital signature schemes, Schnorr's authentication scheme, and a hierarchical cash tree based on two one-way hash functions. The scheme has the following properties: privacy of payment, off-line payment, non-reusability of cash, transferability of cash, and dividable payment of cash. It is suited for smart card implementation.

7 Computational Number Theory

033701 'On Primality Testing Using Purely Divisionless Operations'
B Arazi, *The Computer Journal v 37 no 3 (94) pp 219 - 222*

The Miller-Rabin primality test can be transformed using Montgomery techniques so that no divisions are required. The key observation is that instead of calculating $X^Q \bmod N$ for a random X, we can just as well calculate $(X.I)^Q \bmod N$ for a suitable scaling multiplier I.

033702 'On Discrete Logarithm Problems over Elliptic Curves with p-divisible Groups'
J Chao, H Ikemoto, K Tanada, S Tsujii, *JW-ISC 93, pp. 99- 104*

This paper compares the isogeny classes of the p-divisible curves over a primary field and its finite extensions, and calculates the probability that a random curve is p-divisible. It is shown that although there is only one isogeny class of the p-divisible curves over a prime field, there are many candidates over a typical extension field.

033703 R̀ecognising units in number fields'
GQ Ge, *Mathematics of Computation v 63 no 207 (July 94) pp 377 - 387*

The author presents a polynomial time algorithm for deciding whether a product of powers of elements in a finite extension K of the rationals is in the unit group of the ring of integers of K.

033704 'On Pjateckii-Sapiro Prime Number Theorem (II)'
CH Jia, *Scientia Sinica (Series A) v 36 no 8 (Aug 1993) pp 913 - 926*
In this paper, the author proves that, for $1 < c < \frac{13}{11}$, there are infinitely many primes of the form $\lfloor n^c \rfloor$.

033705 'Parallel Factorization on SIMD Machines'
YH Kim, CS Jeong, *JW-ISC 93 pp 123 - 132*

The authors present a parallel algorithm for factoring; this uses the quadratic sieve algorithm repeatedly with a divide-and-conquer strategy on SIMD machines. They show that their algorithm is optimal in terms of the product of time and number of processors.

033706 'Carmichael's Conjecture on the Euler function is valid below $10^{10,000,000}$'
A Schlafly, S Wagon, *Mathematics of Computation v 63 no 207 (July 94) pp 415 - 420*

If $\phi(x) = n$, then there is a $y \neq x$ such that $\phi(y) = n$ for all $x < 10^{10,900,000}$. The proof uses prime certification techniques.

033707 'A Fast Algorithm on Addition Sequences'
Y. Tsuruoka, *JW-ISC 93, pp. 114-122*

This paper proposes a fast algorithm for computing exponentiations simultaneously for a given set of exponents.

033708 'More on Squaring and Multiplying Large Integers'
D Zuras, *IEEE Transactions on Computers v 43 no 8 (Aug 94) p 899 - 908*

The author discusses Karatsuba's squaring algorithm, Knuth's variant of it, and the Toom-Cook methods; he then provides a simpler four-way method. Finally, he plots the performance of all the fast squaring and multiplication algorithms.

8 Theoretical Cryptology

033801 'Universally Ideal Secret Sharing Schemes'
A Beimel, B Chor, *IEEE Transactions on Information Theory v 40 no 3 (May 94) pp 786 - 794*

An access structure is universally ideal if there exists an ideal secret sharing scheme for it over every finite domain of secrets. The authors use a theorem of Tutte's that a matroid representable over GF(2) and GF(3) is representable over every finite field to show that if an access structure is ideal over both the binary and ternary domains, then it is universally ideal. They give examples to show that this result is optimal in that neither condition alone is sufficient.

033802 'Bounds on certain multiplications of affine combinations'
J Boyar, F Fitch, KS Larsen, *Discrete Applied Mathematics v 52 (Aug 94) pp 155 - 167*

The authors improve a bound on the number of variables which can contribute to certain combinatorial products used in zero knowledge proofs.

033803 'A scheme to determine the relationship between two users in a hierarchy'
CC Chang, JK Jan, DJ Buehrer, *Computers and Security v 13 no 3 (May 93) pp 255 - 261*

The authors propose a kind of 'secret sharing' scheme in which the relative seniority of any two players can be computed from their shares.

033804 'Parallel Communications Using Pseudo Randomized Routing Algorithms'
IY Chung, CR Kim, CW Lee, SW Kim, *JW-ISC 93 pp 150 - 159*

This paper proposes a pseudo-random routing algorithm, designed to be used to determine the route data takes over a network.

033805 'The knowledge complexity of quadratic residuosity language'
A De Santis, G Di Crescenzo, G Persiano, *Theoretical Computer Science v 132 nos 1-2 (Sep 94) pp 291 - 318*

Many languages related to quadratic residuosity admit noninteractive perfect zero-knowledge proofs. Noninteractive zero knowledge proofs for an even larger class of languages can be converted into round-optimal zero-knowledge proofs.

033806 'On problems with short certificates'
G Farr, *Acta Informatica v 31 no 5 (1994) pp 479 - 502*

The class of languages in NP whose certificate size is bounded by a slowly growing function of the input size include, as complete members, satisfiability and Hamiltonian circuit.

033807 'Error Bounds for the Euclidean Channel Subject to Intentional Jamming'
G Hedby, *IEEE Transactions on Information Theory v 40 no 2 (Mar 94) pp 594 - 600*

The author analyses the anti-jamming effectiveness of multiplying a coded signal by a secret matrix, and calculates the error probability. Some numerical results are given in support.

033808 'Conference Key Distribution System Using Finite Projective Planes'
SJ Kim, JC Ryou, *JW-ISC 93 pp 71 - 80*

The authors propose an efficient identity-based conference key distribution protocol, based on finite projective planes, which requires only $n^{3/2}$ messages.

033809 'Statistical Properties of Finite Sequences with High Kolmogorov Complexity'
M Li, PMB Vitányi, *Mathematical Systems Theory v 27 no 4 (Jul/Aug 94) pp 365 - 376*

The authors show that if a sequence has high enough Kolmogorov complexity, then it is certain to contain every pattern up to a certain length.

033810 'Efficient Secure Broadcast Communications Systems'
M Mambo, A Nishikawa, S Tsujii, E Okamoto, *JW-ISC 93 pp 23 - 33*

This paper studies how to make secure broadcast communication which is efficient in terms of computation and length of total messages sent. The length of the message for n receivers is improved from the $O(n)$ of the previously proposed methods to $O(mn^{-m})$ by using an m-dimensional method.

033811 'Authentication Codes Using Linear Block Codes'
CS Park, *JW-ISC 93 pp 59 - 66*

Two classes of authentication codes based on linear block codes - general and cartesian authentication codes - are considered.

033812 'On Cryptographic Assumptions'
H Shin, *JW-ISC 93 pp 194 - 201*

The security of many cryptosystems is based on several cryptographic assumptions: one-way functions, pseudo-random generators, one-way permutations, etc. This paper discusses the relationships between these functions.

033813 'Authentication Codes Based on Triangular Graphs'
Y Song, K Kurosawa, S Tsujii, *JW-ISC 93 pp 67 - 70*

This paper shows an authentication code based on triangular graphs. In this code, the number of encoding rules is much smaller than that of the balanced incomplete block design authentication code, with a corresponding sacrifice of the substitution cheating probability P_s.

033814 'Rate-Distribution Theory for Shannon's Cipher System with a Noisy Channel'
H. Yamamoto, *JW-ISC 93 pp 142 - 149*

This paper applies rate-distortion theory for Shannon's cipher system with a discrete broadcast channel or a Gaussian wiretap channel.

033815 'Reusing shares in secret sharing schemes'
Y Zheng, T Hardjono, J Seberry, *The Computer Journal v 37 no 3 (94) pp 199 - 205*

The authors provide a secret sharing scheme based on pseudo random functions such as DES in which a shareholder need not be given a new share at the distribution of each new secret, in which the length of secrets can be variable, and which can be adapted to general access structures.

9 Book Reviews

'COMPUTATIONAL AND ALGORITHMIC PROBLEMS IN FINITE FIELDS'
IE Shparlinksii
Kluwer Academic Publishers 1992, Mathematics and its Applications Series, ISBN 0-7923-2057-3

This book is devoted to problems such as polynomial factorisation, finding primitive polynomials, constructing bases, elliptic curve techniques, and applying finite field techniques to various applications. It also covers some of the recent Russian work on algebraic geometry codes, whose consequences for lattice packing and the number of rational points on a curve are explored - important new material which is still not all that widely known.

The book touches on a lot of other material with implications for cryptography, and explores some of these (including permutation polynomials and bounds for linear recurrence relations). However, it is written in a fairly dense style and addressed to the working mathematician, for whom there are a large number of research problems set as challenges in the text. Its main value to a cryptographer is more likely to be as an up-to-date reference to the state of the art in finite fields, and as a survey of the research frontier as of late 1991. There is a bibliography of over 1300 references, many of which are in Russian, and were previously not well known in the West.

'SPREAD SPECTRUM SYSTEMS WITH COMMERCIAL APPLICATIONS'
RC Dixon
Wiley 1994, ISBN 0-471-59342-7

Spread spectrum techniques provide a number of benefits, most notably signal hiding, jamming margin, selective addressing, multiple access, interference rejection and high-resolution ranging. For nineteen years, Dixon was the standard reference work on spread spectrum, but was relatively unknown outside a circle of military specialists. Recent advances in integration, as well as a 1985 decision by the FCC to allow commercial use, have led to rapid growth in commercial applications ranging from GPS to digital cellular telephones; Dixon has just rewritten his book to take account of all this.

The mechanics of spread spectrum systems can be quite complicated. The basic techniques - direct sequence, frequency hopping and time hopping - are simple enough in concept, but there are many complex tradeoffs between error rate, process gain, chip or hop rate, synchronisation, and the various strategies available to participants and opponents; and the linkage between coding, cryptographic and RF engineering aspects is uniquely complicated.

Dixon provides a guide to the underlying theory which should be accessible to a graduate student in either discipline, and goes on to discuss the engineering aspects of satellite uplinks, GPS, military tactical radios and modems, digital cellular radio and vehicle location. There are also hundreds of references which provide a lead into the research literature.

'EDI SECURITY, CONTROL AND AUDIT'
AJ Marcella, S Chan
Artech House 1993, ISBN 0-89006-610-8

Electronic Data Interchange is often touted as the next big application areas for cryptography. Up till now, it has been driven by a number of large companies in particular industries (such as cars and textiles) and by trade documentation. This has led to the proliferation of a number of standards, ranging from the international (EDIFACT) down through the national (ANSI X.12, TDI) to the industry specific (ODETTE). Many of these standards are mutually incompatible, and most do not support cryptography effectively or at all; thus the security of most EDI systems is based on passwords and batch totals.

This environment is an auditor's nightmare, and the authors do their best to explain the various problems which can arise. They also provide a useful roadmap to the standards jungle. Experienced practitioners may find that the book's extremely extensive bibliography is invaluable in tracking down the publications in which various obscure protocols and data formats are specified.

'CHEATING AT CARDS'
B Clough
RMDP Ltd., The Hideaway, Furze Hill, Hove, East Sussex BN3 1PA

This book describes recent problems with the security of credit and debit cards, and fraud against automatic teller machines (ATMs) in particular. The author starts out with a history of plastic money, from its conceptual beginnings among 19th century utopians, through the launch of the four major international brands after the second world war, to more recent developments such as the introduction of ATMs and eftpos and the launch of non-bank credit cards by firms such as General Motors.

There is quite a lot of material on fraud techniques. These range from the earliest attacks on credit card systems through to sophisticated false terminal scams in which unsuspecting customers are lured into inserting their cards and PINs into devices which appear to be ATMs or other banking equipment.

Frauds have implications for customer service, and there have been a number of episodes in which publicity about 'phantom withdrawals' leads to pressure for government or other public action. The book concentrates on recent UK experience through the 1980's, and describes the failure of the banking industry to deal with customer complaints effectively. Although some of the author's criticisms are extreme, his book will be useful for people working in the field of payment systems reliability.

'CARD WORLD INDEPENDENT 1994 USER GUIDE'
Published by Card World Independent Ltd., ISSN 0967-8026

This book has a articles on the credit and debit card scene in the UK, Eastern Europe, Germany, Belgium, Switzerland, India, Singapore and the USA, and half a dozen articles on fraud and related topics. It also discusses the future of smartcards, and mentions a number of new applications such as road tolls and smart telephones.

'SECURE DATA NETWORKING'
M Purser
Artech House 1993, ISBN 0-89006-692-2

This is a general textbook on the security of computer communications. It contains the usual elementary material on cryptography, with presentations of a number of algorithms and protocols of variable quality, and there is material on a number of actual and draft ISO and other standards. However, the book's main contribution is in providing a concise and reasonably up-to-date reference to the main applications which may use or support cryptographic security services, such as X.400, X.500, EDI, SWIFT, ETEBAC 5, and GSM, as well as a guide to a number of fielded and proposed security solutions, from line encryptors through Kerberos to the EC's new SESAME (in fact, this may be the first publication of the actual SESAME protocols).

'COMPUTER COMMUNICATIONS SECURITY'
W Ford
PTR Prentice Hall 1994, ISBN 0-13-799453-2

This book provides a detailed guide to the various international and other standards which specify how cryptographic services ought to be implemented in computer communication networks. It focuses on intersystem, rather than intrasystem, security functions, and on open rather than proprietary architectures.

The first part of the book consists of a tutorial on the basics of computer security, the OSI layer model, cryptographic techniques, authentication mechanisms and access control. This does not go into the details of algorithms or protocols, but provides a systems perspective on what one must do in order to provide (for example) a nonrepudiation service.

The second part then proceeds to discuss the OSI security architecture, and the frameworks developed for authentication, access control and nonrepudiation. It continues to describe the various cryptographic standards, smart card standards, and protocols for use at the various OSI layers. There is extensive material on the X.400 and X.500 standards for electronic mail and directory services, a reasonable amount on current EDI proposals, and finally sections on security management standards and evaluation criteria.

This book lacks the technical detail or application examples which one would expect in a textbook, but is nonetheless the most up-to-date guide to the rapidly proliferating alphabet soup of standards and proposals, and could be a useful reference for anyone learning to navigate through this maze.

'COMPUTER ETHICS
T Forester, P Morrison
MIT Press 1994, ISBN 0-262-56073-9

This is an undergraduate textbook on computer ethics which was first published in 1990, but which has now been updated with information on a number of recent computer security failures ranging from the Internet worm to disputes about automatic teller machine withdrawals. It also covers data protection and intellectual property aspects, and has sections on reliability and liability, and on the effects of automation on the workplace. There is an extensive bibliography.

'AUTHENTIFIKATIONSDIENSTE FÜR SICHERE INFORMATIONS-SYSTEME'
B Klein
Doctoral dissertation, Karlsruhe University, November 1993 (in German)

Klein's thesis elaborates on the issues summarised in her paper on trust-based navigation in distributed systems (**032433**). Her problem is how to reason about complex trust relationships, such as those which arise when reliance is placed on a chain of authentication certificates. After a discussion of authentication and freshness, she investigates the nature of trust, and examines the algorithms which can be used to search for a trusted path in a network. Although these are in general exponential, the search can be speeded up by imposing various structures on the set of authentication servers. She then describes the authentication mechanisms of SELANE, and shows how they could be extended to cope with wide area networking.

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. Subscribers may receive a complimentary electronic version of the journal by notifying us of their Internet email address.

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 subscription for 1995 (volume 4) plus a complete set of 1993 and 1994 back numbers (volumes 2 and 3) at a price of £90 for individual subscribers and £145 for regular subscribers. This back number offer is only available while stocks last. Sorry, volume 1 is completely sold out!

Individual subscription for 1995 - Please debit my VISA/MasterCard £60 □ I enclose a cheque for £60 □ / US$90 □

Individual subscription for all 1993, 1994 and 1995 issues - Please debit my VISA/MasterCard £90 □ I enclose a cheque for £90 □ / US$135 □

Regular subscription for 1995 - Please debit my VISA/MasterCard £95 □ I enclose a purchase order / cheque for £95 □ / US$142.50 □

Regular subscription for all 1993, 1994 and 1995 issues - Please debit my VISA/MasterCard £145 □ 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, Cambridgeshire CB5 9HF, United Kingdom