Computer and Communications

Security Reviews

Volume 4 Number 4 (December 1995) 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 December 1995; and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

WWW 94: Second International World Wide Web Conference, 17–20 October 1994; *selected papers published in 'Computer Networks and ISDN Systems' v 28 no 1&2 (December 1995)*

FSE 94: Second International Workshop on Fast Software Encryption, 14–16 December 1994, Leuven, Belgium; *proceedings published by Springer as Lecture Notes in Computer Science no 1008, ISBN 3-540-60590-8*

IFIP 95: Eleventh international conference on information security, 8–12 May 1995, Cape Town, South Africa; *proceedings published by Chapman & Hall, ISBN 0-412-64020-1*

Usenix Security 95: 5th USENIX UNIX Security Symposium, 5–7 June 1995, Salt Lake City, Utah; *proceedings published by the Usenix Association, ISBN 1-880446-70-7*

Crypto 95: 15th Annual International Cryptology Conference, 27–31 August 1995, Santa Barbara, California; *proceedings published by Springer as Lecture Notes in Computer Science no 963, ISBN 3-540-60221-6*

LISA 95: Ninth Large Information Systems Administration Conference, 17–22 September 1995, Monterey, California; *proceedings published by the Usenix Association, ISBN 1-880446-73-1*

SIGSOFT 95: Third ACM SIGSOFT Symposium for the Foundations of Software Engineering, 10–13 October 1995, Washington DC; *proceedings published as ACM 'Software Engineering Notes' v 20 no 4 (Oct 95)*

We have decided to place postscript versions of this journal in the public domain one year after publication. The goal is to strike a balance between providing a universal service and maintaining enough revenue to cover the costs of publication. Subscribers get paper copies, full latex source code for each issue, and a PGP key which enables them to download and decrypt the source code of all back numbers. The archives can be found at

`ftp.cl.cam.ac.uk/users/rja14`

or

`http://www.cl.cam.ac.uk/users/rja14/#SR`

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

1 Applications and Engineering

044101 'Joining Security Realms: A Single Login for NetWare and Kerberos'
WA Adamson, J Rees, P Honeyman, *Usenix Security 95 pp 157–166*

The authors compare the security mechanisms of NetWare and Kerberos, and discuss ways of providing a single signon capability. The logon protocols are described, as are a number of sniffing, spoofing and Trojan attacks. Solutions using common or distinct pass phrases are described and some of their weaknesses outlined.

044102 'Moving Naval C^{4}I into the Next Century'
RT Allen, SE Arkin, RE Lawrence, *IEEE Communications v 33 no 10 (Oct 95) pp 96–105*

Existing US Naval systems had compatibility problems with those of other forces during joint operations such as Haiti. The Navy architecture is now evolving towards increasing use of open standards including Unix, X and Motif; in addition to commercial LAN encryption products, standard software is being developed to decode, unify and disply sensor information, and there is a style guide for user interfaces. Full multilevel security will be an area of engineering focus, but significant challenges remain.

044103 'Shape of cash to come'
D Austin, *Banking Technology (Sep 95) p 16*

This article summarises a report on EFTPOS that suggests that acceptance of new products depends on the ebb and flow of power in the relationship between banks and retailers. Currently the retailers' investment in embedded magnetic strip equipment is blocking the introduction of smartcards.

044104 'The smart way to fight fraud'
M Baggott, *Scottish Banker (Nov 95) pp 32–33*

The Royal Bank of Scotland introduced photos on credit cards in a 1991 pilot scheme and has now issued 31,500 of them. The total cumulative losses are only £702 as against the £200,000 that would normally have been expected in a card population of this size. Meanwhile APACS, which represents the UK banking industry, is concentrating on smart cards. In industry as a whole, most fraud is done by insiders against companies rather than via technical attacks on payment mechanisms. A new dongle chip is also reported.

044105 'Pseudonymous Medical Registries'
E Boe, *Norwegian Official Report 1993:22 (English language summary)*

This report endorses by a majority a proposal for allowing confidential medical information to be made available to health researchers. The idea is that medical records, with the names and addresses replaced by pseudonyms, would be stored in regional databases. The pseudonyms would be based on dual-control cryptography. To make inference attacks harder, there would be no national database, and access would be limited to approved researchers who travelled to the regional registry in person. The minority of the committee recommended that even such controlled registries be prohibited on the grounds that gathering so much confidential information together would have unpredictable consequences.

044106 'Making ATMs pay'
R Callender, *Banking Technology (Oct 95) pp 54–58*

This article analyses ATM use in Europe by country: Finland has the highest with 37 cash withdrawals per person per year, while Greece is bottom with two. Various ways to market ATMs are discussed; there are also negative factors such as publicity about phantom withdrawals which seriously damaged ATM use in Italy in the 1980's.

044107 'Security Administration in an Open Networking Environment'
KA Casella, *LISA 95 pp 67–73*

Sun has developed a number of security tools that constantly scan the network looking for weaknesses. The one described in this article is designed to ensure that Solaris users are complying with network security policy.

044108 'Security layer added to smartcards'
Computer Fraud and Security Bulletin (Nov 95) p 8

Motorola Scotland has patented a precision sawing technique for removing test circuitry from smartcard chips after the testing is complete.

044109 'Will the NHS get wired?'
M Cross, *Health Services Journal (14/9/95) pp 24–27*

The UK National Health Service is building a nationwide network, but doctors are expressing serious concerns over the confidentiality of patient data and the project is something of a political orphan. Some of the arguments over security and over the status of existing medical datacomms are presented.

044110 'Security within financial information systems'
W de Koning, *IFIP 95 pp 26–40*

The model of Clark and Wilson is extended to make it suitable for application in commercial information systems and in particular from the view point of a financial auditor. The extension includes suggestions for checking the consistency of business data, based on the concept of value streams, segregation of duties and comparison with standards. Recommendations for implementation of the model on midrange computer systems, and systems with distributed processing, are also given.

044111 'Design of a neural network for recognition and classification of computer viruses'
A Doumas, K Mavroudakis, D Gritzalis, S Katsikas, *Computers and Security v 14 no 5 (95) pp 435–448*

The authors describe a neural net based virus classification system they built using a commercially available neural network toolkit.

044112 'WWW-based home banking services in Switzerland: a case study'
R Dratva, *WWW 94 pp 199–208*

Swiss home banking services have traditionally been videotex based. The current reluctance to upgrade to WWW is analysed, and ascribed to the size of the existing investment; the paucity of ISPs in Switzerland; the lack of standards; and the need for banks to modularise their underlying products if they are to compete in a rapidly changing market.

044113 'Information for the Warrior'
JB Evanivsky, *IEEE Communications v 33 no 10 (Oct 95) pp 106–112*

This article describes the US Air Force's communications strategy. It is investing heavily in ATM which it is scaling to speeds as low as 64kbit/sec for tactical systems, and adding security checks for cells with corrupted headers. These systems may be integrated in theatre at the physical, link or network layer, while work is proceedings with Canada, the UK and Australia on creating an ATM based military Internet. The distinctive features of this will include multilevel security and priority dependent on traffic patterns, which will be highly variable. There will be considerable interaction with civilian service and equipment providers, and testing is being done by Air Mobility Command.

044114 'Computer criminals target banks'
Financial Technology International Bulletin v XIII no 1 (Sep 95) p 5

This article describes a number of recent bank frauds including Vladimir Levin's hack of Citibank, a credit card phone fraud and two ATM incidents.

044115 'Sicherheitsmechanismen für rechnerbasierte ISDN-Anwendungen'
D Fox, *Datenschutz-Berater v 19 no 10 (Oct 95) pp 1–4*

The author describes S-CAPI, a security API and supporting services for ISDN. It combines an authentication protocol with the facility to encrypt user data with DES or IDEA.

044116 'Discovery of computer-related fraud left to chance in the UK'
Fraud Watch (Q3 95) p 10

41% of computer related fraud was discovered purely by chance, and computer related losses amounted to 55% of total fraud losses, according to a recent UK survey.

044117 'MIME Object Security Services: Issues in a Multi-User Environment'
JM Galvin, MS Feldman, *Usenix Security 95 pp 217–223*

The authors describe the MOSS protocol, which adds PEM based security to MIME objects, and allows them to be encrypted, signed and concatenated in arbitrary ways. They also discuss some of the implementation issues, such as protecting private keys and ensuring that random number generators are random enough.

044118 'Brainwaves in fraud busting'
T Gandy, *Banking Technology (Dec 95/Jan 96) pp20–24*

The author talks about some applications of neural network techniques to the detection of plastic card fraud. MasterCard and Europay are following VISA's lead, and some aspects of their strategies are described. Their advantage is claimed to be that they de-skill the process of building statistical models; statisticians are few and expensive.

044119 'Security for the future'
T George, *Banking Technology (Dec 95/Jan 96) p 16'*

Security First Network Bank in the USA is the world's first bank to do business solely on the Internet; it uses a mixture of encryption, firewall and trusted O/S technologies and has full Federal deposit insurance.

044120 'Randomness and the Netscape browser'
I Goldberg, D Wagner, *Dr Dobbs Journal no 243 (Jan 96) pp 66–70*

The authors describe how they broke Netscape's SSL implementations by analysing the pseudorandom number generator that supplied session keys. This used a hash of the process id and the time of day in seconds and could be determined by another user of the same machine, while an outsider could guess it.

044121 'Internet trading gathers pace'
T Groenfeldt, H Mackenzie, *Banking Technology (Sep 95) p 5*

US discount brokers are starting to offer services via the worlwide web, and it may rapidly become the standard because it cuts the hardware and support costs of traditional dealing systems. It will also make US brokers easily available to investors worldwide.

044122 'Protecting availability in complex computer environments'
B Gubbins, *Information Management and Computer Security v 3 no 4 (95) pp 20–22*

The author talks about a command centre software product that enables mainframe, Unix and LAN systems to be managed from one console.

044123 'Information security issues in mobile computing'
T Hardjono, J Seberry, *IFIP 95 pp 143–154*

This paper investigates various security issues in mobile computing within the framework of the four categories of mobility, disconnection, data access modes and scale of operation. The paper concludes by proposing to add security as a major category for future developments in mobile computing.

044124 'Two guilty of £120,000 home-made cashpoint fraud'
Information Security Monitor v 10 no 11(Oct 95) pp 1–2

Two men were recently convicted in London of conspiring to defraud banks by extracting customer card and PIN information using a home-made ATM. The ringleaders escaped.

044125 'RAMeX: a prototype expert system for computer security risk analysis and management'
MP Kailay, P Jarratt, *Computers and Security v 14 no 5 (95) pp 449–463*

The authors describe a risk management expert system they have built that classifies computer security threats.

044126 'Sicherheitszertifikät für Chipkarten'
D Kruse, *Datenschutz und Datensicherung (9/95) pp 537–542*

The German information security agency is responding to commercial demand for security evaluation of smartcards based products. Their standards for PIN management and card personalisation are described, as is a Siemens/Nixdorf card that has been evaluated to E4.

044127 'Dynamic Authentication for Smartcards'
J Leach, *Computers and Security v 14 no 5 (95) pp 385–389*

The Europay-MasterCard-Visa consortium's smartcard specification calls for smartcards to possess digitally signed certificates of authenticity, but not to do signatures themselves because of chip costs. The author argues that zero knowledge schemes could make up the dynamic authentication deficit, and discusses the performance parameters of Fiat-Shamir.

044128 'Capital Markets Trading Floors Current Practice'
S Lipson, *LISA 95 pp 35–45*

The contingency planning and redundancy measures used by financial trading houses in the Boston area are described in this article. The emphasis is on duplicating everything in production systems; thus, for example, alternate trading stations are fed from different LANs and servers, and half of the communications circuits go to each of two exchanges (each having dial backup to the other). In the event of failure, dealers share screens; this is preferred over internally redundant systems such as Stratus for cost, flexibility and reliability reasons.

044129 'SPM: System for Password Management'
MA Looper, *LISA 95 pp 149-170*

The author describes a new password manager developed at USC for Unix systems. It adds syntax checking, password aging, and challenges for auxiliary passwords such as the user's mother's maiden name that can be invoked according to some pattern. It also provides a uniform logon interface for multiple versions of Unix.

044130 'Card fraud nets Esc6 billion'
F Mollet, *Cards International (22/9/95) p 3*

A criminal removed and copied a chip from a smartcard that is used to give Portuguese farmers rebates on fuel. He conspired with petrol stations who registered other fuels sales to the bogus cards in return for a share of the proceeds. The fraud, which took place in February/March 1995, is reported to have netted a large sum of money and 190,000 litres of fuel.

044131 'WAN-hacking with Autohack — Auditing Security behind the Firewall'
A Muffett, *Usenix Security 95 pp 21–34*

Configuration errors accumulate in large systems, and opponents may either start inside the firewall or get through it somehow. This motivated the development of

Autohack, a bulk probing tool for wide as opposed to deep auditing; it looks for simple flaws such as promiscuous trust in large numbers of machines on a network. The main lesson learned from this exercise is that network security only evolves in a hostile environment.

044132 'Keeping an eye on the counterfeiters'
J Newton, *Cards International (27/10/95) p 13*

An Interpol General Assembly held at Beijing in October called for all countries to make card counterfeiting illegal, and give card payments the same protection as cash.

044133 'Using the Internet — A Guide for Auditors'
A Oliphant, *Computer Audit Journal — supplement to Computer Audit Update (9/95) pp 1–8*

This article provides a list of Internet resources for internal auditors.

044134 'Privacy, Anonymity and Accountability'
C Oliver, *Computers and Security v 14 no 6 (95) pp 489–490*

The author discusses the meaning of anonymity and accountability in the context of a project to computerise emergency medical records. Names were replaced by numbers so that subsequent use of the records in care outcomes studies would not disclose any personal information.

044135 'Electronic Data Interchange — What are the Security Measures?'
S Ongetta, *Network Security (Aug 95) pp 16–19*

The author describes some common weaknesses of EDI systems.

044136 'A Fast Homophonic Coding Algorithm Based on Arithmetic Coding'
WT Penzhorn, *FSE 94 pp 329–345*

The author describes a homophonic coding scheme designed to cut the redundancy in plaintext prior to encryption.

044137 'Password Files'
TJ Pope, *Dr Dobbs Journal no 243 (Jan 96) pp 72–76*

The author presents source code and explanation of a routine to protect passwords by one-way encrypting them with MD5.

044138 'Improving the Trustworthiness of Evidence Derived from Security Trace Files'
E Pozzetti, V Vetland, *Usenix Security 95 pp 187–197*

The authors discuss some of the issues involved in making system trace files usable as evidence. The relevant entries are part of very large files, yet editing them can destroy their value. They describe a tool designed to extract relevant data in a repeatable way.

044139 'Post-2000 Tactical Communications Systems for NATO'
WC Quan, ER Sive, *IEEE Communications v 33 no 10 (Oct 95) pp 113–118*

NATO is planning its communications architecture for the next century to enable units of different nationalities to be welded together into an army corps. It is based on ATM using local fibre systems where mobility is not paramount; these can be scaled over wider areas and connected to mobile units by a variety of radio technologies from EHF through meteor burst. Subscriber bandwidths will be limited to enhance resilience, while AI-based management of AI and other services will be located at the subsystem level.

044140 'SYSTEMS 95: Sonderschau "Chipkarten und Sicherheit" '
H Reimer, *Datenschutz-Berater v 19 no 11 (Nov 95) pp 4–6*

Germany has recognised digital signatures for some legal purposes since 1993 and this report on a smartcard exhibition describes a project, MailTrusT, that will enable German companies to bring products to market using public key technology. The central element is a policy certification authority, which will act as the root CA; its design has been influenced by the SESAME and PASSWORD projects.

044141 'Multi-platform Interrogation and Reporting with Rscan'
N Sammons, *LISA 95 pp 75–87*

This describes a tool developed at Colorado State University to scan Unix machines remotely for security flaws and that is now available for free.

044142 'Auctioning by satellite using trusted third party security services'
P Sanders, S Rhodes, A Patel, *IFIP 95 pp 205–222*

The work is motivated by a new auctioning service in Europe for livestock using satellite broadcast. Security requirements include integrity of data and purchasing decisions, the anonymity of authenticated bidders, and non-repudiation; a system that efficiently provides these requirements is suggested. It is based on the use of digital signatures and trusted third parties forming a hierarchy based on X509 mechanisms.

044143 'Communications for the Digitized Battlefield of the 21st Century'
PF Sass, L Gorr, *IEEE Communications v 33 no 10 (Oct 95) pp 86–95*

This article describes the US Army's communications strategy, which is oriented towards increasing use of civilian capabilities. both for infrastructure and for equipment during rapid force build-up, as happened prior to Desert Storm. That campaign also emphasised the need to communicate across the traditional command hierarchy, and the need for field units to filter vast quantities of data. The vision is 'battlespace domination through availability of the right information ... while denying the same to the enemy'; the goal is to keep as many personnel as possible in the continental USA; the plan is to merge the existing voice and data networks, use ATM/ISDN, Internet and satellite cellular technologies. Key products include the Speakeasy radio (**042155**) and an ATM cell encryptor under development by the NSA.

044144 'A New Perspective on Firewalls'
EE Schultz, *Network Security (Oct 95) pp 13–17*

Firewalls are disproportionally represented in security product ranges and in conference papers, where the debate had got to the point of nitpicking. However, although generally helpful, firewalls have bad effects: providing a false sense of security, degrading performance and becoming a single point of failure for both security and communications. Testing is often cursory; firewalls are increasingly attacked, yet few are monitored well enough to detect even massive numbers of intrusion attempts. In the words of General Patton, "Forts are monuments to those stupid enough to build them". Future firewalls, to be effective, must be smarter and more flexible; they may even take the form of network agents.

044145 'Authentication product where fibres hold key to identity'
W Sipman, *Fraud Watch (Q3 95) pp 6–7*

A new marking product is based on embedding random fibres in a small plastic window, that may be installed in a payment card, product label or other token. The fibre pattern is read from two different angles giving a claimed diversity of 10^{36}. The idea is a low cost token that is expensive to forge.

044146 'Digital Decoder Ring'
Smart Card News v 4 no 9 (95) pp 170–171

Dallas Semiconductor has embedded a smartcard-compatible chip in a signet ring; the product is being aimed at computer user authentication.

044147 ‘Electronic Purses — A Comparative Review’
Smart Card News v 4 (95): part 2 — no 9 pp 166–169; part 3 — no 10 pp 186–189; part 4 — no 11 pp 206–209

This series of articles continues from **043155** and covers smartcard payment systems that exist or are planned in Switzerland, Taiwan, Australia, Indonesia, Lebanon, Singapore, South Africa, Spain and Thailand.

044148 ‘From Here to There’
Smart Card News v 4 (95): part 8 — no 9 pp 176–179; part 9 — no 10 pp 196–198; part 10 – no 11 pp 216–218

This article describes smartcard-to-card-reader communications protocols and the means of switching between them.

044149 ‘Tip von Urmel’
Spiegel magazine no 38 (11/9/95)

A hacker called Urmel tipped off Deutsche Telekom that it was possible to make phone cards which gave unlimited free calls. He had discovered this by putting a laptop between a card and a phone to analyse the traffic. However, Telekom’s experts refused to believe him; eventually he exploited his knowledge by selling handmade chip cards in brothels and hostels for asylum seekers, and was arrested. It is also reported that health cards can be manipulated.

044150 ‘The need for decentralization and privacy in mobile communications networks’
F Stoll, *Computers and Security v 14 no 6 (95) pp 527–539*

The author describes the overall architecture and security functionality of GSM, including the key management hierarchy and the generation of temporary mobile subscriber IDs. He describes a number of security weaknesses; for example, only the air link is encrypted, and the handover procedures facilitate the profiling of subscriber movements. In any case, a large amount of personal information is stored in the network, and this might cause problems for German data protection law. He calls for A3/A8 to be published, and suggests that the next generation of mobile systems (UMTS) should use a different mechanism: a called user would be paged by broadcast, and then call the relevant exchange, using an anonymous prepaid token, if she wished to connect.

2 Operating System and Database Security

044201 'A Domain and Type Enforcement UNIX Prototype'
L Badger, DF Sterne, DL Sherman, KM Walker, SA Haghighat, *Usenix Security 95 pp 127–140*

The authors discuss an access control policy called Domain and Type Enforcement (DTE) whose goal is to partition Unix systems effectively into domains and thus strengthen them against penetration attacks. There is a high level language in which other security policy details can be expressed, as well as support for NFS and TCP/IP. A prototype built at TIS is described.

044202 'Using the Domain Name System for System Break-ins'
SM Bellovin, *Usenix Security 95 pp 199–20*

The author describes DNS and a number of attacks that can be mounted when part of it is subverted; he also discusses how to overcome most of the current or proposed defences. Only cryptographic authentication provides a real solution, though some protection can be obtained against weak attacks by comparing the forward and reverse mapping trees and being careful with cacheing. This paper's publication was in fact held up for four years, but the attacks described are now well known to hackers.

044203 'Information security and the Internet'
GR Doddrell, *Information Management and Computer Security v 3 no 4 (95) pp 15–19*

The author talks about a number of possible firewall configurations.

044204 'Safe use of X window protocol across a firewall'
BL Kahn, *Usenix Security 95 pp 105–116*

The author discusses how to use X safely across a firewall and describes an X gateway built by MITRE. This is a proxy server that permits outside clients provided they do not interact with other X clients or the resources created by them. The access control policy is described in some detail.

044205 'AS/400 system access monitoring'
K Lester, *Computer Audit Update (dec 95) pp 9–14*

This article describes the access control mechanisms of OS/400 version 2 release 3, discusses what can go wrong, and recommends what an auditor should do. The actions focus on the control of service tools and privileged utilities.

044206 'On the validity of the Bell-LaPadula model'
EEOR Lindgreen, IS Herschberg, *Computers and Security v 14 no 4 (95) pp 317–333*

The authors rehearse a number of objections to the Bell-LaPadula model, from technical observations by McLean and others to the fact that it is not very relevant to commercial concerns.

044207 'MCF: a malicious code filter'
RW Lo, KN Levitt, RA Olsson, *Computers and Security v 14 no 6 (95) pp 541–566*

The authors describe a tool developed at UCD for spotting malicious code from its telltale signs, such as file system calls coming from device drivers in which viruses may have lodged. They discuss possible stealth countermeasures that virus writers could take, and well-behavedness properties that could detect or contain stealth viruses.

044208 'Providing Policy Control Over Object Operations in a Mach Based System
SE Minear, *Usenix Security 95 pp 141–155*

The author describes a modified Mach kernel that can support multiple security policies without large changes to the kernel or applications. The goal was to separate policy from enforcement. The main innovation was a way to control the use of transferred port rights by adding identification to kernel objects, extra access checks in the kernel, and an interface to an external security server. A type enforcement policy was implemented in a Unix system running over Mach and performance figures are reported.

044209 'An Architecture for Advanced Packet Filtering'
A Molitor, *Usenix Security 95 pp 117–126*

The author discusses an architecture to support packet filtering within a network rather than leaving all the controls at the boundary and allowing promiscuous trust inside. This a language that defines the circumstances in which various filters get invoked, and is being developed to allow filtering on TCP state.

044210 'Improving the security of medical database systems'
G Pangalos, D Gritzalis, M Khair, L Bozios, *IFIP 95 pp 11–25*

A security policy for medical databases combining mandatory and discretionary access control is proposed. Access is by passing through three layers: identification, a role-based discretionary model and finally a multilevel mandatory model. An experimental implementation of the model in a hospital is also reported.

044211 'Exu — A System for Secure Delegation of Authority on an Insecure Network'
K Ramm, M Grubb, *LISA 95 pp 89–93*

Large and complex systems often rely on many semiskilled local administrators, and often a sensitive task must be delegated to one of them. It may not be desired to give them unrestricted access, yet current systems are usually inflexible: either the administrator has superuser/root access or not. A system was therefore developed to sit on top of Kerberos and provide restricted delegation of sensitive functions.

044212 'Open System Security: Traps and Pitfalls'
J Reid, *Computers and Security v 14 no 6 (Dec 95) pp 496–517*

This article gives a detailed overview of the weaknesses of Unix security, with particular reference to SunOS v 4. It covers poor defaults, such as the large number of files that are owned by the superuser yet need not be, configuration problems with demons such as inetd, bugs in library routines and setuid shell scripts. It also discusses the recurrent problems with sendmail, portmap, NIS, NFS, X, WWW, MIME and DNS; password cracking; session stealing and routing attacks; firewall defeats; and the BSD print spooler bug.

044213 'An Application-Access Security Model'
M Robinson, *Dr Dobbs Journal no 237 (12/95) pp 82–88*

The author describes a generic access control model for object oriented systems in which a security handler interacts with all windows, child windows, buttons and other controls in a consistent way. Source code listings for an implementation in Powerbuilder are given.

044214 'File-Based Network Collaboration System'
T Takahashi, A Shimbo, M Murota. *Usenix Security 95 pp 95–10*

The authors describe a system for supporting cooperative work. It permits encrypted files to be edited and merged without decryption in the server; this is based on cipher feedback mechanisms.

044215 'DNS and BIND Security Issues'
P Vixie, *Usenix Security 95 pp 209–216*

The author describes a number of common attacks using DNS. Many of these depend on flaws in BIND, some versions of which omit important checks. He discusses various ways in which the situation might be improved; meantime he advises using the most recent version of BIND available for any given system.

3 Security Management and Policy

044301 'Making It a Policy to Protect Yourself'
M Alexander, *Datamation (1/12/95) pp 59–62*

This article sets out a model infosec policy statement for distribution to company employees.

044302 'Physical Layer Network Security: what your LAN can do for you'
DW Barnes, *Network Security (October 95) pp 17–19*

The author discusses how a LAN's configuration affects the cost of attacking it.

044303 'Comment on Biometrics Papers'
R Courtney, *Computers and Security v 14 no 5 (95) pp 373–375*

The author dismisses much writing on computer security management as concerning itself with the interesting but relatively unimportant problem of stopping outside access. The real problem is abuse by insiders, and often abuse resulting from ignorance, laziness, carelessness or poorly designed systems as much as from malice. He is also pessimistic about the possibility of getting realistic threat assessments by talking to company managers.

044304 'The New Law for the Protection of Software'
D Davis, *Computer Audit Journal — supplement to Computer Audit Update (9/95) pp 9–17*

This article describes the EU directive on copyright and the Copyright (Computer Programs) Regulations 1992. The users' rights of backup, decompilation and copying for interoperability reasons may not be excluded by software vendors.

044305 'A Risk Control Strategy for Corporate Computer Operations'
N den Boer, *Computer Audit Journal — supplement to Computer Audit Update (9/95)*

This describes a risk management methodology used by Shell in the Netherlands.

044306 'Security environment reviews'
GR Doddrell, *Information Management and Computer Security v 3 no 4 (95) pp 3–14*

The author gives an extensive guide to minimising the harm likely to be done to computer equipment by a number of environmental factors such as fire, flood, sabotage, utility disruption, EMI and physical attack.

044307 'Ecash boon to launderers'
Financial Technology International Bulletin v XIII no 1 (Sep 95) p 12

A recent report on the law of digital cash points out that if it is anonymous, it could leave little for investigators to work with; but if not, there could be data protection problems. For example, from 1998 it might be illegal to send it from Europe to countries like the USA whose data protection laws do not meet EU standards.

044308 'Electronic purse technology ready to take a share of hard cash markets'
Financial Technology International Bulletin v XIII no 3 (Nov 95) p 4–5

This article surveys electronic cash systems in Finland and elsewhere; it also relates testimony by US officials to Congress to the effect that regulation of electronic cash would be premature.

044309 'Establishing an effective continuity strategy'

KJ Fitzgerald, *Information Management and Computer Security v 3 no 3 (95) pp 20–24*

The author talks about the management aspects of continuity planning, such as leadership, discipline, planning and the need to be realistic about scenarios.

044310 'Security and data integrity for WANs and LANs'
KJ Fitzgerald, *Information Management and Computer Security v 3 no 4 (95) pp 27–33*

The author talks about some of the products and management actions that can be used to reduce risk in distributed computer systems.

044311 'Telearbeit: Der Arbeitsplatz zu Hause'
H Gliss, *Datenschutz-Berater v 19 no 7-8 (July 95) pp 5–7*

This article discusses the data protection and security problems of teleworking such as the difficulty that organisational data protection officers have in exercising the necessary oversight over such processing.

044312 'Technologically Enabled Crime: Shifting Paradigms for the Year 2000'
S Gordon, *Computers and Security v 14 no 5 (95) pp 391–402*

The author discusses the social and epidemiological factors of virus transmission; an important role is played by virus distribution sites (often bulletin boards) from which people without the skills to write self-replicating code themselves can download viruses for release. Such parasitic behaviour greatly enhances the effect that the few competent authors would otherwise have. Hacking tools still appear to be limited to small groups of competent people, but this may be starting to change.

044313 'Export of Cryptographic Information from the US: A Brief Look at the Problem'
W Hancock, *Network Security (Oct 95) pp 9–11*

The author talks about crypto export and argues that a relaxation of the rules would lead to crypto being built into network products.

044314 'Internet Hacking Resources'
W Hancock, *Network Security (Dec 95) pp 11–15*

The author lists the names of dozens of alleged 'hacker' web sites, mailing lists and bulletin boards without giving contact details for most of them.

044315 'Recent History of Known Network Breaches'
W Hancock, *Network Security (Nov 95) pp 6–9*

The author describes recent attacks on MCI, Continental, Citibank, Florida State University, General Electric, the New York Times, MGM and Intel.

044316 'Internet: A Certain Insecurity'
B Herschberg, ER Lindgren, *Network Security (Sep 95) pp 16–19*

This points out that a January 1995 CERT advisory on IP spoofing reported weakness that had been described by Morris and others years before.

044317 'Disasters: real, potential and near misses'
S Hinde, *Computer Audit Update (Dec 95) pp 1–3*

The authors describes computer failures that have recently affected a number of organisations, including a bank, an insurance broker, a charity, a food producer and others.

044318 'Flying a kite for computer security'
S Hinde, *Computer Audit Update (Oct 95) pp 1–3*

The British Standards Institute's "Code of Practice for Information Security Management" (BS7799) specifies a minimum baselines of controls, that are described in this article, plus a number of optional extras.

044319 'Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology'
J Hitchings, *Computers and Security v 14 no 5 (95) pp 377–383*

This journal version of **033332** reports a survey of 132 British organisations that returned questionnaires on computer security; many of them admitted inadequacies.

044320 'Encryption policy for the global information infrastructure'
L Hoffman, *IFIP 95 pp 63–78*

It is argued that cryptology policy should not just deal with the technological side of encryption algorithms but also political and administrative issues. The paper presents a survey of U.S. policy issues including digital telephony initiative, the clipper chip key escrow encryption initiative, export control and law enforcement and civil liberties issues. It concludes that it will be a challenge to address these issues in a timely and open fashion.

044321 'Information as an asset — the board agenda'
NW Horne, *Computer Audit Update (9/95) pp 5–11*

The Hawley Committee, an eminent UK committee chaired by a senior businessman, has devised a list of things that a public company's board of directors should do to discharge its responsibilities for the business's information assets.

044322 'New Operating Systems and Old Viruses'
J Hruska, *Computer Fraud and Security Bulletin (Nov 95) pp 11-14*

The author describes the effect of DOS viruses on operating systems such as Windows and OS/2; often they fail to replicate. However this is no reason for complacency, as the spread of data communications and the arrival of macro viruses for products such as WinWord provide plenty of opportunities for malicious code writers.

044323 'Security in group applications: Lotus Notes as case study'
A Hutchison, *IFIP 95 pp 190–204*

This paper identifies security requirements for applications supporting co-operative work by giving seven attributes of a group that determine its nature and the required protection mechanisms. It examines Lotus Notes as a case study and gives a list of its strengths and weaknesses.

044324 'US computer crime on the increase'
Information Security Monitor v 10 no 12 (Nov 95) pp 1–2

This article reports a survey of computer crime carried out on 200 US firms.

044325 'Datenschutz bei der Verwendung von e-Mail — Forschung und öffentliche Verwaltung'
F Jendro, *Datenschutz und Datensicherung (10/95) pp 588–592*

Data protection law can affect machines that process electronic mail. This is obvious if it is sent in the clear, but even if it is encrypted, the headers contain information about the identities of the sender and the receiver, and these fall within the law's scope. Networking can thus bring about a qualitative change in the legal aspects of data processing.

044326 'Kontrolle der modernisierten Verwaltung durch die Gerichte'
W Jöhnk, *Datenschutz und Datensicherung (11/95) pp 664–665*

One of the most serious problems facing constitutional lawyers is that the computerisation of administrative files makes it hard to get access to government documents in administrative law cases. Electronic records are easy to manipulate, and may in any case contain information about third parties to the dispute which may not be revealed under data protection law.

044327 ‘Cryptology in Cyberspace’

M Johnson, *Cryptologia v XIX no 4 (Oct 95) pp 392–396*

This article lists a number of Internet crypto resources, and describes some encryption products that are available for free download.

044328 ‘Datenschutzbeauftragte drängen den Gesetzgeber’

U Jurgens, *Datenschutz-Berater v 19 no 12(Dec 95) pp 8–10*

German state and federal data protection authorities decided in November to request the government for stronger laws in a number of areas, particularly telecommunications reform and health cards. The former should limit the use of caller ID; the latter will include the patient’s right to determine which personal health information, if any appear on the card, the right for patients to refuse to carry a card and not thereby suffer discrimination, and a prohibition against the creation of any new central aggregates of data as a result of automation.

044329 ‘Justification of Decisions in Auditing’

L Koonce, U Anderson, *Journal of Accountancy Research v 33 no 2 (Autumn 95) pp 369–382*

The authors performed a controlled experiment in which auditors either were or were not told in advance that their audit decisions would be subject to review, and the managers of the auditee companies presented either no evidence, good evidence or contradictory evidence to support their spending explanations. Both of these variables were found to affect the quantity, but not the nature, of the documentation that the auditors kept to support their findings.

044330 ‘Controls in the Next Millenium: Anticipating the IT-enabled Future’

AR Krull, *Computers and Security v 14 no 6 (Dec 95) pp 491–495*

The author discusses the organisational basis of control failure. Many organisations are struggling to become less bureaucratic, to shed layers of management (and associated controls) and build employee trust, in order to get staff to use their initiative; yet this can be damaged by computer security and other controls sending contradictory messages. This conflict may help frustrate attempts at corporate reform, and can also negate much of the security benefit as well. People must use controls willingly; if they just intimidate people into compliance, they will not be particularly effective.

044331 ‘Der Schutz des Fernmeldegeheimnisses auf den Telekommunikationsmarkt’

H Kubicek, *Datenschutz und Datensicherung (11/95) pp 656–663*

The author describes the legal situation of telephone taps in Germany. Access is granted to both prosecutors and intelligence services, but control is being made more complex by forthcoming privatisation. This led to a controversial surveillance regulation being introduced in May 1995.

044332 ‘Security Considerations of Network Outsourcing’

J Leach, C Brown, *Network Security (Nov 95) pp 10–14*

The authors describe a number of points that it is prudent to tie down contractually when outsourcing a network, such as incident management, emergency response and reporting lines.

044333 ‘Integrity in Information Systems — Executive Summary’

W List, R Melville, *Computers and Security v 14 no 4 (95) pp 295–301*

The authors summarise a document they have written for IFIP on hierarchies of controls in business information systems.

044334 'Combatting the Spread of Calling-Card and Telephone Fraud'
M McCormack, *Computer Fraud and Security Bulletin (Nov 95) p 19*

This article reports the views of AT&T's security manager including a call for international cooperation on telephone calling card fraud.

044335 'Control Concepts — Who's Buying?'
K McLean, *Computer Audit Update (Oct 95) pp 3–14*

The author discusses how to go about marketing an organisational security programme.

044336 'Cyberlaw — legal issues online'
N Miller, *Computer Audit Update (Dec 95) pp 4–9*

In England and Wales, a number of contracts such as guarantees, sale of land and transfer of copyright may only be done in writing. Since telegrams count as writing, electronic mail might do too, but the law still needs testing.

044337 'Audit Commission Fifth Triennial Survey'
A Mills, T Richards, L Kappelman, *ACM SIGSAC v 13 no 4 (Oct 95) pp 10–13*

The authors summarise a 1994 survey by the UK government's audit commission of 537 incidents of computer fraud and abuse reported during 1991-1993.

044338 'A methodology to include computer security, safety and resilience requirements as part of the user requirement'
DNJ Mostert, SH von Solms, *Computers and Security v 14 no 4 (95) pp 349–364*

The authors present a way to identify constraints on processing and to incorporate them in the user requirements specification when systems are built. It is illustrated by a discussion of a hypothetical runway control system for an airport.

044339 'Security should pay: it should not cost'
WH Murray, *IFIP 95 pp 3–10*

The author argues that the real choice an organization has about security costs is whether to pay in a regular, orderly manner or in an irregular, unpredictable way. The price paid for security should not be more than the cost of tolerating failures. The rest of the paper discusses various security measures and argues that effectiveness and efficiency are inversely related and the cost of security is determined by how wisely money is spent.

044340 'Common Criteria for IT security evaluation — update report'
IP Overbeek, *IFIP 95 pp 41–49*

The paper introduces the Common Criteria (CC) and reviews its current status and future direction. It discusses its usage, goals, scope, boundaries, structure and concepts. The criteria' foundations are protection profiles, security targets, assurance levels and functionality classes which are all briefly discussed. They are undergoing a review process and a definitive workplan for its completion will depend on the comments received.

044341 'A new framework for information security to avoid information anarchy'
DB Parker, *IFIP 95 pp 155–166*

The paper argues insufficiency of the three elements confidentiality, integrity and availability for information security and suggests addition of three more elements of authenticity, utility and possession. The need for these six elements is justified by reviewing six infosec loss scenarios in which each loss is explicitly covered by one and only one of the elements. It is envisaged that with advance in information technology, more elements may be needed to cover additional types of losses.

044342 'Managing security on an open network'
R Perry, *Information Security Monitor v 10 no 11 (Oct 95) pp 5–7*

The author describes the security management philosophy of the UK banking group 3i, together with some of the protective measures in place.

044343 'The Fortress Mentality Part IV: Telecomputing, Telecommuting and Serving Remote Customers'
P Peterson, *Network Security (Sep 95) pp 12–14*

The author talks about a number of authentication mechanisms.

044344 'Data Interchange and Legal Security — Signature Surrogates'
K Rihaczek, *Computers and Security v 14 no 4 (95) pp 287–293*

There are many ways in which a system that has been successfully evaluated under ITSEC could still cause legal problems for its owners. It might provide perfect security against outsiders, while not protecting them from each other; or it might be too hard to use; or the evidence it produced might be too hard for the court to understand. A number of requirements for signatures are described; for example, the signer must be able to see the material as he signs it, he must be aware that he is changing his legal status, the act of signing should be system independent, and everything needed to verify the signature must be in the public domain. He argues that the necessary legal framework and human interface rules should be defined by the EU.

044345 'Datenschutz in Sicherungsinfrastrukturen offener Telekooperation'
A Roßnagel, *Datenschutz und Datensicherung (10/95) pp 582–587*

Building public key management structures will involve collecting significant personal information about individuals and making it available. There will therefore be data protection problems that should be considered before rushing to implement certification authorities. The legal aspects are discussed in this article; it will not be sufficient simply to pass a law giving force to digital signatures.

044346 'ITS-spezifische Absicherung von Geschäftsprozessen'
W Schäfer, R Muth, *Datenschutz und Datensicherung (10/95) pp 604–606*

It is important to involve the IT security team in business process reingeneering, even if only to conduct a risk analysis.

044347 'Unify Security to Speed Development'
R Schreibner, *Datamation (15/11/95) pp 78–82*

This article describes an organisation that was motivated to migrate its systems to DCE after it found that access controls had been embedded in the application code of 45 separate systems.

044348 'The Ethical and Legal Quandary of Email Privacy'
JC Sipiar, BT Ward, *Communications of the ACM v 38 no 12 (Dec 95) pp 48–54*

The authors discuss employers' and employees' attitudes to email monitoring and discuss some of the legal aspects. For example, failure to monitor might be construed as a failure to protect trade secrets under SEC rules. However the overall legal position is still not settled, at least in the USA.

044349 'Business continuity planning and service level agreements'
R Smith, *Information Management and Computer Security v 3 no 3 (95) pp 17–19*

Business continutity can only be incorporated effectively in service agreements by incorporating backup and audit in the contract and testing extensively.

044350 'Multimedia und Datenschutz'
F Stoll, *Datenschutz-Berater v 19 no 10 (Oct 95) pp 8–10*

This article reports a conference on data protection in multimedia hosted by the Berlin data protection registrar in August 1995. Multimedia systems introduce a host of new problems from media privilege through the definition of broadcasting and the sheer size of the objects involved to the ease of manipulation. Integrating security measures effectively is extremely hard.

044351 'DNA-Analysen und ein Recht auf Nichtwissen'
K Stumper, *Datenschutz und Datensicherung (9/95) pp 511–517*

DNA testing creates an interesting new protection category — personal information about an individual, that he can only learn from third parties, and which in some cases he might strongly prefer not to know. The fact that the third party learns the facts first may cause problems with some data protection laws.

044352 'Chipkarten — viel Komfort und viele Probleme'
J Vahle, *Datenschutz-Berater v 19 no 7–8 (July 95) pp 9–10*

Germany's data protection supremo commented on the phenomenal growth of chipcard applications in his 1993-94 report. The three main problems he perceived were the growing number of PINs that people had to remember, the lack of controls on back-end processing of data, and the fact that the mere presence on a shared chipcard of certain applications (such as dialysis management) would reveal protected information about the individual to the owners of other applications (such as banks).

044353 'Information security accreditation — The ISO 9000 route'
R von Solms, LR Meyer, *IFIP 95 pp 50–62*

The importance of international standard for certification schemes is argued and ISO 9000 certification for quality assurance is discussed. The aim of ISO 9000 is to provide a set of generic standards that apply to all phases of design, development, installation and servicing of software and hardware products. The paper discusses structure and security issues addressed in the standard and notes that the main shortcomings of the standard is not giving enough attention to information security management.

044354 'An object-oriented approach to an IT risk management system'
G Wahlgren, *IFIP 95 pp 79–86*

This paper discusses the need for an IT risk management tool that can automatically advise on measures to be taken when a change occurs. It is argued that present systems are too inflexible and using an object-oriented approach can increase flexibility while reducing risk.

044355 'Legal lightweights'
I Walden, *Banking Technology (Oct 95) p 22*

In the UK, the 1882 Bills of Exchange Act insists that cheques be cleared in paper form, and this has held up electronic commerce. Promised reform has not been forthcoming from the government. On the general topic of electronic evidence, there may be a move for deciding the worth of evidence during rather than before the main hearing.

044356 'Seward's other folly: the fight over America's first encrypted cable'
RE Weber, *Cryptologia v XIX no 4 (Oct 95) pp 321–348*

America's first encrypted transatlantic cable was instrumental in getting French troops out of Mexico in 1866, but was inefficient and expensive; a message of 780 words became 1237 number groups and 88 control characters, contained over 35 transmission errors and cost $19,540.50. This led to the first shake-up of government cryptography there for half a century.

044357 'Managing User Perceptions of Email Privacy'
SP Weisbund, BA Reining, *Communications of the ACM v 38 no 12 (Dec 95)*

The authors discuss a number of factors that affect the attitudes of both employers and employees to email privacy; for example, experience of typing in passwords may create the impression that no-one is watching when matter is typed into a terminal. Possible corporate policies range from right-to-monitor to hands-off; the choice will depend on management style and will in turn have knock-on effects that will depend on the explicitness and enforcement of the policy.

044358 'Information Security Technology? Don't Rely on It — A Case Study in Social Engineering'

IS Winkler, B Dealy, *Usenix Security 95 pp 1–5*

The authors report attempts to penetrate the computer security of client organisations by persuading staff to reveal passwords and other sensitive information over the telephone. Such techniques are routinely used by industrial spies and hackers. By impersonating company officials, the authors built up knowledge of procedures and structures, and finally obtained access at a typical cost of three days' work, with very little risk.

044359 'New Developments to combat computer crime'

K Wong, *Datenschutz und Datensicherung (9/95) pp 543–547*

The author talks about various topics in computer and communications security.

044360 'Background checks for employees in computer-related positions of trust'

CC Wood, *Information Management and Computer Security v 3 no 5 (95) pp 21–22*

In the US, it may be imprudent for firms not to do background checks on trusted employees, thanks to a 1984 court ruling.

044361 'Information Security Problems as Evidence of Management Failures'

CC Wood, *Computer Fraud and Security Bulletin (Nov 95) pp 14–16*

Most security problems are caused by mismanagement, and overzealous cost cutting in particular stops continuing education, hinders contingency planning and wears down staff. Even internal auditors may be afraid of the sack.

044362 'The Charles Cresson Wood file'

CC Wood, *Information Management and Computer Security v 3 no 4 (95) pp 23–26*

The author talks about security management problems.

044363 'A Holistic Approach to IT security'

L Yngstrom, *IFIP 95 pp 98–112*

This paper presents a 'systemic-holistic approach' developed and used for IT security in an academic educational program. It is based on 'general systems theory', 'soft system methodology' and 'general living system theory'. The approach offers a meta model within which particular views on IT security may be investigated and allows people to study various alternatives.

4 Formal Methods and Protocols

044401 'Feature Interactions in the Global Information Infrastructure'
AV Aho, ND Griffeth, *SIGSOFT 95 pp 2–4*

The growing functionality in telecommunications networks often leads to clashes that force the compromise of security and other features; one example is that between unlisted numbers and calling number identification. In general, the environmental assumptions underlying many features are eroded as systems evolve and eventually they no longer work. designers should specify services in a platform-independent way and this may necessitate the use of formal methods.

044402 'Programming Satan's Computer'
RJ Anderson, RM Needham, *Computer Science Today — Recent Trends and Developments, Springer LNCS v 1000 pp 426–440*

The authors provide an overview of cryptographic protocols at the level of a general scientific audience. They describe some practical cases in which protocols failure has led to real attacks on banking, electricity meter and pay-per-view systems; they provide new attacks, on the wide-mouthed frog and on a protocol of Woo and Lam; and discuss the relative merits of protocol logics and robustness principles. Designing crypto protocols is called 'programming Satan's computer' because it amounts to writing a program to run on a machine that will give the the most subtle wrong answer at the most inconvenient moment. The guiding principle of this black art is to make as many things explicit as possible.

044403 'Robustness Principles for Public Key Protocols'
RJ Anderson, RM Needham, *Crypto 95 pp 236–247*

The authors present a number of attacks on public key protocols. For example, where messages are first signed and then encrypted, it is often possible to find another plaintext that encrypts to the signed ciphertext using a different public key; this provides attacks on X.509 and the draft ISO 11770. There is also a simplification of Burmester's attack on authenticated key exchange, and a discussion of the lack of redundancy in ISO 11166 key certificates and the effect this has on prudent implementation. Eight principles are presented that would have prevented these attacks, together with other existing ones; these principles may be used to avoid design errors and to find attacks.

044404 'A State-Based Approach to Noninterference'
WR Bevier, WD Young, *Journal of Computer Security v 3 no 1 (95) pp 55–70*

In this journal version of **033206**, the authors argue that state-based modeling is richer and more intuitive than event-based modeling of noninterference style security properties, and can deal with both transitive and intransitive security policies.

044405 'Session-Layer Encryption'
M Blaze, S Bellovin, *Usenix Security 95 pp 85–93*

The authors describe an encrypting authenticated telnet and an encrypting session manager that they have developed. The latter permits secure sessions to be tunneled through firewalls using transparently encrypted BSD pseudo-tty. These protocols are based on Diffie-Hellman but have a number of defences against middleperson attacks, including use of the Rivest-Shamir interlock scheme.

044406 'Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX'
PC Cheng, JA Garay, A Herzberg, H Krawczyk, *Usenix Security 95 pp 41–*

The authors describe an IP secure tunnel protocol, together with its associated key management. IP level security is attractive because it is suited to an internetwork environment, need not interfere greatly with higher layer protocols, and can support high integrity packet filtering firewalls. The basic mechanism is that IP packets are encapsulated in other IP packets and protected by DES-CBC and/or keyed MD5 MACs, and performance figures are given for the various combinations. The protocols will be supported in an IBM firewall product.

044407 'Network Randomization Protocol: A Proactive Pseudo-Random Generator'

CS Chow, A Herzberg, *Usenix Security 95 pp 55–63*

The authors consider how to provide good random numbers in a replicated security service whose components may be subverted by an adversary who is mobile — he may attack any machine — but limited to penetrating a minority of them in any epoch. They provide a protocol that will produce numbers unpredictable to him provided either the seed or one of the update functions is unknown to him.

044408 'Internet Holes — Part 1: Internet Control Message Protocol'

F Cohen, *Network Security (Aug 95) pp 8–10*

This article describes ICMP vulnerabilities that can be used in service denial and rerouting attacks. It recommends that firewalls be configured to keep ICMP packets away from all hosts except those that really need them, such as name servers and gateways.

044409 'Internet Holes — part 2: Packet Fragmentation Attacks'

F Cohen, *Network Security (Sep 95) pp 14–16*

Most current firewalls can be defeated by packet fragmentation attacks. A typical modus operandi is to fragment a harmful packet, replace the TCP header with something innocuous, and then later send a packet with an offset of 0 to reinstate it. The only real solution to this problem is to reassemble all packets in the firewall before making access control decisions.

044410 'Internet Holes — part 3: The Sendmail Maelstrom'

F Cohen, *Network Security (Oct 95) pp 11–12*

This article describes six sendmail attacks that were notified in CERT advisories between 1990 and 1995, and discusses a number of mail security strategies.

044411 'Internet Holes — part 4: Network News Transfer Protocol'

F Cohen, *Network Security (Nov 95) pp 15–19*

The author describes how one can forge usenet postings, create bogus groups, send out bogus message and group cancellations, and launch service denial attacks on news servers. Misfeatures in some news readers allow malicious code to be executed, or the names of people who read a particular article to be collected. Some specified features, such as automatic routing, are not implemented (and will cause further vulnerabilities if they ever are); and many of the existing weaknesses are unlikely ever to be fixed.

044412 'Internet Holes — part 5a: 50 Ways to Attack Your Web System'

F Cohen, *Network Security (Dec 95) pp 7–11*

Nineteen of a promised fifty ways to attack or abuse the world wide web are presented. For example, malicious code may be contained in postscript files, or in Java aplets; and a server can easily mimic a respectable company's web page in order to harvest credit card numbers.

044413 'Kerberos Security with Clocks Adrift'

D Davis, DE Geer, *Usenix Security 95 pp 35–40*

The need for synchronised clocks has limited the application of Kerberos in many environments. Using NTP can create a circularity as it assumes the existence of secure key distribution, while Kerberos assumes secure time. The proposed solution is a challenge-response preauthentication protocol that lets users get tickets without having synchronised their clocks; they can then calculate the clock skew between their own machine and the server and use this for the rest of the Kerberos protocol. The advantage of this approach is that it requires minimal changes to the Kerberos and secure time protocols.

044414 'On Key Storage in Secure Networks'
M Dyer, T Fenner, A Frieze, A Thomason, *Jounral of Cryptology v 8 no 4 (Autumn 95) pp 189–200*

The authors consider set intersection schemes, in which a key distribution centre issues n users with sets of k keys each such that each pair of users has some set of common keys that is not available to any colluding set of w other users. By applying random graph theory, they show that provided one is prepared to accept that the security property holds only with a very large probability, k need be only $[(w+2)^{w+3}/4w^w]$ ln n. Such schemes can be very simple to generate as keys can be assigned randomly, and they are within a small multiple of optimality. The results can be easily generalised to conference key schemes.

044415 'A Classification of Security Properties for Process Algebras'
R Focardi, R Gorrieri, *Journal of Computer Security v 3 no 1 (95) pp 5–33*

In this journal version of **033214**, the authors provide a process algebra similar to CCS that contains a number of security notions and use it to classify nondeducibility and possibilistic flow properties with particular reference to the composability of these properties under parallelism and action restrictions.

044416 'Authentifizierung und Schlüsselmanagement'
W Fumy, *Datenschutz und Datensicherung (10/95) pp 607–613*

The author describes some of the ISO 9798/ISO 11770 mechanisms for entity authentication and key establishment, as well as four other protocols that have not been standardised. The variety of internationally proposed authentication protocols is now rather large.

044417 'Escrow Encryption Systems Visited: Attacks, Analysis and Designs'
Y Frankel, M Yung, *Crypto 95 pp 222–235*

The authors present attacks on a number of escrow protocols including Clipper and the systems of Micali and TIS. For example, Clipper LEAFs can be 'squeezed' from one chip using feedback and then employed in traffic between two other chips; in this way, innocent parties could be framed. Thus two rogue government officials could talk to the President and the Vice-President and use their LEAFs in an illegal private conversation between the two of them. 'Fair cryptosystems' are unfair in that they require the opening of the keys of law-abiding citizens who are called by criminals.

044418 'Efficient network authentication protocols: lower bounds and optimal implementations'
L Gong, *Distributed Computing v 9 no 3 (95) pp 131–146*

In this article, the author summarises existing knowledge on the number of messages needed for various types of authentication and presents a number of new results. For example, protocol designers cannot simultaneously minimise messages and rounds: a nonce based authentication handshake in which the server chooses the key may be done in five rounds containing seven messages, or six rounds containing six messages. He also proves that the existence of keyed one-way hash functions is necessary and sufficient for authentication.

044419 'Attacking Network Routers'
W Hancock, *Network Security (Sep 95) pp 11–12*

The author describes an attack in which malicious code updated a router table with false information that certain links were down.

044420 'Applications of smartcards for anonymous and verifiable databases'
T Hardjono, J Seberry, *Computers and Security v 14 no 5 (95) pp 465–472*

The authors present an adaptation of the Leighton Micali key distribution scheme (**024514**) to escrow; instead of escrowing session keys, the system protects linkage information such as between the names of individuals and their pseudonyms in large databases. It uses combinations of hashing, public key and tamperproofing mechanisms.

044421 'A LAN voting protocol'
V Hassler, R Posch, *IFIP 95 pp 176–189*

This paper proposes a collection of protocols that provides a secure voting service. It combines the voting protocol of Salomaa with Boyd's multiple key ciphers to ensure only legitimate voters may vote and nobody else but the voter him/herself knows what vote was cast. An analysis of the scheme is presented and the required assumptions for its secure operation are underlined. In the proposed system, clients are voters who establish connections with the voting server.

044322 'Proactive Secret Sharing Or: How to Cope With Perpetual Leakage'
A Herzberg, S Jarecki, H Krawczyk, M Yung, *Crypto 95 pp 339–352*

The authors present a protocol for periodically renewing shares in a secret (without changing the secret) so that information leaked about any of the old shares is useless in attacking the new ones. Methods for detecting corrupt shares are also provided. The system is based on verifiable secret sharing, and adding a random polynomial with zero constant term to the sharing polynomial at each update. its effect is that an adversary needs to compromise a quorum of shares in the one time period.

044423 'On the Matsumoto and Imai human identification scheme'
CH Wang, T Hwang, JJ Tsai, *IEE Transactions on Computers and Digital Techniques v 142 no 5 (9/95) pp 313–317*

An identification scheme that involved a user in mentally shuffling a challenge string using memorised code numbers is shown to be more vulnerable to active and passive attacks than had previously been thought. A more complicated alternative is also proposed.

044424 'Secure and minimal protocols for authenticated key distribution'
P Janson, G Tsudik, *Computer Communications v 18 no 9 (September 1995), pp 645–653*

This paper describes a braiding technique for authenticated key distribution in distributed systems.

044425 'A Simple Active Attack Against TCP'
L Joncheray, *Usenix Security 95 pp 7–19*

The author describes in detail an attack on TCP, in which the opponent creates a desynchronised state at both ends of the connection so that the client and server can no longer exchange information. He then creates acceptable packets for both parties that mimic the real packets. Finally, he compares his attack with Morris's.

044426 'Systematic approach to security risk investigation'
D Jokanovic, *IFIP 95 pp 87–97*

The author proposes a formal method for systematic investigation of a system security breaches, This is based on constraint diagrams, which are graph-like structures where each vertex contains a different set of constraints imposed on the system. The method helps a designer to assess the size of the damage and the cost of repair for a given security breach. A property-oriented specification language, Larch, is used to implement the method. The working of the system is explained by presenting the example of acquiring unauthorised capability in an e-mail system.

044427 'Fair Cryptosystems, Revisited'

J Kilian, T Leighton, *Crypto 95 pp 208–221*

The authors present an attack on Micali's key escrow scheme; it is possible to generate two keypairs (P, S) and (P', S') with $P' = f(P)$ for a publicly known function f. Criminals could then escrow S, publish P and communicate securely using S' and P', thus leveraging off the official public key infrastructure. In RSA, this works by encoding the modulus of P' in the exponent of P. This is called a shadow public key system; in general, any available subliminal channel might be utilised (such as names, if these are not restricted in length). The authors then propose an improved scheme and discuss the formal security requirements of escrow in general.

044428 'Implementing a Secure rlogin Environment: A Case Study of Using a Secure Network Layer Protocol'

GH Kim, H Orman, S O'Malley, *Usenix Security 95 pp 65–73*

The authors designed an rlogin protocol that is secure against opponents spoofing DNS or forging IP source addresses, but which does not require as extensive software modification as Kerberos or encrypted telnet. It uses a secure network layer and a number of server extensions.

044429 'A Key Escrow System with Warrant Bounds'

AK Lenstra, P Winkler, Y Yacobi, *Crypto 95 pp 197–207*

The authors point out that an ideal escrow system would provide keys valid for only a set period of time; it would also allow either node surveillance (all traffic to or from an individual) or edge surveillance (all traffic between two individuals). They present a design based on Diffie-Hellman with hashing to incorporate time periods.

044430 'An attack on the Needham-Schroeder public-key authentication protocol'

G Lowe, *Information Processing Letters v 56 no 3 (10/11/95) pp 131–133*

The Needham-Schroder public key protocol is shown to be vulnerable to a middleperson attack, which can be fixed by including participants' names explicitly in the messages.

044431 'Effect of key generators on the automatic search for flaws in key management schemes'

D Longley, S Vasudevan, *Computers and Security v 14 no 4 (95) pp 335–347*

The use of key generators can complicate formal analysis of protocols by some dependency techniques as they produce multiple outputs, that must be independent, from a single input. The authors discuss how to cope with this in the context of an analysis tool previously developed by Longley and Rigby.

044432 'One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication'

DL McDonald, RJ Atkinson, C Metz, *Usenix Security 95 pp 177–186*

The US Navy Labs have used an extended form of S/Key to study the implementation and usability aspects of one-time passwords. Improvements included replacing MD4 with MD5. The deployment issues turned out to be user resistance to a more complex logon procedure, the difficulty of scaling on large networks, and the need to carry either a password calculator or a printed list of passwords; users often fail to anticipate the need to carry lists, and the business case for calculators is unclear.

044433 'A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems'

S Micali, R Sidney, *Crypto 95 pp 185–196*

Shared pseudorandom functions can be constructed by exclusive-or'ing the result of a number of conventional pseudorandom functions such as DES. They discuss how to add resilience and apply the constructions to key escrow.

044434 'Unwinding Forward Correctability'

J Millen, *Journal of Computer Security v 3 no 1 (95) pp 35–54*

In this journal version of **033241**, the author proves an unwinding result for information flow and shows that regular expression notation provides an easy mechanical tool for verifying forward correctability for small systems.

044435 'How to Reverse Engineer an EES Device'

M Roe, *FSE 94 pp 305–328*

The author describes the known protocol attacks on the US escrowed encryption standard, and discusses a number of ways in which the protocols used with such a scheme might leak information about the structure and relationship of the components. Of particular interest are correlations, such as between initialisation vectors and keys, that might be used by an unscrupulous designer to leak key material.

044436 'Independent One-Time Passwords'

AD Rubin, *Usenix Security 95 pp 167–176*

The author proposes a new technique for generating one-time passwords: it is based on triple DES, and used in a Bellcore billing server with the client end implemented in paper booklets. Future smartcard implementation is suggested.

044437 'Single Sign-on'

C Shaer, *Network Security (Aug 95) pp 11–15*

The author describes a number of single sign-on solutions from simple logon scripting to more complex authentication systems such as SESAME and DCE.

044438 'The Role of Trust in Information Integrity Protocols'

G Simmons, C Meadows, *Journal of Computer Security v 3 no 1 (95) pp 71–84*

There is a partial order or shared control schemes: X is weaker than Y if adding trust relationships between individuals can produce X out of Y. The set of shared control schemes for a given set of individuals becomes a distributive lattice under this order, and an algorithm for its construction is given. The lattices for three and four individuals are given. These are symmetric: for every trust, there is an equal and opposite mistrust.

044439 'STEL: Secure TELnet'

D Vincenzetti, S Taino, F Bolognesi, *Usenix Security 95 pp 75–83*

The Italian CERT team has recorded a large number of sniffing attacks and has thus designed a secure telnet system as an interim measure. It uses Diffie-Hellman key exchange with DES, 3DES or IDEA; authentication can be based on Unix passwords, Skey or SecurID depending on the requirements. Sources are freely available and it is proposed to issue the protocol as an Internet draft.

044440 'Cryptographic implementation of dynamic access control in user hierarchy'

TC Wu, *International J of Information and Management Sciences (ROC) v 5 no 2 (September 1994) pp 73–85*

This paper presents a cryptographic key assignment scheme for access control in an arbitrary partially ordered user hierarchy. The proposed scheme aims to handle dynamic access control such as changing secret keys of users, and adding/deleting both users and immediate relationships between them.

5 Secret Key Algorithms

044501 'On Fibonacci Keystream Generators'
R Anderson, *FSE 94 pp 346–352*

The author shows that the Fibonacci shrinking generator (**033504**) can be broken with effort about 2^{40} depending on the amount of keystream available. This works because the recurrence relations are sparse and the nonlinear processing leaks the least significant bits and half of the other bits of every other keystream word, allowing a correlation attack that reconstructs the initial state. An improved Fibonacci generator called PIKE is then presented; it is based on the GSM A5 stream cipher.

044502 'Searching for the Optimum Correlation Attack'
R Anderson, *FSE 94 pp 137–143*

The author presents a new attack on the nonlinear filter generator. Nonlinear Boolean functions such as those used in filters possess mutual information with shifted copies of themselves; thus for example if k successive bits of a shift register sequence are input to a filter function to calculate the next keystream bit, one expects to find correlations between k-tuples of keystream and $(2k-1)$-tuples of underlying shift register sequence. In fact one finds even more: the set of $(2k-1)$-tuples that could have generated an observed output may possess parity checks that may halve the search space.

044503 'Clock-controlled pseudorandom generators on finite groups'
U Baum, S Blackburn, *FSE 94 pp 6–21*

A new class of stream ciphers is presented in which a controlling sequence selects one of a set of elements of a group to transform the state. Where this gives a two-generator Abelian group, results can be proved on the cycle length; a simple example might be a clock controlled shift register where the clock chooses one of two possible recurrence relations. An example that is discussed more thoroughly is based on quaternion groups.

044504 'XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions'
M Bellare, R Guérin, P Rogaway, *Crypto 95 pp 15–28*

The authors present two new MAC schemes based on block ciphers. The input string's blocks are encrypted and the results are xor'ed together in various ways; the result is a MAC that is proven secure in the sense that a forgery or collision would break the underlying block cipher. These schemes are both incremental and parallelisable.

044505 'A Known Plaintext Attack on the PKZIP Stream Cipher'
E Biham, P Kocher, *FSE 94 pp 144–153*

The authors present an attack on the stream cipher bundled with the freeware product PKZIP. This can find a key in a few hours on a PC given a few hundred bytes of known plaintext and was used to find the key in the PKZIP contest. The cipher used coupled congruential generators with added nonlinearity, but this turned out to be insufficient; the generators can be guessed one after the other, giving a total attack complexity of 2^{27}.

044506 'The MacGuffin Block Cipher Algorithm'
M Blaze, B Schneier, *FSE 94 pp 97–110*

The authors proposed an unbalanced 64-bit Feistel cipher in which 16 bits are modified by a function of the other 48 at each round. The cipher's name came from 'generalised unbalanced Feistel network'; a differential attack on it is presented in **044538**.

044507 'Problems with the Linear cryptanalysis of DES Using more than one Active S-Box per Round'

U Blöcher, M Dichtl, *FSE 94 pp 265–274*

Matsui's piling-up lemma is not strictly applicable to approximate expressions that use neighbouring S-boxes in the same round, as the boxes share inputs and thus have correlations. Statistical evidence suggests that the errors are severe enough to lead to the computation of wrong key bits.

044508 'Analysis of DES double key mode'

G Carter, A Clark, E Dawson, L Nielsen, *IFIP 95 pp 113–127*

The authors propose a new mode of operation for DES called double key mode; this uses 112 bits of key while retaining the same speed of operation as 64-bit DES, is proposed. Its security against differential and linear cryptanalysis, and hardware keysearch, is discussed. It is concluded that the double-key mode does indeed have increased security.

044509 'On Random Mappings and Random Permutations'

WG Chambers, *FSE 94 pp 22–28*

The author discusses the properties of random functions versus random permutations from the point of view of using them in stream ciphers. Systems that modify their own lookup tables may have short periods. In addition, the A5 algorithm has the strange property that over 40% of keys lead to a cycle of the shortest possible length, namely $(2^{23} - 1).4/3$ bits.

044510 'Correlation Matrices'

J Daemen, R Govaerts, J Vandewalle, *FSE 94 pp 275–285*

Matrices that express the correlation between the inputs and outputs of a Boolean function can be derived from the Walsh transforms of its component functions, and provide a natural setting for describing the mechanisms of linear cryptanalysis.

044511 'Binary Cyclotomic Generators'

CS Ding, *FSE 94 pp 29–60*

The author discusses the use of cyclotomic functions as nonlinear filters and combiners in stream ciphers, whether shift register or counter based. These have a number of interesting properties in that one can prove the equivalence of the obvious linear, differential autocorrelation, and stability attacks. These results follow from the equitable distribution of the values at which such functions' characteristic sets intersect shifted copies of themselves.

044512 'Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity'

H Dobbertin, *FSE 94 pp 61–74*

The known bent function constructions of Maiorana-MacFarland and Dillon may be subsumed as special cases (corresponding to cartesian and polar coordinates) of a new construction in which one starts out with a possible intersection of a bent function with a line or set of lines and then works back to construct the function. It is also possible to modify bent functions to get balanced highly nonlinear Boolean functions in a canonical way; their nonlinearity is the best known so far.

044513 'A sufficient and necessary condition of judging the independence of boolean functions system'

DG Feng, GZ Xiao, *Chinese Science Bulletin v 40 pp 1406–1408*

This paper discusses the properties of independent and balanced boolean functions, and described the applications of such functions in cryptology.

044514 'The Cylinder-cipher'
J Gaddy, *Cryptologia v XIX no 4 (Oct 95) pp 385–391*

The author describes the history of the wheel cipher, of which variants are the M-94, the Jefferson wheel cipher and the Bazeries cylinder.

044515 'Ciphertext-only cryptanalysis of Enigma'
JJ Gillogly, *Cryptologia v XIX no 4 (Oct 95) pp 404–413*

The author develops a method to break Enigma ciphertexts without a crib. The Index of coincidence is used to recover the message key and rotor order using exhaustive search, then get the ring settings and finally the plug settings. The technique is demonstrated on a 647 character message. With up to six plugs, the methods will work for messages of several hundred characters; but it becomes ineffective with ten or more plugs.

044516 'Linear Cryptanalysis of Stream Ciphers'
JD Golić, *FSE 94 pp 154–169*

The author discusses a general attack on stream ciphers, namely approximation by a linear finite-state machine. This can in certain circumstances yield divide-and-conquer attacks, and its effectiveness against existing designs is estimated. He then proposes a new stream cipher: a 32-bit Fibonacci generator has its bits added pairwise to yield 16 binary sequences, each of which is then passed through a combiner with 15 bits of memory and one bit of input and output. Finally, the vector is passed through a 1–2 clock control to give a 16 bit output.

044517 'On the Weighing Matrices of Order $4n$ and Weight $4n-2$ and $2n-1$'
M Gysin, J Seberry, *Australasian Journal of Combinatorics v 12 (Sep 95) pp 157–174*

Weighing matrices are a generalisation of Hadamard matrices: their entries may be 0 as well as +1 and -1, but the total number of nonzero entries must be constant in all rows and columns. The authors give a number of constructions for these matrices.

044518 'Linear Cryptanalysis Using Multiple Approximations and FEAL'
BS Kaliski, MJB Robshaw, *FSE 94 pp 249–264*

The authors explore the implications of doing linear cryptanalysis using multiple approximate expressions on four and eight round FEAL. They tabulate the success probability for different numbers of plaintexts, and find that using multiple approximations and key ranking together is preferable to either method in isolation. These results suggest that one should look for improved ways of using the information that linear approximations yield.

044519 'Message Authentication with MD5'
B Kaliski, M Robshaw, *RSA Laboratories' CryptoBytes v 1 no 1 (Spring 95) pp5–8*

The authors describe how MD5 works and propose three ways of using it as a keyed hash function.

044520 'Multiple Encryption: Weighing Security & Performance'
BS Kaliski, MJB Robshaw, *Dr Dobbs Journal no 243 (Jan 96) pp 123–127*

The authors describe the pros and cons of double and triple encryption with DES and the various attacks that are possible on different modes. They also discuss mixing ciphers, such as by combining DES with a simple substitution, to defeat keysearch attacks.

044521 'On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm'
BS Kaliski, YL Yin, *Crypto 95 pp 171–184*

The authors present a differential attack on RC5 that is based on degenerate rotations that requires 2^{62} chosen plaintexts to attack the recommended 12 rounds, and a linear attack that uses more known plaintexts for 5-round RC5 than are needed for 16-round DES. These are conjectured to be the best possible.

044522 'On the Security of the RC5 Encryption Algorithm'
BL Kaliski, YL Tin, *RSA Laboratories' CryptoBytes v 1 no 2 (Summer 95) pp 13–14*
The authors summarise their best results for differential and linear cryptanalysis of RC5.

044523 'Feedback with Carry Shift Registers over Finite Fields'
A Klapper, *FSE 94 pp 170–178*
The author generalises his work with binary sequences over the 2-adic numbers to arbitrary number fields. the possible cryptographic interest might come from the difficulty of generalising correlation attacks to such structures.

044524 'Cryptanalysis Based on 2-Adic Rational Approximation'
A Klapper, M Goresky, *Crypto 95 pp 262–273*
The authors present an improved algorithm for reconstructing feedback-with-carry shift registers which, as with Massey-Berlekamp, requires only twice as much keystream as the length of the target shift register. This algorithm uses 2-adic rational approximation. Thus if a keystream generator combines shift register sequences of length $2^n - 1$ for $n = 7, 11, 13, 15, 16$ and 17 with a full adder, at most 2^{19} bits of keystream will be needed to recover the key quickly.

044525 'A Key-schedule Weakness in SAFER K-64'
L Knudsen, *Crypto 95 pp 274–286*
Almost all keys of SAFER K-64 have the property that changing a single byte will leave the first six rounds of encryption unaffected for a non-negligible fraction of plaintexts. The output transformation then causes the ciphertexts to differ in a single byte. As a result, when six-round SAFER is used in feedforward hashing mode, collisions can be found; the effort required is about 2^{23} encryptions.

044526 'Truncated and Higher-Order Differentials'
LR Knudsen, *FSE 94 pp 196–211*
The author considers differential attacks in which only part of the output difference can be predicted, and develops an attack on 6-round DES using only 46 chosen plaintexts. He exhibits a 5-round Feistel cipher for which the new attack is much more efficient than the traditional technique.

044527 'On chaotic synchronization and secure communications'
LM Kocarev, TD Stojanovski, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci. v E78-A no 9 (September 1995) pp 1142–1147*
This paper introduces a system for communications by means of chaotic synchronization; the authors also describe the application of chaos for securing communications. An algorithm for secret key cryptography is suggested and evaluated through statistical tests.

044528 'Additive and Linear Structures of Cryptographic Functions'
XJ Lai, *FSE 94 pp 75–85*
The author considers certain linear structure in Boolean functions and shows that if a certain number of them exist, then the function can be decomposed into a linear function on some of its variables and a nonlinear one on the rest. These linear structures are relevant to linear and differential attacks on block ciphers.

044529 'The Length of Message Authentication Codes'
J Lindballe, *Computers and Security v 14 no 4 (95) pp 303–305*
The author takes issue with an analysis of MAC collisions presented by Allinson, Dawson and Bergen in **03150**. He argues that in most computer systems an attacker would have to mount a target rather than collision attack.

044530 'A Free Energy Minimization Framework for Inference Problems in Modulo 2 Arithmetic'
DJC MacKay, *FSE 94 pp 179–195*

The problem of finding good correlation attacks on shift register based stream ciphers may be stated as inferring a binary vector s given noisy observations of $t = As$ modulo 2, where A is an n x m binary matrix. The author tackles this problem using variational techniques derived from statistical physics. As with existing attacks such as those of Meier and Staffelbach, the performance depends on the noise level and the sparsity of the relations; however the new technique works with more noise or less sparsity. It also yields a principled explanation of why such attacks work in general, and it can be improved still further using ad-hoc techniques such as simulated annealing.

044531 'SAFER K-64: One Year Later'
JL Massey, *FSE 94 pp 212–241*

The author reviews his SAFER K-64 block cipher a year after its launch (**033532**) and defines a variant with 128 key bits called SAFE K-128. This is backwards compatible in that setting two halves of the key equal yields the original algorithm. The nonlinearity of the structure is reviewed, as are the cryptanalytic results published meanwhile. A hashing weakness pointed out by Knudsen (**044525**) is countered by specifying that whenever either variant of the algorithm is used for hashing, at least ten rounds should be employed.

044532 'S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity'
K Nyberg, *FSE 94 pp 111–130*

The author discusses how the properties leading to differential and linear strength of S-boxes are preserved under various transformations such as composition with linear or affine input or output mappings, adding coordinate functions, restriction to subspaces and adding functions with independent inputs. A number of these are used in proposed and fielded systems.

044533 'Properties of Linear Approximation Tables'
L O'Connor, *FSE 94 pp 131–136*

The author uses his analysis of the expected largest entry in the linear approximation table of a block cipher to show that the best approximation to 64-bit ciphers such as DES would be 2^{-30} if the cipher were random rather than constructed from an iterative process.

044534 'Improving the Search Algorithm for the Best Linear Expression'
K Ohta, S Moriai, K Aoki, *Crypto 95 pp 157–170*

The authors present new techniques for searching for linear approximations to block ciphers. These perform about as well as Matsui's for DES, but much better for FEAL; improved results for FEAL with more than eight rounds are presented.

044535 'On the Security of the Gollmann Cascades'
SJ Park, SJ Lee, SC Goh, *Crypto 95 pp 148–156*

The authors present an improved attack on cascades of 0-1 clock controlled shift registers. They construct transition matrices of the conditional probabilities of various inputs and outputs of each stage, and then look for vulnerable outputs (specifically, runs of consecutive zeros or ones) from which they can work back to likely initial states. They managed to break cascades of up to 9 stages of degree 100.

044536 'MDx-MAC and Building Fast MACs from Hash Functions'
B Preneel, PC van Oorschot, *Crypto 95 pp 1–14*

The authors present some new birthday attacks on MAC and keyed hash functions which rely on looking for internal collisions and have certificational implications for the way in which keys are used with hash functions; a new way of keying is suggested. The technique also succeeds against MAA with $2^{24.5}$ known texts and 131071 chosen texts authenticated with the same key.

044537 'Cryptanalysis of McGuffin'
V Rijmen, B Preneel, *FSE 94 pp 353–358*

The authors show that 32 rounds of McGuffin (**044506**) are more vulnerable to differential attack than 16 rounds of DES: a 27-round characteristic with probability about 2^{-48} can be used. Linear attacks are slightly harder, with the best linear relation having probability about 2^{-30}.

044538 'Improved characteristics for differential cryptanalysis of hash functions based on block ciphers'
V Rijmen, B Preneel, *FSE 94 pp 242–248*

The authors discuss the type of characteristics needed to find collisions in hash functions based on block ciphers with feedforward. In such an application the attacker has some control over the choice of key. They show that hash functions based on 15-round DES can be attacked with less then 2^{26} encryptions, i.e. faster than by brute force.

044539 'The RC5 Encryption Algorithm'
RL Rivest, *FSE 94 pp 86–96*

This paper contains the definition of RC5, a fast compact software block cipher based on using data-dependent rotations. Its word size, number of rounds and key length can be parametrised so that security may be upgraded as necessary. The basic round function is to add both halves, shift them by a number of bits determined by one of the halves, add key material and use the result to replace the other of the halves.

044540 'The RC5 Encryption Algorithm'
RL Rivest, *RSA Laboratories' CryptoBytes v 1 no 1 (Spring 95) pp 9–11*

This is a shortened version of the above paper, together with some preliminary performance figures.

044541 'Performance of Block Ciphers and Hash Functions — One Year Later'
M Roe, *FSE 94 pp 359–362*

The author updates his league table (**033539**) of the software performance of various block ciphers, stream ciphers and hash functions to include ciphers such as RC4, RC5, Blowfish, WAKE and SEAL.

044542 'Bucket Hashing and its Application to Fast Message Authentication'
P Rogaway, *Crypto 95 pp 29–42*

The author presents a new, extremely fast, way to authenticate messages in software. Each word of the input string is xor'ed to a small number of accumulators that are chosen using a keystream generator from among perhaps 100–200 depending on the level of collision resistance required; the accumulators are then combined using a more conventional hash function.

044543 'Differential and Linear Cryptanalysis'
B Schneier, *Dr Dobbs Journal no 243 (Jan 96) pp 42–48*

The author provides a fairly detailed discussion of the strength of the Data Encryption Standard aimed at a general computer science audience. He describes how differential and linear cryptanalysis work and explains how they apply to DES; he also explains some recent results such as Knudsen's attack on 6-round DES (**044526**) and the Langford/Hellman attack on 8 rounds (**034521**).

044544 'A generation method for a kind of linear independent Latin arrays'

RJ Tao, SH Chen, *Scientia Sinica (Series A) v 38 no 7 (July 1995) pp 884–896*

Latin arrays have found applications in cipher design. This paper introduces the concept of correlation of Latin arrays, and discussed the generation of Latin arrays with independence degree ≥ 1. It also gives a method for generating linearly independent invertible boolean vector functions.

044545 'On applicability of linear cryptanalysis to DES-like cryptosystems – LOKI89, LOKI91 and s^2 DES'

T Tokita, T Sorimachi, M Matsui, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci. v E78-A no 9 (September 1995) pp 1148–1153*

This paper discusses the linear cryptanalysis of LOKI89, LOKI91 and s^2 DES. The authors apply Matsui's algorithm to search for the best differential and linear approximate expression to LOKI89, LOKI91 and s^2 DES, and completely determine their best probabilities.

044546 'Werftschlüssel — a German navy hand cipher system, part 1'

M van der Meulen, *Cryptologia v XIX no 4 (Oct 95) pp 349–364*

This article describes the hand cipher used by German dockyards and fleet auxiliaries in world war 2. It is a fractional digraphic system with added elements of transposition; although quite strong for a hand cipher, it was broken by the Allies and provided cribs for machine-based attack on naval Enigma systems.

044547 'On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER'

S Vaudenay, *FSE 94 pp 286–297*

The author shows how to construct collisions for two-round MD4 that yield near-collisions for the full three-round version. Furthermore, if the S-box of SAFER (the 8-bit exponentiation) is replaced with a random S-box, then in over 6% of cases it leaks information giving a known-plaintext attack faster than exhaustive search.

044548 'TEA, a Tiny Encryption Algorithm'

DJ Wheeler, RM Needham, *FSE 94 pp 363–366*

The authors present a block cipher designed to have very small code size and to be easy to program in many languages. It uses 64 rounds of a simple Feistel structure with a round function that mixes addition with exclusive or and shifting. It gets its nonlinearity from carry propagation, and runs several times faster than DES.

044549 'Resistance of balanced s-boxes to linear and differential cryptanalysis'

AM Youssef, SE Tavares, *Information Processing Letters v 56 no 5 (8/12/95) pp 249–252*

The authors develop combinatorial bounds on the likelihood that randomly chosen balanced s-boxes will have an entry larger than a given bound in its linear approximation or xor difference table, and thus show that the number of s-boxes that resist differential and linear analysis increases dramatically with the number of input variables.

044550 'Linear approximation of injective s-boxes'

AM Youssef, SE Tavares, S Mister, C Adams, *Electronics Letters V 31 no 25 (7/12/95) pp 2165–2166*

The authors consider s-boxes whose outputs are larger than their inputs, as with CAST and Blowfish. They obtain combinatorial bounds on the maximum entries in the linear approximation and xor distribution tables of random injective Boolean functions, and this theory is supported by simulation results.

044551 'A generalization of Gröbner bases and a synthesis algorithm of multisequence over $Z/(m)^*$'
JJ Zhou, WF Qi, YJ Zhou, *Scientia Sinica (Series A) v 38 no 5 (May 1995) pp 552–561*

This paper proposes a mathematical model for algorithms that synthesise multisequences. It generalises Gröbner bases over the ring $(Z/(p^e)[x_1, \cdots, x_n])/I$, where Z is the integers, p is a prime, $e \geq 1$, and I is an ideal. By applying this generalisation, the authors present an $O(N^2)$ algorithm that can synthesize multisequences with an equal or unequal length over $Z/(m)$.

6 Public Key Algorithms

044601 'Fast Server-Aided RSA Signatures Secure Against Active Attacks'
P Béguin, JJ Quisquater, *Crypto 95 pp 57–69*

The authors present an algorithm for server-aided RSA signatures that resists the currently known active and passive attacks. It is based on the fast exponentiation algorithm of Brickell, Gordon, McCurley and Wilson, and it can achieve a speedup of about ten times.

044602 'Some Remarks on Lucas-Based Cryptosystems'
D Bleichenbacher, W Bosma, AK Lenstra, *Crypto 95 pp 386–396*

The Lucas public key cryptosystems are simply a reinvention of a system based on Dickson polynomials proposed by Müller and Nöbauer in 1981. In effect one operates in the corational group of $GF(p^2)$ rather than in its rational group; once this is appreciated, homomorphic properties can be found, together with subexponential time attacks.

044603 'Cryptanalysis and improvement on a conference key distribution system'
CC Chang, WB Wu, TC Wu, *J of the Chinese Institute of Engineers (ROC) v 18 no 3 (1995) pp 391–396*

This paper shows that the Wu and Yeh conference key distribution system is breakable, and proposes a modified scheme which can achieve better security.

044604 'A new fast RSA algorithm'
Y Chen, *Journal of UEST of China v 24 no 8 (August 1995) pp 223–228*

This paper presents a fast exponentiation algorithm for software RSA. The algorithm reduces the number of modulo operation by about 30% by exploiting various symmetries and by reducing the absolute values of the multiplicands.

044605 'A practical conference key distribution scheme'
V Chrissikopoulos, D Peppes, *IFIP 95 pp 167–175*

The author propose a conference key distribution protocol which is a modification of a protocol defined by Burmester and Desmedt for the same purpose. Security of the system is based on discrete logarithm problem and is proved to be secure against passive attack. However the protocol can be subverted by a dishonest insider who has access to session keys constructed in two-party applications of the protocol.

044606 'Cryptanalysis of a public key system based on Diophantine equations'
TW Cusick, *Information Processing Letters v 56 no 2 (27/10/95) pp 73–75*

The author breaks a public key system proposed by Lin, Chang and Lee (**041626**) by showing how to recover plaintext without having to solve the number theoretic problem on which the system had supposedly been based.

044607 'Practical and Provably Secure Release of a Secret and Exchange of Signatures'
IB Damgård, *Journal of Cryptology v 8 no 4 (Autumn 95) pp 201–222*

The author shows how RSA/Rabin and ElGamal signatures can be released in a secure way using interleaved bit commitment techniques that allow the parties to a simultaneous signature exchange to prevent cheating. Unlike previous work, it does not require a trusted third party.

044608 'Cryptanalysis of the Immunized LL Public Key Systems'
Y Frankel, M Yung, *Crypto 95 pp 287–296*

The authors provide attacks on RSA and ElGamal variants that had been proposed by Lim and Lee as resistant to adaptive chosen ciphertext attack (**024613**).

044609 'A new approach to constructing a provably secure variant of Schnorr's identification scheme'
S Hada, H Tanaka, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci. v E78-A no 9 (September 1995) pp 1154–1159*

This paper describes a new approach to construct a provably secure variant of Schnorr's identification scheme. The authors show that this scheme, while provably secure, does not suffer in efficiency.

044610 'Comment — Cryptanalysis of the blind signatures based on the discrete logarithm problem'
P Horster, M Michaels, H Petersen, *Electronics Letters V 31 no 21 (12/10/95) p 1827*

The authors dispute Harn's claim (**043611**) that their blind signatures are not truly blind and point out a flaw in his attack.

044611 'Meta-multisignature schemes based on the discrete logarithm problem'
P Horster, M Michels, H Petersen, *IFIP 95 pp 128–142*

This paper describes two attacks on a signature scheme proposed by Harn and suggests countermeasures. A modification of Harn's scheme is generalised first to an ElGamal type signature scheme and next to a signature scheme with message recovery. The security of each system under various attacks is analysed, and its performance is compared with previous systems.

044612 'An encryption/signature scheme with low message expansion'
SJ Hwang, CC Chang, WP Yang, *J of the Chinese Institute of Engineers (ROC) v 18 no 4 (1995) pp 591–595*

This paper proposes a concurrent encryption/signature scheme for providing secrecy, authenticity and integrity with a low message expansion ratio.

044613 'Threshold DSS Signatures without a Trusted Party'
SK Langford, *Crypto 95 pp 397–409*

The author presents a 2-out-of-n threshold scheme for DSS that does not require a trusted dealer to distribute the shares. Extending the quorum to more than two can be done under restrictive assumptions such as lists of precomputed message keys.

044614 'The security of He and Kiesler's signature scheme'
NY Lee, T Hwang, *IEE Transactions on Computers and Digital Techniques v 142 no 5 (9/95) pp 370–372*

The authors show that an enhanced version of ElGamal's signature scheme (**033610**) does not possess all the advantages claimed for it.

044615 'Security and Performance of Server-Aided RSA Computation Protocols'
CH Lim, PJ Lee, *Crypto 95 pp 70–83*

The authors extend Anderson's attack on server assisted signature protocols to break Matsumoto's S1M and S2M schemes whenever the result is not checked. They discuss some other security factors and possible optimisations such as blinding factors and the use of specially chosen decompositions.

044616 'Elliptic Curve Cryptosystems'
A Menezes, *RSA Laboratories' CryptoBytes v 1 no 2 (Summer 95) pp 1–4*

The author reviews elliptic curve cryptography; for a given level of security, elliptic curve operations over fields of characteristic two require much fewer gates than conventional modular arithmetic.

044617 'An Efficient Divisible Electronic Cash Scheme'
T Okamoto, *Crypto 95 pp 438–451*

A divisible electronic cash scheme is presented that requires less computation than previously. For example, where coins divisible into cents may have a value of up to \$1000, previous schemes needed about 200 exponentiations and the one proposed here needs about 20.

044618 'Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88'
J Patarin, *Crypto 95 pp 248–261*

The author attacks a scheme of Matsumoto and Imai; he shows that for almost all keys, most ciphertexts can be decrypted in less than the square of the time needed to perform the encryption in the first place.

044619 'Extending the Håstad attack to LUC'
RGE Pinch, *Electronics Letters V 31 no 21 (12/10/95) pp 1827–1828*

The author extends Håstad's small enciphering exponent attack to LUC; the constraints on exponent size in terms of the number of linearly related messages turn out to the same as with RSA.

044620 'Extending the Wiener attack to RSA-type cryptosystems'
RGE Pinch, *Electronics Letters V 31 no 20 (28/9/95) pp 1736–1738*

Wiener's small deciphering exponent attack on RSA is generalised to systems based on other groups; the details are worked out for the LUC system and for two systems based on elliptic curves.

044621 'Message authentication using quadratic residues'
F Rubin, *Cryptologia v XIX no 4 (Oct 95) pp 397–404*

The author describes variants on the Rabin signature scheme.

044622 'On R_a R_b transformation and inversion of compound finite automata'
RJ Tao, *Technical Report ISCAS-LCS-95-10, Chinese Academy of Sciences, September 1995*

The author discusses the mechanics of FAPKC3, a finite automaton public key cryptosystem. This is based on a compound finite automaton of which one part is quasilinear and the other is weakly invertible. The paper goes into detail about the inversion and key generation techniques.

044623 'How to Break Shamir's Asymmetric Basis'
T Theobald, *Crypto 95 pp 136–147*

The author presents an attack that recovers the key for the asymmetric variant of Shamir's identification scheme based on birational permutations (**024617**).

044624 'A new access control scheme with high data security'
CR Tseng, WP Yang, *International J of Information and Management Sciences (ROC) v 5 no 3 (December 1994) pp 35–48*

This paper presents a generalised Merkle-Hellman cryptosystem and proposes a single-key access control scheme based on this cryptosystem.

044625 'Cheating detection and cheater identification in secret sharing schemes'
TC Wu, TS Wu, *IEE Transactions on Computers and Digital Techniques v 142 no 5 (9/95) pp 367–369*

Cheater identification can be added to Shamir's secret sharing scheme if the dealer publishes a weighted modular sum of hashed shadows. This is recalculated when the shadows are presented to reconstruct the secret and a comparison will reveal any incorrect shadow.

7 Computational Number Theory

044701 'NFS with Four Large Primes: An Explosive Experiment'
B Dodson, AK Lenstra, *Crypto 95 pp 372–385*

When factoring with the three large prime variant of the general number field sieve, the authors found that the number of useful combinations suddenly exploded in an unpredictable way. This is not yet understood but makes factoring faster than anticipated. Numerical evidence shows that the crossover between quadratic and number field sieves is at most 115 digits.

044702 'Analysis of sliding window techniques for exponentiation'
CK Koç, *Computers Math. Applic. v 30 no 10 (1995) pp 17-24*

This paper gives algorithmic descriptions of two recently proposed sliding window exponentiation techniques, and calculates the average number of multiplications by modeling the partitioning process as a Markov chain. The author tabulates the optimal values of the partitioning parameters, and shows that the sliding window algorithms require up to 8% fewer multiplications than the m-ary method.

044703 'A cardinalised binary representation for exponentiation'
KY Lam, K Sung, L Hui, *Computers Math. Applic. v 30 no 8 (1995), pp 33-39*

This paper introduces a new binary representation of integers, called the cardinalised binary representation. It can be exploited to achieve performance improvement for large integer exponentiation operations. A family of algorithms are described for converting integers to it, and the paper demonstrates that both software and hardware exponentiation algorithms operate more efficiently using the new technique than with binary redundant representations.

044704 'The Future of Integer Factorization'
AM Odlyzko, *RSA Laboratories' CryptoBytes v 1 no 2 (Summer 95) pp 5–14*

This article reviews the state of the factoring art. It tabulates historical factoring records and the relative contribution of computer power and algorithmic efficiency. He concludes that it is not prudent to expect even 1024 bit moduli to remain secure for a decade, and that for extremely sensitive data it might be prudent to use 10,000 bit moduli.

044705 'Fast Key Exchange with Elliptic Curve Systems'
R Schroeppel, H Orman, S O'Malley, O Spatschek, *Crypto 95 pp 43–56*

The authors report an elliptic curve version of Diffie-Hellman implemented over $GF(2^{155})$ using a fast technique that computes reciprocals in about the same time as three multiplications. This technique is described in detail. Exponentiation takes hundreds of milliseconds on a 25MHz SPARC and tens on a 155MHz Alpha.

044706 'Improved generalisation common-multiplicand multiplications algorithm of Yen and Laih'
TC Wu, YS Chang, *Electronics Letters V 31 no 20 (28/9/95) pp 1738–1739*

Yen and Laih produced an algorithm for multiplication where one of the multiplicands is used repeatedly (**024624**); this paper points out a minor optimisation.

8 Theoretical Cryptology

044801 'Precomputing Oblivious Transfer'
D Beaver, *Crypto 95 pp 97–109*

The author shows how an oblivious transfer may be precomputed at the cost of a number of transfers that depends only on the security parameter.

044802 'Secret Sharing with Public Reconstruction'
A Beimel, B Chor, *Crypto 95 pp 353–366*

Secret sharing schemes traditionally use a private channel for reconstruction; if this is not available, then each participant could have $O(n)$ one time pads. A more efficient scheme is to allow multiple reconstructions by different subsets of parties.

044803 'On General Perfect Secret Sharing Schemes'
GR Blakely, GA Kabatianski, *Crypto 95 pp 367–371*

The authors provide a new bound for the cardinality of general perfect secret sharing schemes, and show that for every IT-ideal perfect secret sharing scheme the independent sets A such that $h(A) = \mid A \mid$ define a matroid.

044804 'Quantum Cryptanalysis of Hidden Linear Functions'
D Boneh, RJ Lipton, *Crypto 95 pp 424–437*

The authors show that Shor's result on quantum factoring can be extended to break a large class of cryptosystems, namely those based on a 'hidden linear form' over a suitable algebraic structure. Systems now vulnerable to a quantum computer include those based on elliptic curves.

044805 'Collusion-Secure Fingerprinting for Digital Data'
D Boneh, J Shaw, *Crypto 95 pp 452–465*

The authors define a c-frameproof code to be one such that the only codewords in the feasible set of a coalition of up to c users are the codewords of members of the coalition. They show that for $l = 16c^2 \log n$, there exists an (l, n) error correcting code that is c-frameproof. None of these codes is completely secure against the possibility that colluding attackers could generate a string that was not a codeword; however, if a small probability of error is introduced, some security properties can be established. The size of collusions must be at most the logarithm of the number of users n, and codes of length $\log^6 n$ are constructed.

044806 'A Quantum Jump in Computer Science'
G Brassard, *Computer Science Today — Recent Trends and Developments, Springer LNCS v 1000 pp 426–440*

The author reviews quantum cryptography and quantum computation at the level of a general scientific audience. He starts off with quantum coin flipping and goes on to discuss entangles states. A discussion of Shor's quantum factoring algorithm leads into a description of elementary quantum cryptography and finally to the prospect of teleportation.

044807 'Associative one-way function and its significance to cryptographics'
LR Chao, YC Lin, *International J of Information and Management Sciences (ROC) v 5 no 2 (September 1994) pp 53–59*

The authors showed that associative one-way functions are sufficient to construct public key distribution protocols and public key cryptosystems.

044808 'Secure Signature Schemes based on Interactive Protocols'
R Cramer, I Damgård, *Crypto 95 pp 297–310*

The authors show that strong signatures can be constructed from any secure zero-knowledge protocols. In particular, a three pass public coin proof of knowledge for a hard problem and a collision free hash function are enough to give signatures that are unforgeable under adaptive chosen message attacks.

044809 'Committed Oblivious Transfer and Private Multi-Party Computation'
C Crépeau, J van de Graaf, A Tapp, *Crypto 95 pp 110–123*

The authors present a protocol to transfer committed bits in an oblivious way. It uses standard bit commitment and oblivious transfer as black box primitives.

044810 'Honest verifier versus Dishonest Verifier in Public Coin Zero Knowledge proofs'
I Damgård, O Goldreich, T Okamoto, *Crypto 95 pp 325–338*

Public coin Arthur-Merlin proof systems that are zero-knowledge for an honest verifier can be turned into systems that are zero-knowledge for all verifiers. Two different transformations are provided for this.

044811 'Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver'
S Halevi, *Crypto 95 pp 84–96*

The author shows how any claw-free family of permutations can be used to provide an efficient bit commitment scheme where only the sender is bounded.

044812 'Authentication Codes for Nontrusting Parties Obtained from Rank Metric Codes'
T Johansson, *Designs, Codes and Cryptography v 6 no 3 (Nov 95) pp 205–218*

The author uses rank distance codes to construct new authentication codes that permit arbitration and protect against deception by the participants as well as by third parties. The level of protection against different parties can be traded off in this scheme.

044813 'Improved Efficient Arguments'
J Kilian, *Crypto 95 pp 311–324*

New, more efficient ways of constructing zero knowledge arguments from hard problems such as discrete log are exhibited. The complexity of arguing a proof can be tightly bounded by the complexity of verifying it. The construction combines the features of a number of different probabilistically checkable proofs.

044814 't-Cheater Identifiable (k, n) Threshold Secret Sharing Schemes'
K Kurosawa, S Obana, W Ogata, *Crypto 95 pp 410–423*

The authors demonstrate a t-cheater identifiable (k, n) threshold secret sharing scheme for $k > 3t + 1$ and the size of the set of shares is independent of n.

044815 'How to Exploit the Intractability of Exact TSP for Cryptography'
S Lucks, *FSE 94 pp 298–304*

The author proposes a one-way hash function and a pseudorandom generator based on the exact travelling salesman problem.

044816 'On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols'
D Mayers, *Crypto 95 pp 124–135*

The author shows that the security of a quantum oblivious transfer from Alice to Bob against Bob implies its security against an eavesdropper Eve, and that it also implies the security of a quantum key distribution protocol.

044817 'Information-Theoretic Bounds for Authentication Codes and Block Designs'
DY Pei, *Journal of Cryptology v 8 no 4 (Autumn 95) pp 177-188*

The author derives an information theoretic bound for rth order spoofing, that is, successfully changing the $(r+1)$st of a series of encoded messages. He shows that partially balanced t-designs may achieve this bound.

044818 'Group commitment protocol based on zero knowledge proofs'
TC Wu, TS Wu, *Computer Communications v 18 no 9 (September 1995) pp 654–656*

This paper presents a group commitment protocol which can verify the members of a certain group without revealing the prover's or verifier's secret. It is based on zero knowledge proofs that succeed only if both the prover and verifier are in the same group. The paper also discusses the problems of dynamically adding and deleting group members in the existing system.

9 Book Reviews

'CHIPKARTEN IM GESUNDHEITSWESEN'
Bundesamt für Sicherheit in der Informationstechnik
Bundesanzeiger, 4 May 1995; ISSN 0720-6100 (in German)

This report from the German information security agency looks at the security aspects of introducing smart cards into health care. It tackles the problems from a number of different aspects; it castigates the traditional IT security culture of considering only the security technology and occupational psychology approaches, and considers the legal, social, political and professional problems as well.

The many points it makes include that when systems create so many dependencies that they become a threat, it is irrelevant how many external threats they withstand; that automation can lead to the loss of context of data; that the security culture of all participants needs to be developed; that the ownership and allowable uses of the data need to be defined; and that patients must maintain control over information sharing between doctors. It recommends evaluation levels of E2/E3 for administrative data, E4/E5 for diagnoses and E3/E4 for treatments.

When building such systems, one must be very clear about goals, and it is particularly dangerous to talk about security on the surface when the real underlying issue is power and control. If the only goal is to control health costs, then one could end up with systems which financially penalise doctors who spend more time with their patients, and to an increasing perception of illness as self-inflicted. Such developments might not be in patients' interests, and this could greatly complicate the security, reliability and even legal acceptability of the system.

'PRACTICAL COMPUTER NETWORK SECURITY'
Mike Hendry
Artech House, 1995; ISBN 0-89006-801-1

This book explains the basic concepts of encryption and access control at the level of a non-technical beginner in the subject. Some typical products, such as line encryptors and dongles, and applications such as banking, are described in a general way.

'HANDBUCH DER CHIPKARTEN'
Wolfgang Rankl, Wolfgang Effing
Carl Hanser Verlag, 1995; ISBN 3-446-17993-3 (in German)

The authors provide an overview of the smartcard state of the art. They cover physical and electrical characteristics, the elements of cryptography and random number generation, operating system architectures and typical communications protocols. They also discuss some of the possible defences against microprobing attacks, such as covering EEPROM cells with metallisation that is critical to the chip's function; using capacitance to check for the continued presence of the passivation layer; having under- and over-voltage detectors and minimum clock speeds. A number of software security measures are also described.

They go on to describe a number of typical smartcard applications, including public and GSM telephone cards, the health insurance cards used in Germany since late 1994, and possible future electronic purses.

'INTEGRITY PRIMITIVES FOR SECURE INFORMATION SYSTEMS'
Antoon Bosselaers, Bart Preneel (Editors)
Springer Lecture Notes in Computer Science vol 1007, 1995; ISBN 3-540-60640-8

This volume is the final report of the European Commission's RACE Integrity Primitives Evaluation project, which set out to provide a set of integrity primitives for use in Europe.

The emphasis is on hash functions. The first section describes MDC-4, a has function based on DES that processes messages in 64-bit blocks, using 4 rounds of DES per block, to provide a 128-bit output. this design is aimed at systems using DES hardware devices. The second, RIPE-MD, is an MD4 derivative, and the third is a MAC based on RIPE-MD; since the break of MD4, RIPE-MD has been superseded by new proposals. The final proposal of this type is IBC-hash, a provably secure authentication code system with the usual drawback that each key may only be used once.

The rest of the book sets out SKID, a pair of challenge-response protocols for entity authentication; COMSET, a similar protocol that also yields a shared secret for use as a key by the parties; and a description and discussion of RSA, including how to generate good keys. Source code in C is given for the hash functions, but not for the authentication protocols or RSA.

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: Corporate subscriptions cost £95, and individual subscriptions are available at the reduced rate of £60. Purchase orders are accepted for corporate 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 1996 (volume 4) plus a set of the remaining back numbers (currently v 2 no 1, 3 and 4 and all of v 3 and v 4) at a price of £90 for individual subscribers and £145 for corporate subscribers. Electronic copies of back numbers a year and more old may be fetched from `http://www.cl.cam.ac.uk/users/rja14`.

Individual subscription for 1996 — Please debit my VISA/MasterCard £60 ☐ I enclose a cheque for £60 ☐ / US$90 ☐

Individual subscription for all available 1993–1996 issues — Please debit my VISA/MasterCard £90 ☐ I enclose a cheque for £90 ☐ / US$135 ☐

Corporate subscription for 1996 — Please debit my VISA/MasterCard £95 ☐ I enclose a purchase order / cheque for £95 ☐ / US$142.50 ☐

Corporate subscription for all available 1993–1996 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: ....

We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint `E5C7 93BE 379D 2842 49DC A809 A147 05F6` can be fetched from `http://www.cl.cam.ac.uk/users/rja14`. You can also 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