Volume 7 Number 1 (March 1998) ISSN 1352-6278

CONTENTS

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

'Computer and Communications Security Reviews' is published quarterly by, and is copyright of, Northgate Consultants Ltd. 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 March 1998, and most books and technical reports received by the editor prior to this date. We also have reviews of papers in the following conference and workshop proceedings:

SEISMED 96: Data Security for Health Care – Volume I (Management Guidelines), Volume II (Technical Guidelines), Volume III (User Guidelines); Material presented by the SEISMED Consortium; *published by IOS Press, ISBN 90-5199-263-7, 90-5199-265-3, 90-5199-266-1*

FC 97: Financial Cryptography: First International Conference; February 24–28 1997, Anguilla, British West Indies; *proceedings published by Springer-Verlag as LNCS v 1318, ISBN 3-540-63594-7*

NISSC 97: 20th National Information Systems Security Conference, October 7–10, 1997, Baltimore, Maryland; *proceedings published by NIST*

MIE 97: Medical Informatics Europe; *proceedings published by IOS Press as Studies in Health Technology and Informatics v 43, ISBN 90-5199-343-9*

IICIS 97: First IFIP TC11 WG11.5 Working Conference on Integrity and Internal Control in Information Systems, December 4–5 1997, Zürich, Switzerland; *proceedings published by Chapman and Hall, ISBN 0-412-82600-3*

ITSP 97: Usenix Symposium on Internet Technologies and Systems, December 8–11, 1997, Monterrey, California; *proceedings published by the Usenix Association, ISBN 1-880446-91-X*

Usenix Security 98: Seventh USENIX Security Symposium, 26–29 January 1998, San Antonio, Texas; *proceedings published by the Usenix Association, ISBN 1-880446-92-8*

FSE 98: Fifth International Workshop on Fast Software Encryption, March 23–25, 1998, Paris, France; *proceedings published by Springer-Verlag as LNCS v 1372, ISBN 3-540-64265-X*

Conference proceedings from which only one or two papers have been abstracted are cited inline in the review.

We place an electronic version 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 and up-to-date electronic versions as well; subscription information may be found inside the back cover. The archives can be found at `http://www.cl.cam.ac.uk/users/rja14/#SR`.

1 Applications and Engineering

071101 'A Cautionary Tale'
N Barron, *Secure Computing Magazine (Feb 98) p 21*

The author uses the example of a flawed M-228 designed by Friedman to warn about rushed systems implementation and the dangers of skimping on independent verification (see also **071138** below).

071102 'Secure Software Distribution System'
T Bartoletti, LA Dobbs, M Kelley, *NISSC 97 pp 191–201*

A practical tool for managing software authentication, upgrades and patches management is presented. The system operates in a distributed environment; its server part reviews releases of new system software, stores the software and evaluates target systems' state, while the agent part is responsible for a single target system, operating under the server's commands.

071103 'A Coding Approach for Detection of Tampering in Write-Once Optical Disks'
M Blaum, J Bruck, K Rubin, W Lenth, *IEEE Transactions on Computers v 47 no 1 (Jan 98) pp 120–125*

The authors present a method for detecting tampering with supposedly write-once media; it uses an additional layer of error detection codes.

071104 'Security of Healthcare Information Systems Based on the CORBA Middleware'
B Blobel, M Holena, *MIE 97 pp 10–14*

The paper reviews security aspects of CORBA applicable in healthcare informatics and discusses the role of security in middleware.

071105 'Macro virus identification problems'
V Bontchev, *Computers and Security v 17 no 1 (1998) pp 69–89*

This is a detailed review of macro virus issues, including problems with independent macro identification and VBA5 identification. The author also discusses virus authors' exploitation of such problems and gives some suggestions for antivirus product improvement.

071106 'Cognitive, associative and conventional passwords: Recall and guessing rates'
J Bunnell, J Podd, R Henderson, R Napier, J Kennedy-Moffat, *Computers and Security v 16 no 7 (1997) pp 629–641*

The paper reports an experiment with conventional passwords; they turn out to provide better results than both cognitive and associative passwords. Guessability is too high with cognitive passwords and recall rates are too low with associative passwords.

071107 'Copyright Labeling of Digitized Image Data'
S Burgett, E Koch, J Zhao, *IEEE Communications Magazine v 36 no 3 (Mar 98) pp 94–100*

The authors outline a method for embedding frequency-hopped randomly sequenced pulse position modulated code into JPEG images. Experimental results on this watermark resistance to some image processing methods are described.

071108 'A Gracious But Tragic Special ULTRA Message'
C Burke, *Cryptologia v XXII no 1 (Jan 98) pp 29–32*

The author relates that US bombing of trains with UK prisoners of war was kept secret to protect UK access to Enigma communications between Italy and Germany.

071109 'National rollouts improve diagnosis for healthcards'
Card World Independent (Jan 98) pp 4–5

This article reviews various European healthcare smartcard projects, setting a clear distinction between administrative and clinical cards. Privacy issues are briefly mentioned.

071110 'Improving the Fault Tolerance of GSM Networks'
MF Chang, YB Lin, SC Su, *IEEE Network v 12 no 1 pp 58–63*

The authors review current mechanisms for recovering from failures in the GSM visitor and home location register databases and suggest a new algorithm for home registers to identify visitor registers after a failure.

071111 'Chips on banknotes only a matter of time'
D Cooke, *Fraud Watch v 6 no 1 pp 6–7*

The article reviews recent developments in applying microchips to banknotes, focusing on the De La Rue Kryptal technology.

071112 'Secure Spread Spectrum Watermarking for Multimedia'
IJ Cox, J Killian, FT Leighton, T Shamoon, *IEEE Transactions on Image Processing v 6 no 12 (Dec 97) pp 1673–1687*

The authors argue for watermarks to be independent and identically distributed Gaussian random vectors placed in the most significant components of the image spectrum. They should then resist most signal processing operations as well as multiple watermark or collusion attacks.

071113 'StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks'
C Cowan, C Pu, D Maier, H Hinton, J Walpole, P Bakke, S Beattie, A Grier, P Wagle, Q Zhang, *Usenix Security 98 pp 63–77*

The authors describe their StackGuard tool which protects against buffer overflow attacks by preventing and detecting modifications to the return address of a function. No change to the source code is required and the compiler patch is publicly available. Results of a performance analysis are given.

071114 'Basic rules for the security of frozen section diagnosis through image transmission between anatomo-pathologists'
P Dusserre, FA Allaert, L Dusserre, *MIE 97 pp 171–175*

The confidentiality, integrity and availability of information communicated during remote pathology examinations are discussed.

071115 'Secure Network Communications and Secure Store & Forward Mechanisms within the SAP R/3 System'
B Esslinger, J Schneider, *FC 97 pp 395–407*

The authors describe how cryptographic capabilities and security features have been integrated into SAP's R/3 business software. They show how 'real world' business applications must contend with emerging standards, export controls, and open networks in achieving their security objectives.

071116 'Nationwide to test biometrics at ATM'
Financial Technology International Bulletin v 15 no 5 (Jan 98) pp 1, 12

The article reports on UK and US trials of an NCR/Sensar iris verification system for cash machines.

071117 'Security in data networks'
SE Forrester, MJ Palmer, DC McGlaughlin, MJ Robinson, *BT Technology Journal v 16 no 1 (Jan 98) pp 52–75*

This paper outlines the security features of the Concert IP SubNet, a managed switched multi-megabit data service (SMDS) provided by British Telecom. Encryption

is done by DES in most cases, with default 24-hour re-keying using Diffie-Hellman key agreement for Concert end-to-end keys. SMDS uses mainly link-layer encryption with keys software-updated using RSA. ATM security is also discussed.

071118 'Secure Provision of UMTS Services over Diverse Access Networks'
JC Francis, H Herbrig, N Jefferies, *IEEE Communications Magazine v 36 no 2 (Feb 98) pp 128–136*

The article overviews the European ACTS framework projects EXODUS, COBUCO, and namely ASPECT, briefly outlining security features within these.

071119 'Security Tools – A "Try Before You Buy" Web-Based Approach'
S Frankel, *NISSC 97 pp 443–451*

This describes a NIST website providing security and other tools together with comprehensive information on them.

071120 'Banking on the mobile operators'
Fraud Watch v 6 no 1 pp 8–9

This is a discussion on the suitability of GSM as a delivery platform for mobile financial services, with some comments on the authentication aspects.

071121 'Standards issues hamper chip adaption'
Fraud Watch v 6 no 1 p 10

The article voices some comments on the lack of security standards and on card issuer confidence problems arising when academics expose smartcard vulnerabilities.

071122 'Modern Times'
H Fuhs, *Information Security Bulletin v 3 no 1 (Feb 98) pp 13–19*

The author reviews various aspects of storage media deterioration and implications for data backups.

071123 'How to Make Personalized Web Browsing Simple, Secure, and Anonymous'
E Gabber, PB Gibbons, Y Matias, A Mayer, *FC 97 pp 17–31*

The authors present a solution that automatically creates and manages user login IDs and passwords for accessing websites. The tool protects the true identity of a user, and supports 'anonymous personalised web browsing' that elaborates on Chaum's idea of digital pseudonyms.

071124 'Security Modeling for Public Safety Communication Specifications'
DW Gambel, *NISSC 97 pp 514–521*

Since 1989, the USA has had a project to create uniform standards for public safety communications (police, fire, ambulance and so on). The resulting architecture is based loosely on Bell-LaPadula and was described abstractly in **054206**; this article sets it in its engineering context.

071125 'Antivirus Technology offers New Cures'
L Garber, R Raucci, *IEEE Computer (Feb 98) pp 12–14*

The authors review IBM's net-based immune system project, the University of New Mexico's T cell algorithm and other novel approaches to virus protection.

071126 'What Is Wild?'
S Gordon, *NISSC 97 pp 177–190*

The author reviews the two concepts of virus testing — on more-or-less superficial virus collections or 'in the wild'.

071127 'Digit-serial multiplier for finite fields $GF(2^m)$'
JH Guo, CL Wang, *IEE Proceedings in Computers and Digital Techniques v 145 no 2 (Mar 98) pp 143–148*

A digital systolic array for computing multiplications in finite fields $GF(2^m)$ with the standard basis representation is presented. It is aimed at a VLSI implementation with a fault-tolerant design.

071128 'Software Generation of Practically Strong Random Numbers'
P Gutmann, *Usenix Security 98 pp 243–257*

The author reviews current applications of random number generators and some of the known problems. He then suggests a generator that does not require special hardware or access to privileged system services, yet provides sufficient randomness for most cryptographic applications. The mixing function is based on a hash function and the randomness collector uses data sources that are relatively safe from a non-privileged attacker; the system data it uses are described for DOS, Wintel, OS/2, Mac and Unix platforms.

071129 'Automated Intrusion Detection Systems and Network Security'
B Hancock, *Network Security (Jan 98) pp 14–15*

This is a general overview of intrusion detection systems for networks.

071130 'Smarter Smartcards'
P Hofland, L Janowski, *Byte – ByteExtra International (Feb 98) pp 7–10*

This is a discussion of smartcard operating systems, Java support and security applications.

071131 'Secure Videoconferencing'
P Honeyman, A Adamson, K Coffman, J Janakiraman, R Jerdonek, J Rees, *Usenix Security 98 pp 123–130*

The authors overview their modification of a videoconferencing application to support the Internet Generic Security Services interface. RC4, VRA (a DES-based Goldreich-Levin PRNG seeded stream cipher) and DES are implemented, together with the Shoup-Rabin smartcard-based key distribution protocol (**053434**).

071132 'A Process of Data Reduction in the Examination of Computer Related Evidence'
MF Horvath, *NISSC 97 pp 381–393*

The author discusses systems developed for the FBI to examine large quantities of files seized in evidence. Known files can be excluded by virtue of their CRCs, which are computed anyway to secure the evidence; a new version will identify file types by histograms of byte frequencies.

071133 'Review of High Capacity Media'
CF Hughes, A Jepson, *Information Security Bulletin v 2 no 6 (Dec 97) pp 21–27*

The authors review the future of high-capacity storage devices for use in data backup, and suggest that hybrid magnetic-optical technology will be the main contender after the year 2000.

071134 'Automated Information System – (AIS) Alarm System'
W Hunteman, *NISSC 97 pp 394–405*

The paper provides a high-level overview of an intrusion detection and response system for small to medium sized local networks.

071135 'Smart card security'
P Hunter, *Information Security Monitor v 13 no 3 (Feb 98) pp 5–7*

The article briefly reviews smartcard security issues, concluding that smartcard security is still at a relatively embryonic stage.

071136 'Beyond the Phone Card: Emerging Smart Card Opportunities'
CR Jarvis, *GEC Review v 12 no 3 pp 131–137*

This article reviews some security issues of phone smartcard applications, namely authentication and the use of cryptography.

071137 'Exploring Steganography: Seeing the Unseen'
NH Johnson, S Jajodia, *IEEE Computer (Feb 98) pp 26–34*

The authors review the basics of steganography, noting that steganography should supplement rather than replace cryptography. They also test the image degradation and usability of StegoDos, White Noise Storm and S-Tools software.

071138 'Soviet Comint in the Cold War'
D Kahn, *Cryptologia v XXII no 1 (Jan 98) pp 1–24*

The author reviews the history of Soviet communications intelligence, and suggests that bugging and traitors provided substantially more information to the Soviets than cryptanalysis. He notes, for example, that the Soviets' break of Purple and their knowledge of how to break Enigma were not fully exploited because of a shortage of trained manpower and technology. He also describes recent reforms which merged the 8th and 16th directorates of the KGB into the new Russian sigint agency FAPSI, whose roles include running the national election system.

071139 'The SIGCUM Story: Cryptographic Failure, Cryptologic Success'
SJ Kelly, *Cryptologia v XXI no 4 (Oct 97) pp 289–316*

This article tells the story of a wartime US teletype cipher machine, the SIGCUM or M-228, which used a keystream generated by a rotor maze. The maze design was designed by Friedman, broken by Rowlett, and an improved version agreed and fielded without theoretical analysis. After their introduction in January 1943, a monitoring facility observed reuse of a key giving a depth. This led Rowlett to attempt a reconstruction of the M-228 circuitry, like Tutte's of FISH, and he was successful (the details are given). The M-228 was taken out of service at once, and modified; top priority was given to the introduction of one-time tape systems. One of the main lessons learned was the value of trying to break one's own traffic.

071140 'Cryptanalytic Attacks on Pseudorandom Number Generators'
J Kelsey, B Schneier, D Wagner, C Hall, *FSE 98 pp 168–188*

The authors describe a number of generic attacks on the algorithms used in random number generators to accumulate environmental randomness into a pool of state which is then used to generate keys, IVs or nonces. An attacker may manage to compromise the state; such compromises should be localised in time with the generator able to recover (and to protect outputs generated before the compromise). In addition, an attacker who can control the environmental input may be able to force the generator into a predictable state, or cause it to cycle with a known period. The vulnerabilities of the ANSI X9.17, DSA, Cryptolib and RSAREF generators are discussed in the context of this model, and some design principles for generators are enunciated.

071141 'Implementing Security On a Prototype Hospital Database'
M Khair, G Pangalos, F Andria, L Boizos, *MIE 97 pp 176–180*

The paper outlines an experiment with a prototype secure database implementation in a Greek hospital.

071142 'The Maginot License: Failed Approaches to Licensing Java Software Over the Internet'
MD LaDue, *Information Security Bulletin v 3 no 1 (Feb 98) pp 33–43*

This article reviews issues faced by Java code developers providing try-before-you-buy software and argues that the current common means of protection just amount to security by obscurity.

071143 'An Application of Machine Learning to Anomaly Detection'
T Lane, CE Brodley, *NISSC 97 pp 366–380*

The authors present a system that extends anomaly detection by machine learning. This is implemented for UNIX command tracking and is based on characteristic sequences of user actions.

071144 'Single-Chip Implementation of a Cryptosystem for Financial Applications'
N Lange, *FC 97 pp 135–144*

The design of a hardware General Crypto Device is described; it has an 8 bit controller, a 32 bit RISC processor to do arithmetic, a hardware DES engine and 4K of internal memory. It is claimed to run DES in any mode at 100 Mbit/s, IDEA at 16Mbit/s and average 40 RSA encryptions of 512 bits every second.

071145 'Data Mining Approaches for Intrusion Detection'
W Lee, SJ Stolfo, *Usenix Security 98 pp 79–93*

A framework for deployment of data mining techniques in intrusion detection is presented. This provides data classification and two algorithms implemented — using association rules and frequency episodes programs. Pattern identification for the two algorithms is discussed, together with some experimental results for *tcpdump* and *sendmail*.

071146 'Bodily Power'
A Lewcock, *Computer Business Review v 6 no 2(Feb 98) pp 24–27*

The article reviews current biometric technology, noting that sales of fingerprint-based products account for 78% of the total. It predicts that we will see decent technology and market maturity in 5-10 years.

071147 'Firewalls fend off invasions from the Net'
SW Lodin, CL Schuba, *IEEE Spectrum v 35 no 2 (Feb 98) pp 26–34*

The article provides an overview of firewall technology, discusses relevant TPC/IP issues and makes some suggestions for firewall evaluation.

071148 'Investment Appraisal of the Protection, Confidentiality and Security Arrangements of Patient Data'
D Loftus, T Carroll, *MIE 97 pp 186–190*

This paper discusses the implementation of access and related controls at a major Dublin hospital. Problems detected ranged from password sharing to software piracy. Patient awareness of confidentiality issues was low, except for patients from outside the EU and from the former USSR in particular.

071149 'Defending from the Unthinkable'
P Loshin, *Byte (Dec 97) pp 67–74*

Extranet access is discussed in terms of the available authentication protocols and of devices like SecurID ACE and Bellcore S/Key. Firewall issues are also discussed.

071150 'Document Identification for Copyright Protection Using Centroid Detection'
SH Low, NF Maxemchuk, AP Lapone, *IEEE Transactions on Communications v 46 no 3 (Mar 98) pp 372–383*

The authors describe a text document watermarking method that shifts selected lines of text vertically, or moves words horizontally, on different copies of a document. A prototype implementation is presented together with experimental results that show a high degree of robustness against scanning, faxing and photocopying.

071151 'Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective'
DP Maher, *FC 97 pp 109–121*

The author discusses various recently published hardware attacks, and in particular differential fault analysis. He denies that these attacks could be effective against Mondex and criticises the hype surrounding their announcement.

071152 'Network and data security design for telemedicine applications'
L Makris, N Argiriou, MG Strintzis, *Medical Informatics v 22 no 2 (Apr-Jun 97) pp 133–142*

The authors propose a framework for applying cryptography to protect the privacy of personal medical information in networks, developed in the context of the SEISMED programme. PGP key formats were used.

071153 'Forming a Health Care Incident Reporting Scheme'
KG Mavroudakis, SK Katsikas, DA Gritzalis, *MIE 97 pp 839–843*

The authors discuss several issues in the design of an incident reporting scheme for healthcare information systems undertaken under the EU ISHTAR programme.

071154 'Towards Continuously Auditable Systems'
NH Minsky, *IICIS 97 pp 23–41*

The author introduces the concept of sensors to be introduced in a system in such a way that the system can be audited continuously without interfering with its normal operation.

071155 'An Introduction to Macro Viruses'
I Muttik, *Information Security Bulletin v 3 no 1 (Feb 98) pp 21–30*

This is a comprehensive introduction to macro viruses, particularly those infecting Microsoft applications.

071156 'The Spectrum of Modern Firewalls'
M Nacht, *Computers and Security v 17 no 1 (1998) pp 54–56*

This is a review of current firewall technology, with some discussion of stateful inspection technology.

071157 'Bro: A System for Detecting Network Intruders in Real-Time'
V Paxson, *Usenix Security 98 pp 31–51*

The paper describes an Internet-oriented network intrusion detection system. Its first basic component is an 'event engine' that translates filtered packet streams into a high-level network event stream and its second component is a specialised-language policy script interpreter dealing with event handlers. Implementations for finger, FTP, portmapper and telnet are described.

071158 'EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances'
PA Porras, PG Neumann, *NISSC 97 pp 353–365*

A distributed network tool for network surveillance, attack isolation and management of response activities is presented. It uses dynamically deployable, highly distributed and independently controllable service monitors that can be positioned at various levels of the monitored system. The tool also supports coordinated dissemination of analyses from the monitors to counter network-wide coordinated attacks.

071159 'A computerized record hash coding and linkage procedure to warrant epidemiological follow-up data security'
C Quantin, H Bouzelat, L Dusserre, *MIE 97 pp 339–342*

French privacy law, and the EU data protection directive, are in tension with local crypto policy; the former promote the use of de-identified data while the latter render some of the obvious mechanisms ineffective. A solution described in this paper is to

use a one-way hash of the patient name together with unique keys for both sender and recipient. Mechanisms for record linkage are also supported; their effectiveness was tested in the teaching hospital at Dijon.

071160 'Datenschutz im Transplantationsgesetz'
S Rixen, *Datenschutz und Datensicherheit v 22 no 2 (Feb 98) pp 75–80*

The author discusses the data protection aspects of organ transplantation, about which a new law was recently enacted in Germany. Problems considered include maintaining the anonymity of donors and potential recipients of organs in case where the donor is deceased, the availability of clinical information in cases of medical need, the complexities of dealing with organs traded internationally, and protecting waiting lists from manipulation.

071161 'Security of the Electronic Health Record'
FH Roger France, *MIE 97 pp 167–170*

The author discusses the electronic patient record concept and its associated security issues.

071162 'Go Ahead, Visit Those Web Sites, You Can't Get Hurt ... Can You?'
JS Rothfuss, JW Parrett, *NISSC 97 pp 80–94*

This article talks about web security, mobile code, and so on.

071163 'Go Ahead, Visit Those Web Sites, You Can't Get Hurt ... Can You?'
JS Rothfuss, J Parrett, *Computer Fraud and Security Bulletin (Feb 98) pp 11–15*

This is a magazine version of the above article.

071164 'Nigeria backs high value e-purse'
M Rowe, *Banking Technology (Mar 98) p 6*

An e-purse project whose smartcards can be loaded with more than £100,000 has been launched in Nigeria, motivated by the fact that the supply of banknotes is inadequate.

071165 'Paper High Availability Configurations for Large UPS Systems'
H Ruff, *Information Security Bulletin v 3 no 2 (Mar 98) pp 23–31*

The author reviews some current UPS features and typical configurations.

071166 'Die Entwicklung enier ärztlichen Kommunikationsordnung'
HD Schirmer, *Datenschutz und Datensicherheit v 22 no 2 (Feb 98) pp 69–75*

The author examines the ethical implications of medical telematics in the contexts of safety and of professional and patient privacy, for which new regulations were introduced in Germany in July 1997, heavily influenced by the EU data protection directive and the issue of health insurance cards to the population.

071167 'Securing Third Party connections'
EE Schultz, *Network Security (Jan 98) pp 10–13*

This article discusses security issues with third-party connectivity and suggests several generic solutions both for networks with firewalls and for more general systems.

071168 'Communications Security Solutions'
Secure Computing Magazine (Feb 98) pp 48–54

This review of desktop Internet security add-ons ranges from Java and ActiveX code scanners and unauthorised access alarms through S/MIME e-mail clients with LDAP support to challenge-response tokens.

071169 'Companies to Watch in 1998'
Secure Computing Magazine (Jan 98) pp 18–22

The article suggests that new business growth could come in biometrics, PC marking and tagging, access control tokens, forensics software, network security and Y2K solutions.

071170 'Weaving Technology and Policy Together to Maintain Confidentiality'
L Sweeney, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 98–110*

The author compares three systems for de-identifying medical records for use in research. She presents an analysis of the circumstances in which various strategies fail to work; local effects such as concentration of ethnic groups and the effects of rare events and unusual cases have the potential to discredit many systems: phrases such as 'he developed Hodgkin's while US ambassador in England' can be a complete give-away but are very hard to spot using automatic mechanisms. Bin size is always a problem, and there must be explicit procedures between the data owner and user to share the residual risk.

071171 'FOIN: a Nominative Information Occultation Function'
G Trouessin, FA Allaert, *MIE 97 pp 196–200*

The authors discuss the use of SHA hash function and Shamir's threshold scheme for de-identifying patient records in a French system for communication between healthcare insurers and hospitals.

071172 'Medical Record Confidentiality — Law, Scientific Research, and Data Collection in the Information Age'
RC Turkington, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 113–129*

The author discusses how to maintain confidentiality in the proposed national US medical record system. He covers a number of nonconsensual disclosure abuses from coerced consent through government privileges, judicial discovery and law enforcement access and provides a very extensive bibliography of US legal precedents.

071173 'Security of Medical Image Databases'
S Tzelepi, G Pangalos, M Khair, *MIE 97 pp 470–474*

The authors describe implementing security of a medical image database in a Greek hospital along Bell-LaPadula lines.

071174 'In Search of SSL Spidering'
J Udell, *Byte (Feb 98) pp 97–100*

The author outlines some of the lessons of using WinInet and SSLeay for choosing a tool for secure document monitoring and download.

071175 'The Value of Free Software'
J Udell, *Byte (Dec 97) pp 109–112*

Free software packages such as Apache and Stronghold web servers are discussed with some notes on SSL support.

071176 'A First German Cryptologic Exhibition'
M van der Meulen, *Cryptologia v XXII no 1 (Jan 98) pp 33–48*

An overview of the German Information Security Agency's historic exhibition is provided. The museum is located close to Bonn and hosts mechanical and electromechanical rotor machines.

071177 'A Practical Approach to Design and Management of Secure ATM Networks'
V Varadharajan, R Shankaran, M Hitchens, *NISSC 97 pp 213–232*

The design and layer positioning of security services in ATM networks is discussed in this version of **064192**.

071178 'Constructing Computer Virus Phylogenies'
LA Goldberg, PW Goldberg, CA Phillips, GB Sorkin, *Journal of Algorithms v 26 no 1 (Jan 98) pp 188–208*

Many computer viruses incorporate code fragments from earlier viruses, and in this paper the authors analyse the problem of constructing a phylogeny or family tree of viruses. Finding the best such turns out to be NP-hard, although quite usable phylogenies can be found in practice; the complexity of the algorithms is discussed in detail. The application lies in building better virus scanners. It emerges that computer viruses are more like bacteria than mammals, in the sense that genetic material can be incorporated from multiple sources simultaneously.

071179 'High-tech Security: The Eyes Have It'
W Webb, *EDN (18/12/97) pp 75–78*

The author discusses the applicability of iris scanning for bank cash machines, with a note that the iris has about 170 degrees of freedom compared to the 30 of the fingerprint. He gives a high-level overview of the Sensar system which uses wavelets to decompose the iris pattern into a 256-byte iris code; this system can capture and verify an iris image within 3-5 seconds.

071180 'DVD cracked'
E Wehde, *Computer Fraud and Security Bulletin (Jan 98) p 7*

The article reports a breach of the Content Scrambling System introduced by the DVD Forum.

071181 'Introduction: Medical Record Confidentiality and Data Collection'
B Woodward, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 85–87*

This article gives an overview of the medical systems privacy debate in the USA and Canada, as a background to the legislation currently going through Congress.

071182 'Medical Record Confidentiality and Data Collection: Current Dilemmas'
B Woodward, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 88–97*

The author describes many of the ways in which US healthcare information systems are falling down on privacy. The creeping failure of the Institutional Review Board system means that more and more identifiable records are available in academia, and the very broad waivers that patients are compelled to sign have destroyed the principle of consent to data sharing. De-identification is a possible solution but the increasing complexity of systems drives implementation costs ever higher. Restrictions on data migration and linkage could also help but are opposed by powerful commercial interests. The upshot is that clinical records will in future be used routinely for research and this will change the nature of medicine.

071183 'A flawed hero'
L Zaidi, *Banking Technology (Mar 98) pp 38–42*

The author introduces basic crypto principles and discusses SET features, noting incompatible standard implementations and complexity. Competing projects Datacash and Café are also mentioned.

2 Operating System and Database Security

071201 'Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies'
V Anupam, A Mayer, *Usenix Security 98 pp 187–199*

The authors describe a class of vulnerabilities in the most common scripting languages: JavaScript and VBscript. The attacks described here can use Trojan horses to steal browser users' private information such as passwords or credit card numbers. The article proposes some design principles that would enhance the security of browsers that allow the execution of scripts and also would lead to design of safer scripting languages.

071202 'View Constraints: an Interpretation of Integrity Constraints for Security'
P Asirelli, *IICIS 97 pp 237–252*

The author discusses integrity constraints checking in logical databases and reviews issues concerning view constraints.

071203 'Enforcing mandatory and discretionary security in workflow management systems'
V Atluri, WK Huang, *Journal of Computer Security v 5 no 4 (1997) pp 303–339*

This paper addresses the problem of specifying and enforcing security constraints in workflow management systems. It tackles both multilevel mandatory and discretionary authorization-based security constraints. Mandatory constraints are enforced by assigning security labels to each task. The proposed approach detects task dependencies which cannot be enforced because of security constraints. Discretionary access control is based on authorizations whose assignment and revocation are synchronized with the workflow so that a subject can gain access to objects only during execution of tasks. Both mandatory and discretionary policies are modeled by Petri nets.

071204 'Role Based Access Control for the World Wide Web'
JF Barkley, AV Cincotta, DF Ferraiolo, S Gavrila, DR Kuhn, *NISSC 97 pp 331–340*

The paper discusses the potential for deploying role-based access control on the web, and in particular for Intranet-type applications.

071205 'The CRISIS Wide Area Security Architecture'
E Belani, A Vahdat, T Anderson, M Dahlin, *Usenix Security 98 pp 15–29*

An architecture for distributed wide area system security is outlined. It uses identity certificates and tickets, encrypted caching, redundancy and local domain administration.

071206 'Using Datatype-Preserving Encryption to Enhance Data Warehouse Security'
M Brightwell, HE Smith, *NISSC 97 pp 141–149*

The authors discuss using simple lossy encryption techniques to mask data in a relational database while preserving data types and most of the relational value.

071207 'Query Answering in Information Systems with Integrity Constraints'
F Bry, *IICIS 97 pp 113–130*

The author argues that current approaches to formalise information system consistency are inadequate, and introduces 'minimal logic' to deal better with local inconsistencies.

071208 'A Comparison of Methods for Implementing Adaptive Security Policies'
M Carney, B Loe, *Usenix Security 98 pp 1–14*

Four methods for implementing adaptive security policies in a separated security server/database and kernel environment are discussed. These include reloading a new security database, expanding the state and security database, implementing a new security server, and implementing task-dedicated security servers. In general, the second and fourth options appear to be the most attractive for implementing adaptive security.

071209 'Automated derivation of global authorizations for database federations'
S Castano, S De Capitani di Vimercati, MG Fugini, *Journal of Computer Security v 5 no 4 (1997) pp 271–301*

This paper presents an approach to designing and enforcing authorizations in federated database systems. The approach derives authorizations at the federation level on the basis of authorizations defined in the component systems. The proposed process, based on the concepts of similarity and abstraction, produces authorizations which allow federated users to execute on remote objects the same accesses they can exercise on "similar" local objects. This derivation can be enforced at the time the federated schema is designed or afterwards.

071210 'Stupid JavaScript Security Tricks'
W Cooke, *NISSC 97 pp 116–127*

Some JavaScript security flaws are outlined. Some examples are given of scripts that will crash systems, steal email addresses, refuse connections referred by particular sites, and so on. His advice 'switch it off and don't use it'.

071211 'Key Concerns in a Review of CA-ACF2/MVS'
N Crocker, *Computers and Security v 17 no 1 (1998) pp 42–53*

The article points some very common problems in CA-ACF2, focussing on the MVS environment. It looks in some detail at system access controls, user privileges and database integrity.

071212 'Towards a definitive paradigm for security in object-oriented systems and applications'
SA Demurjian, TC Ting, *Journal of Computer Security v 5 no 4 (1997) pp 341–382*

This paper presents an approach to specifying and enforcing authorizations in object-oriented systems which is strongly based on the use of encapsulation; it embeds security constraints in application code. The authors address the problem of generating application code enforcing security constraints starting from specified authorizations. Authorizations are stated in terms of user roles and of profiles describing the elements of the data model. The paper illustrates the different design and analysis phases necessary to state security specifications and produce the application code enforcing them.

071213 'A Multi-level Secure Object-Oriented Database Model'
GB Durham, K Kalpakis, *NISSC 97 pp 488–497*

A database model meeting the Orange Book requirements is outlined. The authors develop policies for access control, inference controls, and an implementation strategy based on mandatory and/or discretionary access control.

071214 'The DGSA: Unmet Information Security Challenges for Operating System Designers'
EA Feustel, T Mayfield, *ACM Operating System Review v 32 no 1 (Jan 98) pp 3–22*

The US DoD Goal Security Architecture (DGSA) framework is presented. This might lead to a broader understanding of information security in the DoD, yet practical implementations are still to come. The framework center-pieces are the use of

public networks, support for multiple security policies and deployment of commercial and government-off-the-shelf software.

071215 'Threats And Vulnerabilities For C4I In Commercial Telecommunications: A Paradigm for Mitigation'
J Fowler, RC Seate, *NISSC 97 pp 612–618*

This is a discussion of threats, vulnerabilities and risk reduction in open networks.

071216 'An Extensible Framework for Repairing Constraint Violations'
M Gertz, UW Lipeck, *IICIS 97 pp 89–111*

The paper reviews methods for repairing violations of integrity constraints in relational databases and suggests an algorithm to enumerate alternative minimal repair strategies.

071217 'Outsourcing – A Certification & Accreditation Dilemma?'
H Gillespie, M O'Neill, *NISSC 97 pp 265–275*

The authors discuss outsourcing for government data processing and the problems with certification and accreditation that arise.

071218 'The Gateway Security Model in the Java Electronic Commerce Framework'
T Goldstein, *FC 97 pp 340–354*

The author describes the Gateway extension to the Java security model, within the context of the Java Electronic Commerce Framework, an open platform for financial applications. He reviews the safety and isolation properties of the Java programming language with its 'sandbox' security model, and explains how the Gateway extension provides a complementary model to implement contractual trust relationships.

071219 'Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java Development Kit 1.2'
L Gong, M Mueller, H Prafullchandra, R Schemers, *ITSP 97 pp 103–112*

This is an overview of the Java Development Kit v1.2 security architecture, which enables a clear definition of a security policy, introduces a new hierarchy of typed and parametrised access permissions and supports domain-based access control with easy protection domain definition.

071220 'The Extended Commercially Oriented Functionality Class for Network-based IT Systems'
A Herrigel, R French, H Siebert, H Stiegler, H Tabuchi, *NISSC 97 pp 641–653*

The authors argue for an 'Extended Commercially Oriented Functionality Class' to be used for security evaluation in the commercial environment.

071221 'Observations on the Real-World Implementation of Role-Based Access Control'
B Hilchenbach, *NISSC 97 pp 341–352*

The author outlines features of a tool for enterprise security management that implements role-based access control.

071222 'Protecting databases from inference attacks'
TH Hinke, HS Delugach, RP Wolf, *Computers and Security v 16 no 8 (1997) pp 687–708*

The paper reviews some inference detection approaches, both automated and manual, and concluded with some remarks on future research directions.

071223 'Operating System Protection for Fine-Grained Programs'
T Jaeger, J Liedtke, N Islam, *Usenix Security 98 pp 143–157*

Operating system based security models for control of downloaded executable content are compared with language based protection. An operation system security model

is then presented, together with its implementation on Lava Nucleus – a fast microkernel O/S.

071224 'Design and Assurance Strategy for the NRL Pump'
MH Kang, AP Moore, IS Moskowitz, *IEEE Computer (Apr 98) pp 56–63*

The authors review work on the Network version of the NRL Pump (**031217**) which supports one-way communication between low and high-level systems.

071225 'Vulnerability of "Secure" Web Browsers'
RA Kemmerer, F De Paoli, AL Dos Santos, *NISSC 97 pp 476–487*

The paper reviews the security of Netscape and Microsoft browser security, and particularly the issues relevant to mobile code. Two attacks based on thread name monitoring are presented and the resulting threats to user privacy are discussed.

071226 'Maintaining temporal integrity of World Wide Web pages'
GF Knolmayer, T Buchberger, *IICIS 97 pp 43–63*

The authors discuss the management of temporal data on the web, and present a Java applet to scan for temporal data.

071227 'When Java Was One: Threats From Hostile Byte Code'
MD Ladue, *NISSC 97 pp 104–115*

The author demonstrates that there is no one-to-one correspondence between Java source code and byte code — it is possible to create byte code that no Java compiler can produce and yet it passes through the Java Verifier. Several examples of hostile byte code are discussed in detail.

071228 'A Model for Specifying Individual Integrity Constraints on Objects'
Y Lahlou, *IICIS 97 pp 217–235*

The author presents an integrity constraints specification model which uses assertions and a class-based object data model that allows objects to have individual references to other objects.

071229 'Optimistic Concurrency Control for Maintaining the Global Integrity Constraint in MDBSs'
K Lee, S Park, *IICIS 97 pp 131–151*

A transaction model supporting global integrity constraints in multidatabase systems is presented, together with the optimistic concurrency control to serialise both direct and indirect conflict operations.

071230 'Practical Defenses Against Storage Jamming'
J McDermott, J Froscher, *NISSC 97 pp 162–176*

The paper reviews the problem of storage jamming and defences provided by cryptography, detection objects and replication; the crucial distinction is between internal and external jammers. Replay and replication defences are discussed.

071231 'Expanding and Extending the Security Features of Java'
NV Mehta, KR Sollins, *Usenix Security 98 pp 159–172*

The paper presents an enhancement of applet control features, which relies on using applet activity logs and a newly developed constraint language. The elimination of unauthorised communication via storage channels is one potential benefit. The model implementation is described and its use outside the Java environment is discussed.

071232 'Unified Support for Heterogeneous Security Policies in Distributed Systems'
NH Minsky, V Ungureanu, *Usenix Security 98 pp 131–142*

The authors use an experimental toolkit supporting a range of security policies to build a mechanism that can support different policies in a unified manner in distributed heterogeneous environments.

071233 'Dynamic integrity constraints definition and enforcement in databases: a classification framework'
MA Pacheco e Silva, *IICIS 97 pp 65–87*

The concept of database dynamic integrity constraints is reviewed, and methods for enforcing them are also summarised.

071234 'A network-centric design for relationship-based security and access control'
M Röscheisen, T Winograd, *Journal of Computer Security v 5 no 3 (97) pp 249–254*

The authors propose a capability-based model for the management of heterogeneous network environments. An interface for access control is also discussed.

071235 'Multilevel Architectures for Electronic Document Retrieval'
JA Rome, JS Tolliver, *NISSC 97 pp 505–513*

The paper presents three architectures for multilevel secure document retrieval system — with single or multiple compartmented mode workstations (CMW) and single non-CMW Unix workstations. The system is based on intranet technology and commercial-off-the-shelf software.

071236 'Surviving Denial of Service on the Internet'
W Schwartau, *NISSC 97 pp 619–640*

The author talks about past and potential denial of service attacks on the Internet.

071237 'Managing with Less than Absolute Integrity'
A Sheth, *IICIS 97 pp 195–202*

The author discusses some issues of multidatabase data integrity and quality that arise in operation-centric rather than data-centric systems.

071238 'TRANSMAT Trusted Operations for Untrusted Database Applications'
D Thomsen, *NISSC 97 pp 555–564*

The paper outlines an approach where trusted operations are performed by untrusted database applications with a commercial database and TCB subset architecture. A copy of the database management system then runs at each level.

071239 'Use of SSH on a Compartmented Mode Workstation'
JS Tolliver, D Dillow, *NISSC 97 pp 498–504*

The authors describe implementing Secure Shell (ssh) for compartmented mode workstations, where proper privilege assignment to processes is crucial.

071240 'The Help of Formal Models for Healthcare Security Policies'
G Trouessin, B Barber, *MIE 97 pp 786–790*

The authors argue for the use of modal logic in expressing a healthcare security policy.

071241 'Integrity: Do You Know Where Your Objects Are?'
AE Wade, *IICIS 97 pp 203–215*

Integrity issues in object database systems are compared with those arising in relational databases and in heterogeneous environments with network and node failures; various replication and transaction issues are discussed.

071242 'A New Strategy for COTS in Classified Systems'
SR Wiseman, CJ Whittaker, *NISSC 97 pp 250–264*

The paper outlines the UK MOD strategy for deployment of COTS software (namely Windows NT) in a domain-type environment. Several types of countermeasures against generalised attacks are discussed together with their implementation.

3 Security Management and Policy

071301 'Risiken von Key Recovery, Key Escrow und Trusted Third Party-Verschlüsselung'
H Abelson, R Anderson, SM Belovin, M Blaze, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier, *Datenschutz und Datensicherheit v 22 no 1 (Jan 98) pp 14–23*

This is a German translation of May 97 testimony to the US Senate by a group of cryptologists about the sacrifices in security and cost that a key escrow infrastructure would impose on computer users; its conclusion is that building a secure infrastructure of the breathtaking scale and complexity demanded by US government requirements is far beyond the experience and current competency in the field.

071302 'NRO Reveals Secret Recon Contractors'
JC Anselmo, *Aviation Week and Space Technology 26/1/98 pp 64–66*

The National Reconnaissance Office, which deals with intelligence from satellite photographs, has declassified the names of its contractors; the list is reprinted here.

071303 'Some Systems Implications of EU Data Protection Directive'
B Barber, FA Allaert, *MIE 97 pp 829–833*

The paper reviews some aspects of applying the EU Data Protection Directive to healthcare.

071304 'A Critique of Digital Terrorism'
N Barrett, *Information Security Bulletin v 3 no 2 (Mar 98) pp 13–20*

The author talks about information warfare issues, and suggests that the UK is as vulnerable as US.

071305 'Commentary: Quality, Costs, Privacy and Electronic Medical Data'
DW Bates, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 111–112*

The author argues for changes in policy on electronic medical record privacy.

071306 'High-Tech Security and the Failings of President Clinton's Commission on Critical Infrastructure Protection'
A Bequai, *Computers and Security v 17 no 1 (1998) pp 19–21*

The author criticises the presidential commission for its lack of action and of a comprehensive strategy.

071307 'Software Pirating and Management's Quagmire'
A Bequai, *Computers and Security v 17 no 1 (1998) pp 22–26*

This article discusses software license issues and makes some suggestions for a compliance programme.

071308 'Electronic Cash – Technology Will Denationalise Money'
DGW Birch, NA McEvoy, *FC 97 pp 95–108*

The authors discuss the role of electronic cash and near-money instruments such as loyalty points, focusing on issues of regulation and shifts in the positions of money issuers.

071309 'Hacking: Myth or Menace'
C Blatchford, *Computer Fraud and Security Bulletin; part 1: Feb 98 pp 16–19; part 2: Mar 98 pp 16–19*

The author discusses hackers' background, styles of attack and impact on the computer community.

071310 'Guideline for Cryptographic Mechanisms for Health Care Management, IT and Security Personnel, System Users'
G Bleumer, *SEISMED 96 v 1,2,3*

SEISMED developed guidelines on cryptography are presented here.

071311 'A New Paradigm for Performing Risk Assessment'
JL Bramlage, *NISSC 97 pp 565–576*

A new risk assessment method is presented that is useful for a repeated assessment process.

071312 'Sicherheit von Client-Server-Systemen'
J Brinkrolf, *Datenschutz und Datensicherheit v 22 no 2 (Feb 98) pp 86–90*

This is an introductory overview of computer security concepts, threats and protection measures in distributed systems.

071313 'Firewalls and the Five Domains of Network Security'
S Broderick, *Information Security Bulletin v 3 no 2 (Mar 98) pp 35–42*

This is a management-level overview of net security.

071314 'The Interplay of Information and Mind in Decision-Making: Signals Intelligence and Franklin D. Roosevelt's Policy-Shift on Indochina'
KE Brown, *Intelligence and National Security v 11 no 3 (Spring 98) pp 109–131*

This article suggests that Roosevelt's way of perceiving politics not only formed many of his stances, but also had a great deal of influence on what types of sigint material were passed to him before decision making.

071315 'Extranets at Your Service'
M Brownstein, *Byte (Dec 97) pp 75–77*

This is a general introduction to virtual private networks.

071316 'Determining the Quality of Anti-Virus and Anti-Malware Products'
K Brunnstein, *Information Security Bulletin v 2 no 5 (Oct 97) pp 19–30*

The article reviews the activities of the Hamburg University Virus Test Centre and presents some results of its recent tests of anti-virus products.

071317 'Certificate Authorities: Who Do You Trust?'
L Bruno, *Data Communications International (21/3/98) pp 54–63*

This is a comprehensive management-level overview of public key certification issues, CA products and services, and hierarchical model vs. web of trust considerations.

071318 'Health Informatics Deontology Code'
S Callens, H Nys, *SEISMED 96 v 1 pp 27–42*

The European Deontology Code is introduced and discussed here; the idea is to represent basic ethical principles for healthcare informatics that conform to all EU countries' legislation.

071319 'Information Integrity In End-user Systems'
D Chadwick, J Knight, P Clipsham, *IICIS 97 pp 273–292*

The authors discuss end-user errors in spreadsheet operations and the importance of user education.

071320 'Key Recovery – Why, How, Who?'
AJ Clark, *Computers and Security v 16 no 8 (1997) pp 669–674*

The author discusses strong cryptography, key escrow and recovery. He then reviews options for corporate key recovery.

071321 'Managing Network Security'
F Cohen, *Network Security (Jan-Feb 98)*

The first article of this pair discusses alternative solutions to the Y2K problem while the second looks at the problem of attackers and vendors spreading fear of low probability attacks among users.

071322 'Software's Nuclear Winter – Special Report'
Computer Business Review v 6 no 2 (Feb 98) pp 31–47

This special report brings five articles dedicated to the Y2K problem and the euro conversion.

071323 'Radio Intelligence and Security'
IW Comstock, *Cryptologia v XXI no 4 (Oct 97) pp 368–377*

This is a reprint of a 1926 classified lecture on 'radio security' — essentially the cryptanalysis and traffic analysis techniques available at the end of World War 1.

071324 'The sky's the limit'
A Courtenay, *The Banker (Feb 98) pp 52–53*

The author suggests that one effect of technology will be to allow individuals and small companies to follow the multinationals' lead in tax evasion; this will also make money laundering much easier, and demand more flexibility and cooperation between revenue authorities.

071325 'Protecting American Assets – Who is Responsible?'
AC Crescenzi, *NISSC 97 pp 290–294*

The author talks about US government agencies and their role in protecting US assets in the information society.

071326 'Out of data already'
LW Darrant, *Banking Technology (Mar 98) p 57*

The author criticises the UK Data Protection Act as falling behind technology and progress in communications.

071327 Guidelines on IT Security Risk Analysis For Health Care Management, IT and Security Personnel, System Users'
J Davey, S King, *SEISMED 96 v 1,2,3*

These guidelines are a product of the EU SEISMED project, intended to assist healthcare managers, IT and security staff and users to understand and participate in risk analysis.

071328 'C is for Cookie'
PT Davis, *Secure Computing Magazine (Feb 98) pp 60–61*

This is a management level article on cookies and how to avoid them.

071329 'Kryptographie und Menchenrechte'
E Diregger, *Datenschutz und Datensicherheit v 22 no 1 (Jan 98) pp 28–31*

The author explores the extent to which various existing and proposed crypto controls may be held to contravene the European Convention on Human Rights.

071330 'The Department of Defense Information Assurance Support Environment'
J Eller, P Klein, J Sachs, B Stauffer, D Winchell, *NISSC 97 pp 276–284*

This article outlines the activities and roles in the US DoD Information Assurance Support Environment for implementing certification and accreditation practices.

071331 'Computer Evidence'
A Endeshaw, *Computer Law and Security Report v 14 no 1 (Jan-Feb 98) pp 29–33*

The admissibility of computer evidence in the English courts is discussed and the Levin-Citibank case is reviewed.

071332 'Integrated Circuit Card Standards and Specifications'
DB Everett, *Smart Card News; part 16: v 7 no 1 (Jan 98) pp 15–18; part 17: v 7 no 2 (Feb 98) pp 35–38; part 18: v 7 no 3 (Mar 98) pp 56–59*

These articles outline the SET protocol and discuss the use of smartcards in security and payment protocols.

071333 'Drawbacks of the One-Time Pad'
CC Foster, *Cryptologia v XXI no 4 (Oct 97) pp 350—352*

This article discusses the economics of key distribution for one-time pad systems.

071334 'Experts disagree on future of public key for card security'
Fraud Watch Q4 1997 p 10

This article discusses problems with public key management overheads and the computational demands of public key operations.

071335 'Digital Signatures Today'
AM Froomkin, *FC 97 pp 287–290*

The author argues that electronic commerce is unlikely to develop until two important sets of issues are resolved: the scope and nature of the liability of certification authorities, and the form of public-key infrastructures. He concludes that this process can and should begin with an international standard for the syntax of security policy statements in certificates.

071336 'Electronic Information Channels Used by Virus Programmers'
H Fuhs, *Information Security Bulletin v 2 no 6 (Dec 97) pp 51–52*

This is a note on the on-line communications used by virus programmers.

071337 'Remote Access Services – Open Doors for Crackers'
H Fuhs, *Information Security Bulletin v 2 no 5 (Oct 97) pp 47–48*

This is a note on some potential problems with remote access control.

071338 'Addressing information security training and awareness within the European healthcare community'
S Furnell, P Sanders, M Warren, *MIE 97 pp 707–711*

Issues of user training in computer security for healthcare and initiatives of the EU ISHTAR project are briefly discussed.

071339 'Using Electronic Markets to Achieve Efficient Task Distribution'
I Grigg, CC Petro, *FC 97 pp 329–339*

The authors argue that the experience of large, relatively uncoordinated software development projects such as the Internet protocol suite suggests that the combination of electronic payment methods, authentication, and electronic markets may be a practical way of managing the software development process. They discuss several models for such markets, such as a bounty, one-round and multiple-round markets, which provide for various tradeoffs between allocational inefficiencies and coordination requirements.

071340 'A baseline security policy for distributed healthcare information systems'
D Gritzalis, *Computers and Security v 16 no 8 (1997) pp 709–719*

The author discusses security issues in healthcare informatics and outlines the baseline policy guidelines presented also in **071359** below.

071341 'Establishing an information security strategy'
E Guldentops, *IICIS 97 pp 5–21*

The paper discusses security issues in SWIFT and its outlook for the future, considering in particular public key technology and biometrics.

071342 'Privacy and Confidentiality Practices for Research with Health Information in Canada'
J Hagey, *Journal of Law, Medicine and Ethics v 25 no 2–3 (97) pp 130–138*

The author describes the Canadian healthcare system and its privacy provisions. Two federal acts and the laws of six provinces give various protections, which are gone through in some detail.

071343 'Wie nennen wir Infrastrukturen für die Schlüsselverwaltung'
V Hammer, *Datenschutz und Datensicherheit v 22 no 2 (Feb 98) pp 91–92*

The author discusses the currently used terminology for the management of cryptographic keys. He argues for the term "security infrastructure" instead of "certification infrastructure", "key management infrastructure" or "public key infrastructure" since the latter terms exclude aspects such as timestamping services, symmetric cipher keys, or the user training that is expected to be part of this infrastructure.

071344 'Encryption Policy – A UK Perspective'
N Hickson, *Computers and Security v 16 no 7 (1997) pp 583–589*

The author argues for the need of public key certification regulations, digital signature legislation and escrow/recovery support. The examples given include pro-escrow countries and conveniently omit countries like Germany and Italy.

071345 'Time to get personal'
A Hinde, *The Computer Bulletin (Jan 98) pp 24–25*

The author reviews the current data protection law in the UK and the likely impact of the new EU Data Protection Directive. She also outlines the results of a recent industry survey which shows that a fifth of UK companies break the law right at the start by not registering under the Data Protection Act.

071346 'Hot Water, Icebergs and Other Disasters'
S Hinde, *Computers and Security v 17 no 1 (1998) pp 31–33*

This note covers natural disasters, disaster recovery and the 'millennium bug'.

071347 'Telecoms Fraud, The Gory Details'
P Hoath, *Computer Fraud and Security Bulletin (Jan 98) pp 10–14*

Various aspects of telecoms and card fraud are discussed.

071348 'Hacking: Motivation and Deterrence'
P Hoath, T Mulhall, *Computer Fraud and Security Bulletin (Apr 98) pp 16–19*

The authors discuss hackers' motivation.

071349 'Role-Based Risk Analysis'
LJ Hoffman, A Yoran, *NISSC 97 pp 587–602*

The authors present so-called 'role-based risk analysis' that should better reflect support outsourcing and information sharing over networks.

071350 'Digital Signatures and Trusted Third Parties'
SM Huydecoper, *Information Security Bulletin v 2 no 6 (Dec 97) pp 35–42*

This is a management-level article on certification authorities and the legal issues surrounding digital signatures.

071351 'The Law on Computer Crime in Italy'
Information & Communication Technology Law v 6 no 3 (1997) pp 249–265

This article author reviews Italian computer crime legislation in some detail.

071352 'British government delays encryption proposals'
Information Security Monitor v 13 no 4 (Mar 98) p 3

The article claims that the UK government has postponed releasing new crypto regulations due to heavy criticism of the preceding draft and the negative response to suggestions about a revised draft.

071353 'Internet credit card fraud explosion predicted'
Information Security Monitor v 13 no 2 (Jan 98) pp 1–2

The article reviews fraud numbers provided by a UK company and suggests that one of their products might solve this alleged problem.

071354 'The NPS CISR Graduate Program in INFOSEC: Six Years of Experience'
CE Irvine, DF Warren, PC Clark, *NISSC 97 pp 22–30*

The authors summarise the development and outlook of the Naval Postgraduate School's INFOSEC curriculum.

071355 'Penetration testing and system audit – Experience gained during the investigation of systems within the UK'
A Jones, *Computers and Security v 16 no 7 (1997) pp 595–602*

The author makes generalised comments on penetration testing undertaken by the UK Defence Evaluation and Research Agency on non-Ministry of Defence systems.

071356 'Cellular Technology and Security'
R Jones, *NISSC 97 pp 31–40*

This article on cellular phone network security in the US mentions a number of common fraud prevention products.

071357 'Extranet Security: A Technical Overview from a Business Perspective'
J Jordan, *NISSC 97 pp 53–71*

The article outlines many issues related to the net and security.

071358 'Calculating the Cost of Year-2000 Compliance'
LA Kappelman, D Fent, KB Keeling, V Prybutok, *Communications of the ACM v 41 no 2 pp 30–39*

The authors provide detailed results of a survey of the cost of solving the Y2K problem and estimate the average cost at $1-2 per a line of code, $512 per function point repaired or $42 for every function point in an enterprise. An alternative estimate is 30% of the annual IS operating budget.

071359 'High Level Security Policy Guidelines'
S Katsikas, D Gritzalis, *SEISMED 96 v 1,2,3*

The authors introduce and present guidelines to help provide a basic framework for security and privacy implementation in healthcare systems.

071360 'Embedded Systems: The Other Problem'
A Kemp, *Computers and Security v 16 no 8 (1997) pp 663–668*

The author overviews a number issues relevant to embedded systems, including the interaction of integrity controls with the year 2000 problem.

071361 'Secrets, Lies, and IT Security'
G King, *NISSC 97 pp 7–21*

The author challenges the simplified 'confidentiality — integrity — availability' view of security.

071362 'Überwachung der Telkommunikation'
M Kiper, I Ruhmann, *Datenschutz und Datensicherheit v 22 no 3 (Mar 98) pp 155–161*

The authors discuss the recent erosion of privacy by the enactment in Germany of a surveillance law that greatly increases police powers to intercept communications. They tabulate the number of wiretap warrants granted in Germany, the UK and the USA for 1990–96; Germany is already a clear leader. They also discuss some recent technical developments such as the IMSI-catchers used to mount active attacks on GSM.

071363 'Cryptography as a Teaching Tool'
N Koblitz, *Cryptologia v XXI no 4 (Oct 97) pp 317–326*

The author gives some examples of how basic ideas from cryptology, ranging from monoalphabetics to the dining cryptographers' problem, can be used in teaching young children various concepts of number and complexity.

071364 'Connecting Classified Nets to the Outside World: Costs and Benefits'
CP Kocher, *NISSC 97 pp 534–542*

The author discusses the costs and benefits of connecting a dedicated classified network to an unclassified environment via e-mail.

071365 'Software Encryption in the DoD'
A Kondi, R Davis, *NISSC 97 pp 543–554*

This article discusses the dependence of hardware crypto solutions such as Fortezza on the underlying software, talks about DMS implementations using Microsoft Exchange, and argues that software encryption would provide an acceptable solution in many government environments.

071366 'Who Should Really Manage Information Security in the Federal Government'
AD Korzyk, AJ Wynne, *NISSC 97 pp 295–304*

This is a snapshot on US government information security management.

071367 'How to Market Yourself as an ISSO'
G Kovacich, *Computers and Security v 16 no 8 (1997) pp 657–662*

This article has some job interview hints for security managers.

071368 'Information Systems Security Metrics Management'
G Kovacich, *Computers and Security v 16 no 7 (1997) pp 610–618*

This is an attempt to describe the development and use of security metrics.

071369 'Die Kryptodebatte in den USA'
C Kuner, *Datenschutz und Datensicherheit v 22 no 1 (Jan 98) pp 5–7*

This is a brief overview of US crypto policy developments in 1996–7 and of the US crypto export rules.

071370 'Medical Liability, Safety and Confidentiality in Maritime Telemedicine – The MERMAID position on issues of importance'
P Ladas, P Giatagatzidis, G Anogianakis, S Maglavera, *MIE 97 pp 181–185*

The liability and patient record confidentiality issues of maritime telemedicine are discussed in brief.

071371 'Strategic Tasks for Government in the Information Age'
P Lampru, *FC 97 pp 315–327*

The author argues that governmental intervention is a key element in ensuring the establishment of a national infrastructure for certification, and determination of liability of CAs. He suggest providing individuals with dual certificates, where identification certificates would carry a maximum identification liability value for which CAs are accountable, and authorization certificates would be used to grant local privileges. He argues that such an infrastructure will prove critical in moving away from proprietary networks and towards an 'Internet-centric' Information age.

071372 'Evaluating the Security of Electronic Money'
SL Lelieveldt, *FC 97 pp 91–94*

This is a Dutch view of electronic money's legal, security and application aspects.

071373 'Detecting Data Integrity Failures'
W List, *IICIS 97 pp 341–348*

The paper talks about detection of integrity errors in systems.

071374 'Integrity in Information Systems'
W List, WR Melville, *IICIS 97 pp 295–340*

The authors present an extended discussion paper on integrity in information systems (substantially a reprint of **034346**, **044333**).

071375 'The effects of Time on Integrity in Information Systems'
W List, *IICIS 97 pp 349–358*

The author talks about time relevant issues in information systems integrity, as also discussed in **054368**.

071376 'The Use of Information Technology Security Assessment Criteria to Protect Specialized Computer Systems'
VA Lykov, AV Shein, AS Piskarev, DM Devaney, RB Melton, WJ Hunteman, JM Prommel, JS Rothfuss, *NISSC 97 pp 319–330*

The paper describes how the Russian security evaluation criteria were applied to a nuclear material control and accountancy system, and compares them with the comparable US criteria. The two approaches turned out to be very similar although they diverged in their organisation and terminology. A synopsis of the Russian system is given.

071377 'Measuring Innovation'
S Macdonald, B Lefang, *Computer Law and Security Report v 14 no 1 (Jan-Feb 98) pp 8–13*

The authors discuss some issues of concern to patent attorneys, such as dealing with national security issues in research.

071378 'Implementing Data Privacy and Security (The Slovenian Experience)'
M Markota, G Raič, *MIE 97 pp 879–883*

The Slovenian experience in applying a Data Protection Law to a healthcare information system is outlined.

071379 'An Attorney's Roadmap to the Digital Signature Guidelines'
CR Merrill, *FC 97 pp 291–297*

The author provides a concise guide to the American Bar Association's Digital Signature Guidelines — a close relative of Utah's 1995 Digital Signature Law — and offers a step-by-step analysis of a dispute, using these guidelines.

071380 'Internet Law – Parts I, II'
SP Meyer, U Sieber, *Computer Law and Security Report v 14 no 1 (Jan-Feb 98) pp 14–28*

The first part of this paper discusses intellectual property issues, while the second reviews questions of criminal liability for international data transfer.

071381 'Changing Definitions of Internal Control and Information Systems Integrity'
RR Moeller, *IICIS 97 pp 255–272*

The author discusses a US model of internal control of information systems and other issues of systems auditing.

071382 'Auditing The IT Security Function'
K Osborne, *Computers and Security v 17 no 1 (1998) pp 34–41*

The author provides some suggestions to auditors and for setting a security policy and enforcing it.

071383 'GSSP Preface/Overview'
W Ozier, *Computers and Security v 17 no 1 (1998) pp 14–18*

This papers states the goals, current status and international committee list of 'Generally Accepted System Security Principles'.

071384 'Security of Medical Database Systems for Health Care Management, IT and Security Personnel, System Users'
G Pangalos, *SEISMED 96 v 1,2,3*

The author introduces medical database security issues and presents SEISMED developed guidelines targeted at managers, computer people and users.

071385 'The Strategic Values of Information Security in Business'
DB Parker, *Computers and Security v 16 no 7 (1997) pp 572–582*

The author outlines some of his thoughts on security, together with some recommendations to security professionals.

071386 'The Importance of IT Security'
RK Parkin, *Computer Fraud and Security Bulletin (Mar 98) pp 12–15*

This is a discussion of computer security in enterprises.

071387 'Network Security Guidelines for Health Care Management, IT and Security Personnel, System Users'
A Patel, I Kantzavelou, C Clissman, D Maroulis, *SEISMED 96 v 1,2,3*

The authors present separate SEISMED-developed network security guidelines for healthcare information systems, targeted at managers, computer people and users.

071388 'INFOSEC Risk Management: Focused, Integrated & Sensible'
DR Peeples, *NISSC 97 pp 577–586*

The paper presents an NSA risk analysis methodology and tool that assists security managers in decisions about specialised consultant involvement.

071389 'Application of the IT Baseline Protection Manual'
A Plate, *NISSC 97 pp 305–318*

The author describes the philosophy behind the German IT Baseline Protection Manual, and some of its contents.

071390 'Cyberterrorism – Fact or Fancy?'
MM Pollitt, *NISSC 97 pp 285–289*

This is an FBI forensic scientist's perception of computer-related risks.

071391 'Cyberterrorism – Fact or Fancy?'
MM Pollitt, *Computer Fraud and Security Bulletin (Feb 98) pp 8–10*

This is a magazine version of the above.

071392 'First Step Towards a European Union Policy on The Securing of Electronic Communications'
C Pounder, *Computers and Security v 16 no 7 (1997) pp 590–594*

This is an outline of EC Communication COM 97 (503) regarding security and trust in electronic communication, together with comments on it.

071393 'Homeworking: No Longer An Easy Option?'
C Pounder, *Computers and Security v 17 no 1 (1998) pp 27–30*

This is a brief discussion of the security, liability and responsibility issues of teleworking.

071394 'Legal Issues in Cryptography'
EJ Radlo, *FC 97 pp 259–286*

The author, an attorney, offers a wide overview of legal issues pertaining to cryptography. He reviews export controls and legal challenges to them, Federal Information Processing Standards, recent policy developments, international laws, nongovernmental standards, and patent disputes.

071395 'EDI Security – Re-evaluation of Controls and its Implications on the Organizations'
P Ratnasingham, *Computers and Security v 16 no 8 (1997) pp 650–656*
This is an outline of EDI controls and security framework.

071396 'Perspectives on Financial Cryptography'
RL Rivest, *FC 97 pp 145–149*
The author presents his ideas on the future of financial crypto and e-commerce.

071397 'How to Panic the Stock Markets with a Computer Virus Hoax'
B Rosenberger, *Information Security Bulletin v 2 no 5 (Oct 97) pp 39–42*
This is a discussion of virus hoaxes, media over-reaction and the like.

071398 'Exportkontrollen für Verschlüsselungsprodukte'
H Roth, *Datenschutz und Datensicherheit v 22; part 1 no 1 (Jan 98) pp 8–13, part 2 no 2 (Feb 98) pp 81–85*
While the import of encryption hard- and software is unrestricted in Germany, the export — even to other EU countries — is strictly controlled and violations of export regulations are a serious criminal offences (with fines of up to a million marks fine and jail sentences of up to 10 years). Unlike in the US however, freeware and mass market encryption software is excluded from export controls in Germany. The article discusses the relevant German cryptography export regulations as well as the EU Dual Use directive of 1995.

071399 'Macro Attacks: A New Generation of Security Threats'
P Simpson, *Information Security Bulletin v 2 no 5 (Oct 97) pp 33–38*
This is a summary of MS Windows macro features, problems and implications.

0713A0 'Privacy Protection – A US Perspective'
M Rotenberg, *Computer Law and Security Report v 14 no 1 (Jan-Feb 98) pp 38–40*
The author discusses the US data protection situation and argues that the current private industry self-regulation should be strengthened by privacy legislation.

0713A1 'Baseline Security Guidelines for Health Care Management, IT and Security Personnel, System Users'
P Sanders, S Furnell, M Warren, *SEISMED 96 v 1,2,3*
The authors present guidelines for achieving a minimal acceptable standard of security in healthcare information systems. These guidelines are presented separately for managers, computer people and users.

0713A2 'A fundamental framework for network security'
HJ Schumacher, S Ghosh, *Journal of Network and Computer Applications v 20 no 3 (Jul 97) pp 305–322*
This article contains a high-level overview of network security issues and a network security rating model.

0713A3 'Managing Security for Outsourcing Contracts'
J Sherwood, *Computers and Security v 16 no 7 (1997) pp 603–609*
The paper suggests an organisational structure formalising responsibilities and liabilities for an outsourcing agreement.

0713A4 'Physical Security and Insurance'
Secure Computing Magazine (Feb 98) pp 26–31
The problems of computers' physical security and Y2K failure are discussed in the context of insurance costs.

0713A5 'Teleworking'
Secure Computing Magazine (Mar 98) pp 22–26

The article discusses issues of teleworking such as remote access control, authentication and liability.

0713A6 'Integrity: definition, subdivision, challenge'
L Strous, *IICIS 97 pp 187–194*

The author talks about information and system integrity.

0713A7 'Security Posture Assessment'
L Sutterfield, T Schell, *Information Security Bulletin v 2 no 6 (Dec 97) pp 45–50*

This is an alternative view of risk assessment and of defining a protection perimeter.

0713A8 'The Uses and Limits of Financial Cryptography: A Law Professor's Perspective'
PP Swire, *FC 97 pp 239–258*

The author challenges a number of assumptions widely held in the cryptographic research community. He argues that even if strong cryptography were to become widely available, anonymous transactions would still only account for a highly restricted subset of all financial transactions; that users do not come equipped with the technical and scientific savvy of cryptographers. and that cryptographers' noted dislike for privacy protection through legislation is not only misplaced but may ultimately prove harmful to electronic privacy.

0713A9 'China's New Internet Regulations: Two Steps Forward, One Step Back'
Z Tan, M Mueller, W Foster, *Communications of the ACM v 40 no 12 pp 11–16*

This article reviews the Chinese Internet regulations: anyone opening an Internet account or using a cyber-café must fill out a police form for the Ministry of Public Security. However, the authors deem the government's blocking efforts to be for show rather than a serious measure.

0713B0 'The Integrity of Electronic Evidence'
M Tenhunen, *IICIS 97 pp 153–186*

The issues of preserving and proving the integrity of computer evidence in criminal investigations and in court are discussed. The role of hash functions and digital signatures in relevant practical situations is then reviewed in some detail.

0713B1 'Network Security: Locking In To Policy'
R Thayer, *Data Communications International (21/3/98) pp 77–80*

The author discusses issues to be considered for writing network security policy, particularly for intranet/extranet systems.

0713B2 'Guidelines for Secure Systems Procurement, Development and Design for Health Care Management, IT and Security Personnel'
H van Dorp, J Dubbeldam, *SEISMED 96 v 1,2*

SEISMED developed guidelines for secure systems procurement are presented.

0713B3 'Guidelines for Secure Systems Implementation for Health Care Management, IT and Security Personnel'
G van Veenen, *SEISMED 96 v 1,2*

SEISMED developed guidelines for secure systems implementation are presented.

0713B4 'A formal, mathematics oriented method for identifying security risks in information systems'
HU van Piggelen, *MIE 97 pp 191–195*

A methodology for system risk identification is suggested.

0713B5 'Towards a Framework for Security Measurement'
C Wang, WA Wulf, *NISSC 97 pp 522–533*

The authors propose a security measurement framework and discuss measurement validation.

0713B6 'Commanding the Enterprise'
K Watterson, *Byte (Dec 97) pp 93–98*

This is an overview of several network management tools and of their security-relevant features.

0713B7 'Money Laundering: Past, Present and Future'
PC Wayner, *FC 97 pp 301–305*

The author muses on the problems which designers of e-cash systems will face with regard to money laundering.

0713B8 'Computer Forensics; Trends and Concerns'
E Wilding, *Information Security Bulletin v 2 no 6 (Dec 97) pp 15–18*

The author discusses three challenges to computer forensics — greater storage device capacity, growing use of the net, and the use of encryption software.

0713B9 'Information Security is Information Security'
IS Winkler, *NISSC 97 pp 1–6*

The author discusses the concept of information security and argues that more care should be taken about the casual generation of open source material.

0713C0 'Background Checks for Employees in Computer-Related Positions of Trust'
CC Wood, *Information Security Bulletin v 2 no 5 (Oct 97) pp 43–44*

The author stresses the importance of employee history checks in minimising insider threats.

0713C1 'Escorts Required for All Visitors'
CC Wood, *Information Security Bulletin v 3 no 2 (Mar 98) pp 33–34*

The author talks about the importance of escorting visitors to offices.

0713C2 'Essential Controls for Internet Electronic Commerce'
CC Wood, *Network Security (Feb 98) pp 13–18*

This is a discussion of electronic commerce, associated risks and deployed control techniques.

0713C3 'Mandating the Information Security Management Function'
CC Wood, *Information Security Bulletin v 3 no 1 (Feb 98) pp 31–32*

This is a note on information security management responsibility.

0713C4 'Removal of All Unauthorized Access Paths in Production Software'
CC Wood, *Information Security Bulletin v 2 no 6 (Dec 97) pp 33–34*

This is a note on the importance of removing trapdoors from deployed systems.

0713C5 'Alternative Visions for Legal Signatures and Evidence'
B Wright, *FC 97 pp 299–300*

The author suggests that the 'Utah model' for legislating digital signatures places an oppressive burden of proof on the proper care of individuals' private keys. Handwritten signatures, he argues, come already equipped with the necessary cultural understanding. Legal disputes of electronic evidence will most likely involve assessment of numerous environmental factors, such as standards of care, rather than solely relying on proper management of the private key, as cryptographic schemes seem to imply.

0713C6 'Multimedia Law-Germany'

U Wuermeling, *Computer Law and Security Report v 14 no 1 (Jan-Feb 98) pp 41–44*

The German multimedia law is discussed, with particular attention given to data protection and digital signatures.

0713C7 'The Security of Electronic Banking'

YJ Yang, *NISSC 97 pp 41–52*

This article discusses electronic banking, the net and security.

4 Formal Methods and Protocols

071401 'The Use of Belief Logics in the Presence of Causal Consistency Attacks'
J Alves-Foss, *NISSC 97 pp 406–417*

The author analyses the Lowe attack on Needham-Schroder, and argues that BAN logic is often used in an appropriate way. His suggested modification is that the claim 'K is a good key for communicating between A and B' should only be permitted if the two principals' names are mentioned explicitly in the relevant message.

071402 'Securing 'Classical IP over ATM Networks"
C Benecke, U Ellermann, *Usenix Security 98 pp 95–105*

This paper reviews major types of attacks on IP over ATM, assuming two logical IP subnets with a firewall-controlled connection; suggestions for the proper configuration of ATM services and switches are given. These should require no changes to switches or protocols, yet give some protection against spoofing and denial of service, and better integration of firewalls into such networks.

071403 'Strong authentication and privacy with standard browsers'
F Bergadano, B Crispo, M Lomas, *Journal of Computer Security v 5 no 3 (97) pp 191–212*

The authors present a scheme for securing the web using standard browsers. Client-server communication is secured using a Java applet with security functionality on the client side and by an appropriate remote application on the server side. The scheme deploys public keys in the X.509 format, with the CA using separate certification and revocation authorities in order to maintain operational evidence independently of any single failure. The CA has on-line and off-line parts and the whole scheme is implemented for SunOS and Ultrix.

071404 'Secure Electronic Transactions – the New SET Standard'
NJ Bjergstrom, *Information Security Bulletin v 2 no 5 (Oct 97) pp 49–58*

This is a comprehensive overview of the SET protocol suite, its trust model and certificate use, and other relevant issues.

071405 'CWASAR: a European infrastructure for secure electronic commerce'
C Bryce, W Kühnhauser, R Amouroux, M López, H Rudnik, *Journal of Computer Security v 5 no 3 (97) pp 225–235*

This article describes the European Cooperative Wide-Area Service Architecture (CWASAR) at the end of the project's first stage. The idea is to provide a low-cost platform for electronic commerce; it is currently based on SecuDE, X.509 and PEM.

071406 'Implementation of Key Escrow with Key Vectors to Minimise Potential Misuse of Key '
WJ Caelli, D Longley, *NISSC 97 pp 431–442*

The paper suggests that key tagging and key vectors are used in key escrow schemes. Control of key use and accountability for that use could be achieved this way provided some trust in hardware holding the keys and administration of the scheme can be held.

071407 'Anonymity Control in E-Cash Systems'
G Davida, Y Frankel, Y Tsiounis, M Yung, *FC 97 pp 1–16*

The authors suggest that e-cash anonymity should be treated as a control parameter, allowing for revocable anonymity and other features. Anonymity control models — owner tracing and coin tracing — are reviewed and a simplified version of a protocol from **061614** is presented. The concept of 'distress cash' is introduced that uses a covert channel to mark cash released under threat.

071408 'Framework for Evaluating Security Protocols in a Banking Environment'
JHP Eloff, S van Buuren, *Computer Fraud and Security Bulletin (Jan 98) pp 15–19*
A general framework for the evaluation of security protocols is presented.

071409 'Web Spoofing: An Internet Con Game'
EW Felten, D Balfanz, D Dean, DS Wallach, *NISSC 97 pp 95–103*
The authors give several examples of web spoofing attacks, describe some of them in detail and provide suggestions for countermeasures.

071410 'GUMP: Grand Unified Meta-Protocols Recipes for Simple, Standards-Based Financial Cryptography'
B Fox, B Beckman, D Simon, *FC 97 pp 375–394*
The authors propose a framework for designing electronic protocols suitable for transactions dependent on trusted and on-going relationships, such as those between a customer and a financial institution. The protocols require only off-the-shelf components, with the aim of reducing design, implementation and deployment costs.

071411 'Das Royal Holoway-System'
D Fox, *Datenschutz und Datensicherheit v 22 no 1 (Jan 98) pp 24–27*
This is a summary of the UK government's proposed architecture for trusted third party services that first appeared in **043616**, and which allows the national TTPs of both communicating partners to recover the session key. It has been proposed by GCHQ as a European standard for key recovery.

071412 'Auditable Metering with Lightweight Security'
MK Franklin, D Malkhi, *FC 97 pp 151–160*
This paper outlines a lightweight protocol for metering low-cost services. A proxy is used for metering and web server access, using an incremental protocol based on hash functions and an auditing function.

071413 'Some Critical Remarks on "Dynamic Data Authentication" as Specified in EMV '96'
LC Guillou, *FC 97 pp 123–134*
The author suggests alternative cryptographic methods for the Europay – MasterCard – Visa (EMV) smartcard specifications, which would base the authentication on zero-knowledge techniques, use MACs for transaction authentication and use digital signatures only for additional services. The workload would then be 20 times less for card issuing and 10 times less for transaction processing, while the volume of authenticating data per transaction would be 50 times less.

071414 'Authentication methods'
P Hunter, *Information Security Monitor v 13 no 2 (Jan 98) pp 5–7*
This is a management level overview of authentication.

071415 'Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System'
M Jakobsson, M Yung, *FC 97 pp 217–238*
Based on the architecture, trust, and threat models developed in **051604**, the authors propose using the distributed blind signatures of **062613** to distribute the revocation and tracing powers of both judges and trustees.

071416 'An Efficient Micropayment System Based on Probabilistic Polling'
S Jarecki, A Odlyzko, *FC 97 pp 173–191*
The authors propose a way to bridge the gap between on-line and off-line e-cash systems by adding a form of probabilistic polling. Payments are directly forwarded by vendors to the bank, with a probability dependent on the amount of the payment: large transactions are almost certainly polled, affording the security of on-line systems,

while micropayments approach the communication overhead of an off-line system. This gives a clear trade-off between risk and traffic volume.

071417 'Multistage Algorithm for Limited One-Way Functions'
WT Jennings, *NISSC 97 pp 150–161*

This is an extension of work from **054433** suggesting a multi-stage variant of a key recovery delay mechanism whose purpose is to limit the abuse of escrowed keys by the authorities.

071418 'Internet Protocol Next Generation: Saving the Internet in the New Millennium'
RA Kondilas, *NISSC 97 pp 452–475*

The author discusses the difference between the current Internet Protocol (v4) and the next generation IPv6, focussing on security.

071419 'Towards Web Security Using PLASMA'
A Krannig, *Usenix Security 98 pp 173–186*

A web-based security system for multimedia applications — PLASMA — is presented. This uses HTML comment tags to embed cryptographic objects, CGI scripts to enable interaction with PLASMA server application, and a proxy on the client side to communicate with the client PLASMA application. The goal of PLASMA is to support security just beneath the application level, with different strengths of cryptographic protection for different types of communicated data.

071420 'Highly Scalable On-line Payments Via Task Decoupling'
DW Kravitz, *FC 97 pp 355–373*

The author proposes an on-line payment system which does seek not emulate physical world transactions, but rather, uses decoupling as its basic design principle: each component is only involved in a narrow set of transactions and responsibilities and time-varying issues, such as actual delivery of digital goods, are handled outside of the payment flow. The system provides for anonymous payments and high scalability, while reducing cryptographic computational overhead to a strict minimum.

071421 'Attack-resistant trust metrics for public key certification'
R Levien, A Aiken, *Usenix Security 98 pp 229–241*

The paper reviews several trust metrics from the point of view of different attacks, and suggests a metric that is an enhancement of the Reiter-Stubblebine work (**062433**, **064445**). This new metric is more resistant to attacks against delegation certificates than it is to certified key attacks. Multiply certified keys give better protection against attacks on the trust graph.

071422 'Comment and Reply to "Reparable Key Distribution Protocols for Internet Environments" '
XD Lin, YS Xing, YX Yang, T Hwang, *IEEE Transactions on Communications v 46 no 1 (Jan 98) pp 20–22*

The first of these two notes shows that one of the protocols presented by Hwang and Ku (**042408**) does not preserve the perfect forward secrecy property and suggests a revision, but this is found to be faulty in the second note.

071423 'Lightweight Security Primitives for E-Commerce'
Y Matias, A Mayer, A Silberschatz, *ITSP 97 pp 95–102*

The authors present a framework for extended client-server relationships based on a shared key. The key is computed from client-chosen secrets and client and server identities using a cryptographic hash function. Public keys are used only for establishing the initial relationship, while shared keys at the client side are re-computed by a client proxy on demand.

071424 'Anonymous Networking and Virtual Intranets: Tools for Anonymous Corporations'
J McCoy, *FC 97 pp 33–37*

The paper discusses the dining cryptographers problem and Wei Dai's Pipenet protocol with respect to participant anonymity and use of proxies to enforce user privacy and security.

071425 'Distributed Network Management Security'
P Meyer, *NISSC 97 pp 233–249*

The protocols for Distributed Network Management Security are presented. They are based on SNMP v2, use two proxies and provide some crypto functionality but are conceptually driven by firewall ideas. Message passing from and to a protected interior network is discussed in some detail.

071426 'Finite-State Analysis of SSL 3.0'
JC Mitchell, V Shmatikov, U Stern, *Usenix Security 98 pp 201–215*

The authors extend their work from **064433** analysing SSL protocols using Murφ — an automated finite state verification tool. They establish the main shortcomings in SSL v 2.0 and also discover some minor anomalies in resuming sessions in v 3.0.

071427 'Iolus: A Framework for Scalable Secure Multicasting'
S Mittra, *Computer Communication Review v 27 no 4 pp 277–288*

The author discusses several differences between unicast and multicast security. A new framework for secure multicasting is then presented and a particular protocol implementation discussed. The cryptographic parts of the protocol are fairly similar to those presented in the paper below.

071428 'A Flow-Based Approach to Datagram Security'
S Mittra, TYC Woo, *Computer Communication Review v 27 no 4 pp 221–234*

The authors discuss Internet connectionless security and propose a protocol which is Diffie-Hellman based, relies on X.509 certificates or secure DNS for public key distribution, supports MACs and controlled key caching. The CryptoLib library (**024135**) was used for an implementation and the experimental results are discussed in the context of other IP security work.

071429 'Secret sets and applications'
R Molva, G Tsudik, *Information Processing Letters v 65 no 1 (15/1/98) pp 47–55*

The authors define a new protocol building block: a secret set is a group of principals each of whom can test group membership, but not determine either the identity of other members or the total number of members (even if all the members except the original set constructor collude). Several possible constructions for secret sets are described. Potential applications include tackling the scaling problem of anonymous communication: when supporting location privacy in mobile networks, for example, it can enable a router to decide whether it ought to pass on a given message.

071430 'A Methodology For Mechanically Verifying Protocols Using an Authentication Logic'
Munna, J Alves-Foss, *NISSC 97 pp 202–212*

The paper outlines a methodology for authentication protocol analysis. The theorem prover used is HOL (Higher Order Logic); the underlying logic of authentication is from Lampson et al.

071431 'Certificate Revocation and Certificate Update'
M Naor, K Nissim, *Usenix Security 98 pp 217–228*

The authors discuss and compare public key certificate revocation using standard revocation lists, Micali's revocation system and the revocation trees suggested by Kocher. They then present a new scheme which uses hash-trees whose leaves are

the revoked certificates sorted by their serial numbers. A comparative discussion and performance evaluation are provided.

071432 'Digital Coins based on Hash Chain'
KQ Nguyen, Y Mu, V Varadharajan, *NISSC 97 pp 72–79*

Three digital coin-based micropayment protocols based on hash chains are presented (they were also presented in **063411**).

071433 'A Java Beans Component Architecture for Cryptographic Protocols'
P Nikander, A Karila, *Usenix Security 98 pp 107–121*

The authors outline an object oriented implementation framework for cryptographic protocols that is based on IP (both v4 and v6 are supported) and Java (the Java Conduits protocol component framework). Interoperability with ISAKMP and a PKI is also considered.

071434 'Towards Multiple-Payment Schemes for Digital Money'
H Pagnia, R Jansen, *FC 97 pp 203–215*

The authors address two little-explored problems of electronic commerce: transferability and fair exchange. Their transferable e-cash system trades lesser interaction with the bank for increased interaction with a trusted 'anonymity server'. The fair exchange mechanism involves a passive (blackboard) trustee which logs transactions and act as an intermediary to deliver keys.

071435 'How to Break Fraud-Detectable Key Recovery'
B Pfitzmann, M Waidner, *ACM Operating System Review v 32 no 1 (Jan 98) pp 23–28*

The authors present a generalised superencryption-related attack on the key recovery scheme with binding data of Verheul and van Tilborg (**062619**). They argue that software key recovery cannot be secured against reasonably capable dishonest users.

071436 'Secure Public Internet Access Handler (SPINACH)'
E Poger, MG Baker, *ITSP 97 pp 113–123*

The system described in this article creates a security boundary between public Ethernet ports and the rest of an organisation's networks. Users accessing the networks from the outside have to authenticate themselves via Kerberos tickets for regular users and via passwords for guest accounts. The implementation is done for heterogeneous H/W, S/W platforms and is targeted at large networked campuses.

071437 'Authentication of sequences with the SL_2 hash function: application to video sequences'
JJ Quisquater, M Joye, *Journal of Computer Security v 5 no 3 (97) pp 213–223*

The authors present a method to authenticate a sequence of digital video images in order to detect any modification of the image sequence. It assumes a tamper-proof camera which divides images into smaller blocks to reduce problems of bit errors; the Tillich-Zémor hash function (**034545**) is used to link individual images and the Guillou-Quisquater signature scheme is applied once per sequence to provide non-repudiation.

071438 'Efficient Electronic Cash with Restricted Privacy'
C Radu, R Govaerts, J Vandewalle, *FC 97 pp 57–69*

The authors propose a digital coin based system for small payments. Coins remain untraceable with respect to the user, yet are linkable through use of user pseudonyms. The scheme is based on Brands' 1993 off-line cash scheme (**024604**); withdrawal is executed in three separate transactions with varying frequencies of execution.

071439 'Electronic Lottery Tickets as Micropayments'
RL Rivest, *FC 97 pp 307–314*

The author proposes a probabilistic method for implementing micropayments efficiently based on bets: only 'winning' payments are redeemed to the bank by vendors,

resulting in a low communication overhead for the bank and a minimal increase in computation for users and vendors. The author describes how the PayWord micropayment scheme could be thus adapted.

071440 'An attack on a recursive authentication protocol: A cautionary tale'
PYA Ryan, SA Schneider, *Information Processing Letters v 65 no 1 (15/1/98) pp 7–10*

An attack is shown on an authentication protocol proposed by Bull. The interesting feature is that the protocol had been proved secure by Paulson, and then Bull had adapted it to use the KryptoKnight technique of xor'ing data with keyed hashes instead of encrypting it. This introduced an extra algebraic property which could be exploited to reveal pairwise xors of keys, with the result that anyone knowing one key in the system could derive all the others.

071441 'Cryptographic Support for Secure Logs on Untrusted Machines'
B Schneier, J Kelsey, *Usenix Security 98 pp 53–62*

The scheme outlined in this paper assures log file confidentiality protection and modification/deletion detection on an untrusted machine. The scheme is based on hash-chaining of log entries, on deriving log entry encryption keys from the authentication key, on independent and partly trusted verification of log files, and on role-based access control through the encryption keys.

071442 'SVP: A Flexible Micropayment Scheme'
J Stern, S Vaudenay, *FC 97 pp 161–171*

A simple micropayment scheme is outlined, with conceptual suggestions for additional security, including the use of tamper-resistant devices: a hardware implementation is suggested for merchants, but a software-only solution for both merchants and customers is also discussed.

071443 'Private Web Browsing'
PF Syverson, MG Reed, DM Goldschlag, *Journal of Computer Security v 5 no 3 (97) pp 237–248*

The paper introduces a scheme for protecting web communication confidentiality and end-party identity, thus providing also traffic analysis protection. This is an extension of a similar application for mobile phones (**064444**). The basis of the system is onion routing (**054421**, **061439**) applied through HTTP proxies. Some implementation experiments are discussed.

071444 'Unlinkable Serial Transactions'
PF Syverson, SG Stubblebine, DM Goldschlag, *FC 97 pp 39–55*

The authors outline a protocol for unlinkable serial transaction that supports user anonymity, but allows the service provider to request confirmation of the authorisation to use the service. Issues relevant to service subscription management and various applications are also discussed.

071445 'Achieving Interoperability Through Use of the Government of Canada Public Key Infrastructure'
JH Weigelt, *NISSC 97 pp 418–430*

The options for the public key infrastructure being implemented by the Government of Canada are discussed, with a particular focus on domain interoperability.

071446 'Using digital credentials on the World Wide Web'
M Winslett, N Ching, V Jones, I Slepchin, *Journal of Computer Security v 5 no 3 (97) pp 255–267*

The authors discuss how to use certificates for credential-based access as an alternative to the usual identity-based access in closed user group solutions. Some additional features on both the client and server side are also discussed.

071447 'A Look at Public Key Certificates'
MA Wright, *Network Security (Feb 98) pp 10–13*

This is a management-level overview of public key distribution problems, X.509 v3 certificates, certification paths and revocation.

071448 'On the Continuum Between On-line and Off-line E-Cash Systems – I'
Y Yacobi, *FC 97 pp 193–201*

The author proposes that payment systems may exist anywhere on the continuum between on-line and off-line e-cash systems, by incorporating an auditing mechanism for transactions with a fixed sampling rate d, which fails to detect fraud (double-spending) with a probability $O(\exp(-C_b/d))$, where C_b is the amount the adversary must invest for the fraud to break even.

071449 'Evidence and non-repudiation'
J Zhou, D Gollman, *Journal of Network and Computer Applications v 20 no 3 (Jul 97) pp 267–281*

This paper discusses issues of non-repudiation evidence, reviews some non-repudiation protocols and problems with timestamping and third party trust. The authors also discuss the developed ISO standards on non-repudiation.

5 Secret Key Algorithms

071501 'On the Security of the Hashing Scheme Based on SL_2'
KS Abdulkhalikov, C Kim, *FSE 98 pp 93–102*

The authors consider the hashing scheme of Tillich and Zémor (**034545**) and show that the polynomials can most likely be chosen so as to avoid the attack of Charnes and Pieprzyk (**041504**). They also extend it from characteristic two to a general finite field.

071502 'New Constructions for Secure Hash Functions'
W Aiello, S Haber, R Venkatesam, *FSE 98 pp 150–167*

The authors discuss ways of changing the DES key schedule so that it will accept a much larger key and thus be more efficient at hashing in feedforward mode, while not introducing vulnerabilities that would expose the system to shortcut collision finding attacks. One idea is to use MD5 to create strong redundancy in the input, e.g. to extend a 512 bit input to a 768 bit set of DES round keys. The resulting hash function is slightly faster than SHA.

071503 'Cryptanalysis of Multiple Modes of Operation'
E Biham, *Journal of Cryptology v 11 no 1 (Winter 98) pp 45–58*

Multiple modes of operation of DES are examined for chosen plaintext and chosen ciphertext attacks. Many such modes are shown to be not only weaker than multiple DES, but more comparable to a single DES. The conclusions suggest that strong modes of operation should neither be based on combining simpler modes nor use internal feedbacks. Rather the use of single modes incorporating multiple encryption as the underlying cryptosystems of the single modes is suggested.

071504 'Serpent: A New Block Cipher Proposal'
E Biham, R Anderson, L Knudsen, *FSE 98 pp 222–238*

The authors present a block cipher candidate for AES which is designed for efficient bitslice implementation: at each round, 32 identical 4-to-4-bit S-boxes are used in parallel, with the result that a round can be computed by implementing the gate description of the S-box using register operations on a 32 bit processor, and all 4 by 32 bits evaluated at once. The result, with a 32 round cipher in which the DES S-boxes are reused a row at a time, is a cipher that is about as fast as DES but more secure against known attacks than triple DES.

071505 'JEROBOAM'
H Chabanne, E Michon, *FSE 98 pp 49–59*

The authors present a stream cipher based on a nonlinear filter of stuttered multiplicative congruential generators. It is optimised for 16-bit processors and a C implementation is given.

071506 'Balanced Boolean functions'
K Chakrabarty, JP Hayes, *IEE Proceedings in Computers and Digital Techniques v 145 no 1 (Jan 98) pp 52–62*

The authors present a general theory of balanced Boolean functions, analyse conditions under which functional compositions preserve balance and examine some specific balance-preserving decompositions. A characterisation for balance functional completeness is given and methods for counting equivalence classes of balanced functions are discussed.

071507 'Joint Hardware / Software Design of a Fast Stream Cipher'
CSK Clapp, *FSE 98 pp 75–92*

The author develops his work on high speed variants of WAKE (**033547**) run backwards (**063516**). The trade-offs between speed and efficiency are explored, and

new tricks are presented including splitting tables. Some deep similarities are discussed between such ciphers and nonlinear feedback shift registers on the one hand, and Feistel ciphers on the other hand. Two practical constructions are suggested for concrete implementations, and reference implementations in C are given.

071508 'Cryptanalysis of TWOPRIME'
D Coppersmith, D Wagner, B Schneier, J Kelsey, *FSE 98 pp 32–48*

The authors show several ways to attack the cipher TWOPRIME (**063521**) which are based on exploiting the weak mixing between its left and right halves using birthday and other tricks; these give various combinations of time and space which are well within practical bounds for as little as 64 bytes of keystream.

071509 'Value sets of Some Polynomials Over Finite Fields GF(2^{2m})'
TW Cusick, *SIAM Journal on Computing v 27 no 1 (Feb 98) pp 120–131*

The authors shows a connection between the cross-correlation of m-sequences and the value sets of the polynomials $x^k(1+x)^{2m-1}$ for $k \in \{\pm 1, \pm 2, 4\}$ over GF(2^{2m}).

071510 'Fast Hashing and Stream Encryption with PANAMA'
J Daemen, C Clapp, *FSE 98 pp 60–74*

The authors present a stream cipher and hashing algorithm based on the first author's thesis work (**v 4 no 2**) which claims the crown for the fastest software stream cipher from the second author's version of WAKE (**033547**) — at least for highly parallel 32-bit processors such as the Philips Trimedia TM-1000; such a device with a 100MHz clock encrypted data at 470 Mbit/sec — twice as fast as SEAL. On a Pentium Pro, almost 198Mbit/sec ws obtained using a C implementation.

071511 'The First Two Rounds of MD4 are Not One-Way'
H Dobbertin, *FSE 98 pp 284–292*

The author shows how to construct preimages of zero for MD4 reduced to the first two rounds. He exhibits such a preimage, explains briefly how the attack works, and includes C source code that implements it.

071512 'Cryptanalysis of the Swedish NC-9: A Known-Plaintext Approach'
HP Greenough, *Cryptologia v XXI no 4 (Oct 97) pp 353–367*

The author describes an attack on a Swedish version of the Hagelin machine with five pinwheels and fifteen substitution alphabets; these can be recovered with less than 1000 characters of known plaintext using digraph counting techniques.

071513 'A Colossal Fish'
FP Heider, *Cryptologia v XXII no 1 (Jan 98) pp 69–95*

The author describes the cryptanalysis of the German WWII SZ40/42 encryption machine that used Baudot-coded alphabet. The statistical properties of German Baudot code were exploited to implement the attack on Colossus-type machines. The Germans were apparently aware that compromise of about 500 characters of known plaintext could lead to a break, as well as knowledge of sufficient amounts of ciphertext.

071514 'Characterising the linear complexity of span 1 de Bruijn sequences over finite fields'
PA Hines, *Journal of Combinatorial Theory Series A v 81 (98) pp 140–148*

The author proves a conjecture of Blackburn, Etzion and Paterson that the linear complexity of the set of de Bruijn sequences over a nonprime field in which each element of the field appears exactly once, would assume every possible value for large enough parameters; indeed they show that it works for all GF(p^m) for $m \geq 2$.

071515 'Attacks on Fast Double Block Length Hash Functions'
LR Knudsen, X Lai, B Preneel, *Journal of Cryptology v 11 no 1 (Winter 98) pp 59–72*

This paper discusses attacks on double length hash functions that hash two message blocks using two block cipher encryptions in the compression function. All double block functions of this type are shown to be subject to pre-image and collision attacks of lower complexity than brute-force attacks.

071516 'On the Design and Security of RC2'
LR Knudsen, V Rijmen, RL Rivest, MJB Robshaw, *FSE 98 pp 206–221*

The authors describe the design of RC2, a 64-bit block cipher designed to be especially effective on 16-bit processors. It has a variable key length and intercalates rounds of 'mixing' and 'mashing'. A first attempt at a differential cryptanalysis is made which reveals an interesting interaction between the two types of round: differentials with initial and final one-bit differences can have a variety of possible intermediate Hamming weights. The cipher appears to compare favourably to DES.

071517 'Attacking Triple Encryption'
S Lucks, *FSE 98 pp 239–253*

The author presents various optimisations on the meet-in-the middle attack on triple encryption. These allow triple DES to be broken with about 2^{108} encryptions, or 2^{90} encryptions and 2^{113} faster operations, rather than the 2^{112} encryptions of the standard birthday attack.

071518 'Software Encryption Algorithms for Transparent Protection Technology'
AA Moldovyan, NA Moldovyan, *Cryptologia v XXII no 1 (Jan 98) pp 56–68*

The paper presents four software-oriented algorithms — one for key scheduling and three ciphers based on modulo-2 addition, modulo-2^{32} addition and subtraction. The use of the algorithms in a PC software encryption system called COBRA is discussed, as well as the algorithms security.

071519 'Higher Order Differential Attack of a CAST Cipher'
S Moriai, T Shimoyama, T Kaneko, *FSE 98 pp 17–31*

The authors show how to improve the higher order differential attack of Jakobsen and Knudsen **063534** on a variant of CAST to the point that with five rounds only 2^{17} chosen plaintexts are required to recover the last round key.

071520 'About Feistel Schemes with Six (or More) Rounds'
J Patarin, *FSE 98 pp 103–121*

The increase of pseudorandomness in a Luby-Rackoff model of a Feistel cipher with the number of rounds is studied in this paper, both qualitatively and quantitatively. 'Homogeneous' pseudorandom permutations are defined as those such that for all integers m and all sets of m plaintext-ciphertext pairs, there are always about the same number of possible keys that send all the plaintexts to the ciphertexts; one might say that such ciphers look random to a successful solver. The curious result is then proved that even with six rounds, Feistel ciphers (in the Luby-Rackoff sense) are not homogeneous.

071521 'MRD hashing'
R Safavi-Naini, S Bakhtiari, C Charnes, *FSE 98 pp 134–149*

The authors propose two new hash functions inspired by maximum rank distance codes and whose security can be proved in the Wegman-Carter model; the idea is to control the number of collisions by controlling the number of zeros in the columns. The evaluation of digests reduces to matrix multiplication over GF(2). The selection of parameters for efficient implementation is then discussed.

071522 'New Results in Linear Cryptanalysis of RC5'
AA Selçuk, *FSE 98 pp 1–16*

The author shows that the linear cryptanalysis of RC5 proposed by Kaliski and Yin (**044521**) is wrong as some of the assumptions do not hold. However an improved analysis gives similar results.

071523 'Cryptographic Algorithm Metrics'
LT Smith, *NISSC 97 pp 128–140*

Some issues relevant to developing generic cryptographic algorithm metrics are discussed in this article.

071524 'CS-Cipher'
J Stern, S Vaudenay, *FSE 98 pp 189–205*

The authors propose a block cipher based on ideas from FFT hashing and multi-permutations. It is optimised for hardware, with a fully pipelined 64-bit block cipher taking 30,000 gates; it also has reasonable performance in software, yielding 20Kbps on a 4Mhz 6805 and 8Mbps on a 133Mhz Pentium. However, key setup is relatively expensive. A C implementation is included.

071525 'Global avalanche characteristics and nonlinearity of balanced Boolean functions'
JJ Sun, JI Lim, S Chee, SH Sung, *Information Processing Letters v 65 no 3 (13/2/98) pp 139–144*

The authors introduce two measures of global avalanche for Boolean functions and obtain lower bounds for these measures for balanced functions. They also get an improved upper bound on nonlinearity for balanced Boolean functions.

071516 'A Risk Minimisation Framework For Electronic Commerce'
D Trček, *NISSC 97 pp 603–611*

The author suggests that future attacks against hash functions can be dealt with by adopting suitable message redundancy techniques at the application layer.

071527 'Differential Cryptanalysis of the ICE Encryption Algorithm'
B Van Rompay, LR Knudsen, V Rijmen, *FSE 98 pp 270–283*

The authors demonstrate a practical key-dependent differential attack on ICE with 6 rounds using a four-round characteristic that requires about 2^{15} pairs of plaintexts, and that on 8 rounds ('Thin-ICE') requires just under 2^{24} pairs to have a greater than 50% chance of succeeding. It does not work for more than nine rounds.

071528 'Cryptanalysis of Some Recently-Proposed Multiple Modes of Operation'
D Wagner, *FSE 98 pp 254–269*

This paper provides shortcut attacks on a number of multiple modes of operation proposed by Biham on the assumption that the opponent can choose IVs. This allows him to strip off one layer of encryption at a time on some modes; adding the ability to do adaptive chosen-text attacks opens up still more modes. These results highlight the general fragility of multiple modes that incorporate internal chaining. (One of the ideas developed here, the 'narrow pipe', was later used by the author and others in attacking the COMP128 hash function used in GSM.)

071529 'Differential cryptanalysis of KHF'
D Wagner, *FSE 98 pp 293–296*

The author shows how to attack the keyed hash function primitive proposed in **043503** with just 37 chosen messages by finding an internal collision. Although this function was designed with careful attention to using highly nonlinear Boolean functions, it turns out that a one-bit input difference in the round function will give rise to a zero output difference often enough to be exloited.

071520 'The SPEED Cipher'
Y Zheng, *FC 97 pp 71–89*

A block cipher is presented that has variable key-length between 48 and 256 bits (in multiples of 16), at least 32 rounds (in multiples of 4) and block length of 64, 128 or 256 bits. The cipher uses modular addition, right cyclic shifts, a bit-wise Boolean operation. A security analysis and some application suggestions are provided.

6 Public Key Algorithms

071601 'An active attack on protocols for server-aided RSA signature computation'
G Horng, *Information Processing Letters v 65 no 2 (29/1/98) pp 71–74*

The author points out than when a server-aided signature protocol is attacked by the server, it can use as a blinding factor any previous genuine signatures.

071602 'Authenticated encryption scheme with (t, n) shared verification'
CL Hsu, TC Wu, *IEE Proceedings in Computers and Digital Techniques v 145 no 2 (Mar 98) pp 117–120*

A new threshold authenticated encryption scheme is presented. It is based on the Nyberg-Rueppel signature (**031611**) and on Harn's threshold signature scheme, but provides some efficiency advantages over the latter.

071603 'Efficient group signature scheme based on the discrete logarithm'
WB Lee, CC Chang, *IEE Proceedings in Computers and Digital Techniques v 145 no 1 (Jan 98) pp 15–18*

The authors present a new group signature scheme based on the Nyberg-Rueppel signature (**031611**) that is non-interactive and thus more communication-efficient than older group signature schemes by Chen and Pedersen (**032609**). A trusted party has to set up the group scheme, but should not be able to forge the signature contribution of an individual user.

071604 'On the Security of Park et al's Key Distribution Protocol for Digital Mobile Communications'
NY Lee, TNL Hwang, *Cryptologia v XXI no 4 (Oct 97) pp 327–334*

A public key authentication protocol proposed by Tatebayashi, Matsuzaki and Newmann was broken by Park and others (Eurocrypt 93) who proposed a fix. The authors show that this fix is inadequate and propose a further fix.

071605 'Cryptanalysis and improvement of signcryption schemes'
H Petersen, M Michels, *IEE Proceedings in Computers and Digital Techniques v 145 no 2 (Mar 98) pp 149–151*

The authors review the authenticated encryption schemes by Zheng (**063418**), noting that the confidentiality property is violated by the attempt to provide non-repudiation. They also review some similar schemes not mentioned in Zheng's work and suggest a solution to the problem.

071606 'Signature schemes based on factoring and discrete logarithms'
Z Shao, *IEE Proceedings in Computers and Digital Techniques v 145 no 1 (Jan 98) pp 33–36*

The author proposes two digital signature schemes based on the ElGamal and Harn schemes (**033609**) and shows a weakness in the Harn scheme if a one-way hash function is not used.

071607 'A variant of the public key cryptosystem FAPKC3'
R Tao, S Chen, *Journal of Network and Computer Applications v 20 no 3 (Jul 97) pp 283–303*

The authors review finite automata-based public key systems and suggest a new variant on this theme now that most of the preceding systems have been shown to be insecure.

071608 'Monkey: Black-Box Symmetric Ciphers Designed for MONopolizing KEYs'
A Young, M Yung, *FSE 98 pp 122–133*

The authors continue their work on ciphers with trapdoors from **063626**; in this paper, they exhibit a block cipher that leaks a bit of master key per block encrypted.

7 Computational Number Theory

071701 'Factors of generalized Fermat numbers'

A Björn, H Riesel, *Mathematics of Computation v 67 no 221 (Jan 98) pp 441–446*

The authors describe using a number of techniques to factor numbers of the form $a^{2^n} + b^{2^n}$ for small values of a, b and n.

071702 'Analysis of Iterated Modular Exponentiation: The Orbits of x^α mod N'

JJ Brennan, B Geist, *Designs, Codes and Cryptography v 13 no 3 (Mar 98) pp 229–245*

The authors analyse the structure of the orbits of x^α mod N where N is a product of two large primes. Blum, Blum and Shub had given conditions under which these would have period $\lambda(\lambda(N))$ for $\alpha = 2$, while in **043709** Maurer had given bounds on the probability of a short cycle for the case that α is relatively prime to N. This paper extends these results to the general case where α may not be relatively prime and the factorisation p_i and q_i of the factors p and q of N may be unknown: the probability that an element x belongs to a short cycle is bounded by $\sum 1/p_i + \sum 1/q_i$. As an example, they work out the orbit structure of RSA129. These results give bounds on the iterated encryption attack on RSA.

071703 'Gauss periods: orders and cryptographical applications'

SH Gao, J von zur Gathen, D Panario, *Mathematics of Computation v 67 no 221 (Jan 98) pp 343–352*

The authors show that Gauss periods in finite fields generally have high order, are self-dual and can be exponentiated in quadratic time, making them suitable candidates for cryptographic use. (A Gauss period of type (d, n) is a sum $\sum \beta^\alpha$ where β is a primitive root of unity in $\mathrm{GF}(q^{nk})$ and the sum is over the subgroup of order k of the multiplicative group of the integers mod r, where $r = nk + 1$.) Gauss periods of type $(n, 2)$ had already been known to be candidates; this paper generalises that. Indeed for k even and in characteristic 2, Gauss periods are self-dual. Applications range from pseudorandom generators provably as secure as discrete logarithm to sparse primitive polynomials of large degree.

071704 'Fully Polynomial Byzantine Agreement for $n > 3t$ Processors in $t + 1$ rounds'

JA Garay, Y Moses, *SIAM Journal on Computing v 27 no 1 (Feb 98) pp 247–290*

The authors present a polytime protocol for Byzantine agreement in $t + 1$ rounds wherever $n > 3t$, there being n processors of which t may fail. If less of them fail, then it will terminate proportionally more quickly.

071705 'Distribution of irreducible polynomials of small degree over finite fields'

KH Ham, GL Mullen, *Mathematics of Computation v 67 no 221 (Jan 98) pp 337–341*

Hansen and Mullen conjectured in **021514** that for all a in a finite field $\mathrm{GF}(q)$, there is an irreducible polynomial of degree n whose j-th coefficient is a except in the obvious degenerate cases. This result was proved by Wan in **064707** for $q > 19$ or $n > 35$. This paper finally removes these constraints; specimen polynomials were simply computed.

071706 'Counting Points on Curves over Finite Fields'

MD Huang, D Ierardi, *Journal of Symbolic Computation v 25 no 1 (Jan 98) pp 1–21*

The authors show that for a projective plane curve $\mathcal{C}$ of degree n with $\mathcal{C}$ having only ordinary multiple points, one can compute the number of F_q-rational points on $\mathcal{C}$ in random time $(\log q)^{n^{O(1)}}$ and then also the number of F_q-rational points on the smooth projective model of $\mathcal{C}$, on the Jacobian of $\mathcal{C}$ and the number of F_{q^m}-rational

points on $\mathcal{C}$ in any given finite extension F_{q^m} of the ground field, each in a similar time bound.

071707 'Efficient Multiplier Architectures for Galois Fields $GF(2^{4n})$'
C Paar, P Fleischmann, P Roelse, *IEEE Transactions on Computers v 47 no 2 (Feb 98) pp 162–170*

A new architecture for improving computational complexity of multipliers in the fields $GF(2^{4n})$ using the Karatsuba-Ofman algorithm is presented. Modular reduction can be combined with the last stage of the algorithm by determining suitable optimised field polynomials of degree four.

071708 'A Structural Comparison of the Computational Difficulty of Breaking Discrete Log Cryptosystems'
K Sakurai, H Shizuya, *Journal of Cryptology v 11 no 1 (Winter 98) pp 29–43*

A comparison of five cryptosystems based on the discrete log problem is given. A polynomial-time functionally many-to-one reducibility relation is obtained for Diffie-Hellman, ElGamal, the Bellare-Micali non-interactive oblivious transfer, the Okamoto conference key scheme and the Shamir 3-pass scheme. The authors also show equivalence for the discrete log problem certified over Z_p^* or for the discrete log problem associated with an ordinary elliptic curve over Z_p.

071709 'Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p'
IA Semaev, *Mathematics of Computation v 67 no 221 (Jan 98) pp 353–356*

The author shows that the discrete logarithm problem is trivial in trace one curves; in particular, one can construct an isomorphism from any p-order subgroup of an elliptic curve over a finite field to the field's additive group and this isomorphism can be computed in time logarithmic in the characteristic of the field. The result is proved for elliptic curves and a generalisation of Ruck to curves of arbitrary genus is mentioned.

8 Theoretical Cryptology

071801 'Common randomness in Information Theory and Cryptography – Part II: Capacity'
R Ahlswede, I Csiszár, *IEEE Transactions on Information Theory v 44 no 1 (Jan 98) pp 225–240*

In this paper (which follows a first part of several years ago), the authors discuss common randomness without the secrecy aspect, analysing the 'common randomness capacity' property for several randomness generation models.

071802 'Spreading Rumours Rapidly Despite an Adversary'
J Aspnes, W Hurwood, *Journal of Algorithms v 26 no 2 (Feb 98) pp 386–411*

The authors study the effort involved in n players sharing n values where the network timing is under the control of a content-oblivious adversary, and give a randomised algorithm for doing this in $n \log^3 n$ steps.

071803 'Bounds and Characterizations of Authentication/Secrecy Schemes'
LRA Casse, KM Martin, PR Wild, *Designs, Codes and Cryptography v 13 no 2 (Feb 98) pp 107–129*

The authors consider unconditionally secure authentication schemes that also offer L-fold secrecy, establish entropy bounds on them for both ordered and unordered secrecy, and characterise schemes that meet these bounds in terms of incidence structures.

071804 'Some Consequences of Cryptographic Conjectures for S_2^1 and EF'
J Krajíček, P Pudlák, *Information and Computation v 140 no 1 pp 82–94*

The authors show that the Extended Frege (EF) proof system does not admit feasible interpolation unless the RSA cryptosystem is not secure and give also other results on factoring and discrete logarithm using relation between EF and first-order theory S_2^1 for the EF-proofs.

071805 'An Efficient Noninteractive Zero-Knowledge Proof System for NP with General Assumptions'
J Kilian, E Petrank, *Journal of Cryptology v 11 no 1 (Winter 98) pp 1–27*

The paper introduces a new non-interactive zero-knowledge protocol with the proof system based on shared random string model. The protocol needs only $O(n \lg n)$ random committed bits to prove n-gate circuit is satisfiable with error probability $1/n^{O(1)}$.

071806 'Secure multiparty computations without computers'
V Niemi, A Renvall, *Theoretical Computer Science v 191 no 1–2 (30/1/98) pp 113–134*

The authors extend the work of den Boer who showed that the multiparty computation of an AND gate could be executed using five playing cards. The difficulty in doing this for arbitrary Boolean functions had lain in making a copy of a bit commitment. This is solved by encoding the information in the order of the cards; the result is that many useful functions and crypto protocols can now be implemented in a reasonable number of cards.

071807 'Three Systems for Threshold Generation of Authenticators'
R Safavi-Naini, *Designs, Codes and Cryptography v 13 no 3 (Mar 98) pp 299–312*

The author proposes three methods for shared construction of authenticators by an authorised group of transmitters that provide unconditional security; two are (n, n) schemes and one a (t, n) threshold scheme; one has a public authentication matrix; and in two of them the protection can extend over mutliple messages.

071808 'Linear Sections of the Finite Veronese Varieties and Authentication Systems Defined Using Geometry'

C Zanella, *Designs, Codes and Cryptography v 13 no 2 (Feb 98) pp 199–212*

The author discusses authentication schemes based on algebraic geometry, in which the source states are lines through a point N of $\mathrm{PG}(d, q)$ (the d-dimensional projective space over $\mathrm{GF}(q)$) and the keys are hypersurfaces with the property that every line through N meets them in exactly one point; messages are then these unique points corresponding to a source state and a key. Such systems were first proposed by the author and others in 1990. In this paper, some optimal security bounds are proven, together with some special results for quadrics.

9 Book Reviews

'PRIVACY ON THE LINE'

Whitfield Diffie, Susan Landau
MIT Press, 1998; ISBN 0-262-04167-7

The debate over key escrow that has grown over the last five years may have forced more people to acquire some knowledge of cryptology than in all previous periods of human history combined. This has meant that practitioners of the art have spent an increasing portion of their time explaining the basics to people such as lawyers, politicians and journalists.

It would clearly be a good thing if this could be done once, and well. This new book by Whit Diffie and Susan Landau makes by far the best effort so far at such an exposition. The technical complexities of communications intelligence and cryptographic mechanisms are explained at just the right level of detail for the intelligent layman, as is the recent history of key escrow policy in Washington. The authors clearly benefit from their considerable recent experience at exposition and make the story available to a wider audience.

'OPTICAL DOCUMENT SECURITY'

Rudolf van Renesse
Artech House, 1997; ISBN 0-89006-982-4

The rapidly growing interest in methods of hiding copyright marks in digital audio and video might prompt a thoughful person to ask about the techniques used by more traditional users of information hiding techniques, namely the companies that print documents such as passports and banknotes. Meanwhile, these companies have adopted all manner of tricks ranging from effects of physics and materials science, such as kinegrams, optically variable inks and partially metallised films, to alias band effects and other tricks which have direct analogues in the world of digital information hiding.

The publication of this book on document security could scarcely be more timely. It provides fairly complete explanations of many of the effects used by modern security printers, together with a number of samples and a reference CD. The explanation is pitched at the level of scientific explanation rather than training for forgery, but this is ideal for its legitimate purposes. This book should be read by everyone involved in intellectual property protection.

'EUROPEAN SCRAMBLING SYSTEMS v 5 (THE BLACK BOOK)'

John McCormac
Waterford University Press (1997) ISBN 1-873556-22-5

John McCormac has published a series of books on pay-TV hacking under the generic title of the 'Black Book'. Previous titles have been somewhat fragmentary collections of hacking lore, aimed at people already involved in the scene.

Now the fifth edition of the book has appeared and is greatly expanded in an attempt to become more self-sufficient. Much of the material, such as basic cryptology, is better expounded elsewhere; but there are a number of sections on the design details of particular pay-TV scrambling systems and the practicalities of circumventing them that are simply unobtainable elsewhere.

'E-COMMERCE SECURITY'
Anup K Ghosh
Wiley Computer Publishing, 1998; ISBN 0-471-19223-6

This book attempts to tackle the technical security aspects of setting up a web-based commerce server from a viewpoint of systems engineering rather than crypto or protocol theory. It is full of details of real attacks, and these are grouped under four main headings. The chapter on client vulnerabilities has much information on malicious content, and rather than the traditional description of DOS viruses its focus is on malware written in Word, Java and ActiveX, which has recently taken over as the main threat. There is also a perceptive discussion of the vulnerabilities and drawbacks of various versions of Authenticode, and a number of war stories of browser bugs. This chapter does a very good job of highlighting the severe tensions between security and ease of use facing the application designer or toolsmith.

The next chapter, on the transaction protocols, talks about some of the problems with the TCP-IP protocol suite and what can be done with mechanisms such as SSL and smartcards. This is perhaps the weakest in the book. The next two chapters deal with the commerce server software and the underlying operating system and are much meatier; there are many things that can go wrong when configuring web servers which is difficult to do properly. The book gives some practical information on how to do this and test it. Securing the underlying operating system and the firewall is similar; a number of deadly defaults in common products are described. The book ends with a plea for commercial users to adopt the kind of software certification practices common for twenty years in the military (even if the security policy models are different).

This is one of the better books on electronic commerce to be published, and is a good buy for a system administrator who is just starting to come to grips with running a web site. It is also of value for the system designer and the researcher.

'VIRTUAL PRIVATE NETWORKS'
Charlie Scott, Paul Wolfe and Mike Erwin
O'Reilly, 1998: ISBN 1-56592-319-7

A recent growth business has been the provision of virtual private networks — corporate networks built on top of the Internet using firewalls and encryption. The philosophy, design and economics of such networks are explored, and the book then goes on to describe three of the main protocols in use: PPTP from Microsoft (which is included with NT and various third party products), the AltaVista tunnel from DEC, and PIX from Cisco. This is a practical rather than theoretical book; its focus is on the practical aspects of how to get a VPN up and running using available products, and then maintaining it sensibly.

'INTERNET AND INTRANET SECURITY'
Rolf Oppliger
Artech House, 1997; ISBN 0-89006-829-1

This book presents a majority of the available security techniques and mechanisms for the net and for intranets, as well as some of those currently under development. It starts with a very solid introduction to net standards and the OSI Security Architecture, followed by a basic introduction to crypto. The following section addresses of access control and firewall techniques. A major part of the book discusses security protocols for IP, TCP and the application layer. A brief discussion on e-commerce and security tools concludes the core of the book.

The reader should be familiar with the basics of O/S and networking, with a basic understanding of computer security issues an advantage. The book appears to be well balanced in addressing the relevant issues in TCP/IP networking, does not spend a great deal of space on fast aging Internet applications, yet lacks more depth in areas like Internet server security and mobile code.

'FUTURE CODES – ESSAYS IN ADVANCED COMPUTER TECHNOLOGY AND THE LAW'

Curtis EA Karnow

Artech House Inc., 1997, ISBN 0-89006-942-5

The book provides a comprehensive collection of essays on the law and information technology. It discusses legal issues arising out of intellectual property protection, errors and traps in computer systems, liability for mobile code conduct and viruses, the parts of the criminal law relevant to computer technologies, and also mentions regulations of the export of encryption. Although most case references pertain to US law, the views and reasoning are generally of international applicability: the relevant law-versus-technology issues are treated in a manner that most technology-rooted readers should find comprehensive and readable.

'CRYPTOGRAPHY AND LIBERTY: AN INTERNATIONAL SURVEY OF ENCRYPTION POLICY'

Wayne Madsen

Global Internet Liberty Campaign, www.gilc.org (no ISBN)

This book provides a snapshot of the state of encryption controls, related legislation and governments' announced intentions as of February 1998. Countries are classified as 'green', 'yellow', 'red' (or as borderline cases) according to whether they support the OECD guidelines, have proposed new controls, or have instituted severe controls. This leads to anomalies in places, e.g. Germany and Switzerland get 'green' despite export controls while New Zealand and Luxembourg get 'green/yellow' despite being in a similar condition. Nonetheless the book contains substantial detail about a number of countries and thus makes a worthwhile contribution.

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 £125, 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$1.67 = £1; credit card orders (VISA and MasterCard) are charged in sterling.

Back issues offer: Get a subscription for 1998 (volume 7) plus a set of the remaining back numbers (currently volumes 2 through 6) at a price of £99.50 for individual subscribers and £185 for corporate subscribers. Electronic copies of back numbers over a year old are at `http://www.cl.cam.ac.uk/users/rja14`.

Individual subscription for 1998 — Please debit my VISA/MasterCard £60 □ I enclose a cheque for £60 □ / US$99.50 □

Individual subscription for all available 1993–98 issues — Please debit my VISA/MasterCard £99.50 □ I enclose a cheque for £99.50 □ / US$149.25 □

Corporate subscription for 1998 — Please debit my VISA/MasterCard £125 □ I enclose a purchase order / cheque for £125 □ / US$199.95 □

Corporate subscription for all available 1993–98 issues — Please debit my VISA/MasterCard £185 □ I enclose a purchase order / cheque for £185 □ / US$299.95 □

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 1223 334678, or mail it to us at:
Northgate Consultants Ltd., 10 Water End, Wrestlingworth, Sandy, Beds SG19 2HA, United Kingdom