Computer and Communications

Security Reviews

Volume 5 Number 1 (March 1996) ISSN 1352-6278

CONTENTS

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

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

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by December 1995; and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

EDITT 95: TEDIS EDI trusted third parties workshop, 8–10 February 95, Barcelona, Spain; *proceedings published by Universitat Politècnica de Catalunya, ISBN 84-7653-506-6*

IFIP 95: 11th international conference on information security, 8–12 May 95, Cape Town, South Africa; *proceedings published by Chapman & Hall as "Information Security — The Next Decade", ISBN 0-412-64020-1*

STOC 95: 27th annual symposium on the theory of computing, 29 May – 1 June 95, Las Vegas, Nevada, USA; *proceedings published by ACM ISBN 0-89791-718-9*

EC 95: First Usenix Workshop on Electronic Commerce, 11–12 July 95, New York, USA; *proceedings published by the Usenix Association, ISBN 1-880446-74-X*

NISSC 95: 18th National Information Systems Security Conference (formerly the National Computer Security Conference), 10–13 October 95, Baltimore, MD, USA; *proceedings published by NIST*

Multimedia 95: 5th to 9th November, San Francisco, California, USA; *proceedings published by ACM ISBN 0-89791-751-0*

Mobicom 95: First conference on mobile computing and networking, 13–15 November 95, Berkeley, California, USA; *proceedings published by ACM ISBN 0-89791-814-2*

Cirencester 95: 5th IMA Conference on Cryptography and Coding, 18–20 December 95, Cirencester, UK; *proceedings published as Springer Lecture Notes in Computer Science vol 1025 ISBN 3-540-60693-9*

ACM 96: 3rd ACM Conference on Computer and Communications Security, March 14-16, 96, New Delhi, India; *proceedings published by ACM ISBN 0-89791-829-0*

We have decided to 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

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

or

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

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

1 Applications and Engineering

051101 ‘Striving for Correctness’
MD Abrams, MV Zelkowitz, *Computers and Security v 14 no 7 (95) pp 719–738*

The search for correct security designs has brought forth innovation in formal methods, simulation, testing and process modelling; their relative strengths and weaknesses are assessed. Checkability is very important, as is the correct use of abstraction. These points are all well known to software engineers, but regarded as alien to many practicing security engineers. The authors of this article recommend a pragmatic combination of them that is informed by a knowledge of their limitations.

051102 ‘Simulate Security on Unix Networks’
M Alexander, *Datamation (1/3/96) pp 69–73*

This article describes a number of commercial competitors of SATAN, ranging from TCP/IP scanners that roam a corporate network looking for weaknesses to tools that analyse network traffic looking for attacks.

051103 ‘Detecting Intrusions in Smart Card Applications: using Expert Systems and Neural Networks’
T Alexandre, R Trane, *IFIP 95 pp 549–561*

The authors discuss a prototype system that can be run on a smartcard and that analyses the user’s behaviour; it raises an alarm if transactions are made out of pattern. Neural network and rule based approaches are compared.

051104 ‘Patient Privacy in the Era of Medical Computer Networks: a New Paradigm for a New Technology’
BR Beier, VM Brannigan, *Datenschutz und Datensicherung v 19 no 12 (Dec 95) pp 709–712*

The authors propose enforcing privacy in hospital computer systems by having an openly available database of de-identified fragments of records plus a secure identifier control facility that would link them to actual patients. Their key observation is that most hospital activities — from filling a prescription through lab tests to performing epidemiological studies — use the patient’s name only as an error control mechanism. Coded identifiers could be used instead.

051105 ‘Cryptological devices and machines in the Deutsches Museum, Munich’
FL Bauer, *Cryptologia v XX no 1 (Jan 96) pp 11–13*

A museum in Munich has a number of cryptographic exhibits, from 17th century encrypting rods through to Kryha, Enigma and T52 machines.

051106 ‘Smartcards and Biometrics: An Overview’
E Bovenlander, RL van Renesse, *Computer Fraud and Security Bulletin (Dec 95) pp 8–12*

The authors discuss how TNO, a Dutch evaluation laboratory, goes about assessing high-end security products such as biometric and smartcard systems. The smartcard may be opened and etched, and up to ten microprobes with 0.5μ radius tips may be used in an attempt to capture key material. However, most flaws are found at the interfaces between physical, logical and organisational measures.

051107 ‘Smart cards get green light’
JC Broustra, *Cards International (9/11/95) pp III–IV*

This article contains forecasts of smartcard markets up to the year 2000 made by Solaic and Gemplus, and discusses a few applications.

051108 ‘Firewall Turns up the Heat on Internet Hackers’
C Bruno, *Data Communications International (Mar 96) pp 46–48*

This article describes a proxy firewall from TIS that supports a number of authentication and encryption schemes and whose source code is available to customers.

051109 ‘An Efficient Fair Payment System’
J Camenisch, JM Piveteau, M Stadler, *ACM 96 pp 88–94*

The authors present a payment system with revocable anonymity. Following Chaum and others, they use blinding for anonymity and detection of double spending. Their system also prevents blackmail and money laundering. Payments are on-line, but the bank cannot link account numbers directly to customers; only a judge can do this. Their advantage is that the judge only knows public-private keys and is not on line. Blinded Schnorr signatures are used; Brands’ (1993) result protects the user from forgeries by the bank and judge. A Philips P83c855 smart card with IDEA and Montgomery exponentiation is used in the implementation.

051110 ‘Token and Notational Money in Electronic Commerce’
LJ Camp, M Sirbu, JD Tygar, *EC 95 pp 10-12*

The authors analyze different forms of traditional money based on the degree of privacy they provide, and then apply their evaluation criteria to the DigiCash and NetBill systems.

051111 ‘TESTFIT — TTP and Electronic Signature Trial for Inter-modal Transport’
GD Carter, *EDITT 95 pp 17–26*

The author describes a project to create a pan-European network of trusted third parties that is being organised by a consortium of a dozen users.

051112 ‘Securing ATM Networks’
SC Chuang, *ACM 96 pp 19–30*

The author considers how to secure asynchronous transfer mode communications. His solution involves both the control and data planes and can deal with many configurations: LANs, multimedia desk areas, home area networks, and WAN interfaces. To provide a uniform approach, he designed a CryptoNode: it provides network DMA, buffering, cryptography, synchronisation, and recovery. AALs cannot be encapsulated directly (due to length overflow), so he uses a one-cell crypto tag containing key information, initialisation vectors, and a MAC: this can be used to authenticate arbitrary collections of ATM cells.

051113 ‘Cryptographic techniques — secure your wireless designs’
D Comer, *EDN (18/1/96) pp 57–68*

This article discusses the use of cryptography to protect wireless access systems for vehicles and buildings. These are known in the trade as rolling code, time-based code or challenge-response depending on whether the encryption is applied to a counter, a clock or a received signal. Two families of commercial products are described, and the design tradeoffs discussed.

051114 ‘The Jupiter audio-video architecture: secure multimedia in network places’
P Curtis, M Dixon, R Frederick, DA Nicholls, *Multimedia 95 pp 79–90*

The multimedia environment being developed at Xerox Parc has a very fine grained security model. Virtual rooms are defined in which all users can normally see and hear each other but can ‘whisper’ if they want. There are also tunnels that can be used to link spaces together. The underlying mechanics involves encryption, with a key manager implementing the security policy: this assumes that features added by users will not be trusted by all other users, so everyone can protect their own space while building on others’ innovations as and when they wish.

051115 'Reinforcing password authentication with typing biometrics'
WG de Ru, JHP Eloff, *IFIP 95 pp 562–574*

The authors discuss how one might use 'fuzzy logic' techniques to analyse keystroke patterns while users are entering passwords.

051116 'Location-Based Authentication: Grounding Cyberspace for Better Security'
DE Denning, PH MacDoran, *Computer Fraud and Security Bulletin (Feb 96) pp 12–16*

The authors propose a location signature system that uses GPS to pinpoint a computer user's physical location. The user captures raw GPS signals from all satellites in view and compresses them into a 20Kb message, which may be supplemented by 20 bit/sec updates. The claimed security is founded on the unpredictability of the GPS signals arising from microperturbations of their orbits and the dithering introduced by the DoD selective availability system.

051117 'Network Security Under Siege: The Timing Attack'
E English, S Hamilton, *Computer v 29 no 3 (Mar 96) pp 95–98*

The amount of time taken to perform an operation such as decryption or signature can depend on the value of the key, and in some implementations of systems such as RSA and DSS the key can be recovered by someone who knows the implementation detail and can get accurate timings.

051118 'TeleSeC - a Solution to Implementing Digital Signature in EDIFACT'
P Fjelbye, *EDITT 95 pp 149–160; republished in IFIP 95 pp 409–420*

This article describes a public key architecture being introduced by banks in Denmark to secure commercial banking systems that let corporate clients manage their funds remotely.

051119 'Little acorns'
T George, *Banking Technology (Feb 96) pp 20–24*

This article describes smartcard based electronic purse systems in Denmark, Belgium and the UK. These have shown that controlling costs is critical: the advertising space on a one-time card does not pay for it, and advertisers are not interested in reusable cards. The value of some security features commonly considered desirable is questioned: for example, the Belgian operator did not implement a PIN-based card locking facility.

051120 'Autoassociator-based models for speaker verification'
M Gori, L Lastrucci, G Soda, *Pattern Recognition Letters v 17 no 3 (6/3/96)*

The authors used a multilayer feedforward neural network as an autoassociator to recognise speakers in the DARPA-TIMIT database from a set of 65 male speakers. They had to introduce a penalty function to prevent overtraining, but the cost of admitting new speakers was low and the equal error point while recognising on a single phoneme was under 7%.

051121 'The Impact of ATM on Security in the Data Network'
L Hanson, *Network Security (Jan 96) pp 13–17*

The author describes the basic mechanics of asynchronous transfer mode networks including the user and network interfaces, and discusses various possible abuses. There is still little that users can do to manage security at this level in the network.

051122 'Generic Extensions of WWW Browsers'
R Hauser, M Steiner, *EC 95 pp 147–154*

Existing browsers are a significant barrier to electronic commerce as it can be hard to interface payment protocols to them. The authors discuss ways in which user code can be interfaced to proprietary browsers including MIME extensions, saving the html document in a local file and then reloading it after processing and the use of a proxy http demon at the client. A longer term solution would involve an extension manager that would interface the browser to security, cacheing and remote control facilities.

051123 'ACPO's intruder policy — underwritten?'
M Jay, *Security Surveyor v 26 no 3 (Sep 95) pp 10–15*

A new UK police policy gives priority to burglar alarms that have been confirmed by audio, video or other means, and according to the insurance industry this should create a market for more sophisticated alarm communications. However the underlying problem has been the very success of the alarm industry: there are so many more alarms than a generation ago, and police resources have not expanded in step.

051124 'Smart Catalogs and Virtual Catalogs'
AM Keller, *EC 95 pp 125–131*

The author presents a system to support electronic commerce in which product information is retrieved from multiple distributed catalogues that are indexed using a special markup language so that their content may be searched efficiently.

051125 'Point-of-Sale (POS)-Systeme — Kryptografie, Magnetstreifen- und Chipkarten als Sicherheitsworkzeuge'
A Kiranas, *Datenschutz und Datensicherung v 19 no 12 (Dec 95) pp 721–728*

The author presents an overview of both magnetic card and chip card point of sale systems, including an overview of the protocols used between the chipcard, the terminal and the card issuer.

051126 'Point-of-Sale (POS)-Systeme — Organisatorische Sicherheit'
A Kiranas, *Datenschutz und Datensicherung v 20 no 2 (Feb 96) pp 94–100*

The author continues how overview of point of sale systems. He discusses the levels of threat associated with various kinds of installation and how the associated risks should be controlled.

051127 'Security Assurance Issues for TTP Services'
H Kurth, RPJ Winsborrow, *EDITT 95 pp 27–36*

The 'Ebridge' project aims to build an online electronic business register for Europe, both as a demonstrator for the value of community-wide services and as a full-scale trial of digital signature technology using Unix-based tamper resistant signature devices. It is envisaged that the architecture could be used for land and vehicle registries as well as for businesses.

051128 'Roles and Responsibilities in BOLERO'
P Landrock, *EDITT 95 pp 125–135*

The author describes BOLERO, a project to provide electronic bills of lading, with emphasis on the mechanisms and procedures required for the secure initialisation of the infrastructure. This can be bootstrapped from a chamber of commerce network, or from manual signatures and directories; manual messages can also be used to revoke keys and de-register a company.

051129 'The registration authority for the bank identifier code'
JP Magalhaes, *EDITT 95 pp 185–192*

This article describes the origin and structure of the SWIFT addresses used by banks, and the problems caused by the recent explosive growth of the demand for namespace. Maintaining accuracy is a problem, as closures, mergers and other changes are not always notified. Relationships with national databases, and the wider world of EDI, are also discussed.

051130 'Trusted third parties in the TEDIC project of the interconnectivity platform of the Ile de France teleport'
T Marchiset, *EDITT 95 pp 193–196*

The author provides some information about an EDI pilot in France.

051131 'Human-Computer Cryptography: An Attempt'
T Matsumoto, *ACM 96 pp 68–75*

The idea of "human-computer cryptography" is to use a challenge-response protocol to protect the channel between the human and the terminal. Users' secrets are locations or patterns on a display, and users respond with the labels or colours displayed at these points. Since the correct answers appear in multiple places, the attacker needs several successful interceptions to compute the secret.

051132 'The Ouroboros of the Digital Consciousness: Linear Feedback Shift Registers'
C Maxfield, *EDN (4/1/96) pp 135–142*

The author discusses the engineering detail of implementing linear feedback shift registers, and their use in a number of applications.

051133 'Functional and Operational Security System for Open Distributed Environments'
S Muftic, *IFIP 95 pp 289–301*

The author describes a prototype secure system based on a Kerberos variant, smartcards, X.509, PEM and EDIFACT.

051134 'Probabilistic Quorum Protocols for Biometrical User Authentication in OLTP'
VK Murthy, *SIGSAC Review v 14 no 1 (Jan 96) pp 5–10*

The author considers fortifying biometrics using random challenges, such as by asking users to utter certain words, and does various calculations on error rates.

051135 'NetWare 4: The Climb to C2'
NetWare Connection, Nov/Dec 1995 pp 6-14

Novell NetWare 4 is approaching the completion of its "Red Book" (network) C2 evaluation. Red Book evaluations are more useful than "Orange Book" ones, as they allow for heterogeneous products.

051136 'Internet Information Commerce: The First Virtual Approach'
D New, *EC 95 pp 33-68*

These are reprints of the slides from this talk; they briefly outline the First Virtual information commerce model and the company.

051137 'Doubt cast on photo-id cards'
P Penrose, *Banking Technology (Feb 96) p 4*

A recent study showed that even under ideal conditions supermarket cashiers were not much good at recognising customers from photographs on credit cards: a substantial proportion of the cards with incorrect photos were accepted. Banks who have benefited from photos maintain that they are still effective as a deterrent.

051138 'UK set for national smart card roll out...'
P Penrose, *Banking Technology (Mar 96) p 10*

UK banks have agreed to introduce smart cards to all their customers in 1997 in order to cut losses from card counterfeiting. The cards will conform to the EMV standard and be developed by Gemplus, Schlumberger and Delphic.

051139 'Quantum Cryptography: Protecting our Future Networks with Quantum Mechanics'

SJD Phoenix, PD Townsend, *Cirencester 95 pp 112–131*

The authors describe some experiments performed at British Telecom which have been used to establish key material at rates of 1kbit/sec over optical fibres of length up to 30km. They predict that lengths over 100km and bit rates as high as 20kbit/sec may be possible with improvements in detector technology. Using standard telecomms fibre, at least 8km is possible. Possible many-to-one key distribution techniques are also discussed.

051140 'Security in Smartcards'

W Qureshi, *Card World Independent (Jan 96) pp 4–5*

A Motorola marketing manager discusses the security of smartcards. Their protection feature may include varying the timing of writes to EEPROM and detecting out-of-range voltage, frequency and temperature.

051141 'Setting up a Security Perimeter for Distributed Networks'

E Roberts, *Data Communications International (Feb 96) pp 45–46*

This article describes a dial access security product from Cisco which uses a modified version of the IETF TACACS, with MD5 to encrypt data packets.

051142 'Magic Circles'

M Rowe, *Banking Technology (Feb 96) pp 40–42*

The creation of two new high value settlement systems in France, which will go live from 1997, has prompted a review of the country's payment infrastructure, which is described in this article.

051143 'Unified Login with Pluggable Authentication Modules'

V Samar, *ACM 96 pp 1–10*

In this article, the authentication needs of users, vendors, and administrators are considered. UNIX, S/Key(TM), Kerberos, DCE, and token cards are all different, mostly hard coded, and relatively inflexible. Sun's divides the solution into four modules: authentication, authorisation, password management, and session management.

051144 'The DigiBox: A Self-Protecting Container for Information Commerce'

O Sibert, D Bernstein, D Van Wie, *EC 95 pp 171-183*

The DigiBox is a hardware system that protects information from illegal copying and use; its applications are the protection of copyrights. This paper outlines the needs and uses for such a system, as well as a high-level design.

051145 'Electronic Purses: A Comparative Review'

Smart Card News part 5: Dec 95 pp 226–229; part 6: Jan 96 pp 6–9; part 7: Feb 96 pp 26–29

These articles continue from **044147** with a survey of smartcard payment systems fielded in Austria, Brazil, China, Italy, Russia, Germany, Italy, Switzerland, Australia and the USA.

051146 'From Here to There'

Smart Card News (Dec 95) pp 236–238

This article continues from **044148** and provides a management level overview of communications protocols used between smartcards and readers.

051147 'Coding and Cryptography for Speech and Vision'

EV Stanfield, M Walker, *Cirencester 95 pp 213–236*

The authors review some applications of coding and cryptography in modern consumer electronics, and in particular GSM and its successor systems such as DECT and TETRA.

051148 'Computer networks for test ban monitoring'
W Sweet, *IEEE Spectrum v 33 no 2 (Feb 96) pp 24–33*

Test ban treaty monitoring has been revolutionised by moving to an open system. IRIS has 1000 sensors scattered over 100 sites worldwide and is open to academic seismologists; this lessens the fear by third countries that the USA and USSR might conspire to conceal a secret resumption of testing.

051149 'Using network traffic analysis as a security tool'
P Toxell, C Bartlett, N Gill, *NISSC 95 pp 262–270*

The authors developed a traffic analysis tool for the US Air Force for network intrusion detection. It monitors a number of different points on the network and can be instructed to collect the headers of packets with certain addresses, or that contain certain character strings. It is fielded at Wright Patterson AFB and used to find traffic with suspect parties, such as foreign sites, pornography distributors and the sources of previous intrusion attempts.

051150 'Economic Mechanism Designs for Computerized Agents'
HR Varian, *EC 95 pp 13-21*

This paper reviews the field of economic mechanism design and its possible application to electronic commerce.

051151 'Payments by another name'
I Walden, *Banking Technology (Mar 96) pp 21*

The author raises some questions about the legal status of electronic purses in Britain. Is the purchase of a card a deposit, in which case card issuers will require central bank authorisation, or a simple sale of goods? Will electronic money be legal tender? Will payments be absolute or conditional? And what will be the taxation and data protection issues?

051152 'Downloading on the up?'
K Walters, *Security Surveyor v 26 no 2 (Jul 95) pp 17–19*

The author discusses some of the new problems presented to insurers by burglar alarms whose software can be altered remotely. They can let alarm companies offer new products and features, but create a large number of new control problems.

051153 'Anforderung des Datenschutzes an den "intelligenten Straßenverkehr" '
T Weichert, *Datenschutz und Datensicherung v 20 no 2 (Feb 96) pp 77–82*

The author discusses the data protection problems raised by the next generation of highway traffic management systems. These are wide ranging: many proposed innovations — from the integration of GPS through smartcard driving licences, road toll systems and vehicle alarms through video monitoring of traffic — can reveal or accumulate personal information in ways that could cause legal problems.

051154 'Problems with DCE Security Services'
G White, U Pooch, *Computer Communication Review v 25 no 5 (Oct 95) pp 5–12*

The authors describe DCE security services; these are based on Kerberos, but are criticised on a number of grounds. These include lack of delegation, poor resilience, and scalability problems. For example, the University of Michigan tried to add 50,000 users and crashed the system. The audit facilities are also defective and there is poor support for one-time passwords.

051155 'Secure External References in Multimedia Email Messages'
B Wiegel, *ACM 96 pp 11–18*

Along with multimedia messaging, systems like MIME allow external body parts. These are implemented in BERKOM by a global message store, which introduces new attack points. Existing systems like PGP, PEM, MOSS, and S/MIME do not protect such a global store, so the authors of this paper extended MOSS to protect the external references and referenced objects.

051156 'Secure Coprocessors in Electronic Commerce Applications'
B Yee, JD Tygar, *EC 95 pp 155-170*

The authors describe an electronic commerce system based on the model of a secure hand-held computer. They discuss the architecture of their system, and implement a variety of electronic commerce applications on it, including software copy protection, electronic cash, electronic contracts, and secure postage.

051157 'Experiences with implementing messaging security in MSMail 3.2'
JE Zmuda, R Housley, *NISSC 95 pp 281–290*

The authors added Fortezza-based security to MS Mail; as an adjunct to the address book, they added an 'autograph book' for certificates and used an NSA web page for CRLs. MSP was chosen over PEM for its signed receipt capability. Certificates are user distributed; two users establish trust by exchanging signed messages with their certificates.

2 Operating System and Database Security

051201 'Concurrency control in a secure multilevel database via a two-snapshot algorithm'
P Ammann, F Jaeckle, SD Jajodia, *Journal of Computer Security v 3 no 2–3 (94–95) pp 87–113*

The related database security problems of correctness, starvation and indirect channels are tackled simultaneously without needing a large amount of trusted code using a two-snapshot algorithm: current and previous snapshots of the database are kept for each security level, and the previous version swapped for the next. With more than four security levels, this requires less storage than replicated architectures. Advantages are that untrusted schedulers can be used with only minor modifications, and that execution histories are one-copy serialisable: the delays introduced are equivalent to the high processes' executing earlier.

051202 'A Domain and Type Enforcement UNIX Prototype'
L Badger, GF Sterne, DL Sherman, KM Walker, *Usenix Computing Systems v 9 no 1 (Winter 96) pp 47–83*

Domain and Type Enforcement can be used to constrain the damage done by ill-behaved applications as well as to implement a least privilege mechanism. This paper describes an implementation for UNIX. Its specification language defines rules for subjects, objects, and their interactions. The prototype implementation also supports remote file access in NFS. Hosts with different security policies can be connected by defining them to have a single domain and type. This policy model is claimed to be a superset of lattice-based models such as Bell-LaPadula and Biba.

051203 'A Non-Timestamped Authorization Model for Data Management Systems'
E Bertino, S Jajodia, P Samarati, *ACM 96 pp 169–178*

Cascading discretionary GRANT and REVOKE operations without timestamps requires new semantics, since the order of previous events cannot be determined. Negative authorisations also require policies for conflict resolution — for example, that denials take precedence; second order effects include dealing with authorisations granted by a subject who later receives a negative authorisation.

'051204 An extended authorization model for object databases'
E Bertino, F Origgi, P Samarati, *Journal of Computer Security v 3 no 2–3 (94–95) pp 169–205*

The authors extend their model of object oriented database security to include both explicit and implicit authorisation, negative authorisation and user groups.

051205 'Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions'
M Chang, N Puketza, RA Olsson, B Mukherjee, *NISSC 95 pp 173–183*

The authors tried to fool an intrusion detection system by distributing attack activity over a number of parallel sessions. This strategy works for some kinds of intrusion but not others.

051206 'Providing accurate data labels to the analyst — the secure C^4I workstation'
I Dampier, C Corbett, *NISSC 95 pp 205–210*

The main benefit of multilevel workstations in the intelligence analysis business is expected to be relief of the downgrading bottleneck that characterises the existing system-high installations. Accurate labelling at a paragraph level of granularity could avoid a lot of overclassification.

051207 'Matching Security Policies to Application Needs'
C Eckert, *IFIP 95 pp 237–254*

The author introduces an information flow logic with special support for data integrity. It is based on an action model and can express Bell-LaPadula, Clark-Wilson and the Chinese Wall security policies. In essence it allows the expression of a wide range of possible security requirements and thus provides a uniform specification framework; it enables high level languages to be extended to support various security policies and is being prototyped as an extension of Mach 3.0.

051208 'An Unusual B3-Compliant Discretionary Access Control Policy'
J Epstien, G Grossman, A Donaldson, *NISSC 95 pp 113–122*

ASSURE EC has an access control policy based on pattern matching against a central database of pathnames. These have some of the attributes of capabilities, and some of ACLs: yet they can meet C2+/B3 criteria and thus be integrated with B3/A1 systems.

051209 'SAGE: Approach to Rapid Development of Trusted Guard Applications'
K Goertzel, *NISSC 95 pp 271–280*

Wang has developed a system for trusted guard applications. Based on their B3 STOP operating system, it has various clients that can be programmed to manage individual transactions and servers to filter for addresses, dirty words and so on.

051210 'Several Secure Store and Forward Devices'
DM Goldschlag, *ACM 96 pp 129–137*

A data pump eliminates timing channels by buffering and adding delays that mimic historical response time distributions. Since the entire pump must be trusted, this approach isolates the trusted components physically and logically. The upwards channel is a one-way optical fiber. For high to low acknowledgments, fixed time intervals and flow control provide a minimum delay and smoothing function.

051211 'Computational Issues in Secure Interoperation'
L Gong, XL Qian, *IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 43–52*

In this journal version of **032206**, the authors propose two new principles for system composition. These are autonomy (legal local accesses stay legal) and security (forbidden local access stay so too). They then ask how many cross-domain links can be added without breaking either condition. The main problem is in avoiding loops, and the answer in in general undecidable. Even with simple ACLs it is NP-complete (by reduction to feedback arc set). However, there is a solution if access structures are totally ordered, and interoperation can be imposed on any structure with an acyclic graph.

051212 'Great Unsolved Problems in Applied Computer Security'
MG Graff, *NISSC 95 pp 63–72*

FIRST proposes four problems, with a $1,000 prize for a solution to any of them (which may include a proof that a solution is impossible). They are to design a program that will detect compromise of system files (including itself); to design a fast way to write log files to disk such that subsequent modification can be detected; to develop a way to compare the security of two similar systems; and to explain who is helped or harmed by the publication of details of security flaws.

051213 'Ain't Misbehaving — a Taxonomy of Anti-intrusion Techniques'
LR Halme, RK Bauer, *NISSC 95 pp 163–172*

Intrusion detection techniques can be used for prevention, pre-emption, deflection, deterrence, detection and countering, but detection is perhaps the most interesting. Techniques include threshold monitoring; user, group and resource work profiling (which can be static, adaptive, rule based or whatever); systems that look for specific abuses; and hybrid systems that combine analysis of 'normal' and abnormal event patterns.

051214 'Integrating COTS applications on compartmented mode workstations'

SA Heath, *NISSC 95 pp 221–227*

The problems of running commercial software on a multilevel workstation include dealing with the X default colormap, shell escapes, sendmail and multilevel directories.

051215 'Information Domains Metapolicy'

G Hilburn, *NISSC 95 pp 27–36*

The author models and analyses the metapolicy underlying the US DoD Goal Security Architecture (DGSA). This is based on 'information domains', which this article attempts to formalise. Objects may move between domains only if they have a common subject who may export them from one domain and import them to the other: this can express lattice models. The DoD interpretation restricts flows to systems enforcing common policies; the authors conclude that a standard encoding scheme will be needed for domains and policies before 'plug-in' security becomes a reality.

051216 'A Fast Algorithm for Detecting Second Paths in Database Inference Analysis'

TH Hinke, HS Delugach, A Chandrasekhar, *Journal of Computer Security v 3 no 2–3 (94–95) pp 147–168*

The second-path inference problem arises when a low user can infer higher classified data from low data using joins. It used to be tackled by looking for paths explicitly, but techniques developed to test relational decompositions for a lossless join property do a much better job — especially when combined with filtering to lessen the security significance of any discovered leaks.

051217 'Genser Message Multi-level Secure (MLS) Classification and Categories'

ML Hoffert, J Griffith, *NISSC 95 pp 123–135*

The authors propose a labelling scheme for multi-level general service messages for NATO. The various US and Allied classification schemes are discussed.

051218 'A Context Authentication Service for Role Based Access Control in Distributed Systems — CARDS'

R Holbein, S Teufel, *IFIP 95 pp 270–285*

The authors discuss how the 'need-to-know' principle might be formalised and enforced by making access control decisions context dependent. The suggested mechanism is a 'context notary' that will be activated when certain objects are accessed, and which will be integrated with a distributed authentication service. These mechanisms might be used to tie access control with billing, so that employees would only be able to access data on clients or projects to which they were currently billing their time.

051219 'Maintaining Secrecy and Integrity in Multilevel Databases: A Practical Approach'

S Jajodia, D Marks, E Bertino, *NISSC 95 pp 37–49*

The authors discuss how to design databases so that their integrity checks do not require access to data of higher classification. This is discussed in the context of a system that must see to it that no employee is ever paid more than any manager, where managers' salaries are secret: the idea is to keep bounds at each level and modify them occasionally as required.

051220 'Transaction management for multilevel secure replicated databases'
IE Kang, TF Keefe, *Journal of Computer Security v 3 no 2–3 (94–95) pp 115–145*

Some label orderings in multilevel databases cause problems for consistency. The authors identify 'multilevel-acyclic' partial orders as sufficient to ensure a serialisable global order in the absence of further controls. Where the label lattice is cyclic, they propose using timestamps to serialise data.

051221 'Enforcement of Complex Security Policies with BEAC'
IL Kao, R Chow, *NISSC 95 pp 1–10*

The authors' Boolean expression based access control model (BEAC) is designed to express both multilevel security and dual control. Each object may have a number of labels, and subjects have capabilities that are Boolean expressions of labels: access is granted if the expression evaluates as true. This can express security policies outside the scope of Bell-LaPadula, such as 'only a user may read his electronic mail, but once he has read a message he may forward it to any other user'. State can be bound to objects by letting subjects change labels in defined ways.

051222 'On Paradigms for Security Policies in Multipolicy Environments'
WE Kühnhauser, *IFIP 95 pp 425–435*

The author discusses two alternatives that have been proposed to the reference monitor concept; both have to do with application level security that retains state (as in, for example, dual control). The advanced access control programs of Theimer and others let the state float from the subject to the object with each transaction, while the custodians proposed by the author and others have state at both subjects and objects. The complexity of a general multipolicy framework is further emphasised by discussing possible conflicts when a subject from a Chinese Wall policy domain tries to access an object in an MLS system.

051223 'A Software Architecture to Support Misuse Intrusion Detection'
S Kumar, EH Spafford, *NISSC 95 pp 194–204*

The authors present a model based on coloured Petri nets to specify patterns for intrusion detection. Experiments were done using vulnerability data from COPS¡ CERT and other sources. A server obtains events and dispatches them to clients that do specific checks.

051224 'A Framework for Access Control Models'
B Lau, *IFIP 95 pp 514–533*

The author develops Abrams' general framework for access control in which the access decision facility is an abstract machine that advises the reference monitor and whose input is a set of authorisation objects that describe permitted or forbidden acts.

051225 'Yes, Java's Secure. Here's Why'
L Lemay, C Perkins, *Datamation (1/3/96) pp 47–50*

The authors make the case for Java's security. The language is strongly typed with no pointers, and runtime code contains redundant type information. This is safety checked (with a level of care that can be varied depending on whether the code came from inside or outside); checks ensure no under- or overflows, no types incorrectly used, and no illegal conversions. Finally, applets are protected from each other by the use of different namespaces.

051226 'A Safe Tcl Toolkit for Electronic Meeting Places'
JY Levy, JK Ousterhout, *EC 95 pp 133-135*

Safe Tcl allows the controlled execution of untrusted scripts; the authors have extended it to support multiple scripts that are protected from each other. The idea is to provide a safe place for automated commerce, in which users' applets can interact without being able to penetrate each other.

051227 ‘A General Theory of Composition for a Class of “Possibilistic Properties” ’

J McLean, *IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 53–67*

This journal version of **032421** generalises McCullough’s work on hook-up security by showing that possibilistic information flow constructs are closures with respect to various selective interleaving functions. It studies which composition constructs preserve this closure: product and cascading are generally unobjectionable but feedback, internal composition and refinement are not. These are illustrated by a Trojan horse construction.

051228 ‘Addressing Infosec Analysis Problems Using Rule-based Technology’

RB Neely, JW Freeman, *NISSC 95 pp 73–82*

The authors examine how a security analyst partitions a problem, navigates the components of a system and verifies them. They discuss a number of products that provide some support by allowing rule-based analysis, and report experience with one of these (‘Virtual Software Factory’).

051229 ‘Project Winmill: Using a COTS Solution to Connect LANS of Different Compartments’

A Nessell, C Sawyer, *NISSC 95 pp 228–235*

The authors describe a multilevel LAN project at the US Defence Intelligence Agency that uses Trusted Solaris and a Sun version of DNSIX. The idea is to mediate email communications between Top Secret LANs, on one of which the users have access to one extra compartment.

051230 ‘Merging models: integrity, dynamic separation of duty, and trusted data management’

LA Notargiacomo, BT Blaustein, CD McCollum, *Journal of Computer Security v 3 no 2–3 (94–95) pp 207–230*

The author explore the relationship between the integrity of databases and the Clark-Wilson model; they develop a synamic separation of duty policy that can be interpreted in database management terms.

051231 ‘An Advanced Commit Protocol for MLS Distributed Database Systems’

I Ray, E Bertino, S Jajodia, L Mancini, *ACM 96 pp 119–128*

The Early Prepare commit strategy used in many commercial systems does not extend to multilevel security because of the way read locks are retained during the period of uncertainty. Secure Early Prepare resolves this by aborting transactions. This work provides a more flexible programming interface, so that transactions can proceed. The programmer can control the tradeoff between consistency and atomicity.

051232 ‘Role-based Access Control Models’

RS Sandhu, EJ Coyne, HL Feinstein, CE Youman, *Computer v 29 no 2 (Feb 96) pp 38–48*

This article reviews role based access control for a nonspecialised audience. Users can establish sessions that activate any combination of roles dominated by roles they possess; role hierarchies and constraints can be used to implement mandatory access controls.

051233 ‘TOP: A Practical Trusted ODBMS’

M Schaefer, VA Lyons, PA Martel, A Kanawati, *NISSC 95 pp 50–62*

The Trusted ONTOS prototype is an MLS object store targeted at B1 support for c++ applications. It is illustrated by a hypothetical scenario in which a drug company wishes to keep side effects of its drugs secret.

051234 'Rating Network Components'
G Serrao, *NISSC 95 pp 344–355*

This article describes the DoD Trusted Network Interpretation and discusses how to deal with components that support only part of a security policy.

051235 'Controlling network communication with domain and type enforcement'
DL Sherman, DF Sterne, L Badger, SL Murphy, KM Walker, SA Haghighat, *NISSC 95 pp 211–220*
The authors describe an implementation of their domain and type enforcement policy (see **043203**) in a Unix environment and discuss how they deal with both datagrams and streams. The emphasis is on making security checking one-off by using constrained streams.

051236 'Experience in Application of Composable Security Policies'
Q Shi, N Zhang, *IFIP 95 pp 223–236*

The authors present a heuristic approach to composable security; properties are described as 'independent', 'dependent' or 'strongly dependent'.

051237 'On Guards ... En Garde'
LM Sudduth, *NISSC 95 pp 236–248*

The author discusses the design of mail guards. These prevent both low-side penetration and high-side leakage, which are actually rather different functions and need different kinds of mechanism to do well. The former depends on the strength of basic mechanisms, while the latter depends on whether an MLS system has been used to generate 'reliable' labels, on whether the content includes objects such as Word documents that may contain deleted or even covert matter, and the extent to which automated text analysis can be used.

051238 'The Controlled Application Set Paradigm for Trusted Systems'
DF Sterne, GS Benson, *NISSC 95 pp 11–26*

The authors argue that the TCB should act as the base for protection in a trusted system rather than its totality, and that some of the trust should be moved to a set of applications that have been screened and are presumed to be benign. In their model, the TCB provides a trusted path, and protects the controlled applications from tampering and bypass: the purpose of screening them is to prevent their exploiting covert channels. The trust principle is that any application that processes sensitive data probably has the power to do harm.

051239 'Classification of Subjects and Objects in a Trusted Extensible Client Server Architecture'
TC Vickers Benzel, EJ Sebes, H Tajalli, *NISSC 95 pp 83–99*

This paper presents an overview of Trusted Mach: how subjects and objects are constrained using microkernel mechanisms, and the mechanisms for extensibility that allow the creation of groups of communicating processes with a common security object. The component that mediates access is itself a task run by the microkernel.

051240 'Cooperating Security Managers: A Peer-Based Intrusion Detection System'
GB White, EA Fisch, UW Pooch, *IEEE Network, Jan/Feb 96 v 10 no 1 pp 6-14*

CSM is a distributed intrusion detection system where each host has an intrusion detection module to recognize local intrusions and a security manager module to coordinate with other network hosts. This architecture allows detection of network intrusion attempts such as trying one password on each of a thousand systems, that would be unnoticed by purely local protection mechanisms. A prototype has been built on Sun Solaris 2.3; it detected intrusions fed to it through "intrusion scripts".

051241 'Windows NT Server — an update'

P Wood, *Information Security Monitor v 11 no 3 (Feb 96) pp 5–8*

The author describes the security features of Windows NT Server. Servers are organised in domains, between which trust relationships such as hierarchies can be built. Access permissions can be managed by local groups, with certain classes of operator having special privileges (e.g., direct logon at a server). It provides a trusted path in that users must reboot their machines to log on.

051242 'Distributed Object Systems Security'

V Varadharajan, *IFIP 95 pp 305–321*

The author discusses how security services can be provided in a distributed object oriented model and how primitives such as delegation may be robustly supported. Scalability and the trust dependencies between different mechanisms are also explored.

3 Security Management and Policy

051301 'Italian diplomatic cryptanalysis in world war 1'
D Alvarez, *Cryptologia v XX no 1 (Jan 96) pp 1–13*

During world war 1, the Italian signals intelligence establishment started off with a single officer, who was unaware of even published results. By 1916, the unit obtained its first results (against the Vatican) and finally started to read Austrian traffic in September 1917. It spent at least as much effort on allied and neutral traffic as it did on enemies.

051302 'Analysis requirements for low assurance evaluations'
JL Arnold, *NISSC 95 pp 356–365*

The US DoD proposes to reduce the amount of analysis required for C2 and B1 evaluations, which are respectively for 'a cooperative environment where the product is expected to protect against accidents' and 'a minimally hostile environment where the product is expected to protect against at least casual attacks'. Both often refer to older products developed using 'penetrate and patch' methodologies, where the point of diminishing returns is quickly reached. A number of ambiguities and obscurities in TCSEC had tended to lead to over-evaluation, and these are clarified in this paper.

051303 'Managing computer crime: a research outlook'
J Backhouse, G Dhillon, *Computers and Security v 14 no 7 (95) pp 645–651*

The authors discuss some current criminological theories of white collar crime: greed, culture and so on. They argue from this that better corporate management is at least as important in reducing risk as tougher computer crime laws.

051304 'Watching the Bhang Meter and Flying through Dirt'
T Beth, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 17–26*

The writer reviews work by Gus Simmons on topics peripheral to cryptology, including ring theory and physics. The latter included the design of the Mars penetrator lander, and research on atmospheric physics for the Ferret satellite programme — which were published as a study of the reception on earth of radio signals from space rather than vice versa.

051305 'A Standard Audit Trail Format'
M Bishop, *NISSC 95 pp 136–145*

This article proposes a standard format for system logs and audit trails. He discusses the pros and cons of the standard Sun, VAX, OSF, RACF and CA-Unicenter offerings.

051306 'Kryptokontroverse — Der Schutz der Vertraulichkeit in der Telekommunikation'
J Bizer, *Datenschutz und Datensicherung v 20 no 1 (Jan 96) pp 5–14*

The author analyses German law on the individual's right to privacy versus the state's right to intercept communications. At present there is no duty on individuals to hand over keys, and it is argued that such a duty would be unconstitutional — as would a prohibition on the use of cryptography.

051307 'Information Systems Security and the Multinational Enterprise'
C Blatchford, *Computer Audit Update part 1: Feb 96 pp 18–26; part 2: Mar 96 pp 18–26*

The globalisation of business creates pressure for the free flow of business information, which may be at odds with the interest of nation states. The information control needs are also potentially in conflict.

051308 'A Methodology for the development of secure application systems'
HAS Booysen, JHP Eloff, *IFIP 95 pp 255–269*

The authors discuss how security requirements engineering can be integrated into the spiral model of software development. The main idea is progressive refinement of an information flow model expressed as a matrix.

051309 'A Perspective of evaluation in the UK versus the US'
A Borrett, *NISSC 95 pp 322–334*

The author contrasts the UK and US approaches to trusted product evaluation. In Britain, much more of the analysis and testing is done by the developer, and the evaluator's role is to audit it. Covert channels and hardware testing are considered to be much more important in the USA, while the UK emphasises source code analysis and the quality of the development process. The British emphasis on the repeatability of evaluations is necessitated by the rule that the sponsor pays, which introduces commercial pressure to cut corners.

051310 'EU-Datenschutzrichlinie — Umsetzung in einem vernetzten Europa'
U Brühmann, *Datenschutz und Datensicherung v 20 no 2 (Feb 96) pp 66–72*

A senior EU official gives his position of the recent EU data protection directive, including its political goals and its effect on cooperation with central and eastern Europe. In his view, it is part of a civilising mission.

051311 'Security Management in a Distributed Open Environment'
M Calitz, R von Solms, SH von Solms, *IFIP 95 pp 396–406*

The authors discuss the problems of managing security in distributed systems and talk about a possible solution using role profiles.

051312 'Portrait of the Computer Criminal'
JM Carroll, *IFIP 95 pp 577–589*

The author discusses the evolution of computer crime, especially on US campuses. During the 1960's and 70's, computers were vandalised in protest activity; nowadays, they are more likely to be stolen. Time-sharing and network services spurred 'hackers'.

051313 'Viruses, Corruption, Denial, Disruption, and Information Assurance'
FB Cohen, *IFIP 95 pp 495–509*

The author presents a historical overview of threats to computer systems, in the context that most system reliability measures are designed to prevent random faults rather than malicious attack. This theme is developed with reference to viruses and other malicious code. He advocates the use of mandatory rather than discretionary access controls in commercial systems and argues that this is can be cheap to do in simple ways.

051314 'International Legal Protection for Software'
Computer Law and Security Report v 12 no 1 (Jan/Feb 96) pp 2–14

This is the latest in a series of annual surveys of the countries in which software is protected by copyright, patent or both. It covers 72 countries.

051315 'The EPS CD and CD-ROM Security Conference 1995'
Computer Law and Security Report v 12 no 1 (Jan/Feb 96) pp 28–36

This article presents summaries of a number of presentations at a conference on the security of software and other intellectual property distributed by CD-ROM. It covers the pros and cons of distributing software in encrypted form, the use of holographic identifiers and digital fingerprinting of images.

051316 'Disaster Recovery Planning Case Study: The South African 1994 Election'
W Cooke, *NISSC 95 pp 300-307*

The author describes how he developed the disaster recovery plan for the 1994 elections in South Africa.

051317 'Criminal procedural law and information technology — the main features of the Council of Europe Recommendation No. R (95) 13'
P Csonka, *Computer Law and Security Report v 12 no 1 (Jan/Feb 96) pp 37–42*

The EU is seeking to harmonise member states' provisions for search and seizure in computer systems and the interception of communications, on the pretext of tackling cross-border computer crime. A directive has been issued which also covers compelling cooperation from technical personnel, the admissibility and reliability of evidence, encryption (which should not create 'insurmountable obstacles for the investigating authorities') and international cooperation generally.

051318 'Functional security criteria for distributed systems'
J Cugini, R Dobry, V Gligor, T Mayfield, *NISSC 95 pp 310–321*

The authors summarise work on functional security criteria for distributed systems that they have submitted for incorporation in the common criteria. Their definition of a secure distributed system is a set of trusted hosts or realms, connected by trusted communications channels, and subject to consistent security policies. They discuss how cryptography should be integrated.

051319 'A New View of Intellectual Property and Software'
R Davis, P Samuelson, M Kapor, J Reichmann, *Communications of the ACM v 39 no 3 (Mar 96) pp 21–30*

The authors argue that patent, copyright and trade secret laws are now appropriate for software, and propose a new model. Copyright does not fit, as the value of software lies in its useful behaviour rather than its presentation; neither do patents, as most software is innovative rather than inventive; and it carries its know-how on its face, so trade secret protection should not work. The authors, inspired by the US Semiconductor Protection Act, propose a new format for registering innovation that would give protection against even workalike clones, but for 2–5 years rather than the 17 years of patent and 75 years of copyright. They also propose simpler rules on liability.

051320 'A methodology for the design of security plans'
WF de Koning, *Computers and Security v 14 no 7 (95) pp 633–643*

Dutch municipalities are required by law to have information security plans, because they issue passports and driving licences and because of privacy concerns. This article describes their association's security manual, which gives guidelines on risk analysis and security project planning. The author also describes a $4m fraud perpetrated by a system designer in Rotterdam.

051321 'Trusted third parties when a public body is involved in EDI relationships either as a partner, or an an observer of commercial transactions'
A de la Presle, *EDITT 95 pp 211–214*

This article states the French government's working position on EDI and trust. EDI relationships are not greatly different from traditional ones, and the state is often involved as an observer for the purposes of raising taxes, handing out grants. A number of state bodies already perform trusted third party services in the world of paper, as do a number of bodies authorised by the state (such as notaries, banks and accountants). There will be budgetary limits on the number of dematerialisation techniques that they are able to support. Aspects for debate are presented: for example, as many official declarations need to be accompanied by payment, will the banks become more influential?

051322 'Special Report: Intellectual Property Rights and Smart Card Patents: The Past —The Present — The Future'
J Dethloff, *Smart Card News (Feb 96) pp 36–38*

One of the smartcard pioneers, who patented an IC identification device in 1968, surveys the subsequent patents by Arimura in 1970 (the chipcard), Otto in 1970, Moreno in 1975 (in-card PIN validation), and Ugon in 1978 (microprocessor in card).

051323 'The National Security Establishment and the Development of Public-Key Cryptography'
W Diffie, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 9–12*

This article consists of a short biography of Gus Simmons as an introduction to a special journal issue celebrating his festcolloquium at Fairfax 93.

051324 'Can the Conventional Models Apply? The Microelectronics of the Information Revolution'
B Don, D Frelinger, *EC 95 pp 23-31*

The authors argue that the macroeconomic paradigms that control information-based commerce are different from those that control other types of commerce. They outline the differences and suggest further areas of research, noting the effects of these differences on public policy.

051325 'There are Some Cracks in the Cornerstone of Information Security'
RJ Duncan, *Computers and Security v 14 no 8 (95) pp 675–680*

During 1991–5, Datapro conducted an annual security issues survey: incidents, concerns, level of planning and what had been implemented. The results of these surveys are tabulated here.

051326 'Handling Imprecise Information in Risk Management'
L Ekenberg, M Danielson, *IFIP 95 pp 357–368*

The authors discuss the granularity that it is useful to have when doing a risk analysis, and present a method for dealing with imprecise probabilities of outcomes.

051327 'A cost model for managing information security hazards'
L Ekenberg, S Oberoi, I Orci, *Computers and Security v 14 no 7 (95) pp 707–717*

The authors provide a model of risk analysis that takes into account the vagueness of the risk being assessed and the ways in which risks interact.

051328 'And Now for Something Completely Different (The Egyptologist and the Cryptographer: A Personal Reminiscence'
M Fischer, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 13–15*

This article provides personal reminiscences of Gus Simmons delivered on the occasion of his festcolloquium.

051329 'Position and liabilities of trusted third parties'
H Franken, *EDITT 95 pp 199–203*

The author points out that it will be extremely difficult to insulate trusted third party services against class actions brought by consumer groups.

051330 'Handelsblatt-Enquête 95/96 — Sicherheit in der Informationstechnik'
H Gliss, *Datenschutzberater v 20 no 3 (15/3/96) pp 1–8*

This article reports on a large survey carried out of the computer usage and loss experience of organisations in Germany, as well as their security policies and measures.

051331 'Internet 101'
S Gordon, *Computers and Security v 14 no 7 (95) pp 594–604*

The author talks about a number of security problems with Unix including .rhosts, .netrc, .xhosts and Trojans in various binaries.

051332 'A classification of health information systems security flaws'
D Gritzalis, I Kantzavelou, S Katsikas, A Patel, *IFIP 95 pp 453–464*

The authors present a classification of 180 security flaws reported in the UK National Health Service from 1988-1990, applying Landwehr's taxonomy (**031221**).

051333 'Comprehensive Information Technology Security: A New Approach to Respond Ethical and Social Issues Surrounding Information Security in the 21st Century'
A Hartmann, *IFIP 95 pp 590–602*

The author describes the BSI's technology assessment programme — the first ever by a government signals agency to look systematically at the social and ethical aspects of information security using a multidisciplinary team of scientists, lawyers, officials, businessmen, unionists and social scientists. An example of their output was the report on chip cards in medicine (*book review, volume 4 number 4*). They recommend participative design of systems with full input from ethical bodies at every stage.

051334 'ECMA's Approach for IT Security Evaluations'
A Herrigel, R French, H Tabuchi, *NISSC 95 pp 335–343*

The authors discuss ECMA's proposed Commercial Oriented Functionality Class (COFC — see **031210**), which competes with ITSEC as a framework for low level commercial system evaluation.

051335 'Achieving an Integrated Design: The Way Forward for Information Security'
J Hitchings, *IFIP 95 pp 369–383*

The author presents a system design methodology based on 'soft systems' that emphasises the human factor and seeks to incorporate a model of the organisation when building an information system. The idea is to include the organisation's context — competitors, clients and others — in a systematic way.

051336 'Staatliche Regulierung in der Diskussion'
M Huhn, A Pfitzmann, *Datenschutzberater v 20 no 1 (15/1/96) pp 1–5*

The authors point out a number of technical problems with proposed controls on the commercial use of cryptography. The abuse of escrowed systems (for example, by using them to conceal messages protected under a different cipher system) could only be controlled if escrowed material were frequently inspected.

051337 'Technische Randbedingungen jeder Kryptoregulierung'
M Huhn, A Pfitzmann, *Datenschutz und Datensicherung v 20 no 1 (Jan 96) pp 23 –26*

A ban on cryptography would be difficult for a number of technical reasons. Any infrastructure for certifying signature keys could be used to bootstrap a system for confidentiality; compulsory key-escrow systems can be used to bootstrap non-escrowed systems; ciphertext can be hidden using steganographic techniques; and there is no usable distinction between the protection of stored and transmitted data. For all these reasons, regulators will not be able to ban 'bad' uses of cryptography without hindering 'good' uses too.

051338 'Data Protection in Communications and Storage'
P Kaijser, *IFIP 95 pp 340–354*

The author reviews the kinds of security services that can be applied effectively in storage, communications and other components of a computer system.

051339 'Results from TEDIS EDIPAY: The role and future of TTPs in payment systems'
AMC Kemna, H Roos, *EDITT 95 pp 37–51*

The authors studied the organisational and legal aspects of using trusted third party services in payment systems. Secure time is important for attachment and bankruptcy proceedings; uniqueness is important for negotiable instruments; and some impartial source of trust will be helpful in moving from closed to open environments. Regulation issues need to be addressed: for example, if a trusted third party becomes critical for payment processing, it may end up being regulated as if it were a bank. Examples of banking industry third party services are discussed.

051340 'Measuring correctness and effectiveness: a new approach using process evaluation'
K Keus, KW Schröder, *NISSC 95 pp 366–373*

The authors compare product oriented evaluations such as TCSEC with process oriented ones such as ITSEC. Process control can assure the quality of hardware but software development is a poorly defined problem: one can follow the 'right' steps but end up with the wrong result.

051341 'IT Security — Implementing "best practice" '
R Kisin, *Computer Audit Update (Jan 96) pp 9–21*

The author discusses how an organisation should go about complying with the British Standards Institution's code of practice for information security management.

051342 'From Social Requirements to Technical Solutions: Bridging the Gap with User-Oriented Data Security'
U Kohl, *IFIP 95 pp 612–623*

The author describes a project to let users specify and communicate their security expectations; it was driven by a feeling that current mechanisms do not meet the 'informational self-determination' guaranteed under German law. The prototypes include a hospital application where the originators of objects such as digital X-ray images own them, but can delegate or give away their ownership rights (such as when a radiologist sends a picture together with an opinion to the treating physician).

051343 'A Day in the Life of a Swedish IT Security Officer: An Attempt at an Empirical Study'
S Kowalski, *IFIP 95 pp 384–395*

This paper reports an attempt to collect information about IT security people in Sweden. Ten of them were interviewed; they tended to see their job as more social than technical, intuitive rather than logical, and with many rather than few exceptions needing dealt with. All earned in the top 20 percentile of male earnings.

051344 'The Failure of Anti-Hacking Legislation: a Hong Kong Perspective'
RWH Lau, KY Lam, SL Cheung, *ACM 96 pp 62–67*

The authors explain the history and status of "anti-hacking" legislation in Hong Kong. Prosecutions showed that laws were either too lenient or too difficult too apply. The government passed the Computer Crime Law in 1993, but it did not address issues of intangible property. Hong Kong now has 100,000 Internet users, and the government is now starting to look at Internet use. ISPs were raided by the police for having objectionable content, and now need a license.

051345 'A New Model for Information Security Policies'
KR Lindup, *Computers and Security v 14 no 7 (95) pp 691–695*

The various types of security policy are discussed — system, product, corporate and community. It is suggested that we also need an analogue of the international treaty, which might be negotiated between different companies or different divisions of the same company.

051346 'Securing Access and Privacy on the Internet'
W Madsen, *Computer Fraud and Security Bulletin (Jan 96) pp 9–18*

The author discusses the effect that the Internet has had on repressive regimes including those of Burma, Tibet, China, Cuba, Peru and elsewhere. PGP has been used by liberation groups on a number of these countries to frustrate government surveillance.

051347 'Can computers and epidemiology get along? Health problems in computers'

GM Mallén-Fullerton, F Vargas-Vorackova, E Daltabuit-Godas, *NISSC 95 pp 291–299*

The authors describe a project to measure the incidence of PC viruses at two Mexican universities.

051348 'Reengineering the Certification and Accreditation Process: Security is Free'

SG Mahon, *NISSC 95 pp 374–383*

The common view of system security is of a necessary evil, dictated by policy, that gets in the way of business — just like the view of quality taken in Detroit in the 1970's. Just as quality pays for itself, so should security engineering. Ways to achieve this in the US Army and Air Force are suggested.

051349 'Organisation of Electronic Business in Shell Companies'

NP Mansfield, *EDITT 95 pp 171–184*

The author describes Shell's goals and policies for the introduction of email and EDI worldwide. The legal and evidential aspects are uppermost in this; next follow corporate identity, minimising lost mail, and other security aspects such as confidentiality.

051350 'EDI trusted third parties workshop'

DJ Marsh, *EDITT 95 pp 87–90*

The author analyses the legal requirements for a trusted third party service to operate in the United Kingdom. Such parties already exist — the Land Registry was set up in 1925, and its law and procedures may provide some guidance. The limitation of liability is important. The Land Registry's is limited by statute to the value of the land affected; and a commercial registry that wished to obtain insurance at economic rates would be advised to limit the functionality of its service.

051351 'Technology and Private Security: What does the Future Hold?

RH Moore, *Journal of Security Administration v 18 no 2 (Dec 95) pp 1–9*

The author surveys the technology of corporate protection, and picks out as particularly important the use of neural networks to filter false alarms from perimeter sensors. He also speculates about microbot wasps that will be able to sting an intruder for a DNA sample and then hold him pending arrest.

051352 'The Quiet Jemmy'

N Morris-Cotterill, *Computer Fraud and Security Bulletin (Mar 95) pp 11–14*

One of the main causes of security failure in industry is a failure to check references of both employees and contract staff. Staff with criminal records may be engaged, and real engineers may be impersonated by villains.

051353 'Firewalls —Schutz vor Angriffen aus dem Internet'

M Munzert, C Wolff, *Datenschutz und Datensicherung v 20 no 2 (Feb 96) pp 89–93*

The authors provide a management level overview of Internet threats and the benefits conferred by firewalls.

051354 'Executive Training Needs: A National Survey of Security Professionals'

MK Nalla, KE Christian, MA Morash, PH Schram, *Journal of Security Administration v 18 no 2 (Dec 95) pp 18–25*

A survey of 1490 US security managers revealed that about half were interested in courses on specific computer and technical skills as well as organisational aspects. However, the need for technical training was more pronounced in low-tech sectors whose security staff tended to come from a police background, than in sectors such as banking and government with established computer security communities.

051355 'Hiring Preferences of Security Professionals: A National Survey'
MK Nalla, KE Christian, MA Morash, PH Schram, *Journal of Security Administration v 18 no 2 (Dec 95) pp 29–38*

Two thirds of US security managers surveyed considered that there was a high demand for staff with university training in criminal justice, while under a third sought computer security skills.

051356 'Ethical information security in a cross-cultural environment'
KL Nance, M Strohmaier, *IFIP 95 pp 603–611*

The authors plead for information security developers to be sensitive to cross cultural issues: communication across racial boundaries is hindered by differing assumptions about nonverbal communication, intimacy, facework, respect and perception. They call for research into the effects this has on security.

051357 'Bulletin Boards and the US Secret Service'
J Osen, *Computer Fraud and Security Bulletin (Dec 95) pp 13–18*

Steve Jackson's publishing firm was raided by the US Secret Service, and computer equipment confiscated, when agents mistook bulletin board files for a fantasy game for subversive material. By seizing a publisher's computer systems they violated the US Privacy Protection Act; Jackson sued them and won.

051358 'Sex, Crimes and the Internet: the Jake Baker Case'
J Osen, *Network Security (Feb 96) pp 15–22*

A US student who posted to the Internet a rape-murder short story in which one of his classmates figured as a victim was prosecuted for threatening to injure. The case was eventually thrown out on the grounds that the story was just a savage and tasteless piece of fiction. The legal background to this decision is discussed in detail.

051359 'Fast — First Attempt to Secure Trade'
M Peereman, *EDITT 95 pp 91–99*

The author discusses how the international network of chambers of commerce will handle electronic registration and certification of member companies. This will include key management, time stamping and directory services and should be independent of government agencies, PTTs and equipment vendors.

051360 'Trends in security evaluations'
J Pieters, *Smart Card News (Jan 96) pp 16–18*

The author describes the methodology used by TNO in the Netherlands to evaluate the security of smartcard and other systems.

051361 'Aspects juridiques elementaires des trusted third parties'
T Piette-Coudol, *EDITT 95 pp 205–210*

It would be erroneous under French law to consider a trusted third party to be simply an electronic notary; notaries have statutory authority while electronic services are contractual.

051362 'Aligning Information Security Profiles With Organisational Policies'
D Pottas, SH von Solms, *IFIP 95 pp 477–491*

The authors elaborate their methodology for bringing security into harmony with an organisation's other policies by basing protection profiles for products such as RACF on job descriptions: staff should only be allowed to do what their job descriptions state explicitly.

051363 'Die Kryptokontroverse: das Normungsverbot'
K Rihaczek, *Datenschutz und Datensicherung v 20 no 1 (Jan 96) pp 15–22*

The ISO central secretariat has forbidden the standardisation of cryptographic mechanisms for confidentiality, at the best of national intelligence agencies. European governments have largely been successful in preventing the use of encryption in open systems, despite the fact that many of them do not have the legal power to actually ban cryptography.

051364 'Europäischer Datenschutz and anwaltliche Informationsverarbeitung'
G Rüpke, *Datenschutz und Datensicherung v 19 no 12 (Dec 95) pp 703–708*

The author discusses how data protection law, both national and European, could impinge on data processing by lawyers.

051365 'Intellectual Property Rights and the Global Information Economy'
P Samuelson, *Communications of the ACM v 39 no 1 (Jan 96) pp 23–28*

A European proposal to treat digital video on demand as video rental has angered the USA, which is not a party to the European video rental treaty; the USA wants to extend copyright control to temporary copies held in computer memory, which Europeans say will cause problems for routers, mirrors and cache servers. The Americans say that cacheing deprives the owner of an ftp site the knowledge of who has downloaded his files. There is also no agreement on whether there should be a universal 'digital tattoo' to enforce payment. However there is little technical sophistication in the debate, which is currently captive to copyright owning interests.

051366 'The New Alliance: Gaining on Security Integrity Assurance'
RH Sanchez, DL Evans, *NISSC 95 pp 100–112*

The authors describe NASA's approach to security engineering at its mission operations in the Johnson space centre. This incorporates both QA and configuration management: the bureaucratic processes involved are outlined, as are some of the problems encountered.

051367 'EDI: the challenge for the accountancy profession'
A Sneyers, *EDITT 95 pp 161–167*

The European accountancy profession has set up a network of committees to look at EDI, and their structure is outlined in this article.

051368 'Setting optimal intrusion-detection thresholds'
BC Soh, TS Dillon, *Computers and Security v 14 no 7 (95) pp 621–631*

The authors model attacks on systems as a Markov process, and predict various trade-offs between the false alarm rate and the effectiveness of intrusion detection.

051369 'Extending Distributed Audit to Heterogeneous Audit Subsystems'
CR Tsai, *IFIP 95 pp 331–339*

The authors describe a distributed audit mechanism they constructed for AIX: each machine has a distributed audit daemon that is managed from the centre. The mechanisms interwork with those of RACF under VM.

051370 'Outsourcing — Evaluating Security Compliance'
R Turner, *Computer Audit Update (Jan 96) pp 22–27*

This article describes how an organisation ought to go about building IT security provisions into outsourcing agreements, and checking compliance with them.

051371 'Einsatz van PCs/Arbeitsstationen — kombinierte Richtlinie zu Datenschutz und Datensicherung'
M Wächter, *Datenschutz und Datensicherung v 19 no 12 (Dec 95) pp 718–720*

The author presents a model data protection and security leaflet for use in German businesses.

051372 'Surveillance, Eavesdropping and Citizens' Rights'
DH Wallace, EK Woods, *Journal of Security Administration v 18 no 2 (Dec 95) pp 10–17*

This article surveys the law on surveillance in the USA from the point of view of investigating insurance fraud. Reasonable investigation is allowed, but open and persistent surveillance is actionable as a tort.

051373 '50. Datenschutzkonferenz — Die Beschlüsse'
S Walz, *Datenschutz und Datensicherung v 20 no 2 (Feb 96) pp 83–88*

This article reports the resolutions of a conference of German data protection officials held in November 1995. The first set of recommendations were to the effect that data protection should enshrined in the European constitution, with an independent commissioner to oversee it. The second related to the right to medical privacy, and in particular for patients to decide which of their records (if any) are held on a health card.

051374 'Developing Policies, Procedures and Information Security Systems'
AR Warman, *IFIP 95 pp 465–476*

The author discusses the differences between individual and organisational perceptions of computer related crime, and their consequences, Policies and procedures are often there for 'due diligence': they give employees an excuse rather than reduce risk.

051375 'Der betriebliche Datenschutzbeauftragte im Lichte der EG-Datenschutzrichtlinie'
M Weber, *Datenschutz und Datensicherung v 19 no 12 (Dec 95) pp 698–702'*

This article describes negotiations underway about the interpretation of the EU directive on data protection, which may have various conflicts with the existing high level of protection in Germany.

051376 'The Non-Technical Threat to Computing Systems'
IS Winkler, *Usenix Computing Systems v 9 no 1 (Winter 96) pp 1–14*

'Social engineering' refers to obtaining information through non-technical means, such as by convincing users to disclose their password to a caller or 'dumpster diving' for discarded printout. A study of social engineering in a large financial institution showed that the lack of user education left it quite vulnerable.

051377 'Writing Infosec Policies'
CC Wood, *Computers and Security v 14 no 8 (95) pp 667–674*

The author discusses how to document the process of developing corporate security policy: this can be important in defending against future lawsuits.

051378 'Online-Dienste in rechtsfreien Raum?'
U Wuermeling, *Datenschutzberater v 20 no 2 (15/2/96) pp 1–4*

Despite the lack so far of a German law regulating the infobahn, there are a number of already applicable laws, which are discussed in this article.

051379 'Risiken bei Verstößen gegen Datenschutzrecht'
U Wuermeling, *Datenschutzberater v 20 no 1 (Jan 96) pp 9–10*

The effectiveness of German data protection law is discussed, and the number of criminal convictions obtained nationwide for the years 1988–1994 is tabulated: it fluctuated between 100 and 194. The clear-up rate was 65%.

4 Formal Methods and Protocols

051401 'Prudent Engineering Practice for Cryptographic Protocols'
M Abadi, R Needham, *IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 6–15*

In this journal version of **032401**, the authors present eleven principles to help crypto protocol designers avoid the most common serious errors. The principles help ensure that messages mean what they say, and that the conditions for them to be acted on are clear. Many of them have to do with aspects of typing, especially when encryption is used, while others have to do with ensuring freshness. A new attack, incorporated since the conference paper, breaks an early version of SSL.

051402 'iKP — A Family of Secure Electronic Payment Protocols'
M Bellara, JA Garay, R Hauser, A Herzberg, H Krawczyk, M Steiner, G Tsudik, M Waidner, *EC 95 pp 89-106*

The authors describe IBM's iKP protocols for electronic commerce. They implement credit-card transactions, but can be generalized to debit cards and electronic checks; there are variants with one, two or three passes.

051403 'An Approach to the Formal Verification of Cryptographic Protocols'
D Bolignano, *ACM 96 pp 106–118*

This paper describes an approach to protocol verification with varying levels of granularity and mechanised proofs, compatible with traditional formal methods. This method is applied to authentication protocols by examining a public-key version of the Needham-Schroeder protocol, in which trusted principals are assumed to follow the protocol.

051404 'Edification of the Negotiable Bill of Lading: Registries vs Smart Cards?'
R Bons, R Lee, A Schmidt, T de Vries, *EDITT 95 pp 55–85*

The authors discuss the interaction between technical and legal aspects of electronic negotiable instruments. Ensuring the uniqueness of a bill of lading could be done using tamper-resistant devices, trusted third parties, or some combination of these. The procedures devised in the TEDIS EDIBoL project are described in a formal model that uses Petri nets.

051405 'Internet Holes — Part 5b: 50 Ways to Attack Your Web Systems'
F Cohen, *Network Security (Jan 96) pp 9–13*

The author continues from **044412** a list of ways to attack web servers, including abusing CGI scripts and using various service denial and redirection techniques.

051406 'Internet Holes — Part 6: Automated Attack and Defence'
F Cohen, *Network Security (Feb 96) pp 9–14*

Even at sophisticated sites, the dominant defence is against password guessing. However, there are now automated tools that let even inexperienced people mount much more sophisticated attacks such as guessing NFS file handles. SATAN is described, as well as a tool that reconstructs a target's password file from a series of NIS requests. However, most attacks that work have been known for a long time, and the average organisation that succumbs to them should probably blame inadequate investment of money and time in training, management and testing.

051407 'Maintaining Privacy in Electronic Transactions'
B Cox, *NISSC 95 pp 184–193*

The anonymity provided by the NetBill payment protocol is analysed and compared with the ideal. To get closer, it may be necessary to hide network addresses using anonymous remailers, and for customers to use pseudonyms; the ways in which these could be incorporated are discussed.

051408 'NetBill Security and Transaction Protocol'
B Cox, JD Tygar, M Sirbu, *EC 95 pp 77-88*
This paper describes the NetBill protocol, together with some extensions for handling zero-priced goods. The delivery of these goods can be certified if required.

051409 'Developing and Deploying Corporate Cryptographic Systems'
DE Coe, *EC 95 pp 137-146*
This article describes the problems experienced by Mitre Corporation in securing its information infrastructure. The various products available, such as X.509, Kerberos and SSL, are all incompatible and so trust between different hierarchies cannot be established.

051410 'Kerberos Plus RSA for World Wide Web Security'
D Davis, *EC 95 pp 185-188*
The author shows how Kerberos can enable clients to interact securely with non-Kerberized WWW servers. The protocol allows clients to use the Web server's public-key certificate to get credentials that conform to standards such as SHTTP.

051411 'Kerberos with Clocks Adrift: History, Protocols, and Implementation'
DF Davis, DE Geer, T Ts'o, *Usenix Computing Systems v 9 no 1 (Winter 96) pp 29–46*
Standard Kerberos requires synchronized clocks to prevent replay attacks, but provides no means for synchronizing clocks in a secure way. Extensions to the Kerberos protocol allow servers to synchronize their clocks using a challenge/response system; clients are not required to synchronize. The effort to implement the protocol changes was minimal, and does not increase login time delays. Intended applications include both mobile and home computing.

051412 'A Taxonomy for Key Escrow Encryption Schemes'
DE Denning, DK Branstad, *Communications of the ACM v 39 no 3 (Mar 96) pp 34–39*
The authors describe 29 different key escrow schemes briefly and tabulate some of their features. They also discuss which features might be desirable in certain circumstances.

051413 'Key management and the security of management in open systems: the SAMSON prototype'
GG Endersz, R Zamparo, *IFIP 95 pp 436–449*
The authors report on a project to develop a framework for security management in open networks, and give some details on how the key management mechanisms work. This is bound to credential and authorisation mechanisms, and session keys can be set up using either symmetric or asymmetric techniques.

051414 'A non-repudiation service architecture and certification infrastructure'
S Farrell, P Kaijser, *EDITT 95 pp 113–124*
The authors describe a SESAME based non-repudiation service that uses digital signatures and trusted time-stamping.

051415 'The Yaksha Security System'
R Ganesan, *Communications of the ACM v 39 no 3 (Mar 96) pp 55–60*
The author describes a security system in which an escrow agent can reveal user session keys but not master keys: it uses the multisignature variant of RSA with a private key split into shadows between the user and a corporate signature service. This scheme can also let employers vet the documents that their employees sign.

051416 'Payment Switches for Open Networks'
DK Gifford, LC Stewart, AC Payne, GW Treese, *EC 95 pp 69-75*

This is an Internet payment protocol that provides real-time authorization. The system creates digital representations of conventional financial instruments, and forwards authenticated payment orders based on those instruments to conventional financial institutions.

051417 'Kryptoverfahren und Zertifizierungsinstanzen'
R Grimm, *Datenschutz und Datensicherung v 20 no 1 (Jan 96) pp 27–36*

The author provides an overview of key certification for a nonspecialist audience, and contrasts the approaches taken by PEM and PGP.

051418 'Security policies in OSI — management experience from the DeTeBerkom project BMSec'
R Grimm, T Hetschold, *Computer Networks and ISDN Systems v 28 no 4 (2/96) pp 499-511*

The authors discuss the X.700 proposals for secure network management in the context of a project to build a distributed management system for certification authorities. They conclude that the standards do not adequately support the definition of security policy, and present a protocol that enables systems to negotiate a mutually acceptable policy when an association is set up.

051419 'LTTP Protection — A Pragmatic Approach to Licensing'
R Hauser, K Bauknecht, *IFIP 95 pp 534–548*

The authors develop their stateful access control model, which is used to model software licensing, and discuss the problems of tampering with license servers. Their proposed solution uses public key techniques: there is a network of license servers, at least one of which is tamper resistant and invoked online during the license release protocol. It can also be integrated with Kerberos.

051420 'A Model for Secure Protocols and Their Compositions'
N Heintze, JD Tygar, *IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 16–30*

This journal version of **032409** shows how to base crypto protocol analysis on model theory rather than logic. A secure protocol is one that preserves valid belief (i.e., beliefs that can be derived), and a model is time-secure if all fresh or shared secrets ultimately expire.

051421 'Controlling Digital Signature Services Using a Smartcard'
CJ Holloway, *Computers and Security v 14 no 8 (95) pp 681–690*

The author proposes a corporate signature system in which a central server holds individuals' signing keys, and signs a message when presented with a hash of the message, the signing key and a user secret; this token is calculated by a smartcard that the user carries around.

051422 'Controlling the Use of Cryptographic Keys'
C Holloway, *Computers and Security v 14 no 7 (95) pp 587–598*

The author describes the evolution of IBM's system of key usage control from the early PCF/3848 key variant scheme to the key control vectors used in current CCA products. These allow control structures to be publicly audited without revealing the key material itself. He then discusses how control vectors can be extended to the public key world: secret keys are bound not just to the device in which they are stored, but to the user authorised to invoke them. In addition, user keys are prevented from signing other keys, so that control can be maintained over the possible trust hierarchies.

051423 'A tool for support of key distribution and validity certificate check in global directory service'

B Jerman-Blažič, D Trček, T Klobučar, F Bračun, *Computer Networks and ISDN Systems v 28 no 5 (3/96) pp 709–717*

The authors developed a tool to navigate certification hierarchies. It stores the links between a number of different X.500 certificate hierarchies and constructs a network of paths between them.

051424 'TCP/IP (Lack of) Security'

JM Johansson, *NISSC 95 pp 146–162*

The author describes various TCP/IP security weaknesses, the sendmail hole and the Internet worm, and discusses how these will change with the introduction of IPv6. The hop limit option, the authentication header and the privacy header will all allow better security mechanisms to be added.

051425 'Protocols for Adaptive Wireless and Mobile Networking'

DB Johnson, DA Maltz, *IEEE Personal Communications v 3 no 1 (Feb 96) pp 34–42*

Researchers at Carnegie Mellon have implemented a mobile network based on the draft IETF mobile IP standard: the mobile is bound to a 'home agent' that tunnels traffic to it as 'IP over IP'. Authenticating the mobile is easy until one starts to optimise the routing, but then a common authentication infrastructure is needed to validate binding update messages. An ad hoc way to do this is described.

051426 'Certificate Infrastructure and Unique Identification'

F Jordan, M Medina, *EDITT 95 pp 137–146*

The authors discuss how a global certification structure could be assembled from national, organisational and other structures by adding top level certifiers.

051427 'Creating Security Applications Based on The Global Certificate Management System'

N Kapidzic, *IFIP 95 pp 322-330*

The author discusses how a hierarchy of certification authorities can be set up following RFC 1422 to establish authentication on a global scale, It has a common root — the international policy registration authority — that certifies policy certification authorities, with two further layers of CA to get to the user. The mechanisms and possible application programming interface are discussed.

051428 'Reliable Organisation Identification for EDI'

A Lenoir, *EDITT 95 pp 3–16*

The EDIRA project aims to provide a registration authority for companies in Europe. It will be one of a number of authorities needed in electronic commerce — covering naming, registration, key certification and directory service provision — that should replace the current sectoral, network and national schemes. Currently ISO 6523 concerns the identification of organisations and has a steering committee whose membership includes the British national health service, SWIFT and the Zürich chamber of commerce.

051429 'Crypto Backup and Key Escrow'

DP Maher, *Communications of the ACM v 39 no 3 (Mar 96) pp 48–53*

The author describes an AT&T proposal for key escrow. A corporate key backup facility can be assembled using a number of agents who keep shadows of each user's private master key.

051430 'Proxy Signatures for Delegating Signing Operation'

M Mambo, K Usuda, E Okamoto, *ACM 96 pp 48–57*

The authors survey variations of signature schemes and list requirements for partial delegation. Delegation can be full (giving out the private key), partial (giving out a share of the private key), or by warrant. Several examples of proxy schemes were applied to popular signature schemes and performance measurements are given.

051431 'The Millicent Protocols for Electronic Commerce'
MS Manasse, *EC 95 pp 117-123*

This paper presents a micropayment protocol in which merchants create their own scrip that they then sell through brokers. The idea is that cryptography enables a server to send itself messages through an untrusted medium, which stores this information until required.

051432 'A Secure Group Membership Protocol'
MK Reiter, *IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 31–42*

This journal version of **032217** presents the group membership protocol that forms the heart of AT&T's Rampart system for distributing security processing among a group of servers. It achieves a consistent view of group membership despite corruption of up to a third of the members, which it can remove once exposed given the agreement of two-thirds, and replace given the acquiescence of one-third. The foundations are signed point-to-point messages, atomic multicast, and a group manager. Members must agree the manager's recommendations, or replace him. Proofs are provided of uniqueness, validity, integrity and liveness.

051433 'The Omega Key Management Service'
MK Reiter, MK Franklin, JB Lacy, RA Wright, *ACM 96 pp 38–47*

Omega is an on-line, distributed service that helps prevent private or secret key compromise and also provides key recovery. It is based on Rampart (which provides strong fault tolerance) and supports key generation, registration, look-up, certification, and revocation for RSA and ElGamal keys. Different methods of escrow are provided, including a method of decryption without re covering the escrowed private keys.

051434 'Independent One-Time Passwords'
AD Rubin, *Usenix Computing Systems v 9 no 1 (Winter 96) pp 15–27*

One time passwords allow users to authenticate themselves over a network without significant risk of replay attacks. In this design, users keep paper lists of passwords to respond to challenges by host computers. They can be based on a variety of algorithms, including triple-DES. Given a secure host, persistent (periodic) reauthentication can be done as a background activity to limit the vulnerability to session hijacking. The system is compared to S/KEY and SecureID.

051435 'Revocation and Revocation Certificates'
RA Rueppel, *EDITT 95 pp 103–111*

Certificate revocation lists have disadvantages: there may be a need to perform operations with a revoked public key, users might not wish to download the whole list, and one might want a legally binding status for revoked certificates. It may therefore be better to issue certificates that a given key has been revoked, and that the compromise is believed to have occurred on or about a certain date. A syntax for such certificates is proposed.

051436 'Secure document interchange: a secure user agent'
Y Sameshira, PT Kirstein, *Computer Networks and ISDN Systems v 28 no 4 (2/96) pp 513–523*

The authors describe their experience implementing security for ODA documents by means of a trusted user agent situated between the editor and the document handler. This highlighted a number of problems with the ODA security extension, and some proposed fixes are discussed.

051437 'Untraceability in Mobile Networks'
D Sanfat, R Molva, N Asokan, *Mobicom 95 pp 26–35*

The authors discuss the conflict between user authentication and location privacy in mobile networks. Five different privacy policies are defined, depending on whether the user's identity and/or location is kept private from some combination of eavesdroppers, local stations and the home station. The mechanisms of GSM and CDPD are described, together with their drawbacks. A high level of privacy could be obtained using one-time aliases, and a means of bolting these on top of KryptoKnight is described. The proposed protocol is then verified using a BAN variant.

051438 'Diffie-Hellman Key Distribution Extended to Group Communications'
M Steiner, G Tsudik, M Waidner, *ACM 96 pp 31–37*

The authors describe three implementations of an n-party Diffie-Hellman protocol, membership changes, and an authentication scheme not vulnerable to dictionary attacks. Breaking the n-party DH was shown to be as hard as the 2-party case. Different schemes are used to optimise the computation of these n-party keys.

051439 'An Authentication Logic Supporting Synchronization, Recovery, and Recency'
SG Stubblebine, RM Wright, *ACM 96 pp 95–106*

Logics like BAN have been limited in their ability to reason about time and revocation. This work adds policies for temporal extension of beliefs to BAN as extended by Tuttle and Syverson-van Oorschot. Properties such as "believes" have times associated with them. Clocks may need to be synchronised. Axioms exist for monotonicity of time, synchronisation, originator identification, and nonce verification, among others. Beliefs may be stable (time invariant), based on recency, or valid until revoked.

051440 'A Formal Language for Signature Schemes Based on the Discrete Logarithm Problem'
P Syverson, C Meadows, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 61–81*

The authors explain the protocol description language used in the NRL protocol analyzer and apply it to the Aziz-Diffie protocol.

051441 'A Set of Protocols for Micropayments in Distributed Systems'
L Tang, *EC 95 pp 107-115*

This paper presents several protocols for micropayments, that are essentially variants of Otway-Rees or Kerberos with the bank taking the role of the key server. They are claimed to be "cheap" as they use symmetric rather than public key cryptography, and are aimed at low-value transactions.

051442 'Commercial Key Recovery'
ST Walker, SB Lipner, CM Ellison, DM Balenson, *Communications of the ACM v 39 no 3 (Mar 96) pp 41–47*

The authors describe a key escrow scheme developed by TIS, in which backup keys are kept by the user's employer rather than by a government agency.

051443 'Securing local area and metropolitan area networks: a practical approach'
V Varadharajan, *NISSC 95 pp 249–261*

The author describes a project to integrate LAN security with switched multi-megabit data services (SMDS), and goes into the pros and cons of protecting traffic at the logical link control layer, the medium access control layer, or between them (as recommended by IEEE 802.10). He also discusses the management options for controlling a department-based security policy implemented on bridges and routers.

5 Secret Key Algorithms

051501 'Correlation of Boolean functions and pathology in recursion trees'
I Althöfer, I Leader, *SIAM Journal of Discrete Mathematics v 8 no 4 (Nov 95) pp 526–535*

The authors prove general results to the effect that applying nontrivial Boolean functions to a bit string decreases any correlation that may exist (in some sense) between the bits. Their results arose from studying the performance of tree searching algorithms in computer chess.

051502 'Differential-Linear Cryptanalysis of FEAL-8'
K Aoki, K Ohta, *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences, v E79-A n 1 (Jan 96) pp 20-28*

The authors apply Langford and Hellman's differential-linear cryptanalysis to FEAL-8, which they can break with just 12 chosen plaintexts.

051503 'Fast decoding algorithms for First Order Reed-Muller and Related Codes'
AE Ashikham, SL Litsyn, *Designs, Codes and Cryptography v 7 no 3 (Mar 96) pp 187–214*

The authors present modified maximum likelihood soft and hard decoding algorithms for first order Reed-Muller codes. These work best for codes of slightly lower weight than the average.

051504 'Differential Cryptanalysis of Lucifer'
I Ben-Aroya, E Biham, *Journal of Cryptology v 9 no 1 (Winter 96) pp 21–39*

In this journal version of **024502**, the authors use key-dependent characteristics to show that over half the keys of Lucifer are insecure and can be found with about 2^{36} chosen texts; 90% of the keys of eight round Lucifer can be broken with 256 chosen texts. The same techniques break RDES, a variant of DES with added key-dependent swaps of left and right halves.

051505 'The Viterbi Algorithm for Sparse Channels'
N Benvenuto, R Marchesani, *IEEE Transactions on Communications v 44 no 3 (Mar 96) pp 287–289*

The authors present a simplified Viterbi algorithm for decoding a sparsely generated shift register sequence in the presence of noise using maximum likelihood techniques. Their algorithm reduces the complexity of decoding an 8PSK modulation with a multiple channel of length 16 and 3 nonzero coefficients by over ten orders of magnitude.

051506 'Information transmission by chaotizing'
F Böhme, A Bauer, U Feldmann, W Schwarz, *International Journal of Electronics v 79 no 6 (Dec 95) pp 767–773*

The authors describe a system which encodes data using a 'chaotizer' — a chaotic oscillator whose behaviour is a function both of the signal and a key. Various possible analogue and discrete realisations are presented.

051507 'Linear Span Analysys of a Set of Periodic Sequence Generators'
P Caballero-Gil, A Fúster-Sabater, *Cirencester 95 pp 22–33*

The authors present a new algorithm for computing the linear complexity of nonlinear filter generator sequences which works for any sequence with a unique term of maximum order. The basic idea is that not many degeneracies can exist simultaneously. A number of experimental results are presented.

051508 'A world war II German army field cipher and how we broke it'
C David, *Cryptologia v XX no 1 (Jan 96) pp 55–76*

The author recalls how the German double Playfair field cipher was solved during world war 2 by allied forces, and describes the field signals intelligence units that combined interception, analysis and product assessment capabilities. This may have been the last serious pencil-and-paper cryptanalysis undertaken on an industrial scale. It provided advance warning of the Ardennes offensive which was not acted on at first; but their contribution had a significant effect when chasing German troops after the Battle of the Bulge. His article includes a practical and detailed guide to breaking ciphers of the Playfair type — perhaps the best in the open literature.

051509 'Chaotic synchronisation using monolithic Chua oscillators'
M Delgado-Rostituto, A Ródriguez-Vazquez, R López-Ahumada, M Linan, *International Journal of Electronics v 79 no 6 (Dec 95) pp 775–785*

The authors describe a VLSI circuit constructed to encode data using a chaotic oscillator and present some experimental results.

051510 'Composite inversive congruential pseudorandom generators: an average-case analysis'
J Eichenauer-Herrmann, F Emmerich, *Mathematics of Computation v 65 no 213 (Jan 96) pp 215–225*

The authors extend the theory of inversive congruential generators to composite moduli, and obtain an upper bound on the sequence discrepancy.

051511 'A Note on the Hash Function of Tillich and Zémor'
W Geiselmann, *Cirencester 95 pp 257–263*

The author shows how to calculate collisions for a hash function proposed by Tillich and Zémor at Crypto 94 (**034545**). Unlike a previous collision finding technique (**041504**), it is not restricted to implementations with a bad choice of polynomial.

051512 'Linear Models for Keystream Generators'
JD Golić, *IEEE Transactions on Computers v 45 no 1 (Jan 96) pp 41–49*

The author shows how to separate the keystream generated by an arbitrary automaton with M bits of memory into a driven linear feedback shift register of length at most M and a nonbalanced nonlinear sequence. Various correlation results are proved, and linear approximations are derived for a number of keystream generator designs.

051513 'Q-ary Cascaded GMW Sequences'
G Gong, *IEEE Transactions on Information Theory v 42 no 1 (Jan 96) pp 263–267*

This paper shows how to cascade GMW sequences in such a way that they have very large linear spans and two-valued autocorrelation functions.

051514 'On the classification of deBruijn sequences'
ER Hauge, J Mykkeltveit, *Discrete Mathematics v 148 (15/1/96) pp 65–83*

DeBruijn sequences can be classified according to the weight of the feedback function that generates them, and the equivalence classes that result have symmetry groups that allow further classification. The key idea is that certain permutations in the edges of adjacency graphs correspond to certain permutations of sequences, which are tractable in the low weight case. The graphs for a number of minimal weight classes for sequences of length 2^6 and 2^7 are given as an example.

051515 'Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis'
HM Heys, SM Tavares, *Journal of Cryptology v 9 no 1 (Winter 96) pp 1–19*

Assuming that the S-boxes in a SP network satisfy a lower bound on the rate at which changes are diffused, the authors calculate upper bounds on the probability of a differential holding through a given number of rounds, and on the best linear approximation.

051516 'On a nonlinear congruential pseudorandom number generator'
T Kato, LM Wu, N Yanagihara, *Mathematics of Computation v 65 no 213 (Jan 96) pp 227–233*

The authors propose a pseudorandom number generator of the form $r_{n+1} = a/r_n + b + cr_n \pmod{2^n}$, and show that it has period 2^{n-1} if and only if $a + c \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$.

051517 'Partial Period Crosscorrelation of Geometric Sequences'
A Klapper, *IEEE Transactions on Information Theory v 42 no 1 (Jan 96) pp 256–260*

Geometric sequences are obtained by filtering a linear sequence over $GF(q)$ to a field of characteristic two. So long as they are balanced, the partial period crosscorrelation will stay within certain bounds for almost all of the time; this is established by studying the crosscorrelation's variance.

051518 'Maximally equidistributed combines Tausworthe generators'
P L'Ecuyer, *Mathematics of Computation v 65 no 213 (Jan 96) pp 203–213*

If one combines a number of linear feedback shift registers based on trinomials or other sparse polynomials by bitwise exclusive or, then the result is equivalent to another linear feedback shift register, but whose characteristic polynomial will not usually be sparse. In this way, non-sparse sequences can be constructed using few hardware components or software instructions.

051519 'Using Rademacher-Walsh spectral transforms to evaluate the agreement between Boolean functions'
E Macii, M Poncino, *IEE Proceedings in Computers and Digital Techniques v 143 no 1 (Jan 96) pp 64–68*

The authors present a spectral technique, based on decision diagrams, to compute the correlation between two compactly described Boolean functions. It is effective for up to 80 variables.

051520 'Complex Hadamard Matrices Related to Bent Sequences'
S Matsofuji, N Suehiro, *IEEE Transactions on Information Theory v 42 no 2 (Mar 96) p 637*

The author provides a construction for complex Hadamard matrices of order p^n where p is prime and n is even. It is derived from bent functions, and is suggested as a candidate for spread spectrum sequences if a fast factorisation algorithm could be found.

051521 'The Best Linear Expression Search of FEAL'
S Moriai, K Aoki, K Ohta, *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences, v E79-A n 1 (Jan 96) pp 2-11*

The authors improve on Matsui's search algorithm which determines the best linear expressions, and apply it to FEAL. The improved algorithm finds the best expressions much faster: the time is decreased from over three months to two and a half days. Results are given for FEAL-7, FEAL-15, and FEAL-31; the authors prove that FEAL-32 is secure against linear cryptanalysis.

051522 'Generalization of GMW Sequences and No Sequences'
JS No, *IEEE Transactions on Information Theory v 42 no 1 (Jan 96) pp 260–262*

The author presents generalised GMW and No sequences that have full period autocorrelations.

051523 'Hardware implementation of the Lehmer random number generator'
AP Paplinski, N Bhattacharjee, *IEE Proceedings in Computers and Digital Techniques v 143 no 1 (Jan 96) pp 93–95*

A fast hardware implementation is presented for Lehmer's linear congruential generator, which has $r_n = 7^{5n} \bmod (2^{31} - 1)$. It is based on an equivalent additive expression in six rotated copies of r_{n-1}.

051524 'Computation of Low-Weight Parity Checks for Correlation Attacks on Stream Ciphers'
WT Penzhorn, GJ Kühn, *Cirencester 95 pp 74–83*

Meier and Staffelbach showed how to find low weight multiples of polynomials of degree k over F_2 in time and space $O(2^{k/2})$. The present paper discusses tradeoffs that involve more time and less space.

051525 'Distribution of Recurrent Sequences Modulo Prime Powers'
RGE Pinch, *Cirencester 95 pp 188-189*

The author shows that maximal linear recurrent sequences modulo a prime power p^n take each value equally often up to an error of order $p^{n/2}$.

051526 'Non-exhaustive search methods and their use in the minimisation of Reed-Muller canonical expansions'
GI Robertson, JF Miller, P Thomson, *International Journal of Electronics v 80 no 1 (Jan 96) pp 1–12*

The authors describe and compare a number of fast algorithms for finding the canonical expressions of Boolean functions. Tabu search and nearest-ascent hill climbing are often effective.

051527 'A simplified data encryption standard algorithm'
EF Schaefer, *Cryptologia v XX no 1 (Jan 96) pp 77–84*

The author presents a cut-down version of DES designed to teach the underlying concepts to students: it has 2 rounds and 10 bit keys.

051528 'Cryptanalysis of Private-Key Encryption Schemes Based on Burst-Error-Correcting Codes'
HM Sun, SP Shieh, *ACM 96 pp 153–156*

The authors describe a chosen plaintext attack on Alencar's secret key system, which is based on a binary linear block burst error correcting code. The attack repeatedly encrypts vectors of Hamming weight one to recover a row at a time of the generator matrix.

051529 'Werftschlüssel — a German navy hand cipher system, part II'
M van der Meulen, *Cryptologia v XX no 1 (Jan 96) pp 37–54*

This continues from **044546** the story of the German dockyards' and fleet auxiliaries' world war 2 hand cipher.

051530 'An Experiment on DES Statistical Cryptanalysis'
S Vaudenay, *ACM 96 pp 139–147*

This work applies statistical analysis to DES, first by trying to distinguish distributions of input and output bits, round by round, from random distributions. Looking at four bits on the left and one bit on the right in each DES round, the same pattern as the best linear test found by Matsui arises. Attacks on 16 round DES require slightly fewer than 2^{43} known plaintexts and operations.

051531 'Characterising the Structure of Cryptographic Functions Satisfying the Propagation Criterion for Almost All Vectors'
XM Zhang, YL Zheng, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 111–134*

The authors summarise a number of results on propagation criteria, and show that Boolean functions which satisfy these on most inputs are related to bent functions.

6 Public Key Algorithms

051601 'A New Algorithm for Finding Minimum-Weight Words in Large Linear Codes'
A Canteaut, *Cirencester 95 pp 205–212*

The author presents a faster algorithm for finding low-weight words in large linear codes; it can decode random [512,256,57]-linear binary codes in 9 hours on a DEC Alpha. The practical effect of the algorithm is a 128-fold reduction in the work factor of breaking the McEliece cryptosystem.

051602 'Combinatorial optimization and the knapsack cipher'
A Clark, E Dawson, H Bergen, *Cryptologia v XX no 1 (Jan 96) pp 85–93*

The authors rubbish Spillman's claim in **024621** that a certain combinatorial optimisation technique could break knapsack ciphers: they show that it can tackle only trivial sizes of problem.

051603 'On-Line Off-Line Digital Signatures'
S Even, O Goldreich, S Micali, *Journal of Cryptology v 9 no 1 (Winter 96) pp 35–67*

The authors show how to adapt Rabin signatures so that almost all of the effort is in a precomputation. The idea is to sign the information needed for a DES based one time signature in advance, and then apply that to the message.

051604 'Revocable and Versatile Electronic Money'
M Jacobsson, M Yung, *ACM 96 pp 76–87*

Electronic money systems are subject to a wide range of threats to all parties. Banks may also have to prevent tax evasion, money laundering, blackmail (forced withdrawal), or bank robbery (by intimidation). This new scheme addresses the above named threats by providing only escrowed anonymity. Users cannot force blinding (bank robbery), and they must trust an ombudsman to protect their interests.

051605 'Integrating authentication in public key distribution system'
WB Lee, CC Chang, *Information Processing Letters v 57 no 1 (15/1/96) pp 49–52*

The authors present an authenticated key exchange scheme that is designed to avoid the attack of Nyberg and Rueppel.

051606 'Breaking and Repairing a Convertible Undeniable Signature Scheme'
M Michels, H Petersen, P Horster, *ACM 96 pp 148–152*

Undeniable schemes allow signers to decide to whom they will prove or disprove validity. Convertible undeniable schemes can be totally or partially converted to normal schemes. The author shows how to attack a convertible undeniable ElGamal-like signature scheme defined by Chaum and others; the attack occurs after a total conversion, and the repair consists of a heuristic modification to the signing equation.

051607 'Batch Exponentiation—A Fast DLP-Based Signature Generation Strategy'
D M'Raïhi, D Naccache, *ACM 96 pp 58–61*

This work is an improvement on the Brickell-McCurley-Gordon time-memory tradeoff scheme. Here, batch exponentiation is used to speed up discrete log based signatures. Several optimisations minimise the number of multiplications. Working pairwise upwards in a binary tree, they show how to use square-and-multiply in parallel. This saved 42% of the computation.

051608 'Access Control and Signatures via Quorum Secret Sharing'
M Naor, A Woo, *ACM 96 pp 157–168*

Quorum systems are secret sharing schemes such that no two shares are disjoint. An example of a quorum system based on left-right paths in a grid and top-bottom paths in the dual grid is given. An application would be a service where all data are encrypted, and each access server has shares of the keys for each record. The goals are high capacity and availability with small quorum sizes.

051609 'Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem'
K Nyberg, RA Rueppel, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 61–81*

The authors show how to change any of the existing El-Gamal type signature schemes to give message recovery; this applies in particular to DSA. The basic idea is to replace the message key $r = g^k$ by $r = g^k m$.

051610 'Prepaid Electronic Cheques Using Public-Key Certificates'
C Radu, R Govaerts, J Vandewalle, *Cirencester 95 pp 132–141*

An electronic cheque scheme that minimises the computational effort required of the shopper's electronic purse is based on one certified public key pair per cheque, issued in advance by the bank. Guillou-Quisquater signatures are used.

051611 'Key-Exchange in Real Quadratic Congruence Function Fields'
R Scheidler, A Stern, HC Williams, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 153–174*

The authors present a version of Diffie Hellman in the principal ideal class of a number field, rather than in a group. Shanks' attack will still work, but the authors hope that Pollard's methods will not.

051612 'Security of 2^t-Root Identification and Signatures'
CP Schnorr, *European Colloquium on Computational Complexity TR 96-019*

The author proves the security of the Ong-Scnhorr identification and signature scheme, a variant of Fiat-Shamir that uses repeated square roots with respect to a composite modulus. It is shown to be as hard as factoring, even against adaptive chosen-message attacks.

051613 'Key distribution systems based on the ' 'exponential representation" of the linear group $GL_n(F_p)$'
VM Sidel'nikov, *Problemy Peredachi Informatsii v 30 no 4 (94) pp 25–32; translated in Problems of Information Transmission v 30 no 4 (95) pp 310–316*

The author shows how to do Diffie Hellman in subgroups of $GL_n(F_p)$ constructed from a multiplicative subgroup of F_p and a group of affine transformations of dimension two. This has various novel properties.

051614 'An Elliptic Curve Analogue of McCurley's Key Agreement Scheme'
A Smith, C Boyd, *Cirencester 95 pp 150–157*

The authors present an analogue of McCurley's identification scheme for elliptic curves; its security depends on the difficulty of discrete log in curves of composite modulus. An attack on it can be used to factor the modulus and to extract elliptic logarithms in the factor curves.

051615 'Comment: public key cryptosystem design based on factoring and discrete logarithms' *with* **Reply** *and* **Comment**
K Tu, L Harn, *IEE Proceedings in Computers and Digital Techniques v 143 no 1 (Jan 96) p 96*

The two correspondents iron out a bug in **033609**.

051616 'Cryptanalysis of Harari's Identification Scheme'
P Véron, *Cirencester 95 pp 264–269*

Harari proposed an identification scheme based on coding theory in 1988; the prover's secret is a low weight codeword, and the public information is a parity check matrix. The prover responds to a challenge with a vector whose weights and syndrome fulfil certain conditions. The present paper shows that an impostor can pass the protocol every second time.

7 Computational Number Theory

051701 'Further investigations with the strong probable prime test'
R Burthe, *Mathematics of Computation v 65 no 213 (Jan 96) pp 373–382*

Damgård, Landrock and Pomerance had proved that the probability of a k-bit off composite number passing the Miller-Rabin test to t random bases was less than 4^{-t} for $k \geq 51$. The present author extends the result to all $k \geq 2$.

051702 'Hybrid method for modular exponentiation with precomputation'
CY Chen, CC Chang, WP Yang, *Electronics Letters v 32 no 6 (14/3/96) pp 540–541*

By precomputing and storing the values g^{3i5j}, it is possible to do discrete exponentiation with respect to an n bit modulus using asymptotically less than $0.33n$ modular multiplications.

051703 'Orbits and lattices for linear random number generators with composite moduli'
R Couture, P L'Ecuyer, *Mathematics of Computation v 65 no 213 (Jan 96) pp 189–201*

The authors present a generalised spectral test for linear congruential generators in large dimensions by viewing them as subgenerators of a generator modulo a composite number.

051705 'Redundant Integer Representation and Fast Exponentiation'
D Gollmann, YF Han, CJ Mitchell, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 135–151*

The authors present a number of results about the conversion of integers to and from redundant representations, and apply these to a string replacement algorithm.

051706 'The coefficients of primitive polynomials over finite fields'
WB Han, *Mathematics of Computation v 65 no 213 (Jan 96) pp 331–340*

The author proves that there is a primitive polynomial of every degree greater than 6 over every field of odd order with the first and second coefficients prescribed in advance.

051707 'Minimal Weight k-SR Representations'
YF Han, D Gollmann, C Mitchell, *Cirencester 95 pp 34–43*

The authors investigate string replacement representations — redundant ways of expressing integers that are suitable for fast exponentiation algorithms. The idea is to replace 1-runs in a binary number by a single digit.

051708 'Efficient computation of full Lucas sequences'
M Joye, JJ Quisquater, *Electronics Letters v 32 no 6 (14/3/96) pp 537–538*

The authors present a faster algorithm for computing any Lucas sequence, and apply it to finding the order of an elliptic curve over $GF(2^n)$ where the order of the curve with the same coefficients over $GF(2^m)$ is known for some $m < n$.

051709 'Subquadratic-time Factoring of Polynomials over Finite Fields'
E Kaltofen, V Shoup, *STOC 95 pp 398–408*

The authors present an algorithm for factoring polynomials over finite fields. The use of fast matrix multiplication would give it an asymptotic running time for degree n and $GF(q)$ of $O(n^{1.815} \log q)$; for practical sizes of problem, one can get $O(n^{2.5} + n^{1+o(1)} \log q)$. Factoring a 128 degree pseudorandomly chosen polynomial modulo a 128 bit prime took under two minutes, as against 25 hours for Maple.

051710 'Complex multiplication structure of elliptic curves'
HW Lenstra, *Journal of Number Theory v 56 number 2 (Feb 96) pp 227–241*

The points on an elliptic curve can be viewed as a module over its ring of endomorphisms, and this is unique where the curve is over a finite field. Related results are also proved for other fields.

051711 'Some results on pseudosquares'
RF Lukes, LD Paterson, HC Williams, *Mathematics of Computation v 65 no 213 (Jan 96) pp 361–372*

The authors develop a relationship between primality testing and pseudosquares — the pseudosquare L_p is the least integer congruent to 1 mod 8 that is a quadratic residue with respect to all primes less than p.

051712 'Linear recurring sequences over modules'
AV Mikhalev, AA Nechaev, *Acta Applicandae Mathematicae v 42 no 2 (Feb 96) pp 161–202*

The authors extend the theory of sequences generated by linear recurrence relations to polylinear sequences over rings and modules. Ideals may possess properties such as periodicity and reversibility, and families of sequences can be analysed by studying their annihilators.

051713 'Approximation diophantienne de logarithmes elliptiques p-adiques'
G Rémond, F Urfels, *Journal of Number Theory v 57 no 1 (Mar 96) pp 133–169*

Explicit bounds are given for ϵ_1 and ϵ_2 such that if a linear combination $Au_1 - u_2$ of two elliptic p-adic logarithms if less than ϵ_1 than it is zero, A is an endomorphism of the curve and $h(A) < \epsilon_2$.

051714 'The graph of the square mapping on the prime fields'
TD Rogers, *Discrete Mathematics v 148 (15/1/96) pp 317–324*

The map $f(x) = x^2$ in $GF(p)$ is decomposed into cyclic components and their attached trees. Where $p = 2^k m$ with m odd, there are binary trees of height k attached to each point on cycles whose lengths are the orders of 2 modulo the factors of m.

051715 'A multiple-precision division algorithm'
DM Smith, *Mathematics of Computation v 65 no 213 (Jan 96) pp 157–163*

A new division algorithm is presented which recovers from wrong quotient guesses without separate correction steps. It is about twice as fast as many commonly fielded multiprecision routines.

8 Theoretical Cryptology

051801 'Communication in Key Distribution Schemes'
A Beimel, B Chor, *IEEE Transactions on Information Theory v 42 no 1 (Jan 96) pp 19–28*

A (g, b) key distribution scheme allows conferences of g good chaps to generate shared secrets about which coalitions of b bad chaps have no information. This property can hold for either a restricted or an unrestricted number of conferences. In the former case only, communications can greatly improve the space efficiency of such schemes.

051801 'On the information rate of secret sharing schemes'
C Blundo, A De Santis, L Gargano, U Vaccaro, *Theoretical Computer Science v 154 no 2 (5/2/96) pp 283–306*

The authors exhibit access structures with optimal average information rate less than $\frac{1}{2} + \epsilon$, and that establishing whether such a structure is contained in a given one is NP complete. They also show that any graph with n vertices has a scheme with rate $\Omega(\log n/n)$.

051803 'Subquadratic Zero-Knowledge'
J Boyar, G Brassard, R Peralta, *Journal of the ACM v 42 no 6 (Nov 95) pp 1169–1193*

Previous zero-knowledge proofs of the satisfiability of a Boolean circuit of size n with cheating probability 2^{-k} involved $\Omega(kn)$ bit commitments: the authors improve this to a preprocessing step on $O(n^{1+\epsilon})$ and a proof of $O(k\sqrt{n}^{1+\epsilon})$ that involves $O(k)$ openings of bit commitments; the proof can be given to a number of verifiers. The central ideas are that AND gates can be handled at sublinear cost (about $O(n^{3/5})$ commitments per round), and that the prover can show that previously committed bits are equal pairwise by opening commitments.

051804 'On-line Secret Sharing'
C Cachin, *Cirencester 95 pp 190–198*

An authentic bulletin board can be used to update secrets in dynamic secret sharing schemes. A number of variants on this idea are developed.

051805 'A broadcast Key Distribution Scheme Based on Block Designs'
V Korjik, M Ivkov, Y Merinovich, A Barg, HCA van Tilborg, *Cirencester 95 pp 2–12*

The authors consider unconditionally secure key distribution schemes, and show that block designs can be used to increase the size of the largest admissible coalition and the size of the keys each user has to store. While the resilience of schemes based on projective planes is at most the square root of the number of users, 2-designs can be used with Fiat-Naor techniques to get twice this.

051806 'How Traveling Salespersons Prove Their Identity'
S Lucks, *Cirencester 95 pp 142–149*

This paper proposes an identification scheme based on the exact travelling salesman problem, and presents some empirical evidence for its work factor given current best TSP algorithms.

051807 'Authentication Schemes, Perfect Local Randomizers, Perfect Secrecy and Secret Sharing Schemes'
CJ Mitchell, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 101–110*

The author writes about relationships between bounds on secret sharing schemes, authentication codes, channel bounds and perfect local randomisers. He extends Walker's bounds on Cartesian authentication schemes.

051808 'Storage complexity based analogue of Maurer key establishment using public channels'
CJ Mitchell, *Cirencester 95 pp 84–93*

If there is a public random channel that broadcasts bits at such a rate that they cannot economically be stored by an opponent, then a key can be set up by two parties who select bits at random from it and use as a key those bits they have both selected. It can be optimised be selecting bits a block at a time.

051809 'Randomness is Linear in Space'
N Nisan, D Zuckerman, *Journal of Computer and System Sciences v 52 no 1 (Feb 96) pp 43–52*

Any randomised algorithm with space S and time T using poly(S) random bits can be simulated in space S and time T + poly(S) with $O(S)$ random bits. The idea is that one can use a small number of good random bits to extract randomness from a poor random source using indexing techniques.

051810 'Combinatorial Characterization of Authentication Codes II'
RS Rees, DR Stinson, *Designs, Codes and Cryptography v 7 no 3 (Mar 96) pp 239–259*

The authors provide a cryptologic equivalent of Fisher's inequality by pointing out that an optimal authentication code must have the maximum possible number of encoding rules.

051811 'Authentication Codes in Plaintext and Chosen-Ciphertext Attacks'
R Safavi-Naini, L Tombak, *Designs, Codes and Cryptography v 7 no 1/2 (Jan 96) pp 83–99*

The authors compare known-plaintext with chosen-plaintext attacks on authentication codes, develop the relevant security bounds, and characterise those codes that protect against the latter with a minimum number of encoding rules.

051812 'Authentication codes that are r-fold secure against spoofing'
L Tombak, R Safavi-Naini, *Utilitas Mathematica v 43 (Nov 95) pp 215–224*

The authors characterise authentication codes that remain secure even when the opponent can see r cryptograms encoded using the same rule before emitting one of his own. They extend Stinson's bounds to them in the case of uniform sources.

051813 'Authentication Codes: an Area where Coding and Cryptology Meet'
HCA van Tilborg, *Cirencester 95 pp 169–183*

The author presents an overview of digital signatures and the theory of unconditionally secure authentication codes. The standard results are explained as are the constructions from projective planes and error correcting codes.

9 Book Reviews

'CONTRIBUTIONS TO UNCONDITIONALLY SECURE AUTHENTICATION'
Thomas Johansson
PhD Thesis, Department of Information Theory, Lund University

The main result in Thomas Johansson's thesis is a new way to construct authentication codes from Reed-Solomon and other authentication codes. The key idea is that the substitution attack probability can be viewed as a distance. The new constructions are significantly more efficient than previously known ones, and could potentially extend the use of unconditionally secure techniques to more applications than before. For example, 2^{20} source bits can be authenticated with a 40-bit tag with a message extension of only 150 bits. There are also several results on authentication codes that permit arbitration.

'APPLIED CRYPTOGRAPHY — SECOND EDITION'
Bruce Schneier
John Wiley and Sons, 1995; ISBN 0-471-12845-7

The second edition of Bruce Schneier's encyclopaedic book on cryptographic algorithms and protocols is a significant improvement on the first. It finally tackles stream ciphers and authentication protocols in a reasonably thorough way; in fact, the book has been extensively rewritten and starts off from the point of view of the protocol designer.

It then moves through a discussion of key management to the mathematical core of the subject — the algorithms used for encryption, hashing, digital signatures and other purposes. Next follows a treatment of more exotic topics from how to play poker on the phone through zero knowledge proofs and subliminal channels to quantum cryptography. The book ends up with a discussion of a number of real world applications such as Kerberos and IBM's common cryptographic architecture, and of the real world politics surrounding issues such as export control.

'Applied Cryptography' dispenses with formality, but at little cost in either accuracy or completeness. Schneier is emphatically a software engineer and his presentation is free of the rubric of 'theorem ... proof' adopted by many mathematicians (though not all: vide Harold Davenport's excellent expositions of number theory). This is surely to be welcomed as cryptology matures from a branch of applied mathematics into an engineering discipline in its own right.

'HEALTH IN THE NEW COMMUNICATIONS AGE'
MF Laires, MJ Ladeira, JP Christensen
IOS Press, Studies in Health Technology and Informatics vol 24, ISSN 0926-9630

This book contains papers and talks given at a Lisbon conference on medical telematics that acted as a showcase for some fifty projects sponsored under the EU's AIM programme. A number of the papers are of direct relevance to security, such as a paper by Barry Barber of the SEISMED project on medical security and a paper by Gerd-Guido Hofmann on the chip card now used in Germany to manage medical insurance claims. Many of the other papers are of indirect relevance, as they illustrate the enormous potential scope and complexity of the clinical telematics applications that will have to be protected in some way or another.

'HEALTH CARDS '95'
CO Köhler, O Rienhoff, OP Schaeffer (editors)
IOS Press, Studies in Health Technology and Informatics vol 26; ISSN 0926-9630

This book contains papers given at a conference on the use of smartcards and other portable tokens in health care. Many of them touch on the privacy and other security aspects of health cards; a typical view is that only when a patient is fully informed of who may have access to his data, can she make a valid decision whether to use a system or not. There are short reports on a large number of pilot studies in various countries, proposals in France and elsewhere to issue professionals with cards to authenticate them, and on the national health insurance card being introduced in Germany.

'TOWARDS SECURITY IN MEDICAL TELEMATICS'
B Barber, A Treacher, K Louwerse (editors)
IOS Press, Studies in Health Technology and Informatics vol 27; ISSN 0926-9630

This book contains a number of papers of healthcare informatics security produced as a result of an EU project (SEISMED). The majority of papers concern the legal and ethical aspects of clinical privacy rather than any hard technical matters: they explore the legislative environment from medical and data protection aspects; make recommendations for further legislation; discuss the various possible relevant standards; expound guidelines; and talk about management. There is one actual system reported: a hospital information system in Magdeburg, Germany that incorporates a cancer registry.

'DISASTER RECOVERY PLANNING'
Jon Toigo
John Wiley and Sons, 0-471-12175-4

This book is a step-by-step guide for company managers wishing to draw up and test a disaster recovery plan for their computers and communications. It is supplied with a number of worksheets (and PC software) that enable a manager to go about data collection and analysis in a systematic way. The presentation is more thorough than in most such books, and goes into the need for planning human as well as technical aspects of disaster recovery.

If it does have a weakness, it is the dry presentation, with few case histories. Contingency planning failures are as much failures of imagination as anything else; a book that is designed to be used ab initio, by managers with no previous contingency planning experience, should perhaps mention the banks who found that both their live and backup sites were inside the 800-yard police cordon after the Bishopsgate bomb, or companies who found that their contingency plan was itself consumed in the same fire as the computer centre.

How to Subscribe

Subscription orders are accepted for complete volumes only, starting with the first issue of any year. Continuing orders can also be made, and cancellations are accepted prior to the first issue of the year to which they apply. Claims for replacement of issues lost or damaged in the post should be made within six months. Subscribers may receive a complimentary electronic version of the journal by notifying us of their Internet email address.

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

Back issues offer: Get a subscription for 1996 (volume 4) plus a set of the remaining back numbers (currently v 2 no 1, 3 and 4 and all of v 3 and v 4) at a price of £90 for individual subscribers and £145 for corporate subscribers. Electronic copies of back numbers a year and more old may be fetched from `http://www.cl.cam.ac.uk/users/rja14`.

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

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

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

Corporate subscription for all available 1993–1996 issues — Please debit my VISA/MasterCard £145 □ I enclose a purchase order / cheque for £145 □ / US$212.50 □

Name: ....

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

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint `E5C7 93BE 379D 2842 49DC A809 A147 05F6` can be fetched from `http://www.cl.cam.ac.uk/users/rja14`. You can also fax this order form to us on +44 223 334678, or mail it to us at:

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