Volume 5 Number 4 (December 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. Subscription rates, conditions and ordering details are on the inside back cover; note that the address for subscriptions has changed.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by September 1996, 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:

ANTS II: Second International Symposium on Computational Number Theory, May 18–23 1996, Talence, France; *proceedings published by Springer as Lecture Notes in Computer Science v 1122*

IFIP 96: 12th International Information Security Conference, May 21–24 1996, Samos, Greece; *proceedings published by Chapman & Hall, ISBN 0-412-78120-4*

Info Hiding 96: First International Workshop on Information Hiding, 30 May – 1 June 1996, Isaac Newton Institute, Cambridge UK; *proceedings published by Springer as Lecture Notes in Computer Science v 1174*

SAC 96: Third Annual Workshop on Selected Areas in Cryptography, August 15–16 1996, Kingston, Ontario; *Workshop record published by Queen's University, Kingston*

CMS 96: Second IFIP TC6/TC11 International Conference on Communications and Multimedia Security, September 23–24 1996, Essen, Germany; *proceedings published by Chapman and Hall, ISBN 0 412 79780 1*

Pragocrypt 96: September 30 – October 3, Prague; *proceedings published by CTU Publishing House, Prague, ISBN 80-01-01502-5*

NISSC 96: 19th National Information Systems Security Conference, October 22–25, 1996, Baltimore, Maryland; *proceedings published by NIST*

EC 96: Second USENIX Workshop on Electronic Commerce, November 18–21 1996, Oakland, California; *proceedings published by the USENIX Association, ISBN 1-880446-83-9*

Apps 96: 12th Annual Computer Security Applications Conference, San Diego CA, December 9-13 1996. *proceedings published by the IEEE, ISBN 0-8186-7606-X*

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

We place an electronic version of this journal in the public domain one year after publication. The goal is to strike a balance between providing a universal service and maintaining enough revenue to cover the costs of publication. Subscribers get paper copies and up-to-date electronic versions as well; subscription information may be found inside the back cover. The archives can be found at

`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

054101 'Stretching the Limits of Steganography'
R Anderson, *Info Hiding 96 pp 39–48*

The author provides a brief overview of the state of the art in steganography, and shows how public key steganography is possible — at least in the presence of a passive warden. The basic idea is that if the communicating parties can manipulate at least one out of n bits in the covertext, then the warden can not distinguish the parity of successive blocks of n bits from random noise; accordingly these parity bits can be used to hide ciphertext in plain sight. Information theoretic limits of general steganography are also discussed, and it is shown that parity techniques can make many systems more efficient. Finally, the differential effectiveness of active and passive wardens is discussed.

054102 'Tamper Resistance — A Cautionary Note'
R Anderson, M Kuhn, *EC 96 pp 1–11*

The authors describe a number of ways in which smartcards and other security processors have been, or could be, attacked. These range from using power transients to induce revealing errors through techniques for physical penetration of card packaging and analysis using chip testing tools. They report a protocol attack on the Dallas DS5002 series processors which use encrypted external memory. The attack searches through the range of encrypted instructions until an output instruction is recognised by its effects; this is then used to tabulate the encryption function. Techniques used by professional TV pirates are also described, and the authors conclude that chip-sized security processors are probably impossible to make completely tamper proof.

054103 'Experiences in the Art of Security'
J Arceneaux, *SIGSAC Review v 14 no 4 (Oct 96) pp 12–16*

This article describes an online banking system built for Wells Fargo. It goes into the design choices made and the many problems encountered in getting a reasonably secure http service working.

054104 'Tamper-Resistant Software: An Implementation'
D Aucsmith, *Info Hiding 96 pp 317–333*

The author describes some techniques developed at Intel for making software difficult to debug without processor emulators or other specialised hardware analysis tools. The basic ideas are to have a number of interdependent modules that cooperate to generate threshold signatures, so that the secret key is never present all at once in memory or processed in a single operation; to customise the code to each installation by interleaving and obfuscating operations in varying ways; and to have the modules verify each others' integrity. Signatures of known debuggers and emulators are also detected, and with some processors integrity verification code can be locked in the cache.

054105 'Practical Invisibility in Digital Communications'
T Aura, *Info Hiding 96 pp 265–278*

The author discusses some of the problems of information hiding, including synchronising with a cover message which is a stream such digital audio. Where the cover message is a block, such as a digital picture, his technique is to use the Luby-Rackoff construction to embed the hidden bits pseudorandomly throughout the picture. A test implementation using SHA as the underlying primitive is reported.

054106 'Techniques for Data Hiding'
W Bender, D Gruhl, N Morimoto, A Lu, *IBM Systems Journal v 35 no 3–4 (96) pp 313–336*

The authors survey steganographic techniques used for hiding copyright marks, tamperproofing information and annotations in sound and images. The key is finding 'holes' in the signal that are not suitable for exploitation by compression algorithms, and to fill them with data in a way that remains invariant under a large class of signal transformations. They describe a number of algorithms, including Patchwork, which hides a bit of data in an image by increasing the differential luminance of a large number of pseudorandomly chosen pixel pairs, and echo hiding, which is also described in **054134** below.

054107 'Authentisierverfahren mit Assoziationen'
H Benzler, *Datenschutz und Datensicherheit v 20 no 12 (Doc 96) pp 723–728*

The author proposes a number of schemes for authenticating computer users by presenting them with lists of words that they can associate in pairs, e.g. the first and last names of childhood acquaintances. Different protocols are proposed for online versus offline and software versus smartcard implementations.

054108 'Striking a balance on privacy'
D Birch, *Computer Law and Security Report v 12 no 6 (Nov/Dec 96) pp 390–391*

The privacy aspects of the Mondex system are outlined by one of the company's consultants. He admits that the police, with a warrant, could obtain the identities of the cards used in particular transactions and the names of the people to whom these cards were issued; but he argues that the privacy criticisms of the scheme are unfounded in most practical situations.

054109 'Possible macro virus attacks and how to prevent them'
V Bontchev, *Computers and Security v 15 no 7 (96) pp 595–626*

Macro viruses already pose an almost intractable problem to writers of generic antivirus software, and yet virus writers are using only a fraction of the possibilities open to them. In addition to the small number of automatically executed macros, they could use custom menu replacement, button replacement, key shortcuts and forms. They could also make their viruses language independent and plant boobytraps that would cause antivirus programs to destroy documents or spawn mutated viruses. The possibilities for polymorphism and stealth are discussed, as is an incident in which two viruses 'mated' in the wild to produce a viable 'hybrid'. The antivirus mechanisms of Word v 7.0a are criticised, and it is pointed out that many of the macro attack techniques can be generalised to OLE-capable applications.

054110 'Increasing Firewall Reliability by Recording Routes'
PM Boshoff, MS Olivier, *CMS 96 pp 303–314*

The authors describe the design of a Linux-based firewall which considers the route a packet has taken when making access decisions. They provide source code for it.

054111 'Watermarking Document Images with Bounding Box Expansion'
J Brassil, L O'Gorman, *Info Hiding 96 pp 227–235*

The authors develop their work in **034110**, in which documents were marked by shifting lines, to shifting individual words. This has the effect of increasing the size of the box that bounds a particular piece of text by a few pixels, and turns out to be measurable even on a third generation photocopy.

054112 'Rise in tested telex fraud prompts call for international working party'
J Bryant, *Financial Technology International Bulletin v 14 no 4 (Dec 96) pp 6–7*

The Midland Bank's fraud manager reports that tested telex fund transfers, though highly insecure, are still used by some banks, while many more retain the facility as a backup for SWIFT. This has led to a number of frauds, particularly in the Far East, with the transmitting bank usually ending up liable. He recommends that such backup systems be taken offline in such a way that their use requires suitable management intervention. He also calls for an international working group to devise a better algorithm suite and key management mechanism.

054113 'A Tool for Building Firewall-Router Configurations'
CJ Calabrese, *Computing Systems Usenix v 9 no 3 (Summer 96) pp 239–253*

The big problems with firewalls is configuring them properly; a freeware tool is described that turns a high level functional description into configurations for Cisco and other routers.

054114 'Pre-authorised, off-line debit card launched'
Card World Independent (Sep 96) pp 1–2

This article describes the adoption of UEPS (**021402**) as the VISA 'Chip Off-line pre-Authorised Card' (COPAC). It is fielded in Russia and will be an international VISA product in 1998.

054115 'Smart without chip'
Card World Independent (Nov-Dec 96) p 4

This article describes data glyphs, a technique developed by Xerox and Sandia Imaging Systems for encoding data on paper or on payment cards. Bits are written as diagonal lines, about a hundredth of an inch long, which slope right or left to encode '1' or '0'. A combination of error correction and dispersing the data across the glyph gives high resilience against minor damage.

054116 'The Advanced Intelligent Network – A Security Opportunity'
TA Casey, Jr., *NISSC 96 pp 221–232*

The paper describes how the evolution of the public switched telephone network into an 'advanced intelligent network' involves integrating the control network with processors providing customer service features, and how this will open up many new vulnerabilities: one can expect attacks via the new interfaces provided for service creation, maintenance and law enforcement. In addition, the code implementing new services is expected to be written rapidly by a great diversity of providers. While the old network was protected by obscurity and isolation, the new one will need better; but there are few people who understand both security and the telephone network.

054117 'On The Application of Image Decomposition to Image Compression and Encryption'
H Cheng, XB Li, *CMS 96 pp 116–127*

The authors suggest that when an image is compressed using a technique such as jpeg, it is sufficient to encrypt only its most important components. They describe an example based on quadtree compression and discuss some possible attacks.

054118 'A Secure, Robust Watermark for Multimedia'
IJ Cox, J Kilian, T Leighton, T Shamoon, *Info Hiding 96 pp 185–206*

The authors describe a technique for applying digital watermarks to both video and audio signals. The mark is inserted into the perceptually most significant spectral coefficients of the signal using ideas derived from spread spectrum communications. With marks inserted in still pictures using discrete cosine transform techniques, they show that marks can still be recovered after various common processing operations including scaling, jpeg compression, dithering and clipping. Even when the image is printed, xeroxed and scanned, a mark can still be recovered. A given image cannot be queried for ownership, however, as the original unwatermarked image is required as part of the extraction process.

054119 'Surmounting the Effects of Lossy Compression on Steganography'
DL Currie, CE Irvine, *NISSC 96 pp 194–201*

The effects of the JPEG compression to image-based steganographic information hiding are described. Simplistic information hiding schemes do not work, as the lower four bits are heavily modified and information encoded in them would be corrupted. Information can still be encoded by manipulating pixel colour; but the scheme they used allowed only 30% bit recovery of the embedded data.

054120 'Fractal Based Image Steganography'
P Davern, M Scott, *Info Hiding 96 pp 279–294*

The authors present an information hiding scheme based on fractal compression techniques. The key consists of two non-overlapping regions of the image, selected by the user; the image is then subjected to fractal compression, and message bits of 1 and 0 cause the compression software to use templates in the two key regions respectively.

054121 'Using Fortezza for Transparent File Encryption'
J Epstein, T Williams, *Apps 96 pp 140–147*

The Assure product (a DOS/Windows security add-on) uses DES for transparent file encryption, and the authors replaced this with Fortezza. Several of the Fortezza features that work well for message encryption (such as automatic creation of new initialization vectors whenever data is encrypted) make transparent file encryption very difficult to implement. They ended up using a shadow file structure to hold Fortezza encryption keys and initialization vectors.

054122 'Information and interaction in MarketSpace — towards an open agent-based market infrastructure'
J Eriksson, N Finne, S Janson, *EC 96 pp 271–277*

The authors describe a market system in which human users and broker agents attempt to match buyers and sellers of information objects, which may be presented explicitly or as URLs.

054123 'Kriegsmarine Signal Indicators'
R Erskine, *Cryptologia v XX no 4 (Oct 96) pp 330–340*

The author provides a guide to the signal indicators used with German naval Engima traffic.

054124 'Standards call as battery operated smart cards become reality'
N Fleischer, *Card World Independent (Aug 96) pp 6–7*

This discusses the engineering aspects of making hydrogen ion batteries as thin sheets that can be built into payment cards.

054125 'Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best'
E Franz, A Jerichow, S Möller, A Pfitzmann, I Stierand, *Info Hiding 96 pp 7–21*

The authors discuss a system for hiding ciphertext in the low order bits of an ISDN telephone signal, and report measurements of the perceptibility of various covert signal levels as a function of the cover signal and background noise. They also discuss the meaning of perfect and pragmatic security in the stego context. They argue that steganography is easy, and thus restrictions on crypto will simply force criminals to use stego which will make the law enforcement job harder.

054126 'BigDog: Hierarchical Authentication, Session Control, and Authorization for the Web'
B Fried, A Lowry, *EC 96 pp 165–172*

The authors describe a web authentication system developed by Morgan Stanley for internal use.

054127 'Applications of keystroke analysis for improved login security and continuous user authentication'
SM Furnell, JP Morrissey, PW Sanders, CT Stockel, *IFIP 96 pp 283–294*

The authors examine a static identity verifier that uses a neural network to analyse keystroke dynamics, and a dynamic verifier with added statistical analysis. The effectiveness of both was reviewed; they suggest using the former to enforce password checks and the latter for intrusion detection.

054128 'Approaches to security in healthcare multimedia systems'
SM Furnell, NJ Salmons, PW Sanders, CT Stockel, MJ Warren, *CMS 96 pp 925–36*

The authors discuss the ways in which including image data in medical records can exacerbate the privacy risks and integrity problems. They suggest a protection strategy combining intrusion detection, voice and face recognition, role based access control and hierarchies of trusted third parties. They describe a pilot system they are building for the Ear, Nose and Throat department of Plymouth Hospitals NHS Trust.

054129 'Error Detection Methods'
JA Gallian, *Computing Surveys v 28 no 3 (9/96) pp 504–517*

This paper describes the check digit techniques used on a wide range of product codes, credit cards numbers, drivers' licences and banknotes.

054130 'Secure optical telecommunications using chaos in wavelength for signal transmissions'
JP Goedgebuer, L Larger, A Fischer, *Pragocrypt 96 part 2 pp 1–9*

This paper reports experiments to encipher data using chaotic oscillations generated in a tunable semiconductor laser.

054131 'Telecoms fraud under the microscope'
S Gold, *Information Security Monitor v 11 no 11 (Oct 96) pp 5–8*

This surveys a number of trends in telecommunications fraud including PABX abuse, cellular cloning and pager channel sniffing. It relates attempts to change UK law so that such offences are made more serious.

054132 'Agent Tcl: A flexible and secure mobile-agent system'
RS Gray, *Proc. Fourth Annual Tcl/Tk Workshop Proceedings (Usenix, 1996) pp 9–23*

This article describes Agent Tcl, a mobile agent programming langauge developed at Dartmouth out of Safe Tcl. Potentially dangerous commands are replaced by links to instances of these commands in a trusted interpreter. In addition, it incorporates authentication based on PGP.

054133 'Cybermoney in the Internet: An Overview over new Payment Systems in the Internet'
R Grimm, K Zanganeh, *CMS 96 pp 183–195*

The authors review some proposed electronic money systems including SET, CAFE, CyberCash, Mondex and GeldKarte.

054134 'Echo Hiding'
D Gruhl, A Lu, W Bender, *Info Hiding 96 pp 295–315*

The authors describe how to embed data in an audio signal at typically 16 bits per second by manipulating the echo characteristics of the signal below the level of perceptibility. This is achieved using cepstral transforms and is much more robust against lossy compression techniques than simple noise addition. It is also robust against D/A conversion, but is challenged by gaps of silence, such as inter-word pauses in speech. In addition to copyright protection, this can be used for applications such as annotation, captioning and the automatic monitoring of radio advertisements.

054135 'Secure Internet Commerce – Design and Implementation of the Security Architecture of Security First Network Bank, FSB'
N Hammond, *NISSC 96 pp 173–180*

The security architecture of a new online bank is described, together with some of the mechanisms used. There are separate firewalls for mail and banking transactions; the latter is a multilevel secure product running Netscape's commerce server, with cookie based authentication.

054136 ‘Strongboxes for Electronic Commerce’

T Hardjono, J Seberry, *EC 96 pp 135–145*

The authors talk about possible requirements for an electronic strongbox that would provide anonymous but certificated storage of digital valuables.

054137 ‘Scalable Document Fingerprinting’

N Heintze, *EC 96 pp 191–200*

The author describes a system, Koala, that looks for plagiarism and copyright violation on the net using search engine techniques. The problem is to find documents that are minor edits or reorganisations of an original; the solution is to use fingerprints consisting of a few selected substrings from each document. Postscript is coverted to lower-case ascii and vowels are dropped before choosing strings whose first five letters occur infrequently.

054138 ‘End-to-end Security Over the Internet: Implementation Architecture’

A Herbert, *APM Technical Report 1840.02, 14/10/96*

This report describes a system architecture to support secure use of the Internet for commerce and administration. It uses public key crypto with smartcards and firewalls for primary protection and provides protocols for secure email. browsing, purchasing, payment and other applications; these are implemented on a number of servers.

054139 ‘Combat ID advances on all fronts’

M Hewish, *International Defense Review v 29 (Dec 96) pp 18–19*

Identify-friend-or-foe technology is being extended from aircraft to ground vehicles and foot soldiers. The US army’s new system allows aircraft to broadcast targeting intentions on millimeter wave radio; friendly units respond with ‘don’t shoot me’ messages. Soldiers will have laser challenge transmitters mounted on their gunsights, with transponders on their webbing. This system was tested in November 1996 and will be fielded in the year 2000. The UK is developing a cheaper system called MAGPIE in which friendly vehicles carry a low-probability-of-intercept millimeter wave transmitter, and shooters carry a directional receiver.

054140 ‘Steganography for DOS Programmers’

A Johnson, *Dr Dobbs’ Journal no 261 (Jan 97) pp 48–51*

The author discusses hiding ciphertext between the end of a file and the end of the last block it uses on disk; he provides source code to do this in DOS.

054141 ‘The History of Steganography’

D Kahn, *Info Hiding 96 pp 1–5*

The author describes the history of steganography from its origins in ancient times with letter marking and other techniques, through the development of invisible inks and microdots, and spread spectrum communications. In addition to these technological message concealment techniques, he discusses linguistic techniques, which he classifies into semagrams (which use sign language of some kind) and open codes (in which certain key words have prearranged hidden meanings).

054142 ‘An attack detection system for secure computer systems – Design of the ADS’

I Kantzavelou, A Patel, *IFIP 96 pp 337–347*

A real-time attack detection system is described. It monitors user activities to discover security relevant events. These are examined and the user’s record collects points associated with such events. The cumulative score implies the protective actions to be taken.

054143 ‘Defending networks: The Expert System component of SECURENET’

SK Katsikas, N Theodoropoulos, *CMS 96 pp 291–302*

The authors describe the expert system module in an intrusion detection system being developed under the EU RACE programme. Some experimental results about its performance are summarised, and possible improvements are discussed.

054144 ‘An Authenticated Camera’

J Kelsey, B Schneier, C Hall, *Apps 96 pp 24–30*

A design is proposed for a tamper-resistant electronic camera that digitally signs each picture, including a hash of the image, the time and date, and the identity of the operator. Using a method similar to cipher block chaining ensures that omitting one or more images from the sequence is detected. One goal was a guarantee of location (to prove where the picture was taken), but this was impossible because GPS data is not trusted. The camera also cannot guarantee that what is in the picture is real (i.e., that the image is of an actual scene rather than of a prop). Other considerations are use of an accurate clock and feasible methods of authenticating users to the camera (such as a thumbprint).

054145 ‘Location Management Strategies Increasing Privacy in Mobile Communication’

D Kesdogan, H Federrath, A Jerichow, A Pfitzmann, *IFIP 96 pp 39–48*

Means to provide secrecy of user location and anonymity to GSM users are discussed. For the former, the authors suggest using a home computer as a trusted device for processing incoming calls. Anonymity is to be achieved either by periodic issuing of pseudonyms or by group pseudonyms; the latter could possibly work better given the structure of GSM.

054146 ‘Automatic human face location in a complex background using motion and color information’

CH Lee, JS Kim, KH Park, *Pattern Recognition v 29 no 11 (Nov 96) pp 1977–1889*

The authors describe a preprocessor for face recognition: a velocity vector field is used to extract people from complex backgrounds, and then colour plus a few rules are used to identify the face and its major features.

054147 ‘Recognition of human front faces using knowledge-based feature extraction and neuro-fuzzy algorithm’

SY Lee, YK Ham, RHG Park, *Pattern Recognition v 29 no 11 (Nov 96) pp 1863–1876*

The authors describe an algorithm for recognising faces by applying a neural network to the coordinates of eyes, brows, nose, mouth and chin.

054148 ‘Extracting facial features by an inhibiting mechanism based on gradient distributions’

CC Lin, WC Lin, *Pattern Recognition v 29 no 12 (Dec 96) pp 2079–2101*

The authors present a new technology for detecting multiple faces against an arbitrary background. The main idea is to use the distribution of brightness gradients around bright and dark blobs as an operator — the ‘dual mask operator’ — to find eyes, nose, mouth and facial boundary. This works well in fuzzy and low-resolution images and gives results that are pleasing to the eye. For this reason, the approach is suggested as a plausible paradigm for how face recognition is actually done in the brain.

054149 ‘Securing the NHSnet’

C McCafferty, *British Journal of Healthcare Computing v 13 no 6 (Oct 96) pp 24–26*

This article describes some of the measures contemplated to protect a medical network in the UK.

054150 ‘Fighting Fraud’
M Moloney, *Cards International no 164 (Oct 96) pp 9–11*

Card fraud is rising rapidly in Latin America and is now 0.32% of turnover; organised gangs are taking over from random theft.

054151 ‘Market-Based Negotiation for Digital Library Service’
T Mullen, M Wellman, *EC 96 pp 259–269*

The University of Michigan Digital Library project has developed a mechanism for electronic auctions that match demand for system resources with supply.

054152 ‘Implementing Security policy in a Large Defence Procurement’
M Nash, R Kennett, *Apps 96 pp 15–23*

A large (35,000 user, 100 site) integrated system for the Royal Air Force supplies and engineering was believed to require the ability to simultaneously handle unclassified and classified data (i.e., MLS). However, further study revealed that the classified data was static, so it was cheaper to put the classified data on CDROMs and provide standalone computers for reading them.

054153 ‘NetWare Enhanced Security: Class C2 Security for Your Network’
NetWare Connection (Nov 96) pp 44–53

NetWare 4.11 has nearly completed its C2 evaluation. This article describes how to set up a NetWare 4.11 server to meet the C2 requirements, including physical protection of the server and required configuration parameters.

054154 ‘The AUDITCON Utility: Prove That Your Network is Secure’
NetWare Connection (Nov 96) pp 32–42

NetWare 4.11 has a highly flexible auditing system that allows pre-selection by event, by user, and for file-related events by file. Audit records are generated for accesses to files as well as to NetWare Directory Services (NDS) objects.

054155 ‘Simplifying Quotient Determination in High-Radix Modular Multiplication’
H Orup, *Proc. 12th Symposium on Computer Arithmetic (IEEE, 1995) pp 193–199*

The author presents a highly pipelined version of Montgomery multiplication for use in high-radix arithmetic. He claims 3.5 Mbit/sec for 512 bit exponentiation using 300,000 transistors and a 5nS clock.

054156 ‘Information Hiding Terminology’
B Pfitzmann, *Info Hiding 96 pp 347–350*

The author reports terminology agreed at the plenary session of the first international workshop on information hiding, whose aim is to help workers in copyright marking, steganography, covert channels and related fields to avoid confusion and ambiguity. An embedded datatype (text, image etc) is hidden in a cover datatype, under the control of a key, giving a stego datatype. The recipient can then use the key (or a related one) to extract the embedded data.

054157 ‘ISDN LAN Access: Remote access security and user profile management’
R Posch, H Leitold, F Pucher, *CMS 96 pp 222–233*

The authors describe a system for extending LANs over ISDN and B-ISDN networks with encryption and authentication. It uses the RFC 1334 crypto handshake for entity authentication and was developed for the Austrian National Bank.

054158 ‘A Methodology for Testing Intrusion Detection Systems’
NJ Puketza, K Zhang, M Chung, B Mukherjee, RA Olsson, *IEEE Transactions on Software Engineering v 22 no 10 (Oct 96) pp 719–729*

A methodology for testing intrusion detection systems has been developed at UCD and is described here. The performance objectives are set as detection scope, economy of resource usage and resilience to stress. Testing involves a representative sample of each kind of known intrusion, interspersed with varying levels and kinds of noise. The test results for one product are given as an example.

054159 'Access control system using dynamic hardwriting features'
C Schmidt, *CMS 96 pp 244–255*

The author describes a system for recognising individuals by their signature dynamics. She gives examples of velocity graphs for genuine and forged signatures and exhibits a large number of other features that can be used to spot forgeries, such as total writing time, pressure average and variance, and acceleration. Her classifier is a vector of these components, preprocessed using dynamic time warping. With 20 users, the system had a fraud rate of 1.1% and an insult rate of 9.5%.

054160 'Financial EDI Over the Internet, Case Study II: The Bank of America and Lawrence Livermore National Laboratory Pilot'
A Segev, J Porra, M Roldan, *EC 96 pp 173–190*

This is a report on an EDI pilot carried out in 1994-96 which involved Lawrence Livermore encrypting instructions for employee and supplier payments using PEM/MIME mechanisms and sending them via Internet email to Bank of America. It tabulates error rates and transmission times, and concludes that although the technology is viable, more work needs to be done on automatic error recovery (from lost messages and the like) and on key management.

054161 'The History of Subliminal Channels'
GJ Simmons, *Info Hiding 96 pp 237–256*

The author tells the story of how subliminal channels were discovered in 1978. A system was designed to enable the Russians to check that only a certain percentage of minuteman silos were occupied, without letting them know which ones. This involved sensors in the silos that authenticated their signals by concatenated encryption: first a Russian algorithm would be used, then an American one. Simmons pointed out that if the Russians chose Rabin encryption, in which each plaintext can give rise to two possible ciphertexts, then a bit of unauthorised information could be leaked; ten such bits could locate a silo and thus enable the Russians to identify which silos were full. The choice of ElGamal signatures would have had a similar effect. He also recalls that the first military implementation of RSA — for controlling access to plutonium — used a modulus of only 334 bits.

054162 'Security flaws in smart cards'
Smart Card Bulletin (Oct 96) p 1

This reports the Bellcore claim that chipcards can be attacked by inducing faults, and a denial from Mondex that it threatens their system.

054163 'Modulation and Information Hiding in Images'
JR Smith, BO Comiskey, *Info Hiding 96 pp 207–226*

The authors develop a theory of information hiding in images that sets out to quantify channel capacity and jamming margin. They describe test implementations of information hiding schemes inspired by both direct sequence and frequency hopping spread spectrum concepts. Their relative advantages are discussed; the latter is superior perceptually and has better resistance to accidental removal by compression techniques, while the former is more robust against deliberate removal attempts. They predict a co-evolutionary arms race with compression techniques.

054164 'The Intrusion Detection System AID — Architecture, and experiences in automated audit analysis'
M Sobirey, B Richter, H König, *CMS 96 pp 278–290*

The authors describe a system that performs real-time analysis of a LAN's audit data with a view to detecting intrusions. An instrumented kernel accumulates information supplemental to the usual operating system log files and replaces identities with pseudonyms to protect user privacy; this feeds data to an expert system that looks for attack signatures. They found that a perceptron based neural net was not particularly effective.

054165 'GrIDS – A Graph-Based Intrusion Detection System for Large Networks'
S Staniford-Chen, S Cheung, R Crawford, M Dilger, J Frank, J Hoagland, K Levitt, C Wee, R Yip, D Zerkle, *NISSC 96 pp 361–370*

The authors describe an intrusion detection system for networks of up to several thousand hosts. It aggregates information into 'activity graphs' with a view to rapid detection of large-scale attacks; the idea is to use heuristics to look for patterns of alerts that might result from the spread of a worm or virus across the network.

054166 'Computer Virus Response Using Autonomous Agent Technology'
CM Trently, *NISSC 96 pp 471–482*

The paper proposes that autonomous agents should be used to find and destroy computer viruses in cooperation with a central agent coordination engine.

054167 'WWW Electronic Commerce and Java Trojan Horses'
JD Tygar, A Whitten, *EC 96 pp 243–250*

The authors describe how to construct trojans in Java and use them to capture remote users' keyboard input. They create dialogue boxes that are indistinguishable from the genuine ones generated by Netscape, such as the authentication dialogue box that captures user passwords. These attacks, unlike others reported on Java, do not rely on any implementation failure. The suggested remedy is that trusted dialogue boxes should be able to be personalised easily by the user in ways that are unpredictable to an attacker.

054168 'Proposal of an automatic signature scheme using a compiler'
K Usuda, M Mambo, T Uyematsu, E Okamoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 94–101*

This paper proposes a signature scheme with which one can sign an executable program at the time of its creation. This is achieved by making use of the compiler to create both the executable program and its signature at the same time. The signature key that the compiler uses corresponds to one of its users.

054169 'Design and Management of a Secure Networked Administration System: a Practical Approach'
V Varadharajan, *NISSC 96 pp 570–580*

The author describes a design for secure management of a networked administration system. Architectural issues are discussed and the use of security services and trusted entities are outlined.

054170 'Security Issues in Emerging High Speed Networks'
V Varadharajan, P Katsavos, *NISSC 96 pp 233–249*

The security of broadband networks and services is discussed. Network service providers may wish to protect traffic in different ways from users, and so leaving all the protection to the higher layers of the protocol stack is unwise. Connection oriented Frame Relay networks are discussed in detail; it is proposed that a Secure Frame Relay Connections Layer be provided on the top of the DL-CORE sublayer to support some basic security services of interest to network operators, such as data origin authentication and connection integrity without recovery; other mechanisms, such as session key establishment, can be provided in collaboration with the call setup mechanisms.

054171 'Security Enforcement in a European Medical Device Vigilance System Network'
G Vassilacopoulos, V Chrissikopoulos, D Peppes, *IFIP 96 pp 377–386*

The authors present the conference key distribution scheme from **044605**, provide a comparative analysis, and suggest its use within a European system for reporting and investigating medical device incidents.

054172 'Cooperating Security Managers: distributed intrusion detection systems'
D White, U Pooch, *Computers and Security v 15 no 5 (96) pp 441–450*

Intrusion detection systems must cooperate to detect attackers who, for example, try one password on each of a large number of systems. This can lead to chokepoints at the controllers if the design is centralised. An alternative distributed approach is presented which balances the load more evenly. The main idea is that whenever a user connects from one host to another, the security managers start to exchange intrusion detection information about him.

054173 'Cobra and other bombes'
D Whitehead, *Cryptologia v XX no 4 (Oct 96) pp 289–307*

The author describes high-speed bombes fielded at Bletchley during 1943 to break four-rotor Enigma. These used electronic sensing of stop positions in view of the wheel momentum. A number of engineering problems are described, as well as strategies used to ensure reliability.

054174 'Protecting Collaboration'
G Wiederhold, M Bilello, V Sarathy, XL Qian, *NISSC 96 pp 561–569*

The authors describe TIHI, a system developed at Stanford for protecting health information and other assets where information has to be selectively withheld from colleagues rather than protected from enemies. Each server has a security mediator which filters incoming requests according to a set of rules and shares only the appropriate information. In many circumstances this may be equivalent to view-based mandatory access control.

054175 'Mobile Phone Fraud - Are GSM Networks Secure?'
K Wong, *Computer Fraud and Security Bulletin (Nov 96) pp 11–18*

The added-value features of GSM phones help criminals in various ways. For example, a call-sell operator can initiate a conference call between two analogue lines, and then drop out; and the advice-of-charge facility lets him know how much money to demand from his client. Proposed new services, such as SIM based banking and prepaid SIMs that are rechargeable over the air, will open up still more vulnerabilities. False name service applications are becoming more sophisticated; the targets are typically people who have just moved house. Insider frauds include enabling SIMs with no corresponding billing address, and fraudulently obtained SIMs are used together with corporate PABX fraud techniques to make completely traceless calls.

054176 'Mobile Phone Fraud'
K Wong, *Datenschutz und Datensicherheit v 20 no 11 (Nov 96) pp 736–741*

This article covers essentially the same ground as **054175** above.

054177 'Legal Signatures and Proof in Electronic Commerce'
B Wright, *EC 96 pp 67–75*

The author describes PENOP, a system that enables users to sign documents using a signature tablet; the system then authenticates the statistics of the act of signing with the date and time and the user and equipment IDs. It is proposed as a means of authenticating US tax returns.

2 Operating System and Database Security

054201 ‘Applying the TCSEC Guidelines to a Real-Time Embedded System Environment’
J Alves-Foss, D Frincke, G Saghi, *NISSC 96 pp 89–97*

The authors review ways to adjust TCSEC requirements to real-time embedded systems such as avionics. Trusted path and audit are problematic in this case, and the proliferation of sensitivity labels will depend on whether we try to separate just users or processes as well.

054202 ‘Covert Channel Analysis for Stubs’
MS Anderson, MA Ozols, *Info Hiding 96 pp 95–113*

The authors present a covert channel analysis for the Stubs network security devices developed by DSTO in Australia. The claim is that the use of strong military crypto to seal messages limits an attacker in the ‘high’ part of the network to manipulating the supply of sealed messages. Seal timestamps limit this manipulation to a short time window. A formal analysis is given of the channel capacity under various attack and noise assumptions. This leaves open the possibility of hidden messages in text that passes human reviewers. They suggest a ‘blind man’s filter’ — a filter that will not pass information (such as minor font changes) if they are such that the human reviewer would not discern them; a suggested technique is OCR scanning.

054203 ‘Starlight: Interactive Link’
M Anderson, C North, J Griffin, R Milner, J Yesberg, K Yiu, *Apps 96 pp 55–63*

The authors describe a way of running windows of two classifications on untrusted Unix workstations. A high computer displays the data and runs X applications, a low computer runs X applications, and a ‘Starlight’ device connects them. The keyboard and mouse are connected to this device, and the user selects whether the input should be treated as high or low using a physical switch (thus routing the input to the appropriate workstation). A surrogate X server on the low machine allows unmodified X clients to pass information to high, and a surrogate X client on the high machine allows the real X server to run unmodified with the low X clients. The system does not provide visible window labels, but a device attached to the monitor provides LEDs to indicate whether the user is operating at high or low.

054204 ‘Use of a Taxonomy of Security Faults’
T Aslam, I Krsul, EH Spafford, *NISSC 96 pp 551–560*

The authors define a classification of security faults within Unix environments. Coding faults include synchronisation errors and condition validation errors; emergent faults then configuration errors and environment faults. A database of vulnerabilities was built using this classification; it is being used to prototype tools for failure detection and protection.

054205 ‘Design Analysis in Evaluations Against the TCSEC C2 Criteria’
F Belvin, D Bodeau, S Razvi, *NISSC 96 pp 67–75*

The authors analyse the activities involved in doing a design analysis for a C2 evaluation, with a view to providing input to the evolution of the Common Criteria.

054206 ‘Generic Model Interpretations: POSIX.1 and SQL’
DE Bell, *NISSC 96 pp 378–388*

The paper presents generic model interpretations of POSIX.1 and of SQL to ease the correspondence control between top-Level specifications and the formal security policy model for a TCSEC evaluation at B2 or above.

054207 'A Decentralized Temporal Authorization Model'
E Bertino, C Bettini, E Ferrari, P Samarati, *IFIP 96 pp 271–280*

The authors present a model that allows for the authorisation of database transactions within a specified time interval; both positive and negative authorisations are supported. Recursive revocation considering also a modification of authorisation time intervals is enforced.

054208 'Checking for Race Conditions in File Accesses'
M Bishop, M Dilger, *Computing Systems Usenix v 9 no 2 (Spring 1996) pp 131–152*

Time of Check to Time of Use (TOCTTOU) errors can occur in privileged programs (such as setuid root UNIX utilities) when the results of one system call are used to determine the actions of a second system call, and the potential exists for a user to change the environment between the two to yield a security flaw. While it is impossible to build a perfect static source code analysis tool, the authors describe a tool that finds many potential TOCTTOU flaws, as well as some false alarms. Appendices show the results of running the tool on the SENDMAIL source code, which revealed a half dozen actual TOCTTOU flaws as well as a dozen false alarms.

054209 'An Isolated Network for Research'
M Bishop, LT Heberlein, *NISSC 96 pp 349–360*

The Information Warfare Forensic Center at UC Davis has a lot of data on actual attacks which is very sensitive. It also conducts penetration tests on fielded equipment and proposed patches. An MLS Unix network has been set up in which the Internet is Low and the research network High; this is enforced using removable physical media which are the only way to get information from Low to High. This means that only vendor-implemented protocols need be used.

054210 'MLS DBMS Interoperability Study'
RK Burns, YF Koh, *NISSC 96 pp 495–504*

The interoperability of commercial-off-the-shelf products in a multilevel environment was examined by the USAF Rome Laboratory. The Open Database Connectivity interface from Intersolv, PLEX from Oracle, OmniSQL Gateway from Sybase, and OmniReplicator from Praxis were evaluated. Problems encountered include loss of trust in sensitivity labels (the definitions are different, and there is no universal API), and multilevel network infrastructure issues.

054211 'Security Implications of the Choice of Distributed Database Management System Model: Relational vs. Object-Oriented'
SP Coy, *NISSC 96 pp 428–437*

The author reviews the strengths and weaknesses of relational and object-oriented databases in a distributed environment. The relational model is considered a better choice, as it is more mature; the object-oriented one still lacks important standards, and many marketed systems are simple relational ones with a few object features bolted on top.

054212 'Models and tools for quantitative assessment of operational security'
M Dacier, Y Deswarte, M Kaâniche, *IFIP 96 pp 177–186*

The authors describe assessing operational security by modeling a system as a privilege graph. Nodes represent users or groups with privileges, edges the possibility to extend privileges through given operating system features. The privilege graph is transformed into the potential intrusion state graph through a Markov model based on the mean time and effort to reach the target. An automated tool for performing these assessments on Unix systems is also described.

054213 'Controlling Causal Dependencies over a Secure Network'
B d'Ausbourg, C Calas, *Journal of Computer Security v 4 no 1 (Sep 96) pp 3–25*

This journal version of **041210** describes a practical multilevel LAN. The approach is based on a control of causal dependencies that exhaustively enforces controls on all information flows. Formal definitions and security conditions are presented; an architecture is then proposed and a secure medium access control protocol is defined. The paper also reports results on the protocol performance, by discussing three different cases, and presents an example of the use of this protocol for a secure distributed file system.

054214 'Asymmetric Isolation'
J Davidson, *Apps 96 pp 44–54*

A one-way device using fiber optic cabling allows writing from a low system to a high system without acknowledgments, and hence no potential for covert channels. Some configuration file manipulation was necessary to prevent confusing systems as to how to route packets. The low system must self-throttle to avoid overrunning the high system, which could lose data as a result.

054215 'A High-Performance Hardware-Based High Assurance Trusted Windowing System'
J Epstein, *NISSC 96 pp 12–21*

The author describes Trusted X and discusses why it runs so slowly on many machines. He proposes that a low cost ($300) card could be built that would support trusted windowing on Intel architecture machines. By replacing the software trusted display managers for each window by a dedicated hardware mediating merge unit, performance problems could be eliminated and other benefits (such as improved video capabilities) might also be realised.

054216 'The security architecture of IRO-DB'
W Eßmayr, F Kastner, G Pernul, AM Tjoa, *IFIP 96 pp 249–258*

The authors present a taxonomy of concepts and design choices for secure interoperation of relational and object-oriented databases. Discretionary access control policy for federated databases supports positive, negative and implied authorisations, with a conflict resolution procedure.

054217 'Security for Mobile Agents: Issues and Requirements'
WM Farmer, JD Guttman, V Swarup, *NISSC 96 pp 591–597*

New threats are introduced by the use of mobile agents (after all, one of the earliest examples was the Internet worm). Protection goals are evaluated here according to their feasibility. Some things are easy (such as using code signing to authenticate authors) and other things are impossible (such as preventing tampering with interpreters). Useful research goals are in the category of possible but hard — such as safe languages and support for control of agents' state.

054218 'Migh-Level Security Issues in Multimedia/Hypertext Systems'
EB Fernandez, KR Nair, MM Larrondo-Petrie, Y Xu, *CMS 96 pp 13–24*

The authors talk about the possible combinations of mandatory and discretionary access policies in multimedia systems.

054219 'Developing Secure Objects'
D Fricke, *NISSC 96 pp 410–419*

The effects of object oriented design on the development of secure systems are discussed; techniques for developing libraries and operating untrusted objects safely are suggested. Wrappers, templates and base classes can all help in adding protection to commercial off-the-shelf systems while containing the overall policy enforcement effort.

054220 ‘Designing & Operating a Multilevel Security Network Using Standard Commercial Products’
RA Griffith, ME McGregor, *NISSC 96 pp 515–525*

The authors describe the experience of Barksdale AFB in adding commercial off-the-shelf PCs to a B1 network, and some of the problems encountered.

054221 ‘MISSI Compliance for Commercial-Off-The-Shelf Firewalls’
M Hale, T Mannarino, *NISSC 96 pp 505–514*

The authors describe the NSA approach to the evaluation of Internet firewalls for use in MLS environments. The MISSI Compliance Program includes interoperability testing as well; the goal is that both evaluation and testing should take no more than 90 days. Firewalls evaluated in this way are targeted at protecting sensitive but unclassified data. However, vendors will have to agree to integrate Fortezza into their product to be admitted into the program.

054222 ‘Hiding Data in the OSI Network Model’
TG Handel, MT Sandford, *Info Hiding 96 pp 23–38*

The authors present a systematic analysis of the covert channel capacity of the OSI network model. Some of the available mechanisms at each of the seven layers are described, and estimates given of the overall bandwidth. They argue that eliminating this covert bandwidth would be an immense task and could only be partially automated.

054223 ‘Use of the Zachman Architecture for Security Engineering’
RR Henning, *NISSC 96 pp 398–409*

Security policy development should follow a top-down approach and start from user expectations such as ‘only mission managers can modify plans’. An engineering approach that supports this is described; it facilitates refinement of policy from top-level statements down to the enforcing mechanisms using an automated tool based on a framework for systems modelling by Zachman. It helps in reconciling security requirements derived from doctrine with those from pragmatic user concerns.

054224 ‘E4 ITSEC Evaluation of PR/SM on ES/9000 Processors’
N Htoo-Mosher, R Nasser, N Zunic, J Straw, *NISSC 96 pp 1–11*

The IBM Processor Resource/System Manager was the first to achieve the E4 ITSEC rating; it enables one single physical ES/9000 mainframe to be configured as several distinct logical machines (partitions). The security functionality and evaluation process are described.

054225 ‘Securely executing multilevel transactions’
S Jajodia, KP Smith, BT Blaustein, L Notargiacomo, *IFIP 96 pp 259–270*

The authors describe a multilevel transaction model and a low-first algorithm which enables any multilevel transaction to be converted to one whose only dependency is low writes followed by high reads. Such transactions can be executed with the MUSET DBMS trusted facility, which combines just such a low-first multiversion timestamp ordering algorithm with trusted cacheing.

054226 ‘A Case Study of Two NRL Pump Prototypes’
M Kang, I Moskowitz, B Montrose, J Parsonese, *Apps 96 pp 32–43*

The NRL pump is a secure one-way device that allows information flow from low to high while maintaining performance and minimizing covert channels. Two versions were built: the E-pump which is an application layer pump implemented as trusted software running on a Wang XTS-300, and the D-pump which was built on DOS as a transport layer pump. The E-pump does not lose messages because it waits until the high application acknowledges receipt before discarding a message, while the D-pump (because it operates at the transport layer) can only wait for acknowledgment by the receiving system. The D-pump performed better, since it was running on a system with much lower overhead; but the authors concluded that the applications layer is the right place to build a pump, given a more efficient high-assurance system.

054227 'Extended Capability: A Simple Way to Enforce Complex Security Policies in Distributed Systems'
IL Kao, R Chow, *NISSC 96 pp 598–606*

The authors describe e-cap, a new approach to enforcing complex policies in a capability based system. Object servers mediate requests for access and are also responsible for all capability operations. Strongly typed systems, n-time tickets and access sequencing are supported, and capability propagation, revocation and distribution also discussed.

054228 'PLASMA — Platform for Secure Multimedia Applications'
A Krannig, *CMS 96 pp 1–12*

Plasma is a platform for secure object-oriented multimedia systems designed by the Fraunhofer Institute. Crypto mechanisms support secure object containers and are used to negotiate a cooperative security policy between two partners begin to communicate. The implementations of abstract concepts such as digital signature may vary, for example, between audio and video objects; different platforms might use mechanisms such as PGP, PKCS or SecuDe. However, the system hides this detail from the user applications. Each principal has a personal environment that may be implemented using a smart card.

054229 'Using RAD Tools to Develop Secure Client/Server Applications'
JR Lemieux, *Computers and Security v 15 no 4 (96) pp 289–295*

The author points out some of the protection problems arising from the use of 'rapid application development' tools. Networked SQL is particularly problematic; one approach is to centralise transaction processing on the server.

054230 'Covert Channels — A Context-Based View'
C Meadows, I Moskowitz, *Info Hiding 96 pp 73–93*

The authors propose to classify covert channels according to the context in which they occur rather than the mechanisms that they employ. The main distinction is between low-to-high service, high-to-low service, shared service and incomparable service. The claimed advantage of this method is that covert channels arising in similar contexts can be dealt with in similar ways. Some compositional properties are discussed in the context of the NRL pump.

054231 'A Rough Guide to the Security features of Novell NetWare 3.xx'
C Nelms, *Computer Audit Update (Nov 96) pp 8–12*

This article gives an overview of Netware's security features and architecture.

054232 'Using Workflow to Enhance Security in Federated Databases'
MS Olivier, *CMS 96 pp 60–71*

The author describes how to build protection mechanisms into workflow systems. These organise processing according to which tasks can only be performed after certain other tasks have been accomplished. Access control lists can be inserted into workflow scripts by a TCB, which can also handle audit and alarm messages.

054233 'Design of Secure Medical Database Systems'
G Pangalos, M Khair, *IFIP 96 pp 387–401*

This paper presents a healthcare database design with tuple-level granularity within the multilevel security model. Write-down is also allowed; the user's level of clearance is combined with a role-based need-to-know discretionary type of access to data. An experimental implementation in a hospital is described.

054234 ‘Non-interference through Determinism’

AW Roscoe, JCP Woodcock, L Wulf, *Journal of Computer Security v 4 no 1 (Sep 96) pp 27–53*

One classical problem of some security requirements such as information flow controls is the difficulty of modeling them as abstract specifications that can be preserved through refinements. In this journal version of **041233**, the authors propose a solution where the abstract specifications are first translated in a process-algebraic model (CSP) and then increased to include security specifications. The basic idea is that low level users’ virtual machines must be deterministic. An example is given with abstract specifications written in Z.

054235 ‘Windows NT System-Call Hooking’

M Russinovich, B Cogswell, *Dr Dobbs’ Journal no 261 (Jan 97) pp 42–46 & 82*

This article describes how to intercept and log all system calls from Windows NT to the registry using undocumented features of the kernel. This allows very fine-grained control for intrusion detection and other applications; C source code is provided.

054236 ‘Security mechanism of privacy enhanced shared file system suitable for mobile access’

A Shimbo, T Takahashi, M Murota, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 102–109*

This paper proposes a secure file system for mobile hosts. Files are encrypted and decrypted only by clients; this is invisible to the server, which asynchronously receives the edited parts of ciphertext and merges them.

054237 ‘IGOR: The Intelligence Guard for ONI Replication’

RW Shore, *NISSC 96 pp 607–619*

The author presents an automated dual-host mediator for database replication through a security barrier. The current accredited installation operates in the high-to-low mode and is built on standard Solaris. However, the master and replicated databases could run on different platforms.

054238 ‘Malicious Data and Computer Security’

WO Sibert, *NISSC 96 pp 334–341*

The author surveys system vulnerabilities that arise from ‘malicious data’ threats, such as macro viruses and objects designed to cause buffer overflows or other exploitable system actions. At present, obscurity plays a greater role than one would like; both exploitation and defence are difficult.

054239 ‘Mandatory Protection for Internet Server Software’

R Smith, *Apps 96 pp 178–184*

Three different models of ”mandatory” protection are proposed for firewalls: the change root (chroot) facility, traditional MAC, and type enforcement. Chroot allows creation of restricted portions of a file system that an application can run in, but doesn’t control access to resources such as sockets. MAC is much stronger than chroot, as it allows segregation of applications within the same computer. Type enforcement restricts what applications can do, and is claimed to be stronger than MAC.

054240 ‘Deriving Security Requirements for Applications on Trusted Systems’

R Spencer, *NISSC 96 pp 420–427*

A process for refining a security policy into detailed application requirements is discussed. It was applied to a secure network server and used to incorporate new application requirements when the system was enhanced. The policy model incorporated elements of MLS and integrity controls. Examples of the refinement of specific control primitives are given.

054241 'Trusted Process Classes'
WL Steffan, JD Clow, *NISSC 96 pp 54–66*

The authors present a methodology to manage the trade-offs between protection requirements and mission performance. They discuss the circumstances in which one might override mandatory and discretionary access controls, the tranquility principle and audit requirements. Programming confinement rules are also suggested; for example, software running at Top Secret would have to be written and checked by people cleared to this level..

054242 'An Evaluation of the Java Security Model'
A Sterbenz, *Apps 96 pp 2–14*

This paper describes the Java security model (rather than the actual implementation bugs). This turns out to be a four layer model with the language, virtual machine, runtime library, and runtime environment. Flaws in each of the layers can result in security violations, as the overall security architecture is quite fragile.

054243 'The Privilege Control Table Toolkit: An Implementation of the System Build Approach'
TR Woodall, R Gotfried, *NISSC 96 pp 389–397*

This article describes the development of a toolkit for information flow modelling of multilevel secure avionics software. The toolkit follows on from the work described in **031204**; it is not just a development tool, but a vital part of the distributed TCB. It gathers interface information, checks hardware status and data consistency, builds tables for mediation lookup and system management, and creates a log file.

054244 'A Discretionary Security Model for Object-Oriented Environments'
WJ van Rensburg, MS Olivier, *IFIP 96 pp 306–316*

The authors present a security model in which capabilities (as objects) filter access to protected objects. An object owner can define more than one capability for the same object.

054245 'Security Model for Distributed Object Framework and its Applicability to CORBA'
V Varadharajan, T Hardjono, *IFIP 96 pp 452–463*

The authors discuss how to incorporate a distributed object security model from **051242** in the CORBA framework. Its services include user and object authentication, secure creation and deletion of objects, access control and the delegation of authorisation between objects.

054246 'MoFAC: A Model for Fine-grained Access Control'
JS von Solms, MS Olivier, SH von Solms, *IFIP 96 pp 295–305*

The authors suggest a fine grained access control model in which object groups have permitted transactions associated with user groups (roles).

3 Security Management and Policy

054301 ‘Controversy — Rejoinder: Independent One-Time Passwords’
J Adams, *Computing Systems Usenix v 9 no 3 (Summer 96) pp 255–256*

This is a response from the management of SecurID to criticism in **051434**; it claims that their algorithms are secure and their devices tamper proof.

054302 ‘Encryption and Interception’
MB Andersen, P Landrock, *Computer Law and Security Report v 12 no 6 (Nov/Dec 96) pp 342–348*

The authors review some of the recent legal history of cryptography including police concern over GSM in the early 90’s, the NSA’s assignment of the DSA patent to PKP, the September 95 Council of Europe initiative, the SOGIS proposal and the OECD initiative. They discuss the alternatives open to government, such as the reversal of the burden of proof where criminal defendants do not give access to possibly relevant data or traffic.

054303 ‘A Taxonomy for Analyzing Hazards to Information Systems’
R Baskerville, *IFIP 96 pp 167–176*

The author introduces the term ‘hazard’ to refer to a realised or potential event that would harm a system. Hazards are clasified by dividing them into accidental and deliberate, the latter being subdivided according to mode and motive.

054304 ‘Security Through Process Management’
JL Bayuk, *NISSC 96 pp 323–333*

The information security management process is described, partitioned into policy, awareness, access, monitoring, compliance, and strategy.

054305 ‘Design Analysis in Evaluations Against the TCSEC C2 Criteria’
F Belvin, D Bodeau, S Razvi, *NISSC 96 pp 67–75*

The authors analyse the activities involved in doing a design analysis for a C2 evaluation, with a view to providing input to the evolution of the Common Criteria.

054306 ‘America’s Electronic Godfathers’
A Bequai, *Computer Audit Update (Oct 96) pp 36–39*

The author talks about the relationship of the mob to the US IT industry and claims that more and more technology is being used in crimes like bank fraud.

054307 ‘High-tech mercenaries: hackers turned consultants’
A Bequai, *Computer Audit Update (Nov 96) pp 23–27*

This article emphasises the risks of hiring former hackers as consultants and suggests the due diligence that a company might employ in consultant screening.

054308 ‘Legal Developments for the Internet’
A Bequai, *Computer Audit Update (Dec 96) pp 22–26*

This describes some US federal laws that bear on Internet traffic.

054309 ‘Rise of the mobile state: organised crime in the 21st century’
A Bequai, *NISSC 96 pp iii–ix*

The author describes ways in which information technology may open up new opportunities for organised crime syndicates. He compares them to the Mongols of antiquity: a mobile state.

054310 ‘HMOS: Her Majesty’s Orthography Service’
T Berson, *Info Hiding 96 p 345*

The author presents a spoof announcement of a government policy that digital objects should be submitted to an official censor to remove noise, perform spell checking, straighten out grammar, and so on. The implication of this article is that so long as mistakes in communication are permitted, covert bandwidth is available for the enemies of the state to use.

054311 ‘Datenschutz- und Datensicherheitskonzept für die Telemetropole Ulm / Ostwürttemberg / Oberschwaben’
A Böhm, G Kongehl, *Datenschutz und Datensicherheit v 20 no 12 (Dec 96) pp 716–722*

This article describes a data protection oriented risk analysis and security policy developed for a regional German networking project.

054312 ‘Der Identity-Protector’
J Borking, *Datenschutz und Datensicherheit v 20 no 11 (Nov 96) pp 654–658*

The author stresses the advantages that can be gained from assigning pseudonyms to users; data protection and privacy assurance can be confined to a very small part of the overall system.

054313 ‘Intellectual Property Rights and Computer Software’
DE Bowman, *NISSC 96 pp 296–305*

Intellectual property laws and their application to software protection are discussed from both the US and international viewpoints.

054314 ‘EDI Moves from the VAN to the Internet’
B Bradford, *NISSC 96 pp 98–108*

The author discusses whether EDI applications might move from VANS to the Internet and goes into some of the security considerations.

054315 ‘B is for Business: Mandatory Security Criteria and the OECD Guidelines for Information Systems Security’
WJ Caelli, *NISSC 96 pp 152–162*

The author argues that in order to satisfy the 1992 OECD guidelines on computer security, mandatory protection along the lines of TCSEC should be offered in commercial products. He recognises that cost and time-to-market considerations may mean that this can only be achieved under legal compulsion.

054316 ‘Security Issues for Telecommuting’
LJ Carnahan, B Guttman, *NISSC 96 pp 342–348*

The paper outlines some of the risks in telecommuting and suggests some means of protection.

054317 ‘Feeling Secure’
L Carroll, *Smart Card Bulletin (Oct 96) p IV*

The German Bundesbank’s view on chip cards is that no single security measure is sufficient; designers need to combine tamper resistance, crypto, and policy controls intelligently. It also feels that electronic cash should only be issued by banks.

054318 ‘Cryptographic Controls — The Eternal Triangle’
AJ Clark, *Computers and Security v 15 no 7 (96) pp 576–584*

This article describes crypto controls in Europe, including their evolution from COCOM through the Wassenaar agreement.

054319 ‘A report from the United States — part 1’
Computer Law and Security Report v 12 no 6 (Nov/Dec 96) pp 361–367

This is an extract from a book on the legal aspects of computer security in the USA.

054320 ‘Who controls your encryption’
Computer Audit Update (Oct 96) pp 40–45

This article discusses the increasing interest of European data protectors in privacy-enhancing technologies. It asks how companies can argue that the likes of smartcard-based pseudonym systems are too expensive when they hand out smartcards in marketing promotions. It claims that there are links to the issue of trusted third parties —

as these would presumably know the name behind the card and release it to the police in cases of fraud.

054321 'Operation Chain Link: The Deployment of a Firewall at Hanscom Air Force Base'
J Connolly, *Apps 96 pp 170–177*

The author reports the deployment of a firewall at an air force base. He first surveyed the user community to find what network services were needed, and what the network security policy should be. Using network monitors, he discovered several unexpected services in use. Before installing the firewall, it was staged in a lab using actual IP addresses, which helped find several problems before the system was turned on. Major concerns include ongoing maintenance due to personnel turnover, the presence of (unmonitored) communications to other military bases, and the presence of modem pools.

054322 'Internet Firewalls Policy Development and Technology Choices'
LJ D'Alotto, *NISSC 96 pp 259–266*

The author argues that a carefully thought through reliable security policy is the only way to cut through the current confusion and 'feature wars' in the firewall market.

054323 'Thesen zur Modernisierung des Datenschutzrechts'
U Dammann, *Datenschutzberater v 20 no 10 (15/10/96) pp 1–6*

The author proposes a number of changes in German data protection law to simplify it, treat public and private sectors equally, tackle the proliferation of chip card systems, prevent one-sided contracts (especially in banking and finance), and deal with aspects of the EU directive.

054324 'Sniffers — The Whole Story'
J David, *Network Security (Oct 96) pp 9–13*

The author discusses how network analysers work and can be used to harvest passwords; he points out that active hubs can limit the scope of this threat.

054325 'The Future of PGP on the Internet'
J David, *Network Security (Nov 96) pp 9–12*

The author points out that the main effect of US crypto export controls has been to give PGP a near total monopoly of international public key cryptography. Even if export controls are lifted, users will still need some motivation to replace something that already works adequately.

054326 'Smart Card Threat: From Bellcore'
DW Davies, *Smart Card News v 5 no 11 (Nov 96) pp 217–218*

A leading UK banking security consultant attacks the recent Bellcore announcement of attacks based on inducing faults in smartcards as not new, and as 'wrong and misleading'.

054327 'Establishing Big Brother Using Covert Channels and Other Covert Techniques'
Y Desmedt, *Info Hiding 96 pp 65–71*

The author discusses a number of ways in which covert technologies that are initially deployed for relatively mundane purposes, such as copyright protection, can end up being subverted to provide the means of surveillance. This problem could become progressively more serious as more and more everyday objects become endowed with some kind of intelligence and communications capability.

054328 'Improving Your Organisation's Attitude and Commitment to Security'
J Dickie, *Computer Audit Update (Oct 96) pp 28–35*

The author presents a number of ideas for raising security awareness in organisations.

054329 'Medical confidentiality'
C Dover, *Computer Audit Update (Nov 96) pp 28–30*

This paper describes some aspects of the recent dispute between British doctors and the authorities over the confidentiality of medical records.

054330 'Applying the Eight-Stage Risk Assessment Methodology to Firewalls'
DL Drake, KL Morse, *NISSC 96 pp 276–287*

The authors apply their methodology from **034320** to firewalls, and stress the importance of a proper security policy.

054331 'A Framework for Dealing with and Specifying Security Requirements in Information Systems'
E Dubois, S Wu, *IFIP 96 pp 88–99*

The authors suggest using a requirements engineering methodology called Albert for specifying security as one of the components of an information system. They provide a small worked example; a hypothetical Belgian phone banking system.

054332 'The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)'
J Eller, M Mastrorocco, BC Stauffer, *NISSC 96 pp 46–53*

The DoD has a new standard process for certificating and accrediting systems. This is described and its relationship with existing NCSC procedures (TG-031) is explained. The new process focusses on the infrastructure rather than its components.

054333 'Integrated Circuit Card Standards and Specifications'
DB Everett, *Smart Card News v 5; part 1: no 10 (Oct 96) pp 196–198; part 2: no 12 (Dec 96) pp 236–239*

These articles review the contents of ISO 7816, the standard for smartcards.

054334 'Forschungsbedarf und aktuelle Forschungsarbeiten bei Siemens'
J Fichtner, *Datenschutz und Datensicherheit v 20 no 11 (Nov 96) pp 674–676*

This is an overview of Siemens' security research and development activities.

054335 'E-cash lays the foundations for private corporate currency creation'
Financial technology International Bulletin v 14 no 2 (Oct 96) pp 6–7

This article points out that Hayek predicted electronic cash — and advocated privatising money — years ago.

054336 'RNIB to lobby parliament on bank chip standards'
Financial technology International Bulletin v 14 no 3 (Nov 96) p 5

The Royal National Institute for the Blind is lobbying for electronic cash systems to be easy for visually impaired people to use. They particularly favour the use of contactless smartcards.

054337 'The Information Security Chain in a Company'
T Finne, *Computers and Security v 15 no 4 (96) pp 297–316*

This is a long checklist for use in security assessment of a commercial system.

054338 'The Certification of the Interim Key Escrow System'
E Flahavin, R Snouffer, *NISSC 96 pp 26–33*

The authors describe the accreditation of the 'Clipper' system according to FIPS

PUB 102 and an NSA handbook. This involved a number of short subsystem tests, followed by a wiretap and key recovery exercise performed at an FBI facility.

054339 'Signed, sealed, delivered?'
G Flood, *Computer Business Review v 4 no 10 (Oct 96) pp 38–39*

This article describes some of the ways in which companies hope to make money out of digital signatures.

054340 'Lessons Learned: An Examination of Cryptographic Security Services in a Federal Automated Information System'
J Foti, D Dodson, S Keller, *NISSC 96 pp 288–295*

The authors relate the lessons learned from a NIST review of cryptographic security at a federal agency. These are in the form of a checklist of robustness principles for the design and operation of a scalable key management system.

054341 'Finger minutiae system leaps the 1:100,000 false refusal barrier'
Fraud Watch Q4 96 pp 6–7

One fingerprint recognition system supplier claims that he can meet the 1 in 100,000 insult rate criterion set by the banks; his equipment is being tested by Mastercard.

054342 'Scientists warn of smart card system vulnerability'
Fraud Watch Q4 96 pp 1–2

This article presents a management level overview of the work of Anderson and Kuhn on tamper resistance cited above in **054102**.

054343 'Legal Aspects of Ice-Pick Testing'
BC Gabrielson, *NISSC 96 pp 313–322*

The paper discusses the legal and administrative problems of using a network vulnerability testing tool (Ice-Pick) in the US Navy, and describes what a tester should do to remain within the rules.

054344 'Digital Currency and Public Networks: so what if it is secure, is it money?'
JDP Gauntt, *EC 96 pp 77–86*

The author argues that digital money should be backed by a commodity, namely the bandwidth of the underlying network.

054345 'Delivery and Installation of Software: Disputes and the burden of proof'
L Golvers, *IFIP 96 pp 142–150*

The author stresses the importance of evidence in disputes concerning software delivery and installation. The suggested solutions include detailed delivery notes and cryptographic means to assure conformity of the supply. Proper installation, with formal installation protocols and configuration control, are also advised and discussed.

054346 'Real World Anti-Virus Product Reviews and Evaluations — The Current State of Affairs'
S Gordon, R Ford, *NISSC 96 pp 526–538*

The authors discuss the pros and cons of getting information on anti-virus products from employees, general magazines, trade magazines, bodies such as the NCSA, academics and ITSEC evaluators.

054347 'An International Standard for the Labeling of Digital Objects'
VE Hampel, *NISSC 96 pp 109–122*

The author discusses ways of integrating copyright management and consumer protection systems; he proposes that these be based on the NSA Message Security Protocol, with an official X509 directory that would enable consumers to check that digital objects were genuine.

054348 'Security issues in mobile information networks'
T Hardjono, J Seberry, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 7 (1996), pp 1021–1026*

This paper argues that security will be a major area for future developments in mobile computing, and briefly discusses the potential security problems in a mobile computing environment.

054349 'Computer Security in China'
EB Heinlein, *Computers and Security v 15 no 5 (96) pp 396–375*

This reports a US trade delegation to China on computer security. It briefly describes some of the players in China and a number of the regulations about computer protection and the regulation of Internet access.

054350 'Verschlüsselung in der öffentliche Verwaltung'
A Heuser, *Datenschutz und Datensicherheit v 20 no 11 (Nov 96) pp 659–660*

A senior official at the German information security agency sets out guidelines for the use of encryption in the public sector.

054351 'Protecting Business Information'
S Hinde, *Computer Audit Update (Dec 96) pp 2–5*

This article describes a recent UK government report that seeks to have commercial firms adopt a version of the Bell-LaPadula security policy.

054352 'The counterfactual history of no Ultra'
H Hinsley, *Cryptologia v XX no 4 (Oct 96) pp 308–324*

The author argues that had Britain not managed to break the Enigma during the second world war, then the war would have lasted for between two and four years longer than it did.

054353 'A practical solution to the complex human issues of information security design'
J Hitchings, *IFIP 96 pp 3–12*

A methodology for risk identification is described. This 'Virtual Methodology' considers interactions with other systems and users, and was applied to analysing risk and designing controls at a post implementation stage review of a placing support system at Lloyd's of London.

054354 'The Use of Business Process Models for Security Design in Organisations'
R Holbein, S Teufel, K Bauknecht, *IFIP 96 pp 13–22*

This paper describes a security design method based on use of 'Business Process Models'. Transaction based models can be extended with organisational roles of agents, and role based access rights can then be derived. Prototype implementation and case studies are yet to be evaluated.

054355 'New Security Paradigms: Orthodoxy and Heresy'
HH Hosmer, *IFIP 96 pp 61–73*

This talk elaborates on the importance of new paradigms in information security. The past include those related to the Orange Book and the Rainbow Series in general. The coming are within the Common Criteria framework; in crossing from defense to offense in the Information Warfare strategies, and in risk management paradigms.

054356 'A human approach to security management in HealthCare'
H James, K Andronis, W Paul, *IFIP 96 pp 365–376*

A model for developing security measures and management for an Australian hospital environment is described; it emphasises a user-oriented approach.

054357 ‘Protection money’
P Jones, *Computer Business Review v 4 no 12 (Dec 96) pp 31–36*

The anti-virus business is becoming international as the net smooths out regional variations in virus populations; it is also consolidating. In 1994, the market was worth $71.3m, with Symantec holding 49.5% of this and McAfee 43.5%. Some people had feared that the market would collapse as DOS was replaced by Windows 95 and NT; but the arrival of macro viruses has saved it, and the net has greatly increased the rate of information exchange. Mail filters may shortly start to play a role; but IBM’s direction is to try and develop the analogue of an immune system.

054358 ‘Industrial Espionage Today and Information Wars of Tomorrow’
PM Joyal, *NISSC 96 pp 139–151*

The paper reviews some incidents of trade-related espionage between the US, France, Japan and Russia; it includes a CIA assessment of Japanese intelligence priorities and also mentions commercial espionage, e.g of Hitachi against IBM.

054359 ‘Configuration Management in Security Related Software Engineering Processes’
K Keus, T Gast, *NISSC 96 pp 34–45*

Software configuration management for critical systems is discussed, with particular emphasis on the requirements of ISO 9000 and ITSEC/CC.

054360 ‘An analyst’s view of IS security’
EA Kiountouzis, SA Kokolakis, *IFIP 96 pp 23–35*

The authors discuss divergence of understanding and definitions of Information System (IS), Information Technology and IS Security. Holistic (‘outside-looking-in’) and systemic (‘inside’-looking-out) approaches towards IS security are contrasted, and the author asks whether a Kuhnian crisis is developing in security models.

054361 ‘Aspects of Data Security in Wide Area Academic Networks’
J Kodl, J Přibyl, *Pragocrypt 96 part 2 pp 35–44*

This article reports on some security implementation work done under the auspices of the Czech academic network.

054362 ‘Is there a need for new information security models?’
SA Kokolakis, *CMS 96 pp 256–267*

The author presents a management level summary of a number of security policy models, including Bell-LaPadula, Clark-Wilson, Biba and Chinese Wall. He argues that object oriented and multimedia systems require new or modified models.

054363 ‘A survey of cryptography laws and regulations’
BJ Koops, *Computer Law and Security Report v 12 no 6 (Nov/Dec 96) pp 349–355*

The author reviews the COCOM and Wassenaar agreements, the US ITAR rules, and the domestic crypto laws of a number of countries. He also describes a number of initiatives at the European level and by the International Chamber of Commerce.

054364 ‘Canada’s computer crime laws: Ten years of experience’
MPJ Kratz, *IFIP 96 pp 122–141*

The author provides an overview of relevant Canadian legislation and computer crime cases. These include criminal provisions of copyright law and telecommunication service theft.

054365 ‘GSSP (Generally-Accepted System Security Principles): A Trip to Abilene?’
AR Krull, *Computers and Security v 15 no 7 (96) pp 567–575*

The author argues that the GSSP standards initiative is redundant, merely repeating work already done by the OECD, COBIT and BS7700.

054366 'Activating dynamic countermeasures to reduce risk'
L Labuschagne, JHP Eloff, *IFIP 96 pp 187–196*

The authors review ways of selecting security measures, categorise them as proactive, dynamic and reactive, and discuss an illustrative model of an access control mechanism.

054367 'Internet Acceptable Usage Policy'
S Lichtenstein, *Computer Audit Update (Dec 96) pp 10–21*

This discusses how an organisation should go about defining an internet use policy.

054368 'The effects of Time on Integrity in Information Systems'
W List, *IFIP 96 pp 100–107*

The author discusses various time-related issues which can influence integrity by changing the user's perception of whether data are 'fit for purpose'.

054369 'Goodbye Key Escrow, Hello Key Recovery'
W Madsen, *Computer Fraud and Security Bulletin (Nov 96) pp 8–10*

This article reprints a recent speech on escrow by the US vice-president, and claims that key escrow features were successfully installed in products from Crypto AG by means of a special field in the ciphertext called the 'Hilfsfunktion', which enabled the NSA to decrypt the traffic of over 130 nations. The open key escrow programme may be seen as continuing this activity by other means.

054370 'WWW Technology in the Formal Evaluation of Trusted Systems'
EJ McCauley, *NISSC 96 pp 22–25*

The paper suggests using web pages for delivering TCSEC evaluation documents.

054371 'Security Proof of Concept Keystone (SPOCK)'
J McGehee, *NISSC 96 pp 539–550*

The NSA sponsored program SPOCK is a joint government and industry forum whose purpose is to raise consciousness, share technology, run demonstrators and help validate vendors' security claims.

054372 'System Security Engineering Capability Maturity Model and Evaluations: Partners within the Assurance Framework'
CG Menk, *NISSC 96 pp 76–88*

The author describes features of the capability maturity model and some of its advantages for security engineering. The rating maintenance programme is particularly close to CMM in its philosophy.

054373 'A barrier to network violations'
D Moseley, *Security Gazette (Nov 96) pp 21–23*

This is a management level overview of network security mechanisms.

054374 'Electronic Communications Risk Management: A Checklist for Business Managers'
RT Moulton, ME Moulton, *Computers and Security v 15 no 5 (96) pp 377–386*

This is a checklist of questions a risk manager should ask when assessing the possible impact of the introduction of email in a company.

054375 'Security profile for interconnected open distributed systems with varying vulnerability'
N Nikitakos, S Gritzalis, P Georgiadis, *IFIP 96 pp 428–437*

Some problems relevant to interconnecting networks with different vulnerability levels are discussed and a risk assessment strategy is proposed.

054376 'The Communications Decency Act and the Karma of Chaos'
J Osen, *Network Security; part 1: Oct 96 pp 13–19; part 2: Nov 96 pp 12–18*

This describes the US Communications Decency Act, which was recently ruled to be unconstitutional; it also reviews theories of the interpretation of the first amendment to the US constitution and a large number of relevant precedents.

054377 'Who bears the risk of defective software?'
R Parry, *Computer Audit Update (Dec 96) pp 27–29*

This article discusses the ramifications for British IT auditors of a recent court case won by St Albans' council against ICL.

054378 'EPHOS Security — Procurement of secure open systems'
NH Pope, JG Ross, *IFIP 96 pp 111–121*

The European Handbook for Procurement of Open Systems (EPHOS) security module is outlined. This EC project provides a set of handbooks for system procurement. When specifying protection, procurers can either use a 'Procurement Profile' with a default set of options matching given security concerns, or select options through a decision tree to find associated 'Procurement Clauses'. These currently deal with X.25, X.400 and EDI but are due to be extended.

054379 'Information Systems Security Centre of the Czech Technical University in Prague'
J Přibyl, *Pragocrypt 96 part 2 pp 21–34*

The author describes the growth of computer crime in the Czech republic after 1989 and the response of setting up a security research centre at a local university.

054380 'Heimliches Mithören und Abhóren'
W Reitz, J Vahle, *Datenschutzberater v 20 no 11 (15/11/96) pp 1–7*

The authors set out the legal situation of wiretapping in Germany, both when carried out by the authorities and by employers. In the latter case, only control information can be retained, such as the time and charge and — in the case of business calls only — the number dialled.

054381 'Response: Independent One-Time Passwords'
AD Rubin, *Computing Systems Usenix v 9 no 3 (Summer 96) p 257*

In this response to **054301** above, SecurID is challenged to make their encryption algorithm public.

054382 'Issues '95 – Electronic Commerce'
HH Rubinovitz, *SIGSAC Review v 14 no 4 (Oct 96) pp 2–6*

This is a short survey of electronic commerce.

054383 'The Keys to a Reliable Escrow Agreement'
R Sheffield, *NISSC 96 pp 215–220*

The author discusses the prudent practice to follow when placing software source code in escrow with a third party.

054384 'Work in WIPO on possible new instruments on copyright and related rights: Copy-protection systems and identification systems for use in rights management

B Simpson, *Computer Law and Security Report v 12 no 6 (Nov/Dec 96) pp 356–360*

This article describes, and seeks formal submissions on, a recent draft amendment to the international treaty on copyright. It effect would be to compel all signatory states to criminalise interference with electronic copyright management systems.

054385 'Modeling the Risks and Costs of Digitally Signed Certificates in Electronic Commerce'
I Simpson, *EC 96 pp 287–297*

The author presents a first attempt at a quantitative assessment of the risks of running a certification authority. It looks in particular at the effects of delays in recognising that a compromise has occurred, and in transmitting this to merchants via certificate revocation lists.

054386 ‘Smart Card Threat: “Not a Real-World Risk” ’
Smart Card News v 5 no 10 (Oct 96) pp 181–184

This reports the Bellcore claims of novel attacks on smartcards and its dismissal by industry pundits as impractical.

054387 ‘Organizing Electronic Services into Security Taxonomies’
SW Smith, PS Pedersen, *EC 96 pp 233–241*

The authors describe a way of partially ordering the vulnerabilities of systems using set inclusion as the basis for a systematic taxonomy. The idea is to deal effectively with inherited threats by structuring the countermeasures.

054388 ‘Intention Modelling: Approximating Computer User Intentions for Detection and Prediction of Intrusions’
T Spyrou, J Darzentas, *IFIP 96 pp 319–336*

The authors describe modelling user intentions to detect attacks, and discuss a prototype of a user intention identification system that examines the rationale behind execution of individually authorised tasks.

054389 ‘The Business-Led Accreditor – or ... How to Take Risks and Survive’
MEJ Stubbings, *NISSC 96 pp 123–130*

The author describes how the GCHQ approach to security accreditation has moved from risk avoidance to risk management, and gives some information on how the computer security, accreditation and monitoring functions are organised.

054390 ‘U.S. Government-Wide Incident Response Capability’
M Swanson, *NISSC 96 pp 489–494*

The author discusses NIST’s vision of the incident handling capability that will eventually be required by the US federal government. They propose a central service for agencies that do not have their own capability.

054391 ‘Silverfish in the cupboard’
D Thompson, *Computer Audit Update (Nov 96) pp 13–22*

The author discusses the control problems associated with ‘authorised outsiders’ — non-employees who have logons to corporate systems. He presents checklists for system administrators wishing to create least-trusted accounts on Unix and MVS.

054392 ‘A Case Study of Evaluating Security in an Open Systems Environment’
DL Tobat, ES Weiss, *NISSC 96 pp 250–258*

The authors review the evaluation of an office automation network operating at two levels of sensitivity and with an Internet connection.

054393 ‘Leitbildwechsel: dem (sicherheits-)technologisch aktivierten Danteschutz gehört die Zukunft’
O Ulrich, *Datenschutz und Datensicherheit v 20 no 11 (Nov 96) pp 664–671*

A senior official at the German information security agency calls for data protection mechanisms to be thoroughly integrated into systems from the outset rather than tacked on afterwards as manual procedures. He discusses the relative role of cryptography, evaluation and audit.

054394 'Evaluation of the security of distributed IT systems through ITSEC/ITSEM: experiences and findings'
I Uttridge, G Bazzana, M Giunchi, G Déler, S Geyres, J Heiler, *IFIP 96 pp 405–416*

The authors discuss the evaluation of Sesame against ITSEC in various EU countries. They highlight differences about distributed system decomposition, the evaluation of component security targets and the composition of security targets.

054395 'Making the Internet safe for ecommerce'
HP Vigil, M Mueller, *Datamation (Oct 96) pp 64–65*

Microsoft and Sun present their respective approaches to code signing in this article; the former scheme is proprietary and the latter generic.

054396 'Information Security Management: The Second Generation'
R von Solms, *Computers and Security v 15 no 4 (96) pp 281–288*

The author discusses various security evaluation schemes and claims that the ideal solution for commerce would be a self-evaluation scheme. Five criteria for such a scheme are advanced.

054397 'Information Security on the Electronic Superhighway'
SH von Solms, *IFIP 96 pp 153–166*

The author presents a management level overview of the mechanisms used in the SSL, SHTTP, STT and SEPP protocols.

054398 'Computer Security Policy: Trends and Perceptions'
AR Warman, *International Journal of Risk, Security and Crime Prevention v 1 no 2 (Apr 96) pp 119–129*

The author reports a survey, conducted by both mail and usenet, of security managers' attitudes and how these had changed between 1991 and 1994. Policy was at both times driven by perceived threats and user considerations; open systems were a big problem, but communications security a minor one.

054399 'Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles'
G White, G Nordstrom, *NISSC 96 pp 483–488*

The authors describe how computer security is taught at the US Air Force Academy: it is not a separate course but distributed throughout the curriculum, and used as the means of teaching basic computer science principles.

0543A0 'Security Assurance in Information Systems'
RG Wilsher, H Kurth, *IFIP 96 pp 74–87*

The process of obtaining ITSEC evaluation and system accreditation for five EU sponsored projects is described, together with recommendations for future research and development.

0543A1 'Marketing & Implementing Computer Security''
M Wilson, *NISSC 96 pp 163–172*

A former computer security officer relates his practical experience of organisational and managerial issues and the lessons he learned while trying to get management support and to get users to assume responsibility.

0543A2 'Case Study of Industrial Espionage Through Social Engineering'
IS Winkler, *NISSC 96 pp 306–312*

The author describes a number of the methods used in industrial espionage, and suggests that companies consider adopting at least some of the measures used by the US Department of Defense.

0543A3 'Information Warfare, INFOSEC, and Dynamic Information Defense'

JR Winkler, CJ O'Shea, MC Stokrp, *NISSC 96 pp 581–590*

Information warfare threats are outlined, stressing the need for dynamic defence against attack.

0543A4 'A Conversation with Eva Bozoki'

J Woeber, *Dr Dobbs' Journal no 261 (Jan 97) pp 16–22*

A senior scientist an a crypto products company talks about crypto policy.

0543A5 'A Case for Avoiding Security-Enhanced HTTP Tools to Improve Security for Web-Based Applications'

BJ Wood, *NISSC 96 pp 267–275*

An overview of WWW security products is given, and this leads to the conclusion that proper protection is some way off; consequently, it is preferable to treat web tools as untrusted and rely on other mechanisms behind them.

0543A6 'Removal of all unauthorised access paths in production software'

CC Wood, *Information Management and Computer Security v 4 no 5 (96) pp 22–23*

The author emphasises the importance of a conscious management policy to remove all programmer shortcuts when code is moved into production.

0543A7 'Datenschutz bei Telediensten'

U Wuermeling, *Datenschutzberater v 20 no 12 (15/12/96)*

A recent draft German law sets out provisions for data protection in multimedia which are outlined in this article. The goal is to minimise the quantity of personal information processed; problems foreseen include services offered by foreign companies.

0543A8 'IT Security and Privacy Education'

L Yngström, *IFIP 96 pp 351–364*

The author discusses the gap between interdisciplinary and specialist approaches to security education and considers ways to resolve the resulting problems.

4 Formal Methods and Protocols

054401 'The Eternity Service'
RJ Anderson, *Pragocrypt 96 pp 242–252*

The modern era only started once the printing press enabled seditious thoughts to be spread too widely to ban; yet the move to electronic publication means that many works are available on only a few servers, whose owners can be sued or coerced. In order to create a true electronic equivalent of book publishing, the author suggests using suitable protocols to build a distributed file store that would be highly resistant to denial-of-service attacks. A design is sketched combining mechanisms such as fragmentation, redundancy, scattering and anonymity. This raises a number of research questions such as secure time, digital annuities, and the relationship between anonymity and resilience.

054402 'SNMP-based Network Security Management using a Temporal Database Approach'
TK Apostolopoulos, VC Daskalou, *IFIP 96 pp 417–427*

The paper reviews the use of SNMP for security management within TCP/IP. A model using a temporal database of audit trails for analysis is also described.

054403 'Generic Electronic Payment Services'
A Bahreman, *EC 96 pp 87–103*

The author presents a protocol architecture for electronic payment which separates transactions into a number of layers, from the application at the top down to the payment service details at the bottom.

054404 'Payment Method Negotiation Service'
A Bahreman, R Narayanaswamy, *EC 96 pp 299–314*

The authors describe a set of protcols for customer and merchant agents to negotiate a payment mechanism automatically. This forms part of GEPS (**054403** above).

054405 'Payment Systems for Hypermedia Information Systems'
S Bakhtiari, R Safavi-Naini, R Gonzalez, HWP Beadle, *SIGSAC Review v 14 no 4 (Oct 96) pp 7–9*

The authors argue that a simple electronic cheque protocol is much more suitable for micropayments than a number of systems that have been proposed. Where the amount is small, there is no need to bank the cheque online; it is sufficient to expose the customer if his cheque bounces. A specimen protocol is given and compared with NetCash, NetBill and iKP.

054406 'Plausible Deniability'
DR Beaver, *Pragocrypt 96 pp 272–288*

The author discusses various ways of constructing ciphertext messages which can decrypt to more than one plaintext, in order to protect users against coercive decryption. The one-time pad already offers such plausible deniability; this property can be extended to public key protocols using various techniques. The underlying idea is to send each text once but to deliberately garble one of them, and build the choice into a Diffie-Hellman key exchange in such a way that it cannot afterwards be recovered without the cooperation of the receiver. Reducing this to the bit level enables the participants to agree a secret bit for a one-time pad, but in such a way that they can construct an 'audit trail' of either 1 or 0 later on.

054407 'Oblivious Key Escrow'
M Blaze, *Info Hiding 96 pp 335–343*

The author describes how key escrow could be performed using 'the net' as a highly reliable escrow server. For example, a secret key could be shared using a 500-out-of-5000 secret sharing scheme, so that it could still be recovered after the failure of 90% of network nodes. The sharing can be done with a new protocol technique called 'oblivious multicast', in which each share might end up in one out of a million possible nodes, with the sharer not knowing which. Access to the key would involve broadcast and thus surreptitious abuse of the escrow mechanism would be prevented.

054408 'An implementable secure voting scheme'
J Borrell, J Rifà, *Computers and Security v 15 no 4 (96) pp 327–338*

A scheme for secure voting is presented and claimed to use less computation and communication than other schemes. Each ballot is represented as an error introduced into a polynomial sequence; counting them amounts to error detection, and a threshold decryption scheme is used in place of an anonymous channel.

054409 'Automatic Formal Analyses of Cryptographic Protocols'
SH Brackin, *NISSC 96 pp 181–193*

The author presents some results of the Automatic Authentication Protocol Analyzer tool. This theorem prover is based on the logic of Gong, Needham and Yahalom, formalised using HOL proof tools. Three SPX protocols are analysed, and vulnerabilities are found in two of them; an attacker who gets a user's session key can manipulate the delegation mechanism to impersonate him for a period of time.

054410 'A Proposed Federal PKI using X.509 V3 Certificates'
WE Burr, NA Nazario, WT Polk, *NISSC 96 pp 452–462*

The authors discuss the proposed federal public key infrastructure, which combines a hierarchical service with some discretionary cross-certification of local CAs. The idea is to protect CAs from unwise cross-certification decisions by others; the mechanism is to limit cross-certificates so that the centrally set limits on path length (to root), federal assurance level and subtrees can not be circumvented. The necessary X.509 v 3 extensions are described.

054411 'Anonymous Atomic Transactions'
J Camp, M Harkavy, JD Tygar, B Yee, *EC 96 pp 123–133*

The authors show how blind signature tokens and a world readable audit trail can be used to construct anonymous transactions that are atomic, consistent, isolated and durable.

054412 'A Security Flaw in the X.509 Standard'
S Chokhani, *NISSC 96 pp 463–470*

The author describes a possible modification or replacement of some X.509 certificates using DSS. This attack is based on the fact that for DSS with given public key y to find a new private key x' and parameters p', q', g' is easier than the discrete log problem. Whether an attacker can substitute these within a certificate depends on how public key parameters are protected.

054413 'Internet Holes — Part 13: The SYN Flood'
F Cohen, *Network Security (Oct 96) pp 7–9*

The author describes how SYN flooding attacks work and mentions some of the timeout strategies that have been proposed to block it.

054414 'MIXes in Mobile Communication Systems: Location Management with Privacy'
H Federrath, A Jerichow, A Pfitzmann, *Info Hiding 96 pp 121–135*

The authors describe the present arrangements for hiding the location of users in GSM type systems, and discuss how they could be improved. One approach is to use remailer networks; here, one must pay attention to the bandwidth limitations on the air link. One can also use multiple names for mobiles. Various combinations of these techniques are discussed together with their tradeoffs.

054415 'Models of information networks with security services'
T Feglar, I Vajda, *Pragocrypt 96 pp 177–182*

The authors present a model of how adding security services to a network affects its queueing properties.

054416 'An integrated solution for secure communications over B-ISDN'
J Forné, JL Melús, *CMS 96 pp 96–107*

The authors discuss the options for encrypting B-ISDN traffic. They compare the costs of encrypting above and below the ATM adaptation layer (AAL); the latter makes key agility a requirement and pushes costs up. They propose an architecture in which encryption can be done above the AAL, above TCP/IP, or at the application layer, as appropriate for the application in question.

054417 'Protective Sharing of Any Function: Trust Distribution with Secure Multi-Coprocessors'
Y Frankel, M Yung, *Pragocrypt 96 pp 156–168*

The authors present a general protocol for sharing the computation of an arbitrary function between multiple tamper-proof processors. Each processor computes the function and xors it with a blinding factor; these can be computed so as to enforce an arbitrary access structure for reconstructing the function's output from the outputs of the tamper-proof processors. They discuss its possible application to key escrow.

054418 'Agora: A Minimal Distributed Protocol for Electronic Commerce'
E Gabber, A Silberschatz, *EC 96 pp 223–232*

The authors describe an electronic commerce protocol similar to Millicent (**051431**) but which does not use brokers. It is optimised for web based transactions and generates no more http messages than simple browsing. It can be implemented using Java applets and cgi scripts.

054419 'Token-Mediated certification and Electronic Commerce'
DE Geer, DT Davis, *EC 96 pp 13–22*

The authors discuss ways in which personal tokens such as smartcards may perform many functions similar to that of a certification authority in the course of routine electronic commerce transactions. They argue that the main benefits of public key protocols will not be in traditional terms such as trustless administration and nonrepudiable signatures, but in scalable authorisation, including asynchronous authentication and access control scaling. The technology may succeed because it minimises marginal costs rather than overall costs.

054420 'Smart Cards in Hostile Environments'
H Gobioff, S Smith, JD Tygar, B Yee, *EC 96 pp 23–28*

The authors discuss how to tackle the problem of the corrupt smartcard reader and propose certain equivalences between different possible combinations of trustedness in the card's input and output; either a trusted input or a trusted output will do, given a suitable protocol.

054421 'Hiding Routing Information'
DM Goldschlag, MG Reed, PF Syverson, *Info Hiding 96 pp 137–150*

The authors describe an approach to using multiple 'remailers' which they call 'onion routing' (it actually works with proxies for any type of service, not just mail). The idea is that remailers should be stateless; the initiator chooses routes out and back and constructs an 'onion', a set of remailer addresses successively encrypted under the previous remailer's public key, to enable the responder to reply to a message. The message, plus the reply onion, are then successively encrypted under the public keys of the outbound remailers. The approach has been prototyped for http and telnet.

054422 ‘A Formal Analysis Technique for Authentication Protocols’
S Gürgens, *Pragocrypt 96 pp 307–323*

The author presents a formal logic, based on BAN, that provides an alternative approach to the bug in the Neuman-Stubblebine protocol to those already provided by Syverson (**022421**) and Carlsen (**031405**). Her line of attack is to formalise the notion of type and add it to the logic. She then uses this to expose a reflection attack on the ISO/IEC 9798-2 protocol, that enables a smartcard reader to trick a smartcard into performing both sides of the authentication exchange itself.

054423 ‘A WWW Based Certification Infrastructure for Secure Open Network Transactions’
T Gustavson, *CMS 96 pp 154–165*

The author describes the Internet wide CA hierarchy proposed in RFC 1422, and discusses how this could be adapted to www. Examples are given of how web browsers can provide intuitive user interfaces by displaying lists of users certified by a CA, showing sources of CRLs, and displaying root CA keys for manual verification.

054424 ‘On Shopping Incognito’
R Hauser, G Tsudik, *EC 96 pp 251–257*

Current attempts to provide anonymity to shoppers are compromised by the end to end nature of protocols such as http; the client’s id is available in the clear to the server. Truly anonymous shopping needs to be built on top of an anonymous messaging service, and the authors describe ways of doing this. Removing customer certification has a number of consequences, such as that offers from merchants become transferible, and that dispute resolution mechanisms need careful design.

054425 ‘Robust and Secure Password and Key Change Method’
R Hauser, P Janson, G Tsudik, E Van Herreweghen, R Molva, *Journal of Computer Security v 4 no 1 (Sep 96) pp 97–111*

This journal version of **041216** describes the password change mechanisms of KryptoKnight. These were designed to be more resistant to password guessing attacks than, for example, Kerberos. The idea is to block replay attacks by making the change work whether the authentication server knows the old password or the new one. It is proved that the client and server will always eventually share the same key, and that neither message losses nor replay attacks can cause deadlock.

054426 ‘Attack Class: Address Spoofing’
LT Heberlein, M Bishop, *NISSC 96 pp 371–377*

The authors discuss address spoofing attacks and ways of exploiting them. In addition to impersonating a target, the attacker must also prevent the target from detecting and blocking the spoof. This is discussed with reference to an actual attack, and possible variants and defences are outlined.

054427 ‘Model Checking Electronic Commerce Protocols’
N Heintze, JD Tygar, J Wing, HC Wong, *EC 96 pp 147–164*

The authors adapted the FDR model checker to examine the protocols underlying NetBill and a simplified version of DigiCash. They supply full code for the models in their article.

054428 ‘Anonymous Mobility Management for Third Generation Mobile Networks’
S Hoff, K Jakobs, D Kesdogan, *CMS 96 pp 72–83*

Two proposed approaches to protecting location information in UMTS are for each user to have a ‘Home Trusted Device’ to maintain her location, and to allow anonymous subscribers. This paper proposes a combination of the two ideas. A roaming user will register with a local network service provider via a chain of three MIXes, which will protect her identity from the network while supporting protocols that allow both billing and incoming call routing. The pseudonym thus generated is changed after every call. A mechanism is described for this idea to be implemented on top of X.500, which is proposed as the architecture for UMTS location registers.

054429 'Secure World Wide Web access to server groups'
A Hutchison, M Kaiserwerth, P Trommler, *CMS 96 pp 234–243*

The authors describe some protocols proposed for improving the authentication of web pages, and a mechanism developed by IBM for extending them to authenticate a user to a group of servers simultaneously.

054430 'Strong Password-Only Authenticated Key Exchange'
DP Jablon, *Computer Communications Review v 26 no 5 (Oct 96) pp 5–26*

The author surveys the existing protocols designed to authenticate Diffie Hellman key exchange with a password and proposes a new one, SPEKE. The idea is to use the password to select a base in the group, do a Diffie Hellman exchange with respect to this base, and then exchange encrypted nonces to check that the password was indeed shared. Various attacks are considered and means of blocking them are developed.

054431 'Anonymous Addresses and Confidentiality of Location'
IW Jackson, *Info Hiding 96 pp 115–120*

The author describes how anonymous remailers can be used to process personal location information from active badges. The goal is that each user should be able to control who has access to information about his location; the mechanism is that the remailers forward this information to a server that the user trusts to enforce his security policy. The crypto protocols used in this system are described.

054432 'Message encipherment with minimal expansion and redundancy — doing better than ISO-10126'
CJA Jansen, P van de Vlist, *Computers and Security v 15 no 7 (96) pp 627–632*

The authors point out that one can do much better than the ISO 10126 standard for packing messages prior to encryption by choosing more intelligent coding and compression techniques.

054433 'Key Escrowing Systems and Limited One Way Functions'
WT Jennings, JG Dunham, *NISSC 96 pp 202–214*

The authors point out that in the absence of insider abuse, key escrow systems have the property that there are many more key deposits than withdrawals. They propose fortifying escrow by forcing a keysearch of controllable difficulty to be done whenever a key is retrieved from the escrow database.

054434 'Beacons for Authentication in Distributed Systems'
A Jiwa, T Hardjono, J Seberry, *Journal of Computer Security v 4 no 1 (Sep 96) pp 81–96*

In this journal version of **041415**, the authors pick up on an idea of Rabin to show how a central 'beacon' service that continually broadcasts certified nonces can simplify authentication dialogues, compared with systems involving user chosen nonces. The central service has to be trusted to behave properly (e.g. by not repeating itself) and not to publish its private key, but that is a modest price for the simplicity achieved.

054435 'Authentication in Analogue Telephone Access Networks'
A Jøsang, K Johannesen, *Pragocrypt 96 pp 324–336*

The authors describe the protocols underlying a telephone authentication device developed by the Norwegian phone company to prevent losses due to intruders connecting to other people's analogue telephone lines. After the phone goes off hook, a DTMF challenge and response are exchanged between a wall-socket mounted authentication device and the exchange software before a dial tone is given. The crypto is based on triple DES; the challenge and response are limited to 16 bits for performance reasons, and the security tradeoffs are discussed.

054436 'A collision-free secret ballot for computerized general elections'
WS Juang, CL Lei, *Computers and Security v 15 no 4 (96) pp 339–348*

The authors propose a voting scheme based on 'uniquely blind signatures' whose goals are to ensure independence among voters without the need for any global computation, and to ensure that the returning officer cannot cheat without being caught.

054437 'PayTree: "Amortized-Signature" for Flexible MicroPayments'
CS Jutla, M Yung, *EC 96 pp 213–221*

The authors propose implementing micropayments using hash trees rather than hash chains and discuss a number of variants giving features such as multiple denominations and divisble coins.

054438 'Attack modelling in open network environments'
SC Katsikas, D Gritzalis, P Spirakis, *CMS 96 pp 268–277*

The authors present a formal model of the intrusion of a virus into a networked system, and discuss how the probabilities of infection and protection interact.

054439 'U-PAI: A Universal Payment Application Interface'
SP Ketchpel, H Garcia-Molina, A Paepcke, S Hassan, S Cousins, *EC 96 pp 105–121*

The authors propose a set of application interfaces on which a range of payment protocols can be built, and illustrate it with a sample First Virtual proxy.

054440 'Fast, Automatic Checking of Security Protocols'
D Kindred, JN Wing, *EC 96 pp 41–52*

The authors describe a tool, implemented in Standard ML, that can implement a range of authentication logics. They apply it to BAN, Kessler and Wedel's AUTLOG (**033413**) and Kailar's logic of accountability (**052420**), and duplicate existing analyses of a number of protocols. The implementation of BAN is given as an example.

054441 'Secure Internet banking with Privacy Enhanced Mail: A protocol for reliable exchange of secured order forms'
S Kolletzki, *Computer Networks and ISDN Systems v 28 no 14 (96) pp 1891–1899*

The author proposes that when using PEM or PGP to secure commercial messages, they should be nested for robustness: a payment order sent by a customer would be incorporated verbatim in a response from the bank, and both would then be included in the customer's acknowledgement.

054442 'Integration of Digital Signatures into the European Business Register'
H Kurth, *NISSC 96 pp 131–138*

The outcome of an European project for on-line linking of national business registers (EBRIDGE) is given. The implementation enforces an audit trail, authentication through digital signatures with MD5 and RSA, and separation of duties (which is done using restricted shells on a secure Unix server). These registers can serve as certification authorities by distributing firms' public keys.

054443 'Security Flows Analysis of the ATM Emulated LAN Architecture'
M Laurent, *CMS 96 pp 37–52*

The author describes the LAN emulation protocols proposed as a standard by the ATM forum and points out a number of security flaws in them. Switches rarely check the correspondence between a station's claimed address and the ingress port on which a call arrives, so calls can be redirected by opponents operating at the ATM switch layer in various ways. As routers are implemented in an ELAN layer above AAL5 and are themselves LAN emulation clients, they cannot block such attacks. However, the majority of attacks are inherited from legacy LAN architectures: one can attack the router mapping tables that translate LAN to ATM addresses, the LAN emulation servers, and the server that handles broadcast and LAN legacy traffic. Such attacks could in theory be countered using similar mechanisms to those used in existing secure LANs.

054444 'Verifying Cryptographic Protocols for Electronic Commerce'
RW Lichota, GL Hammonds, SH Brackin, *EC 96 pp 53–65*

The authors describe an authentication tool, 'Convince', which is implemented using Unix tools such as Lex and yacc and a HOL theorem prover. The underlying logic is derived from GNY, and it needed to be extended when used on a protocol in which a server forgets all but the key used to encrypt a ticket that is sent back to it later in the protocol run.

054445 'Security Concepts for the WWW'
P Lipp, V Hassler, *CMS 96 pp 84–95*

The authors review the protocols proposed for securing web traffic, including SSL, SHTTP, PCT, GSS-API and PEP/SEA, and compare the protection that they provide.

054446 'Anonymous Credit Cards and Their Collusion Analysis'
SH Low, NF Maxemchuk, S Paul, *IEEE/ACM Transactions on Networking v 4 no 6 (12/96) pp 809–816*

The authors present an anonymous credit card protocol and analyse it for possible leakage as a result of collusion between banks, merchants etc by using their minimal collusion path search algorithm (**054447** below).

054447 'Modeling Cryptographic Protocols and Their Collusion Analysis'
SH Low, NF Maxemchuk, *Info Hiding 96 pp 169–184*

The authors present a model for analysing failures in crypto protocols due to collusion among two or more of the participants. This is motivated by previous work in electronic payment systems where one wants to prove that a certain number of principals need to collude in order to breach a cardholder's privacy. The basic idea is to examine the structure of collusion paths and thus identify which combinations of initial knowledge suffice for an attack. This saves the effort of exploring a large state transition system.

054448 'A Calculus for Security Bootstrapping in Distributed Systems'
UM Maurer, PE Schmid, *Journal of Computer Security v 4 no 1 (Sep 96) pp 55–80*

In this journal version of **041424**, the authors develop a new calculus for cryptographic protocols. Their central idea is to separate the notions of confidentiality and integrity in channels: $A \rightarrow\!\bullet B$ means that A can send a secret message to B, while $A \bullet\!\rightarrow B$ means that A can send an authentic message to B. Under certain assumptions, $\rightarrow\!\bullet$ is equivalent to $\leftarrow\!\bullet$, which enables one to see whether it is possible to set up a channel between two nodes in a network, given a set of initial trust relationships.

054449 'Management Model for the Federal Public Key Infrastructure'
NA Nazario, WE Burr, WT Polk, *NISSC 96 pp 438–445*

This article describes NIST's management model for a federal public key infrastructure. This is a national hierarchy of CAs providing X.509 certificates, a directory service and a revocation service. At the root, a policy approving authority (PAA) sets naming and path length restrictions on the CAs below it; it also performs initial assessments of candidate CAs as well as periodic reassessments.

054450 'Security Policies for the Federal Public Key Infrastructure'
NA Nazario, *NISSC 96 pp 445–451*

The author elaborates on the envisioned CA operational policy, certificate operations and trust relationships in the above scheme. For example, tamper resistance hardware should be used that is unable to export the CA's private signing key; and each certificate will be assigned a federal assurance level. CAs maintain their own revocation lists, which they export to their directories twice daily.

054451 'A model for the detection of the message stream delay attack'
S O'Connell, A Patel, *IFIP 96 pp 438–451*

The authors address message stream delay attacks through a model avoiding the need of synchronised clocks; means for handling clock drifts are provided. Exception handling is discussed as well as the model implementation, and an alternative way to address attacks that reorder packets through delay.

054452 'Distributed registration and key distribution (DiRK)'
R Oppliger, A Albanese, *IFIP 96 pp 199–208*

A decentralised scheme for electronic conference participant registration and key distribution is presented. It distinguishes active and passive participants, lets active members register new participants, re-key sessions, validate registration and find who registered a given member. An application to the Internet MBone is described.

054453 'Distributed registration and key distribution for online universities'
R Oppliger, M Bracher, A Albanese, *CMS 96 pp 166–175*

The authors describe a scheme developed to support lectures that are traded online among universities and students. The function of a university is seen as enabling professors and students to meet for lectures and tutorials; arranging payments of fees; and issuing legally binding transcripts of work done. It is envisaged that all this will be done over a medium like the MBONE. Each lecture is sponsored by a number of universities, each of which sign a lecture key that certifies the attendance of participants. The system is being prototyped at the University of Berne.

054454 'Internetwork Access Control Using Public Key Certificates'
H Park, R Chow, *IFIP 96 pp 237–246*

A packet-level scheme is described that enforces control on traffic between administrative domains. Authentication is based on X.509 certificates; control of exit and entry points is based on packet signatures created with a key issued by the receiver. The scheme's performance is compared with that of a packet visa scheme.

054455 'Secure Billing — Uncontestable Charging'
S Pütz, *CMS 96 pp 208–221*

The author proposes telecomms charging mechanisms whereby the user is required to acknowledge at regular intervals during the call that he has received service of an acceptable quality. These 'intermediate service tokens', which can be cryptographically authenticated, reduce both sides' exposure to fraud.

054456 'A Peer-to-Peer Software Metering System'
B Schneier, J Kelsey, *EC 96 pp 279–286*

The authors present electronic payment protocols designed for use in software metering applications. There are variants for both online and offline operation.

054457 'Establishing a key hierarchy for Conditional Access without encryption'
J Schwenk, *CMS 96 pp 176–182*

The author discusses the effects that the depth of the key hierarchy has on the volume of message traffic needed to control a pay-TV system, and points out that the deeper the key hierarchy, the more efficient the revocation of pirates can be.

054458 'Java and Web-Executable Object Security'
M Shoffner, M Hughes, *Dr Dobbs' Journal no 259 (Nov 96) pp 38–49*

The authors describe some of the security features of Java and some of the known attacks. They point out that Java 'cracklets' could work together to penetrate the security of local networks on which they run. The long term fix to this is expected to be code signing.

054459 ‘A Protocol for Secure Transactions’

DH Steves, C Edmondson-Yurkanan, M Gouda, *EC 96 pp 201–212*

The authors discuss ways of adding atomicity to electronic transactions and enabling them to be securely serialised. They propose an eight pass protocol for this purpose.

054460 ‘Network security in a telemedicine system’

G Vassilacopoulos, V Chrissikopoulos, D Peppes, *CMS 96 pp 108–115*

The authors present a network security scheme for telemedicine in which the conference key distribution scheme of **044605** is implemented with a trusted third party in each hospital. This is being piloted at a hospital in Athens. A problem that has arisen is that it is necessary to set up a new key whenever a new principal joins the conference; the delay involved may not be acceptable in emergency situations.

054461 ‘Analysis of the SSL 3.0 Protocol’

D Wagner, B Schneier, *EC 96 pp 29–40*

The authors present a number of active attacks on SSL v 3.0, including attacks that rollback to a previous version, change the cipher spec so that the authentication is suppressed, and manipulate the choice of key exchange algorithm so that a server’s Diffie-Hellman modulus p and generator g are misinterpreted by the client as an RSA modulus and exponent, leading to an attack. They also point out that as ‘get’ requests are not padded, the length of the requested URL is visible and this may enable it to be guessed.

054462 ‘Authenticating passwords over an insecure channel’

TC Wu, HS Sung, *Computers and Security v 15 no 5 (96) pp 431–439*

A protocol is presented for combining password authentication with a challenge response exchange using a hash-based one-time signature scheme whose secret key material is generated by hashing the password with a nonce.

054463 ‘Quantitative authentication and vouching’

JD Yesberg, MS Anderson, *Computers and Security v 15 no 7 (96) pp 633–645*

The authors explore the possibilities of authentication that allocates different levels of certainty to user authentication, depending on whether the method used was a password, a password generator, a biometric or whatever. They would allow users to improve the level of certainty by vouching for each other (‘the person in the terminal room with me is X’).

5 Secret Key Algorithms

054501 'Security of private-key encryption based on array codes'
A Al-Jabri, *Electronics Letters v 32 no 24 (21/11/96) pp 2226–2227*

The author shows how to break an encryption algorithm of de Souza based on array codes (**034605**). The idea is that by encrypting a zero plaintext, information is obtained about the secret permutation applied after the encoding step.

054502 'Akelarre: a New Block Cipher Algorithm'
G Álvarez, D de la Guía, FMA Peinado, *SAC 96 pp 1–14*

This article presents a new block cipher based on data dependent rotations and designed to ensure that each plaintext bit will influence at least one of them. It operates on 128 bit blocks; the number of rounds and keybits are user selectable.

054503 'Cryptanalysis of Triple Modes of Operation'
E Biham, *Pragocrypt 96 pp 414–424*

The author develops and extends his results of **041501** to show that with the exception of triple-ECB, none of the double and few of the triple modes of DES are very much more secure than single DES against combinations of keysearch, birthday and differential analysis. Many double DES modes can be broken with 2^{65} to 2^{67} chosen texts, and the internal memory of the feedback allows this many to be harvested. He conjectures that three triple and three quadruple modes are secure.

054504 'A Note on Sequences with the Shift and Add Property'
SR Blackburn, *Designs, Codes and Cryptography v 9 no 3 (Nov 96) pp 251–256*

If a sequence of elements from a finite field has the property that the componentwise sum of any two shifts of the sequence is either a shift of the sequence or the all zero sequence, then it is generated as the projection of powers of a primitive element over the field. Thus if it has prime length, it has this property if and only if it is a maximal length sequence. Furthermore, all sequences with a similar property over an arbitrary finite group are essentially these sequences.

054505 'A better key schedule for DES-like ciphers'
U Blumenthal, SM Bellovin, *Pragocrypt 96 pp 42–54*

The authors propose a system for using DES to generate round keys for a block cipher out of a user key of arbitrary length. The idea is to make the relation between round keys intractable while ensuring that user key bits have an approximately equal effect on round key bits.

054506 'The RIPEMD-160 Cryptographic Hash Function'
A Bosselaers, H Dobbertin, B Preneel, *Dr Dobbs' Journal no 261 (Jan 97) pp 24–28 & 78–80*

The authors of the RIPEMD-160 hash function describe its design and provide C source code for it.

054507 'Nonlinear generators with a guaranteed large linear complexity'
P Caballero-Gil, A Fúster-Sabater, *SAC 96 pp 148–160*

The authors present a new class of functions for use in nonlinear filter generators. These functions are characterised by their maximum order terms; they generate maximal linear complexity and are compatible with the known defences against fast correlation attack.

054508 'Luby-Rackoff: Four Rounds is not Enough'
D Coppersmith, *IBM Research Report RC 20674 (91617) 24/12/96*

A four round Luby-Rackoff cipher on $2n$-bit blocks can be broken using 2^{n+3} chosen plaintexts to recover most of the round functions. The attack significantly extends the

Aiello-Venkatesan technique (**053502**) which merely distinguishes Luby-Rackoff from a random permutation.

054509 ‘Some early Hungarian communist ciphers’
Cryptologia v XX no 4 (Oct 96) pp 347–358

This article describes the use of columnar transposition ciphers by the government of Bela Kun in Hungary in 1919.

054510 ‘Discrete optimisation: a powerful tool for cryptanalysis?’
E Dawson, A Clark, *Pragocrypt 96 pp 415–451*

The authors discuss the use of optimisation techniques in cryptanalysis. As well as toy problems such as polyalphabetic substitutions, they can be used to speed up fast correlation attacks on stream ciphers; experimental results using simulated annealing are presented.

054511 ‘Statistical methods for testing the strength of key generators’
EP Dawson, H Gustavson, *Pragocrypt 96 pp 452–466*

The authors describe a number of the statistical tests they have incorporated in a package for testing keystream generators. The use of birthday techniques can cut the amount of keystream needed to recognise unnaturally frequent substrings.

054512 ‘SAFER, DES and FEAL: algebraic properties of the round functions’
R Dittmar, G Hörnauer, R Wernsdorf, *Pragocrypt 96 pp 55–66*

The authors show that the round functions of SAFER generate the alternating group and present a new proof that the round functions of DES do so too. They also show that if the DES functions, or the FEAL round functions, generate a primitive permutation group, then they generate the alternating group. En route, they show that the round functions of DES and FEAL have more, and shorter, cycles than one would expect of random functions.

054513 ‘The nonlinearity of a class of Boolean functions with short representation’
C Fontaine, *Pragocrypt 96 pp 129–144*

The author shows how to obtain compact Boolean functions of high nonlinearity by looking at the cosets of Reed-Muller codes from which some coordinates have been deleted.

054514 ‘Cryptograms from the crypt’
JJ Gillogly, L Harnisch, *Cryptologia v XX no 4 (Oct 96) pp 325–329*

A psychic researcher left a Playfair encrypted message to test whether he could communicate the keys to anyone living after his death. This has been solved by searching for the keywords and using a number of tricks.

054515 ‘Computation of low-weight parity check polynomials’
JD Golić, *Electronics Letters v 32 no 21 (10/10/96) pp 1981–2*

If a polynomial over GF(2) has degree r, then the number of its multiples of degree n and weight w is about $n^{w-1}/2^r(w-1)!$. This means that the birthday method proposed by Meier and Staffelbach will not work as well as expected; in effect, the residues mod f are not randomly distributed, and the minimum degree of weight-4 parity check polynomials will be about $O(2^{r/3})$ rather than $O(2^{r/4})$. The proposals of Chepyzhov-Smeets and Penzhorn are also criticised. A modified search algorithm is presented and analysed.

054516 ‘Conditional correlation attack on combiners with memory’
JD Golić, *Electronics Letters v 32 no 24 (21/10/96) pp 2193–2195*

The author analyses conditional correlation attacks from the viewpoint of random coding theory and shows that if the number of outputs of a sequence combiner with memory is equal to or grater than the number of inputs then it is potentially vulnerable to a correlation attack. However, the complexity of this is exponential.

054517 ‘Modelling Avalanche in DES-Like Ciphers’
HM Heys, *SAC 96 pp 77–91*

The author develops a statistical model of how the avalanche in a block cipher develops as the number of rounds increases. This is tabulated as a function of S-box size and used to argue for the choice of particular kinds of S-box.

054518 ‘Bounds on non-uniformity measures for generalised linear cryptanalysis and partitioning cryptanalysis’
T Jakobsen, C Harpes, *Pragocrypt 96 pp 467–479*

The authors introduce a measure of non-uniformity called imbalance, similar to Matsui’s bias, and show that it reflects the resistance of a block cipher to both linear cryptanalysis and partitioning cryptanalysis.

054519 ‘A new design concept for building secure block ciphers’
K Kiefer, *Pragocrypt 96 pp 30–41*

The author presents a block cipher constructed by composing the permutations X^{33} over GF(2^{64}) and X^3 over GF(2^{65}) with keyed byte xors and rotations.

054520 ‘Chosen-text attack on CBC-MAC’
L Knudsen, *Electronics Letters v 33 no 1 (2/1/97) pp 48–49*

The author presents an attack on 32 bit DES CBC-MAC using about 2^{17} chosen texts to find internal collisions. It turns out that for optimum security, a DES MAC should be 22 bits long rather than 32 where chosen text attacks are feasible.

054521 ‘Optimisation of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack’
K Kusuda, T Matsumoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 35–48*

The authors extended Hellman’s time-memory tradeoff cryptanalysis and formulate the relationship between its three parameters: breaking cost, time, and success probability. They then optimise the formula and apply it to estimate the security of DES, FEAL-32 and Skipjack.

054522 ‘CRISP: A Feistel cipher with hardened key-scheduling’
M Leech, *SAC 96 pp 15–29*

This article presents a DES-like cipher with a 128-bit block and 11-to-8 bit S-boxes that uses a version of itself to generate its round keys.

054523 ‘Message Encryption and Authentication Using One-Way Hash Functions’
CH Lim, *SAC 96 pp 38–48*

The author proposes a number of simple ways to get block and stream ciphers from hash functions, and presents a new randomised XOR MAC.

054524 ‘BEAST: A fast block cipher for arbitrary blocksizes’
S Lucks, *CMS 96 pp 144–153*

The author presents a security proof for BEAR and LION (**052502**) under chosen plaintext attacks; this leads to the conclusion that a shortcut is possible in the third round of BEAR, leading to a new cipher that is similar but faster. There is also a remotely keyed variant inspired by Blaze’s protocol (**052404**).

054525 ‘Practical S-box design’
S Mister, C Adams, *SAC 96 pp 61–76*

The authors describe techniques for constructing large S-boxes using bent functions as columns and then modifying them slightly to get desired properties. The boxes in question are 8 by 32, as required in CAST.

054526 'Provably secure and efficient block ciphers'
P Morin, *SAC 96 pp 30–37*

The author discusses BEAR and LION (**052502**) and presents a simplified cipher called Aardvark. This has a one-block message extension, and also has the property that part of the ciphertext consists of an unkeyed hash of the plaintext.

054527 'The security of an RDES cryptosystem against linear cryptoanalysis'
Y Nakao, T Kaneko, K Koyama, R Terada, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 12–19*

This paper discusses the security of the RDES cryptosystem against linear cryptanalysis. RDES is a randomised version of DES proposed by the authors in 1994 aiming to counter differential cryptanalysis by introducing a probabilistic swap on the right half of the input of each DES round. This paper uses Matsui's search algorithm to investigate its strength against linear attacks.

054528 'Algebraic properties of permutation polynomials'
E Okamoto, W Aitken, G Blakley, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 4 (1996), pp 494–501*

This paper investigates the algebraic properties of permutation polynomials over a finite field, especially those associated with permutation cycles.

054529 'Cryptographic algorithms: properties, design and analysis'
J Pieprzyk, *Pragocrypt 96 pp 1–17*

This article reviews those aspects of cryptographic algorithm design that enable security dependencies to be proved, such as Luby-Rackoff, and the relationships between various possible S-box design criteria.

054530 'On Linear Dependencies in Subspaces of LFSR-Generated Sequences'
J Rajski, J Tyszer, *IEEE Transactions on Computers v 45 no 10 (Oct 96) pp 1212–1216*

The authors calculate the probability that an arbitrary set of positions from a linear feedback shift register sequence will contain a subset of linearly dependent elements and show that it differs from previously accepted wisdom. They then take a number of small primitive pentanomials and exhibit their smallest trinomial and quadrinomial multiples.

054531 'One-Time Pad Cryptography'
F Rubin, *Cryptologia v XX no 4 (Oct 96) pp 359–364*

The author proposes the use of autokeying to extend a small amount of one-time pad to encipher a larger message.

054532 'A new version of FEAL, stronger against differential cryptanalysis'
R Terada, P Pinheiro, K Koyama, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 28–34*

This paper presents a new cryptographic function called FEAL-N(X)S. It is obtained by introducing a dynamic swapping function to FEAL-N(X) and aims to make FEAL-N stronger against differential cryptanalysis.

054533 'Design of the 8x8 S-Boxes'
P Tesař, *Pragocrypt 96 pp 169–176*

The author presents the results of some experiments at generating random 8x8 S-boxes and then filtering them for various nonlinearity and other properties.

054534 'Algorithm for recursively generating irreducible polynomials'
MZ Wang, *Electronics Letters v 32 no 20 (26/9/96) p 1875*

If f is irreducible over GF(2) of even degree and odd weight, and $g(x) = f(x^2+x+1)$ has degree k, then $h(x) = x^k g(x^{-1})$ is also irreducible.

054535 'A New Class of Substitution-Permutation Networks'
AM Youssef, SE Tavares, HM Heys, *SAC 96 pp 132–147*

The authors propose a block cipher based on a substitution-permutation network with S-boxes having the property that $S^{-1}(x) = S(x \oplus a) \oplus b$ for constants a and b. The idea is that then only a single S-box is needed, thus saving space in smartcards and similar processors. They analyse whether this introduces any weaknesses, such as from fixed points, and conclude that it does not. The resulting cipher runs reasonably well on a wide range of processors from 6811 to Ultrasparc.

054536 'Modelling Avalanche Characteristics of a Class of Substitution-Permutation Networks'
AM Youssef, SE Tavares, *Pragocrypt 96 pp 18–29*

In order for an SP network block cipher to have the property that the same hardware can be used for encryption and decryption, it is sufficient for its S-boxes to be semi-involute, i.e. their inverses can be obtained by a fixed xor on the input and output. The avalanche and other properties of such ciphers are studied in this paper; they work well with diffusive linear transformations between rounds.

054537 'New Bounds on the Number of Functions Satisfying the Strict Avalanche Criterion'
AM Youssef, TW Cusick, P Stănică, SE Tavares, *SAC 96 pp 49–56*

This paper provides a constructive proof of an improvement of Cusick's conjectured lower bound on the number of functions satisfying the strict avalanche criterion **052508**; it also provides a new bound for the number of balanced functions satisfying it.

054538 'Difference Distribution Table of a Regular Substitution Box'
XM Zheng, *SAC 96 pp 57–60*

Regular S-boxes (those whose column sums are equal) are completely characterised by their difference distribution tables.

6 Public Key Algorithms

054601 'Efficient and provably secure key agreement'
N Alexandris, M Burmester, V Chrissikopoulos, D Peppes, *IFIP 96 pp 227–236*

The authors overview the Bellare-Rogaway key agreement protocol and extend the Matsumoto-Takashima-Imai protocol with use of a MAC to actually get a zero-knowledge based protocol. The security of the derived protocol is based on the Diffie-Hellman problem and the properties of a pseudorandom function used for the MAC.

054602 'Cryptosystems based on Dickson polynomials'
H Aly, WB Müller, *Pragocrypt 96 pp 493–503*

The authors discuss public key cryptosystems based on Dickson polynomials, showing that RSA and LUC are simply special cases of these. They use this to put recent work on Lucas based systems into perspective. The general Dickson system is not protected by the RSA patent and has some possible technical advantages too.

054603 'The Newton Channel'
R Anderson, S Vaudenay, B Preneel, K Nyberg, *Info Hiding 96 pp 151–156*

The authors show that ElGamal signatures modulo a prime p can be decomposed into separate signatures in the subgroups of Z_p^*. The signing key may be findable using discrete log computation techniques, or deliberately shared with some third party, module some of the distinct prime power factors of $p-1$ but not others. This gives rise to broadcast and narrowcast subliminal channels respectively. The construction settles in the negative a conjecture of Simmons that all broadband subliminal channels involve compromising the signing key. It also shows that the US digital signature standard is designed to minimise the subliminal channel capacity, rather than maximise it as had previously been thought.

054604 'A Progress Report on Subliminal-Free Channels'
M Burmester, YG Desmedt, T Itoh, K Sakurai, H Shizuya, M Yung, *Info Hiding 96 pp 157–168*

The authors discuss the definition of a subliminal channel and point out some problems. For example, a player can always balk and refuse to complete a protocol if its outcome is going to be unfavourable to him. They review a number of signature and zero-knowledge schemes for subliminal freeness and present a coin flipping protocol that they claim to be subliminal free — although running it twice in succession is not.

054605 'Hyper-bent functions'
C Carlet, *Pragocrypt 96 pp 145–155*

The author defines a Boolean function on GF(2^m) to be (m, k)-bent if all functions obtained by fixing k coordinates are bent. He shows that for m and k even, the set of (m, k)-bent functions is the same for all k in the range 2, 4, $m-2$.

054606 'On the one-way algebraic homomorphism'
E Chida, T Nishizeki, M Ohmori, H Shizuya, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 54–60*

This paper shows that if there exists a one-way group homomorphism $f : U \to V$, then there exists a one-way ring homomorphism $F : Z_n \oplus U \to Z_n \oplus Imf$. Based on this result, the authors imply that there exists a ring homomorphic encryption function based on a group homomorphic encryption function.

054607 'Parallelizing the RSA operator'
A Daniel, V Torres, JL Villar, *Pragocrypt 96 pp 67–75*

Up to eight processors can be used to do RSA in parallel: the idea is to split the operations mod p and q, the squaring and the multiplying, and by pipelining the Dussé-Kaliski variant of Montgomery multiplication. Performance figures for a test implementation are given.

054608 'A new approach for delegation using hierarchical delegation tokens'

Y Ding, P Horster, H Petersen, *CMS 96 pp 128–143*

The authors describe and classify a number of existing schemes for realising delegation, whether based on certificate protocols or on public key mechanisms. They then present a number of new schemes. These vary according to whether the final recipient is known in advance or not, and whether the delegation is to be traceable or not. The underlying mechanisms are variants of Schnorr signatures.

054609 'Dynamic Threshold cryptosystems: A New Scheme in Group Oriented Cryptography'

H Ghodosi, J Pieprzyk, R Safavi-Naini, *Pragocrypt 96 pp 370–379*

the authors present a threshold cryptosystem based on RSA in which the group modulus is the product of users' personal moduli and users can be added or removed at will.

054610 'An Hierarchical Threshold Scheme with Unique Partial Keys'

H Hassler, V Hassler, R Posch, *IFIP 96 pp 219–226*

The authors define a multi-threshold scheme as a scheme whose principals can reconstruct different secrets; the more of them cooperate, the higher the level of the secret that can be reconstructed. Shares are of equal authority and length, and the same share is used for any security level. Any share can be revoked without affecting other shares; in this case, one or more new polynomials are computed. The number of levels is theoretically unlimited, and weighted shares can also be issued at the cost of an increase in the length of the shares.

054611 'Two efficient server-aided RSA secret computation protocols against active attacks'

SJ Hwang, CC Chang, WP Yang, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 9 (1996), pp 1504–1511*

This paper proposes two server-aided RSA secret computation protocols that aim to withstand active and passive attacks.

054612 'Zero-Knowledge Nominative Signatures'

SJ Kim, SJ Park, DH Won, *Pragocrypt 96 pp 380–392*

Nominative signatures, unlike undeniable signatures, have the property that third parties can ascertain their validity by conducting a protocol with the designated verifier. In this paper, nominative signatures and combined with zero knowledge proofs and convertible undeniable signatures.

054613 'Montgomery Multiplication in GF(2^k)'

ÇK Koç, T Acar, *SAC 96 pp 95–106*

The authors show that for a suitable choice of r, abr^{-1} can be calculated more quickly than ab in fields of characteristic two, thus opening up an analogue of Montgomery multiplication for such structures. Detailed algorithms are given, with a worked example for GF(2^4) and tables of empirical performance results.

054614 'A new RSA-type scheme based on singular cubic curves $(y - \alpha x)(y - \beta x) \equiv x^3 (\mathrm{mod} n)$'

H Kuwakado, K Koyama, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 49–53*

This paper proposes a new RSA-type scheme over the non-singular parts of singular curves $E_n(\alpha, \beta) : (y - \alpha x)(y - \beta x) \equiv x^3 (\mathrm{mod} n)$.

054615 'ID-based cryptographic protocols for user identification and digital signature'
Y Lee, SG Hahn, *Pragocrypt 96 pp 393–399*

The authors present protocols for ID-based encryption and signature that are based on ElGamal/Schnorr primitives.

054616 'Sparse RSA Secret Keys and Their Generation'
CH Lim, PJ Lee, *SAC 96 pp 117–131*

The authors discuss ways of generating RSA keypairs so that the secret key is short and/or sparse.

054617 'Proxy signatures: delegation of the power to sign messages'
M Mambo, K Usuda, E Okamoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 9 (1996), pp 1338–1354*

This journal version of **051430** proposes digital proxy signatures that allow designated persons to sign on behalf of a principal. Proxy signature schemes can be based on either the discrete logarithm or factorisation problems.

054618 'A Non-interactive Public-Key Distribution System'
UM Maurer, Y Yacobi, *Designs, Codes and Cryptography v 9 no 3 (Nov 96) pp 305–316*

A public key distribution scheme is presented based on Diffie-Hellman with a composite modulus, with respect to which the authority can work out discrete logarithms. This system, unlike previous ones, does not depend on a per-key randomiser and so can be used on completely non-interactive applications. The idea is to put the randomiser in the users's secret key.

054619 'Cryptanalysis of a voting scheme'
M Michels, P Horster, *CMS 96 pp 53–59*

A voting scheme proposed at Eurocrypt 93 by Park, Itoh and Kurosawa and broken by Pfitzmann at Eurocrypt 94 (**032627**) is shown to have yet more weaknesses in this paper. In particular, if one of the anonymous remailers used is not honest, it is impossible to tell which one, so a disruption can be repeated ad infinitum; and the dishonest party can compute the vote in private without anyone else learning it. This violates the fairness property claimed for the original scheme.

054620 'New El Gamal type threshold digital signature scheme'
C Park, K Kurosawa, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 86–93*

This paper proposes a (k, n) threshold El Gamal type digital signature scheme with no trusted centre. It is a variant of the NIST Digital Signature Standard.

054621 'A Parallel Implementation of RSA'
D Pearson, *SAC 96 pp 107–116*

The author discusses the possible use of parallelism in RSA computations and in particular how it can interact with residue number systems.

054622 'Trials of Traced Traitors'
B Pfitzmann, *Info Hiding 96 pp 49–64*

The author extends **053630** to shows how the traitor tracing scheme of **034127** can be adapted to add practical non-repudiation properties. The user chooses a random identity and signs a one-way hash of it; the content provider stores this signature in case of future disputes and inputs the random identity into the traitor tracing scheme. This system may be made frameproof by multiparty computation techniques.

054623 'A Restrictive Blind Signature Scheme with Applications to Electronic Cash'
C Radu, R Govaerts, J Vandewalle, *CMS 96 pp 196–207*

The authors show how Brands' restrictive blind signatures (**043603**) can be implemented using Okamoto's rather than Schnorr's signature scheme. They outline an electronic cash system based on it.

054624 'Breaking knapsack cryptosystems by L_∞-norm evaluation'
H Ritter, *Pragocrypt 96 pp 480–492*

The author shows how to break the knapsack system proposed by Orton in **032625** using a depth-first search of l_∞-norm short lattice vectors. Using Hoelder's inequality to prune the enumeration makes this efficient.

054625 'Blind Decoding, Blind Undeniable Signatures, and Their Applications to Privacy protection'
K Sakurai, Y Yamane, *Info Hiding 96 pp 257–264*

The authors adapt blind signature techniques to undeniable signatures and to blind decoding. They suggest the latter mechanism might be used by a publisher whose customers wish to buy pages of information without the publisher learning which pages are of interest; the publisher encrypts them using a given public key, whose corresponding decryption function he will perform for a fixed price. Pages can be blinded before decryption.

054626 'A hierarchical and dynamic group-oriented cryptographic scheme'
SJ Wang, JF Chang, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 1 (1996), pp 76–85*

This paper proposes a dynamic group-oriented cryptographic scheme to access a multilevel data hierarchy. It uses a trusted central authority that administers the organisational structure.

054627 'ID-Based Authentication for Mobile Conference Call'
SJ Wang LP Chin, JF Chang, *IFIP 96 pp 49–58*

The authors present an ID-based call setup and conference call protocol. Both the mobile unit and the base station are mutually authenticated and location privacy can also be achieved. The scheme shows low computation complexity and solves some problems with a base station intrusion. Hand-off re-authentication is also addressed.

7 Computational Number Theory

054701 'Counting Rational Points on Curves and Abelian Varieties over Finite Fields'
LM Adleman, MDA Huang, *ANTS II pp1–16*

The authors present improved techniques for counting the number of points on abelian varieties over finite fields,, which underlie their primality testing algorithm.

054702 'Asymptotic semismoothness probabilities'
E Bach, R Peralta, *Mathematics of Computation v 65 no 216 (Oct 96) pp 1701–1715*

The authors call an integer n semismooth with respect to n^a and n^b if all its prime factors are less than n^b, and all but one of them are less than n^a. The probability $G(a,b)$ that n is semismooth turns out to have some useful recurrence properties that enable its value to be computed, and checked by comparison with existing empirical tables of smoothness. Tables for the probability of semismoothness are given and their implications for the quadratic sieve are mentioned.

054703 'On Smooth Ideals in Number Fields'
JA Buchmann, CS Holliger, *Journal of Number Theory v 59 no 1 (July 96) pp 82–87*

There is a lower bound for the number of smooth ideals in an algebraic number field that depends only on its degree.

054704 'Performance Analysis of the Parallel Karatsuba Multiplication Algorithm for Distributed Memory Architectures'
G Cesari, R Maeder, *Journal of Symbolic Computation v 21 no 4–6 (Apr-Jun 96) pp 467–473*

Three different implementations of the Karatsuba algorithm turned out to have noticeably different performance for numbers of practical size; they allocated parallel tasks in different ways.

054705 'Design of secure elliptic curves over extension fields with CM method'
JH Chao, K Harada, N Matsuda, S Tsujii, *Pragocrypt 96 pp 93–108*

The authors show how to extend the complex multiplication method from prime fields to extensions. This is used to generate elliptic curves over fields of characteristic 2 whose order has a large prime divisor. Examples are given over GF(2^{113}) and GF(2^{143}); computation times were of the order of a minute.

054706 'Computing l-isogenies using the p-torsion'
JM Couveignes, *ANTS II pp 59–65*

The Schoof-Atkin-Elkies method for computing the order of an elliptic curve requires the computation of isogenies, which was previously done most quickly with the Lercier-Morain formal groups method. The present paper describes a simpler method for the case of small characteristic, which runs in time $O(l^{2+\epsilon})$ rather than $O(l^{3+\epsilon})$

054707 'On the Reduction of Composed Relations from the Number Field Sieve'
TF Denny, V Müller, *ANTS II pp 75–90*

The authors present a way of reducing the weight of the matrix in the number field sieve. The current cycle finding algorithms combine several hundred partial relations to get one full relation, which leads to many nonzero entries in the matrix. The new idea is to look at points that occur in more than one cycle, and then cut and paste to reduce the average number of partials per cycle. Algorithms for doing this are described and their effect on the sieve's performance are tabulated for both factorisation and discrete log computations; the weight of the matrix can be reduced by up to 30% with relatively little effort.

054708 ‘A Multiple Polynomial General Number Field Sieve’
M Elkenbracht-Huizing, *ANTS II pp 99–114*

The author shows that no great changes are required to use more than two polynomials with the number field sieve. She compares the performance of two, three and four polynomial variants from both a theoretical and empirical point of view, which ended up in fairly close agreement; using three polynomials speeds up classical sieving by about 35%, while four polynomials get an improvement of about 45%. However, there was no improvement in lattice sieving, which is still faster than the classical method.

054709 ‘On Lattices over Number Fields’
C Fieker, ME Pohst, *ANTS II pp 133–139*

The authors show that a form of LLL algorithm can be used in Dedekind domains, despite their lack of a canonical embedding into $\mathbf{R}^n$.

054710 ‘Probabilistic Computation of the Smith Normal Form of a Sparse Integer Matrix’
M Giesbrecht, *ANTS II pp 173–186*

This paper presents a new probabilistic algorithm for diagonalising sparse matrices. An $n \text{ x } n$ matrix A with $O(n \log n)$ nonzero entries needs $O(n^2 \log^2 \parallel A \parallel)$ bit operations to find the Smith form.

054711 ‘The Generalise Gauss Reduction Algorithm’
M Kaib, CP Schnorr, *Journal of Algorithms v 21 no 3 (Nov 96) pp 565–578*

The authors generalise Gauss’s lattice basis reduction algorithm from the l_2-norm to arbitrary norms, and give time bounds for it. The algorithm coincides with the Lovász-Scarf algorithm for the 2-dimensional case.

054712 ‘A primality test involving elliptic curves and a Gauss algorithm’
S Martín, P Morillo, I Gracia, *Pragocrypt 96 pp 87–92*

The authors propose a variant of the elliptic curve primality proving technique. They modify Gauss’ algorithm for finding primitive roots so as to compute the order of given points on the curve, rather than computing the order of the group directly.

054713 ‘Old and New Deterministic Factoring Algorithms’
J McKee, R Pinch, *ANTS II pp 217–224*

The authors survey a number of deterministic factoring algorithms, and present two new ones that run in time $O(n^{1/3+\epsilon})$. One of them, adapted from a technique of Lehmer, will factor numbers some linear combination of whose factors has a large guessable factor. The other, adapted from Pollard’s lambda method, runs deterministically in time $O(n^{1/4+\epsilon})$ in the case where n has two factors of size $O(n^{1/2})$

054714 ‘Efficient Algorithms for Computing the Jacobi Symbol’
SM Meyer, JP Sorensen, *ANTS II pp225–239*

The authors present algorithms for computing the Jacobi symbol that are about two to three times faster than Euclid’s algorithm for numbers in the 100–1000 digit range, and can be efficiently parallelised.

054715 ‘Faster factoring of integers of special form’
R Peralta, E Okamoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 4 (1996), pp 489–493*

This paper presents a speedup of Lenstra’s elliptic curve factorisation method which works for integers of the form $N = PQ^2$, where P is significantly smaller than Q.

054716 ‘Computational Aspects of Curves of Genus at Least 2’
B Poonen, *ANTS II pp 283–306*

This article provides a survey of computational methods of use with higher genus curves, whose Jacobians have been suggested for use in cryptosystems, with over 100 references.

054717 'Cryptography in real quadratic congruence function fields'
R Scheidler, *Pragocrypt 96 pp 109–128*

The author shows how to extend the scheme proposed in **051611** for doing key exchange in the principal ideal class of a number field, to an analogue of ElGamal signatures.

054718 'Discrete Logarithms: The Effectiveness of the Index Calculus Method'
O Schirokauer, D Weber, T Denny, *ANTS II pp 337–361*

The authors survey recent results in the computation of discrete logarithms, concentrating on variants of the index calculus. The number field and function field sieves are presented as are a number of successful discrete log computations from the last few years. They then report a variant of the function field sieve that is efficient at finding discrete logarithms in class groups; it exploits the analogue of smoothness.

054719 'Equivalences between elliptic curves and real quadratic function fields'
A Stein, *Pragocrypt 96 pp 76–86*

In **051611**, Scheidler, Stern and Williams had proposed doing key exchange in the principal ideal class of a number field, rather than in a group. In this paper, a reduction of this problem is given to the discrete logarithm on the corresponding elliptic curve.

054720 'Computing Discrete Logarithms with the General Number Field Sieve'
D Weber, *ANTS II pp 391–403*

The author reports records in calculating discrete logarithms using the general number field sieve. In September 95 he succeeded with a 65-digit prime; in March 96 he completed the precomputation step for McCurley's 129 digit challenge. This involved over 110 MIPS years of sieving and resulted in over 300,000 cycles, and gives the discrete logs of those elements that are in the factor base.

054721 'Parallel Implementation of the Accelerated Integer GCD Algorithm'
K Weber, *Journal of Symbolic Computation v 21 no 4–6 (Apr-Jun 96) pp 457–466*

The author describes an implementation of accelerated integer GCD computation on a shared memory multiprocessor machine. Speedups of up to four times were achieved with very long inputs, but for numbers in the 512 to 2048 bit range the use of parallelism actually slowed things down slightly.

8 Theoretical Cryptology

054801 ‘Codes’
GR Blakley, I Borosh, *Pragocrypt 96 pp 253–271*

The authors present an abstract theory of codes, whether finite or infinite, and whether discrete or continuous; codes are defined by the uniqueness of decodability. The theory encompasses both block and stream ciphers, as well as secret sharing, threshold schemes, and even DNA; but some dictionaries are not codes.

054802 ‘An Interactive τ-Restricted Key Distribution Scheme’
C Blundo, AG Gaggia, *Pragocrypt 96 pp 337–248*

The authors examine unconditionally secure key distribution schemes that allow the computation of up to τ different keys for τ pairwise different conferences. Bounds are calculated; a concrete construction is given for $\tau = 2$ and then generalised.

054803 ‘New Bounds on the Share’s Size in Secret Sharing Schemes’
C Blundo, A De Santis, R De Simone, U Vaccaro, *Pragocrypt 96 pp 349–358*

The authors prove that for any integer d there exists a d-regular graph for which any secret sharing scheme has its information rate bounded by $2/(d + 1)$.

054804 ‘Recent developments in quantum cryptography’
G Brassard, *Pragocrypt 96 pp 183–192*

The author describes the first quarter century of quantum cryptography, with particular emphasis on the development of various approaches to quantum key distribution.

054805 ‘Distributed Delegation Systems’
C Charnes, J Pieprzyk, R Safavi-Naini, *Pragocrypt 96 pp 289–305*

This paper presents unconditionally secure protocol for a group of participants to authorise someone to construct a single authentic message on their behalf, and explains how to solve a threshold indexing problem that arises when trying to implement various access structures in such schemes. It also introduces ideal families of threshold schemes which can be used for multiple delegation systems.

054806 ‘What is going on with Quantum Bit Commitment?’
C Crépeau. *Pragocrypt 96 pp 193–203*

A quantum bit commitment protocol had been thought to be proven secure, but a recent unpublished paper of Mayers has shown that the proof is flawed; the protocol can be attacked using a quantum computer. This attack is claimed to have little practical impact, on the grounds that such an attacker could also break RSA.

054807 ‘Joint Encryption and Message-Efficient Secure Computation’
M Franklin, S Haber, *Journal of Cryptology v 9 no 4 (Autumn 96) pp 217–232*

A joint encryption scheme based on discrete log with respect to a modulus of unknown factorisation is given which enables n parties to evaluate a Boolean circuit of size N privately using $O(nC)$ bits of communication.

054808 ‘Combinatorial bounds and design of broadcast authentication’
H Fujii, W Kachen, K Kurosawa, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 4 (1996), pp 502–506*

This paper presents a combinatorial characterisation of broadcast authentication in which a transmitter broadcasts v messages $e_1(s), \ldots, e_v(s)$ to authenticate a source state s to all n receivers so that any k receivers cannot cheat any other receivers.

054809 ‘Pseudorandom Generators and the Frequency of Simplicity’
YJ Han, LA Hemaspaandra, *Journal of Cryptology v 9 no 4 (Autumn 96) pp 251–261*

The authors show that if there are dense P (or even BPP) languages containing even a sparse set of Kolmogorov-simple strings, then all pseudorandom generators are insecure.

054810 'A Construction for Multisecret Threshold Schemes'
WA Jackson, KM Martin, CM O'Keefe, *Designs, Codes and Cryptography v 9 no 3 (Nov 96) pp 287–303*

The authors develop the concept of multisecret sharing, which they introduced at Crypto 93 (**024823**). They prove lower bounds on the size of the shares that each participant must have and provide a construction that achieves this for small values of one of the parameters.

054811 'Ideal Secret Sharing Schemes with Multiple Secrets'
WA Jackson, KM Martin, CM O'Keefe, *Journal of Cryptology v 9 no 4 (Autumn 96) pp 233–250*

The authors study the set of access structures that can be implemented using an ideal multisecret sharing scheme. It turns out that these structures can be classified completely in terms of the separators of matroids.

054812 'Perfect Secret Sharing Schemes on Five Participants'
WA Jackson, KM Martin, *Designs, Codes and Cryptography v 9 no 3 (Nov 96) pp 267–286*

The authors discuss a number of techniques for obtaining bounds on the information rate of secret sharing schemes, and tabulate these rates for all access structures on five participants.

054813 'On the Reconstruction of Shared Secrets'
J He, E Dawson, *IFIP 96 pp 209–218*

The authors present methods to achieve fair reconstruction of a shared secret with one cheater or minority cheaters. It extends the verifiable secret sharing schemes of Chor and Rabin–Ben-Or. They classify their methods and prove some bounds on cheating probabilities.

054814 'Physical aspects of optical implementation of quantum cryptography'
M Hendrych, M Dušek, O Haderka, *Pragocrypt 96 pp 234–241*

The authors discuss ways of improving the performance of Mach-Zehnder interferometers in quantum cryptography, and argue that balancing considerations favour protocols in which one rather than two detectors are used.

054815 'Q-deformed quantum cryptography and verification of minimal uncertainty'
J Hruby, *Pragocrypt 96 pp 204–211*

The author reports an implementation of quantum key distribution, presents some calculations on q-deformation, and argues that such equipment provides the cheapest experimental verification of the Heisenberg uncertainty principle.

054816 'Efficient Cryptographic Schemes Provably as Secure as Subset Sum'
R Impagliazzo, M Naor, *Journal of Cryptology v 9 no 4 (Autumn 96) pp 199–216*

If the general (as opposed to trapdoor) subset sum problem is hard, it can be used to derive hash functions, pseudorandom generators and other primitives that fall short of full public-key encryption.

054817 'Quantum Computer Implemented by the Coherent Properties of Nonlinear Excitons'
H Matsueda, S Takeno, *Pragocrypt 96 pp 225–233*

The authors discuss some possible mechanisms for building quantum computers.

054818 'Quantum Cryptography Modulating the Spontaneous Emission Rate of Photons'

H Matsueda, F Shibata, C Uchiyama, *Pragocrypt 96 pp 212–224*

The authors suggest novel quentum crypto channels using randomised photon generation which varies over time in a way known in advance to the receiver.

054819 'Detection of cheaters in vector space secret sharing schemes'

C Padró, G Sáez, JL Villar, *Pragocrypt 96 pp 359–369*

The authors present two new secret sharing schemes in which cheaters are detected with high probability; in one of them this happens even if the cheater already knows the secret.

054820 'Authentication codes based on association schemes'

Y Song, K Kurosawa, S Tsujii, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E79-A no 7 (1996), pp 1026–1030*

This paper discusses the problem of reducing the number of keys required to authenticate a plaintext. It also introduces a construction for authentication codes that uses association schemes of triangular and group divisible types.

054821 'Cryptography based on Oblivious Transfer'

A Tapp, *Pragocrypt 96 pp 400–412*

The author discusses ways to use oblivious transfer to do committed circuit evaluation, oblivious circuit evaluation and private multi-party computation.

9 Book Reviews

'ALGORITHMIC NUMBER THEORY VOLUME 1 — EFFICIENT ALGORITHMS'
Eric Bach, Jeffrey Shallitt
MIT Press, ISBN 0-262-02405-5

The goal of this book, as stated in the introduction, is to provide a thorough introduction to the design and analysis of algorithms for problems from the theory of numbers. This is the first of two volumes; the second is planned to cover factoring and discrete logarithms, and so will be eagerly awaited by the crypto community; but even this introductory volume contains much of interest.

It starts off with the basics, such as Euclid's algorithm and basic complexity theory, and moves on rapidly to algorithms for finite fields, such as factoring polynomials, solving binomial congruences and constructing field extensions. A survey of prime number theory from the analytic viewpoint is next, followed by a chapter on computational methods such as primality testing and proving. There is much more, such as Carmichael numbers and primality tests for numbers of special forms.

The level of the book makes it suitable as a text for a first year postgraduate mathematics or computer science course, or as a source for undergraduate teaching. The history of the subject is given in detail as are many exercises; there is a thorough bibliography including many references that deserve to be more widely read. It will also be a valuable reference book for the working scientist.

'PSEUDORANDOMNESS AND CRYPTOGRAPHIC APPLICATIONS'
Michael Luby
Princeton Computer Science Notes, 1996; ISBN 0-691-02546-0

This book contains the amplified notes of eighteen lectures on the complexity approach to pseudorandomness, given by Mike Luby at Berkeley. The first ten lectures develop a proof of how a pseudorandom function can be constructed from any one-way function; the rest of the book shows how pseudorandom functions can be used to construct stream ciphers, block ciphers, universal one-way hash functions, hash-based digital signature schemes and zero-knowlegde proofs. There are also some results on public key issues, such as the proportion of discrete log instances in a given group that can be weak before they all are. The material will no doubt be a useful reference for the cognoscenti.

However, a larger opportunity is missed. The author's approach to cryptography is in need of systematic exposition to a wider audience, as it is hard to reverse engineer from the research literature, and thus relatively inaccessible to people who have not attended a university where it is doctrine. But Luby's book is a solid mass of theorems, with little plaintext explanation of what is going on, and no diagrams — not even of the famous Luby-Rackoff construction. A reader who did not already understand this subject, at least in general terms, would have a hard time learning it here — which somewhat negates its potential value as a textbook.

'INTERNET SECURITY FOR BUSINESS'
Terry Bernstein, Anish B Bhimani, Eugene Schultz, Carol A Siegel
Wiley, 1996; ISBN 0-471-13752-9

This book sets out to introduce the frightened corporate neophyte to the world of Internet security and does a modestly workmanlike job of it. There is a particularly clear explanation of many of the present technical threats, such as IP spoofing, and an intelligent discussion of the risk management versus baseline controls debate. There is also a reasonably complete list of RFCs and proposed security mechanisms, circa February 96. Unfortunately the book is rather weak on cryptography, despite spending many pages on this subject. Political issues, such as key escrow and emerging copyright law, are also not well covered.

‘DECRYPTED SECRETS — METHODS AND MAXIMS OF CRYPTOLOGY’

Friedrich L Bauer
Springer, 1997; ISBN 3-540–60418-9

This book concentrates on pre-computer age encryption methods such as polyalphabetics and Playfair. There is some historical material and snippets on more modern methods, but the bulk of the book is devoted to providing a very thorough exposition of classical ciphers, followed by a systematic and detailed description of attack techniques. This includes quite a lot of material that is not very widely known, from the hidden symmetries of Playfair to the kappa test and other statistical techniques of Friedmann and Kullback. It also covers the theory behind the operation of the bombes, diagonal boards and other devices at Bletchley Park.

‘SECURITY IN COMPUTING’

Charles P. Pfleeger
Second edition; Prentice Hall, 1997; ISBN 0-13-337486-6

Chuck Pfleeger’s book has become one of the commonly used texts in teaching computer security, and an updated second edition is now available. The new book gives good coverage of some areas, such as firewalls, that have become topical, but others — such as Java — get only a brief mention. Macro viruses are ignored, despite their being the fastest growing programmed threat; and while differential cryptanalysis is covered, the much more effective linear cryptanalysis is not. One hopes that the next update will be more thorough.

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 1997 (volume 6) plus a set of the remaining back numbers (currently v 2 no 1 and 4 and all of v 3, 4 and 5) 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 1223 334678, or mail it to us at:

**Northgate Consultants Ltd., 10 Water End, Wrestlingworth, Sandy,
Beds SG19 2HA, United Kingdom**