Computer and Communications

Security Reviews

Volume 4 Number 2 (June 1995) ISSN 1352-6278

CONTENTS

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

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

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 6th June 1995; and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

DCS 94: Fourteenth Annual Conference on Distributed Computing Systems, Poznan, Poland, June 21–24 1994; *proceedings published by the IEEE Computer Society Press, ISBN 0-8186-5840-1*

LISA 94: Eighth Usenix Systems Administration Conference, September 19–23, San Diego, California; *proceedings published by the Usenix Association, ISBN 1-880446-64-2*

NCSC 94: Seventeenth National Computer Security Conference, 11–14 October 1994, Baltimore, Maryland; *proceedings published by the US National Institute of Standards and Technology; no ISBN*

FOCS 94: Thirty Fifth Annual Symposium on the Foundations of Computer Science, November 20–22, 1994, Santa Fe, New Mexico; *proceedings published by the IEEE Computer Society Press, ISBN 0-8186-6580-7*

Apps 94: Tenth Annual Computer Security Applications Conference, December 5–8, 1994, Orlando, Florida; *proceedings published by the IEEE Computer Society Press, ISBN 0-8186-6795-8*

ICS 94: International Computer Symposium, December 12–15, Hsinchu, Taiwan

Usenix 95: USENIX 1995 Technical Conference, January 16–20, 1995, New Orleans, Louisiana; *proceedings published by the USENIX Association, ISBN 1-880446-67-7*

ADC 95: Sixth Australasian Database Conference, Adelaide, 30-31 January 1995; *proceedings published as Australian Computer Science Communications v 17 no 2, ISSN 0157-3055*

ACSC 95: Eighteenth Australasian Computer Science Conference, 1–3 February 1995, Adelaide, Australia; *proceedings published in Australian Computer Science Communications v 17 no 1, ISSN 0157-3055*

ISOC 94: Internet Society Symposium on Network and Distributed Systems Security, 16-17 February 1995, San Diego, California; *proceedings published by the IEEE Computer Society Press, ISBN 0-8186-7027-4*

LATIN 95: Second Latin American Symposium on Theoretical Informatics, Valparaíso, Chile, April 3–7, 1995; *proceedings published as Springer LNCS v 911*

Some of the articles in NCSC were covered in v 3 no 4.

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

1 Applications and Engineering

042101 'Belief in correctness'
M Abrams, MV Zalkowitz, *NCSC 94 pp 132–141*

The authors survey the techniques which can be used to enhance belief in the reliability of security mechanisms, such as formal methods, simulation, testing, CASE, structured programming and process maturity. All of them have shortcomings which prevent their giving us assurance beyond reasonable doubt.

042102 'An Overview of SNIF: A Tool for Surveying Network Information Flow'
J Alves-Foss, *ISOC 94 pp 94–101*

SNIF monitors TCP between local and remote hosts. It logs TCP start and stop times and byte counts in each direction. Alarms and signals have four priority levels. A GUI analysis tool provides real-time feedback on events, and the system is scalable, distributed, extensible, and fault tolerant.

042103 'Ops/Intel Interface Lessons Learned: The Integrator's Perspective'
K Arndt, M Burgoon, J Firey, K Rodenhausen, *Apps 94 pp 268–277*

The authors describe some problems they encountered when providing an interface between operations and intelligence for the US Atlantic Command. This had to support decisions to downgrade information from SCI to secret, and was implemented on Sparcstations running Trusted Solaris with a filtering router. Software licence managers could not run in a multilevel environment, so separate managers had to be run at each level.

042104 'PEMToolKit: Building a Top-Down Certification Hierarchy for PEM from the Bottom Up'
A Bahreman, *ISOC 94 pp 161–171*

PEMToolKit helps establish a public key infrastructure by providing methods to build a certification hierarchy for PEM from the bottom up. The bottom up approach can start with self-signed certificates. Later, organisational CAs may emerge, and larger islands of certification may come into existence. Cross certification can occur between arbitrary CAs. Certificate retrieval may be on-line or off-line.

042105 'Multicast-Specific Security Threats and CounterMeasures'
A Ballardie, J Crowcroft, *ISOC 94 pp 2–16*

This paper addresses eavesdropping and denial of service attacks on the Internet MBone. The proposed improvements are group access controls (to restrict group membership and defend against unauthorized listening) and transit traffic control (to detect unauthorised sending); these use a public key based infrastructure and a linked set of multicast authorisation servers. Multicast group certificates are specified by one group member and signed by an authorisation server; they contain group names, an inclusion or exclusion list, and a sender list.

042106 'Invisible images ensure security'
TE Bell, *IEEE Spectrum v 12 no 4 (April 95) p 17*

This article describes a technique for producing secure holograms; the image is combined with a reference image which acts as the key.

042107 'AOS: An Avionics Operating System for Multi-level Secure Realtime Environments'
MM Bernstien, CS Kim, *Apps 94 pp 236–245*

The authors describe a multilevel secure realtime distributed operating system designed for the next generation of strike aircraft. This is designed for Intel i960 processors, because of the security and object-oriented support features; the basic mechanism is address translation which is used to implement build-time label-based mediation.

042108 ‘Security for decentralized health information systems’
G Bleumer, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 139–145*

A prototype encryption system was developed under the EC’s project SEISMED to secure the transmission and archiving of medical records. It is based on DES and RSA and runs on Apple hardware.

042109 ‘A Prototype Multilevel-Secure DoD Directory’
PK Boucher, TF Lunt, *Apps 94 pp 180–188*

The authors describe a directory being developed for the US DoD based on X.509. It has to handle information ranging from unclassified to secret, and a prototype is implemented in SeaView.

042110 ‘A Practical Approach to User Authentication’
M Brown, SJ Rogers, *Apps 94 pp 108–116*

The authors describe a typing pattern recognition system based on neural networks. Holding the fraud rate at zero, the insult rate was 12–40% for groups of about 1000 users and an average of 16 characters per sample.

042111 ‘When fair is fair’
G Bull, *Banking Technology (June 95) p 15*

From 1st July 1995, the EC Unfair Contract Terms in Consumer Contracts Directive will come into force in the UK. It is expected to affect automatic teller machine and other card based systems in that the burden of proof in the event of disputes will be placed firmly on the bank.

042112 ‘Americans finally wooed by chip’
Card World Independent (Apr 95) p 7

This short article surveys smartcard applications in the USA, including electronic benefits transfer, and describes the work of the Smart Card Forum, a consortium of banks, government agencies, vendors and others.

042113 ‘Australian contactless trial crossing technology frontiers’
Card World Independent (Mar 95) p 4

Australia is introducing a national contactless smart card which will function as a bus and train ticket; it will also pay for taxis and road tolls, and administer incentive schemes. It can be either personalised or anonymous, but in the latter case any value or tickets loaded are lost if the card is.

042114 ‘Electronic notary seal will ensure validity’
Card World Independent (Apr 95) p 2

VISA and Microsoft are working on a certificate system for Internet shopping. The user’s certificate will function as a credit card, and the merchant’s as a VISA logo; six banks will be involved in testing it.

042115 ‘Italy takes the smart option’
Card World Independent (Mar 95) p 6

Italy has at least six regional health card systems. One of them — in San Marino — doubles as an ATM card; another, due to be launched in Treviso, will gather epidemiological information and will also contain tax data, so that doctors and pharmacists can see who qualifies for low income discounts.

042116 ‘Quebec healthcard evaluation almost finished’
Card World Independent (May 95) pp 4–5

For the last two years, smartcard health records have been issued to over 7000 people in Quebec. These have five zones containing different aspects of the record (ID, emergency, medication, vaccinations and the full history); each healthcare profession can access only those it needs. There were robustness problems, especially with men putting the cards in their hip pockets; but the project was judged to be a success, and of especial benefit to the elderly and the chronically ill.

042117 'South Africans push smart cards'
Cards International (10/3/95) p IV

This article discusses the evolution of, and prospects for, smartcard payment systems in South Africa.

042118 'Support for security in distributed systems using MESSIAHS'
S Chapin, E Spafford, *NCSC 94 pp 339–347*

The authors describe a project to support security in distributed systems by providing firewalls and matching security labels across heterogeneous systems, while maintaining local control and keeping system descriptions private.

042119 'Human and Machine Recognition of Faces: A Survey'
R Chellappa, CL Wilcon, S Sirohey, *Proceedings of the IEEE v 83 no 5 (May 95) pp 705–740*

The authors survey the literature of face recognition. They discuss commercial and law enforcement applications, of which the latter appear likely to predominate; discuss the known psychological and neurological factors in human performance of the task; and describe the various algorithms for locating a face in an image, extracting features and recognising these, including a variety of transform and feature based methods. They bring out the lack of benchmarks for evaluating the technology in various contexts, from mugshot matching to crowd surveillance.

042120 'Copyright Protection for Electronic Publishing Over Computer Networks'
AK Choudhury, NF Maxemchuk, S Paul, HG Schultzrinne, *IEEE Network v 9 no 3 (May/June 95) pp 12–20*

The authors discuss the security requirements for electronic publishing; the reasonable goal might be to create a system which is as secure as paper, in that large-scale low-cost anonymous redistribution would be prevented. One solution would be to put trusted hardware in printers; where this is not possible, decryption software is the obvious choice and reverse engineering the obvious threat. They discuss some techniques which might make this less likely or less feasible.

042121 'Inside the set-top box'
WS Ciciora, *IEEE Spectrum v 12 no 4 (Apr 95) pp 70–75*

The author describes the evolution of set-top box technology from the early cable TV converters to current satellite and digital systems with a wide range of features. There is quite a lot of politics involved in box ownership and signal security; both the content provider's intellectual property rights and the viewer's privacy need to be protected. Recent US standards activity on security interfaces will eventually accommodate multiple decoders and 'feature boxes'.

042122 'Speech Coders: From Idea to Product'
RV Cox, P Kroon, JH Chen, R Thorkildsen, KM O'Dell, DS Isenberg, *AT&T Technical Journal v 74 no 2 (Mar-Apr 95) pp 14–22*

The authors describe the engineering constraints and tradeoffs in the design of speech coders, and describe one product, AUDIX, as an example. The current US defence research goal is to develop 2.4 kbit/sec coders for secure telephony which exceed the speech quality of the 4.8 kbit/sec products made to the 1990 standard FS1016; this will enable more efficient use of satellite channels. Other applications driving the technology are digital cellular systems, voice messaging, and improving videophone speech bandwidth from telephone standard to 7KHz.

042123 'A turning grille from the ancestral castle of the Dutch stadtholders'
K de Leeuw, H van der Meer, *Cryptologia v XIX no 2 (April 95) pp 153–165*

The authors describe and solve a turning grille cipher which turned out to be a dispatch from 1745.

042124 'Paknet initiative signals winds of change'
G Dow, *Security Surveyor v 25 no 8 (Mar 95) pp 21–25*

The author looks at the UK suppliers of secure alarm signalling services. A major problem is line faults; the police plan to stop responding at any given site after two false alarms. One option is to move to cellular radio; the Paknet data service is already used is secure applications such as credit card authorisation and electricity meter reading, and is now being promoted for alarm signals as well.

042125 'Were the Japanese army codes secure?'
EJ Drea, *Cryptologia v XIX no 2 (April 95) pp 113–136*

The author describes a number of enciphered code systems used by the Japanese in the second world war, and discusses Allied successes against them.

042126 'The Revolution is Here'
B Dussauge, *International Security Review no 88 (Spring 95) pp 23–25*

The author discusses the move from magnetic strip cards to chip cards, and predicts that this will be a key enabling technology for the Internet.

042127 'A Practical Hardware Device for System and Data Integrity as well as Malicious Code Protection'
TE Elliott, *NCSC 94 pp 274–282*

Following a number of incidents, the Communications Security Establishment of Canada has developed a hardware device which makes part of a PC hard disk read only, so that operating system and application programs can be protected from viruses. They are now looking for commercial licensees.

042128 'How much does the chip cost?'
D Everett, *Smart Card News v 4 no 5 (May 95) pp 97–99*

The author discusses how the cost of a smartcard varies with the type and size of memory installed.

042129 'The making of a chip'
D Everett, *Smart Card News, part 1: v 4 no 3 (Mar 95) pp 56–59; part 2: v 4 no 4 (Apr 95) pp 76–79*

The author explains the MOS transistor technology commonly used in smartcards.

042130 'ATM scams take the shine off fraud figures'
Financial Technology International Bulletin v 12 no 8 (Apr 95) p 3

Two separate groups of people have been charged in the UK with conspiring to steal £2.6m from the Link ATM network, using shoulder surfing and false terminal techniques. However, total fraud losses on credit and debit cards were down from £129.8m in 1993 to £96.8m in 1994.

042131 'European Commission pilots purse scheme as EMU deadlines loom large'
Financial Technology International Bulletin v 12 no 7 (Mar 95) pp 4–5

This article describes the CAFE demonstration project at the EC HQ in Brussels. Staff will use electronic wallets to pay for food, drink and other goods from both vending machines and manned sale points.

042132 'Magnetic "fingerprint" to beat card fraudsters'
T Fitzpatrick, *Banking Technology v 12 no 4 (May 95) p 8*

Researchers in Washington University, St Louis, have developed a technique for identifying individual magnetic cards from the pattern of magnetic domains on the strip. A small area of the strip can be examined at a much finer resolution than that used for the encoding and information about the permanent underlying patterns can be used in authenticating card transactions.

042133 'How to keep thieves guessing'
B Fox, *New Scientist (3rd June 95) p 18*

A UK analogue cellular phone operator has introduced an authentication option to foil phone number thieves. It is based on a challenge-response protocol which yields a temporary electronic serial number. The rival operator has placed its faith in call pattern analysis.

042134 'Artificial Intelligence and Intrusion Detection: Current and Future Directions'
J Frank, *NCSC 94 pp 22–33*

The author discusses how one might use AI to train intrusion detection applications rather than building and tuning them by hand. He reports testing three different feature selection algorithms on network log data.

042135 'Cellular phones providing card fraud access'
Fraud Watch (Spring 95) p 9

Cellular phone fraud is a mixture of subscription fraud (false names, addresses and references), network facility fraud (mostly by insiders) and technical fraud (which affects analogue phones but has not struck GSM operators yet).

042136 'Fake "officials" demand PINs'
Fraud Watch (Spring 95) p 3

UK criminals have been stopping customers who have just used ATMs for a bogus 'security check' in which the customer's card is swiped and their PIN demanded.

042137 'Plastic fraud in the UK down 25%'
Fraud Watch (Spring 95) p 8

The APACS fraud figures for 1994 are given; they are down on 1993.

042138 'A New Attack on Random Pronounceable Password Generators'
R Ganesan, C Davies, *NCSC 94 pp 184–197*

The authors criticise two US government systems for generating random pronounceable passwords — in the NIST standard and the Sandia version of Kerberos. These let users choose one from a list of random strings with alternating vowels and consonants. It was found that user preferences caused an uneven distribution of choices, with the result that the overall attack effort was less than a tenth of what was claimed.

042139 'Chips on their shoulders'
JS Giannone, *Cards International (10/3/95) pp II–III*

In this article, senior managers at VISA, Mastercard and Europay discuss their views of the products which their common smartcard architecture will deliver.

042140 'The MITRE Security Perimeter'
DS Goldberg, *Apps 94 pp 212–218*

MITRE has been using SecurID password generators and a firewall. The few breakings so far involved bugs in home-grown authentication software and in the firewall configuration; in future, proxy gateways may be used.

042141 ‘Devil’s Advocate’
S Gordon, *Network Security (May 95) pp 12–15*

This article describes SATAN, a tool which helps look for holes in Unix security. It checks for common leaks in ftp, NFS, NIS, rexd, xauth, rsh, rlogin and sendmail.

042142 ‘On a Follower Tone-Jammer Countermeasure Technique’
AA Hassan, JE Hershey, JE Schroder,, *IEEE Transactions on Communications v 43 no 2/3/4 (Feb-Apr 95) pp 754–756*

The authors analyse a technique proposed to protect frequency hopped radios from repeater jammers in which information is signalled by the mere presence of a tone in a subset of the available channels. They graph its bit error rates.

042143 ‘Modular design for online protection and observation programs’
R Hörmandser, *Journal of Microcomputer Applications v 18 no 1 (95) pp 23–57*

The author discusses how to minimise the memory requirement of antivirus software by using a modular design with a number of linked drivers.

042144 ‘State Transition Analysis: A Rule-Based Intrusion Detection Approach’
K Ilgun, RA Kemmerer, PS Porras, *IEEE Transactions on Software Engineering v 21 no 3 (Mar 95) pp 181–199*

The authors describe a prototype intrusion detection tool which uses a rule based expert system together with a state transition diagram to detect penetrations. They provide a sample analysis for a flaw in 4.2 BSD Unix in which an attacker exploits the fact that ‘mail’ sometimes fails to reset the setuid bit of a file. The also describe some test results and compare their system to other intrusion detection tools.

042145 ‘Putting on the style’
EP Jensen, *The Banker (May 95) pp 14–15*

In this article, VISA’s CEO predicts that an intelligent device — in most cases a smartcard — will be the cornerstone of banking in the future. It will not just secure ATM, eftpos and home banking transactions, but also contain information on the customer’s loans, tax, insurance and investments thus enabling the relationship to be managed better. He envisages that interbank organisations will become involved in much more than just settlement.

042146 ‘The Structure of the OpenVMS Management Station’
JE Johnson, *Digital Technical Journal v 6 no 4 (Fall 94) pp 75–88*

The author describes a system administration tool for OpenVMS, and the scalability considerations which motivated the design of its mechanisms for managing authentication, communications, access and quotas. It is implemented as client software on a PC which communicates with server object management modules on VMS clusters and other resources.

042147 ‘UK cards get smart’
D Jones, *Banking World v 13 no 6 (June 95) p 27*

The UK banking industry has set up a project to develop smartcards which will comply with the new VISA/Mastercard/Europay standards. These cards will be introduced from 1997, and all British bank cards should have chips by 1999. One driving factor is automatic teller machine security, and the major worry is the politics of forcing retailers to upgrade their terminals.

042148 ‘Enemy codes and their solutions’
D Kahn, *Cryptologia v XIX no 2 (April 95) pp 166–197*

This is a reprint of a 1918 army codebreaking manual which was discovered in the UK Public Records Office.

042149 'The cryptologic origin of Braille'
D Kahn, *Cryptologia v XIX no 2 (April 95) pp 151–152*

Louis Braille developed his idea for raised-dot writing for the blind from a more primitive military system devised for writing secretly in the dark.

042150 'A Certificate Management System: Structure, Functions and Protocols'
N Kapidzic, A Davidson, *ISOC 94 pp 153–160*

CMS is a X.509 certification infrastructure being built for the Swedish post office to handle key management. It is intended for large organisations, and provides the naming authority, certificate repository, and root of the hierarchy. The user is now running a low-level assurance policy with CMS user agents interfaced to PEM.

042151 'Using Application profiles to Detect Computer Misuse'
NL Kelem, DF Sterne, DI Dalva, KM Walker, D Anderson, H Javitz, A Valdes, LI Lankewicz, G Bell, *NCSC 94 pp 400–411*

The authors tried applying intrusion detection techniques to the behaviour of applications rather than users. the results were not encouraging.

042152 'Availability: Theory and Fundamentals for Practical Evaluation and Use'
KJ Keus, M Ullmann, *Apps 94 pp 258–264*

Resistance to service denial attacks has historically been considered in the context of dependability and fault tolerance rather than from the security point of view. The authors recast the model in terms of security functions such as error recognition, resource checking and auditing.

042153 'Smart cards — a security tool for Health Information Systems'
GO Klein, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 147–151*

The author asserts that smartcards should have public key crypto to be useful in medicine.

042154 'Smart cards and their opportunities for controlling Health Information Systems'
E Kühnel, G Klepser, R Engerbrecht, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 153–137*

The authors describe a chip card developed in Germany for patients with diabetes.

042155 'Speakeasy: The Military Software Radio'
RJ Lackey, DW Upmal, *IEEE Communications Magazine v 33 no 5 (May 95) pp 56–61*

The authors describe a US Army project to develop a military radio which uses programmable signal processing to emulate more than 15 existing radios, including GPS, cellular phones, satcom, analogue HF, SINCGARS, HAVE QUICK and low probability of intercept modes. It will operate from 2MHz to 2GHz with interchangeable RF modules and IF digitisation; in addition to software waveform processing, there is also a programmable security processor which emulates the comsec and transec features of five existing crypto devices.

042156 'Gates looks to future of electronic banking'
S Laurie, *Banking Technology v 12 no 3 (April 95) p 4*

This article presents a brief interview with Bill Gates on the future direction of Microsoft's involvement in home banking. This will involve banks, take place over the Microsoft Network, and may have electronic bill payment as an early feature.

042157 'Puzzle palace conducting Internet surveillance'
W Madsen, *Computer Fraud and Security Bulletin (June 95) pp 12–13*

The NSA is monitoring source and destination IP addresses on a number of Internet routes. Nine monitoring points are named, of which two are run by NASA. This 'black' programme is said to be an open secret in the industry; its goal includes monitoring international traffic, but its effectiveness is questioned.

042158 'The information services supermarket — an intelligent network prototype'
IW Marshall, M Bagley, *BT Technical Journal v 13 no 2 (Apr 95) pp 132–142*

The authors describe British Telecom's vision of the service control and management system needed to enable a diverse population of vendors to provide interactive multimedia services over a broadband network. The standards should be published by TINA in 1997.

042159 'An Electronic Retail Payment System with Distributed Control — A Conceptual Design'
T Matsumoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 67–76*

This paper proposes an electronic retail payment system that provides flexible and efficient fund transfers. It addresses security, reliability, circularity, and anonymity in large-scale applications.

042160 'Rechnergestützte Steganographie: Wie sie Funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist'
Steffen Möller, Andreas Pfitzmann, Ingo Stierand, *Datenschutz und Datensicherung v 18 no 6 (94) pp 318–326* (in German)

The authors describe a steganography program called DigiStilz which hides ciphertext or other material in the least significant bits of a digital (ISDN) telephone conversation. It is keyed in that the distance between two ciphertext bits is determined by a pseudorandom number, and transmission is blanked when the speech volume drops below a threshold. They tabulate test results; the rate at which the presence of ciphertext could be detected by ear varied from 1 bit in 8 for a noisy background to 1 in 64 for a quiet one. They argue that the ease with which such a system can be implemented makes legal controls on cryptography pointless.

042161 'The Safety Catch'
S Nassoura, *Data Communications International (May 95) pp 62–77*

Eight brands of authentication token subjected to laboratory tests; they were evaluated for various security and administration features and for their interoperability with different communications servers.

042162 'Mag stripe loses out to chip'
J Newton, *Cards International (27/4/95) p 10*

The author, a police expert on card fraud, perceives the mag strip/chip battle as having been won by the chip card firms. As a result, magnetic strip security enhancement techniques are being sidelined, despite the success of CVV/CVC authentication codes in stopping counterfeiting.

042163 'Tackling counterfeit: "coordination is the key" '
J Newton, *Fraud Watch (Spring 95) pp 6–7*

The author discusses the technologies used to analyse the provenance of fake bank cards, particularly via the holograms. These suggest that most fakes come from a small number of factories, of which one was found in Malaysia; and most people involved in the trade are ethnic Chinese.

042164 'Optically controlled array allows shared functions'
BD Nordwall, *Aviation Week and Space Technology (5/6/95) pp 47–48*

Hughes has developed an optically controlled phased array system which can transmit communications, EW and radar signals at the same time. It is envisaged that shared-aperture conformal or distributed antennae will have advantages in stealth applications. Meanwhile a $9'$ by $3'$ experimental array can transmit on any frequency from 850 to 1400 MHz; it has 4 rows by 24 columns of independent T/R modules.

042165 'It's the business'
R O'Keefe, E Ricketts, W Thompson, *.net (June 95) pp 34–60*

This article surveys commerce on the Internet ranging from various electronic malls through advertising, fashion, porn and prostitution to payment mechanisms.

042166 'X.500 directory services support for Electronic Data Interchange'
D O'Mahoney, N Weldon, *Computer Networks and ISDN Systems v 27 no 5 (May 95) pp 691–701*

The authors describe how X.500 can be used to facilitate EDI by providing a public key certification service. Various products and prototypes are discussed.

042167 'Feeling smart all over'
C Power, JC Boustra, *Cards International (10/3/95) pp 8–11*

This article surveys the smart card scene in France, where 54% of adults carry a banking smartcard. Both customers and retailers prefer cards to any other payment medium; the domestic fraud rate is now 0.037%; and cards are starting to become multifunctional.

042168 'Vaulting with ATM'
B Riggs, *Network Security (Apr 95) pp 8–9*

Asynchronous transfer mode may be heavily used for remote backup of LANs. In fact this is how it was originally envisaged when invented 20 years ago. However, ATM pricing is not yet usage sensitive, and this has held up its adoption.

042169 'EINet: A Secure, Open Network for Electronic Commerce'
D Rosenthal, *Apps 94 pp 219–226*

The author describes a security architecture for Internet commerce. It has various authentication and other services based on Kerberos but augmented with public key features and GSS/API.

042170 'Phone banking security tackled by token'
M Rowe, *Banking Technology (June 95) p 8*

Two French banks are experimenting with a new type of authentication token for telephone banking — a 'jeton securisé' five centimetres in diameter with a single button and a loudspeaker. When the button is pressed, the speaker emits a DTMF modulated one-time password.

042171 'Trusted Distribution of Software Over the Internet'
AD Rubin, *ISOC 94 pp 47–53*

Betsi is a system to protect software, release updates, or patches distributed by insecure channels such as ftp and www. It has three components: authors, users, and a trusted third party. Users trust Betsi and authors, but they do not have to trust the distribution site. MD5 and PGP are the cryptographic primitives.

042172 'Networked Information Discovery and Retrieval Tools: Security Capabilities and Needs'
LJ Schaefer, BW McKenney, *Apps 94 pp 145–153*

The authors discuss the security aspects of world wide web, WAIS and gopher. They present a general security model for such tools, and describe various authentication options which are under development.

042173 'On Goats and Jammers'

SJ Shepherd, PWJ van Eetvelt, *Bulletin of the IMA v 31 no 5/6 (May/June 95) pp 87–89*

The authors generalise the classical 'goat eating a circular field' problem to get techniques for optimising jammer effectiveness and solving other problems concerning the relative positions of mutually interfering emitters.

042174 'NERD: Network Event Recording Device: An Automated System for Network Anomaly Detection and Notification'

DG Simmons, R Wolkins, *ISOC 94 pp 87–93*

NERD is a network based logging system that uses the standard Unix mechanism and also shadows the log files. It provides notification for network events, a real-time video display to identify events as they are happening, public address, pager, and e-mail interfaces, and authorisation controls on logging by hosts according to notification services used. Command line, shell, and C library interfaces are provided.

042175 'Emergency health Card Trials to Start in Ireland'

Smart Card News v 4 no 7 (Mar 95) pp 41 & 43

The EC is funding a trial of an emergency medical card in Ireland, France, Spain and Italy. This will contain information such as next of kin, insurer, and medication data coded in a language independent way.

042176 'Thumbprint card from Sweden'

Smart Card News v 4 no 5 (May 95) pp 91–92

Swedish company Finansforum has developed a smartcard with an integral thumbprint reader. They want it to replace conventional smartcards in banking, GSM and computer access applications.

042177 'A Secure Email Gateway (Building an RCAS External Interface)'

RE Smith, *Apps 94 pp 202–211*

The author discusses the US Reserve Component Automation System, which handles National Guard stores. Its data are mostly unclassified, but with a small number of secret records. Some problems are described; the Boeing MLS LAN (an A1 product) was used to handle the email gateway.

042178 'Constructing a High Assurance Mail Guard'

RE Smith, *NCSC 94 pp 247–253*

The author describes the SNS Mail Guard, which was developed to handle multilevel secure email and also test message contents for security labels, attachment file types, the presence of encrypted data and so on. Performance figures are given.

042179 'Implementing Role Based, Clark Wilson Enforcement Rules in a B1 Online Transaction Processing System'

B Smith-Thomas, CY Wang, YS Wu, *NCSC 94 pp 56–65*

The authors describe a system, currently in beta test, which implements a Clark Wilson TCB. This is based on a B1 operating system (System V/MLS), but the Clark-Wilson properties are implemented in middleware called a User Control Platform.

042180 'IpAccess: An Internet Service Access System for Firewall Installations'

S Stempel, *ISOC 94 pp 31–41*

The author describes a system, IpAccess, for securing outbound TCP connections through a firewall. He discusses both application layer forwarding (e.g., proxy servers) and network layer forwarding (e.g. modifying clients and forwarding at TCP layer). Authorised clients work in a contained environment. Logging, ACLs, quotas and timeouts are provided.

042181 'Design of a Key Agile Cryptographic System for OC-12c Rate ATM'

D Stevenson, N Hillery, G Byrd, D Winkelstein, *ISOC 94 pp 17–30*

A prototype device for providing cryptographic protection of high speed ATM running over 622 megabit per second SONET is described. It addresses privacy through cell encryption, limited access controls, transparency with respect to ATM standards, support for a large numbers of active virtual circuits per crypto operation, sufficient call capacity, and handling of different call types.

042182 'Plastic window sees through card forgery'

Sunday Times (11/6/95) p 2.11

A Dutch invention uses a unique pattern of hair-thin fibres sealed in a transparent window in a plastic card as an anti-forgery device.

042183 'Performance Analysis of a Method for High Level Prevention of Traffic Analysis Using measurements from a Campus Network'

BR Venkataraman, RE Newman-Wolfe, *Apps 94 pp 288–297*

The authors investigated the cost of rerouting and padding the University of Florida's network traffic to provide resistance to traffic analysis. They considered the leakage through a covert channel where a '1' was signified by the presence of traffic on the link from node i to node j. Making the traffic spatially neutral thus corresponds to blocking traffic analysis; thus traffic was rerouted and padded to put the same amount of traffic on each link. Doing this perfectly is a hard linear programming problem, so a number of heuristic solutions were tried and measured.

042184 'Best kept secret'

D Winder, *.net (Jul 95) pp 63–66*

This article describes how to use PGP and explains the configuration defaults.

042185 'Alternatives for signing electronic documents'

B Wright, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 136–139*

A smart card reader and a signature tablet both cost about $200. So conventional digital signatures are not the only option for authenticating electronic documents, and may not be the best from the legal point of view.

2 Operating System and Database Security

042201 'New Thinking about information technology security'
MD Abrams, MV Joyce, *Computers and Security v 14 no 1 (95) pp 69–81*

The authors look at how the concept of a trusted computing base can be generalised to achieve protection with comprehensibility in a distributed system. The relationship between the local protection mechanisms and the communications protocols is the focus of concern.

042202 'Trusted computing update'
MD Abrams, MV Joyce, *Computers and Security v 14 no 1 (95) pp 57–68*

The authors consider how TCB concepts can be extended to object oriented systems and databases. They describe the US DoD's TCB subset and Network TCB approaches, and the ISO access control framework.

042203 'Trusted system concepts'
MD Abrams, MV Joyce, *Computers and Security v 14 no 1 (95) pp 45–56*

The authors discuss the history of the TCB concept, and the large variety of hardware and software combinations which have been used to achieve it. The tradeoff between hardware and software depends both on the environment (e.g., real time) and the falling cost of hardware. However, regardless of the combination, complete assurance is not in sight.

042204 'Sanitisation as a constraint on multilevel secure relational database'
J Aisbett, G Gibbon, *ADC 95 pp 9–16*

This paper proposes an extended MLS relational model which formalises the database as a consistent theory of first order logic where data accessible to a user is a sub-theory of the full theory. In this model, sanitisation can be represented as a set of formulae which constrain the relationship between information versions. This provides a systematic way of incorporating sanitisation procedures into the design and maintenance of MLS databases.

042205 'Achieving Stricter Correctness Requirements in Multilevel Secure Database Management Systems'
V Atluri, E Bertino, S Jajodia, *Journal of Computer Security v 2 no 4 (93) pp 311–352*

This paper shows how, and under what conditions, one can simultaneously achieve both freedom from signalling channels and one-copy serializability. Maximum concurrency is obtained by an analysis of the transaction conflict graph. The paper also supplies a similar analysis for situations where the weaker but less restrictive condition of pairwise serializability is satisfactory. The results of the analysis lead to a transaction ordering that can be enforced by untrusted software running on a commercially available system such as Trusted Oracle that provides levelwise serializability, which guarantees security without the stronger consistency properties.

042206 'Controlled Execution Unix'
L Badger, H Tajalli, D Dalva, D Sterne, *NCSC 94 pp 254–263*

The authors developed a prototype Unix in which only programs on an approved list can be run. It is suggested as a solution for hosts which have to be connected to the Internet yet resist corruption.

042207 'A cryptographic solution to discretionary access control in structurally object-oriented database'
A Baraani-Dastjerdi, J Getta, J Pieprzyk, R Safavi-Naini, *ADC 95 pp 36–45*

A new approach to discretionary access control in structurally object-oriented databases based on pseudorandom functions and sibling intractable functions is proposed. The paper discusses the advantages of this approach and argues that the security of the proposed system is equivalent to the security of the underlying cryptographic primitives.

042208 'Security for the Common Object Request broker Architecture (CORBA)'
SL Chapin, WR Herndon, LA Notargiacomo, ML Katz, TJ Mowbray, *Apps 94 pp 21–30*

The authors discuss the security aspects of an object management standard emerging from a group of vendors which includes IBM, DEC, HP and Sun. This allows the security functionality to be distributed at the developer's discretion among client objects, server objects and the object request broker.

042209 'Implementation of the Sentry System'
SE Chodrow, MG Gouda, *Software — Practice and Experience v 25 no 4 (Apr 95) pp 373–387*

The authors investigate efficient methods of monitoring program execution. They allocate each program a sentry which observes snapshots of its variables; algorithms are provided for doing this is a storage efficient way, and there is a language for expressing properties to be monitored. A prototype system for sentry generation is described and its performance is reported.

042210 'Benchmarking Multilevel Secure Database Systems Using the MITRE Benchmark'
VM Doshi, WR Herndon, S Jajodia, *Apps 94 pp 86–95*

The authors propose benchmarks for multilevel databases, inspired by the Wisconsin benchmark for relational databases. The results presented suggest that the cost of security is usually low in the sense that the time per transaction rises fairly slowly with security level.

042211 'Property-based testing of privileged programs'
G Fink, K Levitt, *Apps 94 pp 154–163*

The authors look at how a privileged program in Unix can be tested for security bugs. They describe tools which work backwards from the variables a program can change, analyse pointer arithmetic, and remark that the rdist security flaw can be found by checking whether a file's permission bits can be changed when the user doesn't own the file. The tools generate test data which will hopefully confirm the existence of flaws.

042212 'A Practical Approach to High Assurance Multilevel Secure Computing Service'
JN Froscher, MH Kang, J McDermott, O Costich, CE Landwehr, *Apps 94 pp 1–11*

The authors explore the interaction between multilevel security and data replication in the context of the SINTRA system, developed by US Navy Labs. This organises the propagation of updates in such a way that distributed multilevel databases remain both secure and consistent. The main mechanism is a trusted replica controller, whose basic algorithms are described; being physically separate from the underlying system, its covert channels are hard for malicious code to exploit. A typical application would be integrating a legacy system into MLS command and control.

042213 'Role-based network security'
WF Jolitz, LG Jolitz, *Dr Dobb's Journal v 20 no 5 (May 95) pp 80–85*

The authors discuss how role-based security was implemented in 386BSD Unix. Roles are controlled by access path as well as user id; this can mitigate the usual exposure to root. Access control is mandatory, in that a file (and all information which might have been derived from it) can be restricted to a given set of terminals; these mechanisms are independent of any encryption or authentication techniques used to tie terminals to physical equipment or to users. The ability to label files is controlled by a hierarchy of privilege levels.

042214 'Information security in mobile databases'
T Hardjono, J Seberry, *ADC 95 pp 103–110*

This paper discusses security issues in mobile databases. It proposes a system for establishing an end-to-end secure communication channel between two mobile units and a method of securely storing data. Smart cards are used for storing users' keys, a modification of the Leighton-Micali protocol is employed for key exchange.

042215 'The Cascade Vulnerability Problem'
JD Horton, R Harland, E Ashby, RH Cooper, WF Hyslop, DG Nickerson, WM Stewart, OK Ward, *Journal of Computer Security v 2 no 4 (93) pp 279–290*

When the balance between system trust level (measured by, e.g., evaluation class) and acceptable risk depends on the range of security levels resident in a system, network connections can upset the balance by enlarging the range. How can one detect when this anomaly has occurred, and restore the balance by upgrading the trust level of a minimum number of machines? The first problem is the cascade detection problem, and an algorithm is given for it in this paper that has lower complexity with respect to the number of security levels, in a system where security levels are linearly ordered. The second problem is the cascade correction problem, and it is shown to be NP-complete by reduction from the vertex cover problem for three-colored graphs.

042216 'The Effects of trusted Technology on Distributed Applications'
MV Joyce, *Apps 94 pp 246–255*

Organisations which introduce multilevel secure technology often have to reevaluate the role of privileged operations, reconfigure applications and rewrite security features. Their users need to acquire greater awareness of security levels in order to operate the system, but this may be a good thing from the organisation's point of view.

042217 'Achieving Database Security through Data Replication: The SINTRA Prototype'
MH Kang, JN Froscher, J McDermott, O Costich, R Peyton, *NCSC 94 pp 77–87*

The authors describe an MLS database under development by the US Navy. It has a replicated architecture, and the database at each level incorporates copies of all lower levels. The global scheduler, query processor, user interface and recovery mechanism are described.

042218 'Architectural Impact on Performance of a Multilevel Database System'
MH Kang, JN Froscher, R Mukkamala, *Apps 94 pp 76–85*

The authors discuss the performance bottlenecks of SINTRA, A US Navy Labs MLS database, which were derived from a simulation model. This predicts that concurrency will be the main problem, but that data dependency analysis will alleviate it.

042219 'Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring'
C Ko, G Fink, K Levitt, *Apps 94 pp 134–144*

The authors consider the problem of bugs in privileged programs, and discuss how audit trail analysis can be used to detect their exploitation. The central idea is a policy specification language based on regular expressions which can capture intended program behaviour. They describe its application to the rdist vulnerability in Unix.

042220 'Handling Passwords with Security and Reliability in Background Processes'
D Libes, *LISA 94 pp 57–64*

When processes are automated, passwords may be stored in clear in shell scripts.

The author describes a number of better techniques which have been implemented in Expect, a Tcl-based shell language.

042221 'Location-Independent Information Object Security'
J Lowry, *ISOC 94 pp 54–62*

This is a report on a one-year-old ARPA project to investigate concepts, services, tools, and prototypes for object security. Confidentiality, authentication, non-repudiation, and access control (e.g., copyright) were considered, as were syntax and encoding. A Unix-based prototype consisting of a toolkit called ESTS was built, and a third party timestamp and signature service was added.

042222 'STU-III — Multilevel Secure Computer Interface'
ED Myers, *Apps 94 pp 170–179*

The author discusses how to connect two multilevel secure systems using STU-IIIs. The TCB requires an extra device driver to manage the STU-III data port and keep the security state consistent between layers; an untrusted process must not issue STU-III port commands, or labelling integrity would be lost. The protocol stack and connection processing are described, and the project is presented as a worked example of secure systems composition.

042223 'Using THETA to implement access controls for separation of duties'
R Pascale, JR McEnerney, *NCSC 94 pp 47–55*

Dual control implies retaining state and thus goes beyond the TCSEC criteria. The authors show how to augment Sandhu's typed access matrix model to cope with it, and describe how it was implemented in a system called THETA.

042224 'Organising MLS Databases from a Data Modeling Point of View'
G Pernul, G Quirchmayr, *Apps 94 pp 96–105*

The authors discuss the design of multilevel databases using data modelling techniques, and outline how association, aggregation and inference constraints might be dealt with.

042225 'Security in the Spring Name Service'
S Radia, MN Nelson, ML Powell, *DCS 94 pp 106–115*

The authors describe a name service made up from distributed autonomous object managers; the security requirements for such a service are discussed. Their solution encodes trust relationships in reusable authenticated objects, similar to capabilities; delegation can be controlled by permitting name resolution only in certain contexts, and not all name servers are necessarily trusted.

042226 'Using Security Models to Investigate CMW Design and Implementation'
CL Robinson, SR Wiseman, *Apps 94 pp 278–287*

The authors consider security models for compartmented mode workstations which use the high watermark principle. The complexity this induces makes it hard to decide how to implement controls, and different vendors' systems are incompatible. The authors attempt to clarify the meaning of the labels, and show that there are covert channels from the label maximum down to its minimum.

042227 'Role-Based Access Control: A Multi-Dimensional View'
RS Sandhu, EJ Coyne, HL Feinstein, CE Youman, *Apps 94 pp 54–62*

The authors discuss the nature of role based access control. According to Ferraiolo and Kuhn, roles differ from groups in being mandatory and based on general transactions rather than simple read and write permissions. They may be able to encompass the LaPadula-Williams hierarchy of trust objectives and the Clark-Wilson idea of mediating access through a set of transformation procedures.

042228 'Modelling a Fuzzy Time System'

JT Trostle, *Journal of Computer Security v 2 no 4 (93) pp 291–309*

The DEC fuzzy time technique was introduced to reduce timing channels. Using a randomised clock with a 20 millisecond mean, timing channels were reduced to ten bits per second. In this paper, Trostle devises a scheduler channel that should work at 50 bits per second under the same assumptions. The channel depends on the way that the fuzzy-time system defers I/O requests and completions, and employs an unusual and subtle method for decoding the high-to-low information.

3 Security Management and Policy

042301 'Security of Health Information Systems in France: what we do will no longer be different from what we tell'
FA Albert, L Duserre, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 201–204*

France is issuing a smartcard to all healthcare professionals; it will act as their ID, manage access control, and sign data.

042302 'X.500 Directory Services: One Big Happy Network'
J Allison, *Data Communications International (21/5/95) pp 55–62*

The author discusses the advantages experienced from implementing X.500 in a number of organisations, including two large medical centres. One of them used cc:Mail and the other Microsoft Mail.

042303 'Technical intelligence in business: understanding technology threats and opportunities'
WB Ashton, GS Stacey, *Journal of Technology Management v 10 no 1 (95) pp 79–104*

The authors describe how to go about running a competitive intelligence operation in a technology business, and discuss a number of companies which succeeded or failed because of the quality of their intelligence.

042304 'Presentation of electronic patient data and medical audit'
AR Bakker, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 65–69*

The author considers the audit requirements on electronic medical information. The emphasis is on assessing the performance of healthcare professionals; the technical mechanisms need to reconstruct the information available at the time of treatment.

042305 'An initial approach to the security techniques required by the electronic patient record'
B Barber, S Douglas, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 33–38*

The authors argue that electronic medical records should carry digital signatures, but ask how the validity of such signatures can be preserved for 25–50 years.

042306 'Clinical requirements for the security of the electronic patient record'
S Bengtsson, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 29–31*

The clinician's information security priorities are presented as availability first, then integrity, and finally privacy.

042307 'Information Security Controls — Are They Cost-Effective?'
C Blatchford, *Computer Audit Update Supplement 3 (1995) pp 11–19*

The cost of controls is often neglected when budgeting IS projects: it may be falsely assumed that the pretechnical procedural controls will be saved on automation.

042308 'System-of-Systems Security Engineering'
DJ Bodean, *Apps 94 pp 228–235*

The collection of systems which support a single mission often end up being treated as a single system. This means that compositional problems come to the fore and are complicated by the need to incorporate legacy systems. A number of principles are put forward, such as focussing on system boundaries, mission critical data, and the end-to-end flow of information and control.

042309 'Public registers for software programs'

R Bond, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 130–132*

At present, UK software authors do not have to deposit a copy of their work anywhere in order to get copyright protection. The author discusses whether this should be changed, as suggested by the WIPO. In the USA, federal registration enables authors to get customs agents to police the importation of pirated programs.

042310 'Digital Technology and Copyright'

British Copyright Council, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 115–118*

In a submission made to the EC, British commercial interests argue that intellectual property rights should explicitly include not just the author's right (copyright), but also performers' rights, producer's rights, moral rights such as attribution and integrity, and economic rights such as the power to restrict distribution and reproduction.

042311 'Computer software protection in the Commonwealth of Independent States'

WE Butler, *Computer Law and Security Report v 11 no 2 (Mar-Apr 95) pp 80–84*

In 1991, the former Soviet Union introduced a software copyright law, which is outlined in this article.

042312 'Tools and techniques for the development of secure software'

J Davey, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 173–178*

The author discusses how quality assurance techniques can be extended from the safety to the security aspects of healthcare systems.

042313 ' "Scope of use" provisions in software licence agreements'

A Davidson, *Computer Law and Security Report v 11 no 2 (Mar-Apr 95) pp 74–79*

The author surveys US law on the use of technical measures such as logic bombs to force a software licencee to succumb to the licensor's will. Such disputes often turn on issues on which the contract is silent, such as corporate takeover of adaptation of the software.

042314 'The technical conditions for an open architecture'

D de Roulet, HS Le, JR Scherrer, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 107–114*

The authors describe difficulties encountered in securing a client-server system for the Geneva University hospital; they recommend the use of standard tools such as Kerberos.

042315 'Security Concerns for Distributed Systems'

R Dobry, MD Schanken, *Apps 94 pp 12–20*

The authors describe the US government approach to certifying distributed systems. The Orange Book is being extended in various ways, and the types of functionality and assurance are briefly described.

042316 'The hacker composite: a necessary security tool?'

B Dwon, *Computer Fraud and Security Bulletin (Apr 95) pp 10–12*

This article profiles three notorious hackers, two of whom were eventually imprisoned. The composite picture is of an adolescent male who is largely self taught and breaks into systems by obsessive persistence rather than by using a high degree of skill.

042317 'Use of Kerberos Authentication'

E English, *Computer Fraud and Security Bulletin (June 95) pp 16–18*

This article provides a management level assessment of Kerberos: it provides a good alternative to firewalls and the code is free, but support is hard to get and auditing features could be better.

042318 'Banks urged to enter security business'
Financial Technology International Bulletin v 12 no 8 (Apr 95) p 3

This article describes a report from SRI which suggested that given their crypto skills and public trust, banks should get into the key management business.

042319 'The Design of an Audit Trail Analysis Tool'
EA Fisch, GB White, *Apps 94 pp 126–132*

The authors describe a tool for sanitising audit trail data to remove sensitive data such as passwords, so that the remainder can be used in analysis. It replaces object names with labels such as user1 and system2.

042320 'Data protection: into the next decade'
E France, *Computer Audit Update (June 95) pp 15–17*

Britain's Data Protection Registrar discusses future changes in UK law and practice. The EC Directive on Data Protection, which should be passed to member states in 1996 and implemented into UK law by the end of the century, will give an opportunity to redefine who should register and to sort out various anomalies. Meanwhile, registration is being simplified, and auditors are asked to help assure compliance.

042321 'The need for security — a clinical view'
FHR France, PN Gaunt, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 189–196*

The authors discuss some security problems of automating health records; medical organisations are less hierarchical and thus harder to control than companies, and data may have to be kept for as long as 30 years.

042322 'A Validated Security Policy Modeling Approach'
JW Freeman, RB Neely, MA Heckard, *Apps 94 pp 189–200*

The authors describe a methodology for developing policy models. This concentrates on the formal and procedural elements of the process, and is driven by the system manager's view.

042323 'Is anything safe any more? The .net guide to Internet Security'
S Gardner, *.net (June 95) pp 60–65*

The author discusses Internet security, the Clipper initiative and the Def Con II hackers' conference held in the USA in July 94.

042324 'The Barrett review — a blueprint for expanding Australian telecommunications interception'
G Greenleaf, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 143–146*

A report to Australia's cabinet on the cost effectiveness of wiretaps recommended that restrictions be relaxed and all carriers compelled to install a wiretap capability. It gives numbers of warrants (527 in 92/3), costs ($570 per day against $1630 for listening devices and $2772 for vehicle tracking), and reveals that despite a complete lack of restrictions on domestic use of cryptography, the agencies do not see encryption as a threat in the foreseeable future. Their problems stem more from the move from analogue to digital systems.

042325 'Network Security in a Client-Server Environment'
CS Guynes, RG Thorn, *SIGSAC v 13 no 2 (Apr 95) pp 6–12*

The authors provide a management level overview of network security issues.

042326 'Stop that email! You are Probably Breaking the Law!'
B Hancock, *Network Security (Apr 95) pp 10–12*

Corporate users are warned that careless use of email can violate laws such as those on export of technical data and encryption algorithms, as well as US Commerce department bans on dealing with particular companies and individuals.

042327 'A voluntary international numbering system — the latest WIPO proposals'

R Hart, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 127–129*

The World Intellectual Property Organisation has proposed a system of numbering for all digital works, including books, sound and video recordings, and computer programs; it is claimed that the boundaries between these are breaking down. Software publishers on the other hand have field experience of fighting digital piracy, and claim to have never had any difficulty in establishing ownership.

042328 'Security Audit Center — a suggested model for effective audit strategies in health care informatics'

A Hayam, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 115–127*

The author proposes that system audit should come under the security manager.

042329 'Business continuity planning'

K Hearnden, *Computer Audit Update, part 1: May 95 pp 3–10; part 2: June 95 pp 3–7*

The author describes a number of surveys of disaster recovery planning, provides bibliographies, and produces a number of figures which might be used to justify contingency planning budgets.

042330 'Security requirements for electronic patient records: the Norwegian view'

KR Iversen, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 51–56*

The Norwegian health ministry insists on paper backups for electronic medical records. Each hospital has an IT security officer, while its chief medical officer is responsible for security policy and contingency planning. Authorisation options are discussed: different departments may control different parts of the data and have different views of it. The information flow controls required are quite different from conventional mandatory and discretionary models.

042331 'Kryptografie: Datenschutzbeauftragte diskutieren Möglichkeiten und Schwierigkeiten'

V Jürgens, *Datenschutzberater v 19 no 6 (14/6/95) pp 1–3*

German data protection officials have recently been discussing encryption algorithms. Criminal suspects are entitled to refuse to decipher data under their right to avoid self-incrimination; nonetheless there are no plans to bring in key escrow or government regulation of cryptography.

042332 'The need for a security policy in health care institutions'

SK Katsikas, DA Gritzalis, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 73–80*

The authors discuss the role of a security policy in healthcare, and report on a policy developed under the EC project SEISMED.

042333 'Secure System Composition: Five Practical Initiatives'

G King, *Apps 94 pp 67–73*

The author describes the five initiatives taken by the US DoD to tackle the composition problem: APP, DGSA, core products, MISSI and security profiles.

042334 'Health information, privacy, confidentiality and ethics'

EHW Kluge, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 23–27*

The author discusses the philosophical aspects of medical record security and argues that the creation of databases without patient consent is justified to facilitate healthcare delivery.

042335 'An accountability server for health care information systems'
S Kowalski, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 129–138*

The author describes a service which collects and maintains audit information on a patient record as it is accessed by different professionals, such as doctors, nurses and physiotherapists.

042336 'Law and disorder?'
A Lawrence, *Computer Business Review v 3 no 4 (Apr 95) pp 22–24*

Laws on topics such as copyright, libel, obscenity, data protection, encryption and official secrets vary so much from one country to another that the Internet faces regulatory chaos.

042337 'The arrest of Kevin Mitnick'
K Lindup, *Network Security (Mar 95) pp 16–19*

The author describes a US hacker's criminal career and his most recent arrest. He had used IP spoofing and 'social engineering' — persuading system users and administrators to give him unauthorised access by telling plausible lies on the telephone.

042338 'The organisation and management of information security issues in health care'
LP Louwerse, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 195–200*

Problems with health information security stem from doctors' professional autonomy and the lack of a generally accepted model of the practice of medicine. Leiden University Hospital is discussed as an example: there, the structures assumed when automation was introduced turned out to be inadequate and had to be decentralised.

042339 'Maintaining patient confidentiality in an electronic world'
P Marr, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 213–217*

The author describes measures implemented at the New York University Medical Center to protect patient confidentiality. These include weekly password changes, application level access controls and alarms, an employee secrecy agreement which is signed annually, and disciplinary measures which have so far led to two sackings.

042340 'UNIRAS computer security made public'
M McCormack, *Computer Fraud and Security Bulletin (Apr 95) pp 1–2*

The UK government's computer security information centre, UNIRAS, is run by MI5 and has a reputation as a 'black hole'; information flows in, but the only recipients of advice are the 1100 holders of classified information. This should change by the end of 1995, when many warnings should be circulated generally.

042341 'Distributed Audit Trail Analysis'
A Mounji, B Le Charlier, D Zampunieris, N Habra, *ISOC 94 pp 102–112*

Audit trails are usually generated on each host in a system. The authors wanted a single point of administration, ability to perform local or global analysis, high availability, flexibility, and scalability in a heterogeneous environment. They designed a host-level architecture to control formats and granularity and a global architecture to filter and evaluate what is collected. Analysis is specified in a rule-based, condition-action, bottom-up language without backtracking.

042342 'Security — state of mind or a state of siege?'
H Nicholson, *Computer Audit Update (Apr 95) pp 11–18*

The author describes how an auditor can most effectively sell computer security services. First, apply pressure through the audit committee on the CEO to pay for a risk assessment; then use this to sell the development of a security strategy and the management consultancy to implement it.

042343 'Cybercash gets go-ahead to export Net encryption'
M Norton, *Banking Technology (June 95) p 5*

The US Commerce Department has given Cybercash permission to export encryption software to most foreign countries. The software encrypts only specific information related to financial transactions.

042344 'Security blankets'
M Norton, *Banking Technology (April 95) pp 38–40*

US bankers' views on the encryption policy debate are recorded. They want a stronger encryption standard than DES, and are frustrated by their government's policies.

042345 'Exporting Evaluation: An Analysis of US and Canadian Criteria for Trust'
P Olson, *NCSC 94 pp 206–214*

Efforts are underway to get mutual recognition for US and Canadian evaluations.

042346 'Modern cryptography and its application in information security'
F Piper, *Information Security Monitor v 10 no 6 (5/95) pp 5–9*

The author gives a management level overview of cryptography; he discusses algorithms such as DES and RSA.

042347 'Audit Reduction and Misuse Detection in Heterogeneous Environments: Framework and Application'
P Proctor, *Apps 94 pp 117–125*

The author describes a system for automatic accounting of audit data which is under development for US Navy use.

042348 'Digital Archives and communication highways in health care require a second look at the legal framework of the seventies'
O Rienhoff, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 13–19*

The digitisation of x-ray images and other medical data raises legal problems with integrity, and cross border mobility makes patient access rights an international issue. Such problems indicate that the laws on medical information need to be overhauled. One can go too far: in Germany, the hospital privacy officer is often feared.

042349 'Health information policy: without confidentiality'
DM Robinson, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 97–104*

The author describes recent legal precedents on medical confidentiality in Canada. Two of them overturned the local conventional wisdom: they established that a patient has a right to a copy of his record, and that a patient who caught AIDS from a blood transfusion was entitled to information on the donors. An institute is now to be set up to develop health information standards.

042350 'Computer crime — can we crack it?

A Routledge, *Computer Fraud and Security Bulletin (May 95) pp 11–15*

The author describes some of the physical and logical access control mechanisms which can help reduce computer crime.

042351 'Could you cope without computers?'
M Sadiwnyk, *Computer Audit Update (May 95) pp 13–16*

The author identifies voltage surges as a significant cause of loss of computing resources, and discusses the possible countermeasures.

042352 'Breaking into heaven'

A Savage, *.net (July 95) pp 36–54*

This article investigates what a 'hacker' is. It ranges from the Mitnick case to interviews with Phiber Optik and other underground personalities.

042353 'Network Review'

C Sheffield, *Network Security, part 1: Mar 95 pp 11–16; part 2: Apr 95 pp 9–13; part 3: May 95 pp 15–19*

The author described the experience gained over three years of network reviews by accountants Touche Ross. controls on distributed systems have not evolved to the level common in mainframes, with deficiencies common in network management, support and fault tolerance.

042354 'The challenges of new technologies applying the UK Data Protection Act to document image processing'

D Smith, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 81–86*

It was illegal in the UK for local authority tax offices to record taxpayers' ages, beyond the fact that they were over 18; this could be implemented easily with text based systems, but not with systems which retained images of the forms. The use of image based systems was therefore banned.

042355 'Business Continuity Planning'

M Smith, J Sherwood, *Computers and Security v 14 no 1 (95) pp 14–23*

The authors report two incidents, which show that the decision on when to formally invoke a disaster recovery plan is not straightforward and should itself be planned for. In the first of these, a wholesaler's junior staff jumped the gun and destroyed the backup data; in the second, the Financial Times were too late in realising that a problem was becoming serious. Both incidents cost large amounts of money.

042356 'Testing for subsistence and infringement of copyright in computer programs: some UK and US cases'

JAL Sterling, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 119–126*

This article describes current US and UK law on what parts of a computer program can be protected by copyright.

042357 'Datensicherheit unter NOVELL NetWare 3.11/3.12'

G Stölting, M Hube, *Datenschutzberater v 19 no 4 (17/4/95) pp 6–9 (in German)*

The authors describe the security mechanisms of NetWare and the administrative measures required to complement them.

042358 'The principles of data protection concerning patient related data in Finland'

R Tervo-Pellikaa, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 39–50*

This article reports a data protection survey of the Finnish health care system. Networks are getting larger, and demands for access by insurers and government bodies are eroding confidentiality; data protection legislation came into conflict with health regulations meant to create a single life-long record, and the latter were repealed. Data protection rules for health records (content, use, inspection rights, protection etc) are now being drawn up.

042359 'Czech mate'

E Thomas, *Banking Technology v 12 no 4 (May 95) pp 32–36*

Poor data security and data protection have not only facilitated a number of frauds in the Czech Republic, but are also a potential problem for its efforts to join the European Union. The government is proposing that bank systems should therefore be certified under ITSEC.

042360 'The use of personal data for medical research: how to deal with new European policy standards'
OFC van der Leer, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 87–95*

The 1992 EC Council of Ministers directive on data protection gives an exemption for 'circumstances where there is manifestly no infringement of privacy or fundamental freedoms'. The author proposes that cross-border sharing of medical data for 'epidemiological programs' and research could be slipped through this loophole.

042361 'The AIM SEISMED guidelines for system development and design'
HD van Dorp, JF Dubbeldam, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 179–186*

The authors describe the security development methodology proposed by the EC SEISMED project and discuss its relationship with ITSEC.

042362 'A threat to freedom'
I Walden, *Banking Technology v 12 no 4 (May 95) p 20*

British banks view the EC Data Protection Directive as a serious threat to the way they conduct business. For example, when they obtain information about a customer from a third party they will have to notify the customer of this fact. Automated credit scoring will be outlawed, and personal data will not be exportable to countries such as the US and Japan which do not have adequate data protection laws. These rules may provide an incentive for banks to adopt payment systems which minimise the amount of personal data processed.

042363 ' "Market realities" in the analysis of copyright infringement of computer programs'
A Wernick, *Computer Law and Security Report v 11 no 3 (May-June 95) pp 133–135*

The author discusses a recent UK copyright case; IPR may be impaired if it becomes an industry standard to conform to a certain format, or if the competing programmer's freedom of choice is otherwise restricted.

042364 'What Color is Your Assurance?'
D Wichers, J Sachs, DJ Landoll, *NCSC 94 pp 215–226*

The authors compare and contrast the assurance goals and techniques employed by a TCSEC, ITSEC, TCPEC, CCEP and a number of other programmes.

042365 'technology Special — Smart Cards'
R Wilson, *Electronics Weekly (8/2/95) pp 21–24*

This article discusses various manufacturers' efforts to create a smartcard which will do an RSA signature in under half a second. Some are using coprocessors, while others are going for 32-bit RISC chips.

042366 'An important reminder'
HS Wolfe, *Computer Fraud and Security Bulletin (Apr 95) pp 16–18*

The author outlines the Tempest threat and the difficulty of taking reliably effective countermeasures. He proposes that Tempest snooping should be made a specific criminal offence.

042367 'New developments in information technology to combat computer crime and fraud'
K Wong, *Information Security Monitor v 10 no 5 (4/95) pp 5–6*

The author discusses the role of pattern recognition software techniques in fighting frauds against cellular phones, insurance firms and credit card systems.

042368 'Information security awareness raising methods'
CC Wood, *Computer Fraud and Security Bulletin (june 95) pp 13–15*

The author discusses some of the PR techniques which a security manager can use to raise employee awareness.

042369 'IT security — the legal challenge'
J Worthy, *Computer Law and Security Report v 11 no 2 (Mar-Apr 95) pp 62–65*

The author surveys UK law on computer security and the recent directives from the European Commission on data protection and telecomms, and points out that the proliferation of private networks is eroding the force of the Interception of Communications Act.

042370 'Privacy protection principles for electronic mail systems'
T Wright, *Computer Law and Security Report v 11 no 2 (Mar-Apr 95) pp 66–73*

This is a report by the Information and Privacy Commissioner of Ontario, Canada. He sets out a number of privacy principles for email which are to be followed in the government sector and are recommended to other organisations.

042371 'Necessity to improve common understanding about the security issues among hospitals in Japan and some feasible approaches'
K Yamamoto, K Ishikawa, M Miyaji, Y Nakamura, S Nishi, T Sasaki, K Tsuji, R Watanabe, *International Journal of Biomedical Computing v 35 (supplement, 1994) pp 205–212*

The authors describe the social background of medical privacy in Japan and present the results of a survey of physicians' attitudes on various privacy and disclosure issues.

4 Formal Methods and Protocols

042401 'Composing System Integrity Using I/O Automata'
E Amoroso, M Merritt, *Apps 94 pp 34–43*

The authors describe Lynch and Tuttle's I/O automata model, and use it to prove composability results for integrity. If one tries to classify systems according to whether transitions from valid to invalid states are impossible, possible only under internal control, or possible even under external control, then these classes turn out to be composible.

042402 'Atomic Broadcast: from Simple Message Diffusion to Byzantine Agreement'
F Cristian, H Aghili, R Strong, D Dolev, *Information and Computation v 118 no 1 (Apr 95) pp 158–179*

Atomic broadcast can be used to implement virtual synchronous replicated storage on an unreliable asynchronous network. A number of protocols are presented to provide resistance to Byzantine and other failures, and some of them are shown to be optimal in certain circumstances.

042403 'The ring based conference authentication service'
D De Paoli, A Gosczynski, *ACSC 95 pp 120–129*

An implementation of an identity based conference key distribution scheme proposed by Koyama and Ohta is discussed. This forms part of RHODOS, a research oriented distributed operating system. Results of simulation in UNIX environment are given for up to 7 participants and a prime size of 180 bits.

042404 'Security enhanced direct store delivery system'
N Devikar, Y Zheng, *ACSC 95 pp 130–135*

This paper describes a security enhancement of a direct store delivery system that uses a trusted third party service provider. The model incorporates authentication based on X.500 standards.

042405 'Dynamic Fault-Tolerant Clock Synchronisation'
D Dolev, JY Halpern, B Simons, R Strong, *Journal of the ACM v 42 no 1 (Jan 95) pp 143–185*

The authors give algorithms for clock synchronisation and resynchronisation based on a fault-tolerant authentication protocol. This tolerates more general network and failure topologies than some previous protocols; it works so long as the subnetwork containing the nonfaulty processors remains connected. The basic ideas are that processors send out synchronisation messages at predetermined times; that clock adjustments are bounded by a linear function of elapsed time; that every correct processor tries to act as a synchroniser; and that at least one succeeds.

042406 'Distributed Computing Column'
C Dwork, *SIGACT News v 26 no 1 (Mar 95) pp 17–19*

The author points out an oracle attack on the challenge-response mechanism described in the Lotus Notes Internals documentation. Apparently the current implementation is not vulnerable as it uses distinct keys for authentication and decryption.

042407 'Yaksha: Augmenting Kerberos with Public Key Cryptography'
R Ganesan, *ISOC 94 pp 132–143*

The author discusses how to augment Kerberos using Boyd's RSA multisignature technique. A user has one piece of the private key, and an on-line server has the other piece; neither can spoof the other, and signatures, once created, are indistinguishable from any normal RSA signature. This arrangement facilitates immediate revocation and realtime audit, but with the obvious limitation that the server must be online. A separate signature protocol is provided.

042408 'Applying the Abadi-Lamport Composition Theorem in Real-world Secure System Integration Environments'
JA Hemenway, J Fellows, *Apps 94 pp 44–53*

Abadi and Lamport examined the problem of composing specifications in 1990, and their ideas have been built into tools such as InaJo. These were used to help integrate a US Navy command and control system, and some examples of the formal verification work are presented.

042409 'Reparable Key Distribution Protocols for Internet Environments'
TNL Hwang, WC Ku, *IEEE Transactions on Communications v 43 no 5 (May 95) pp 1947–1949*

The authors call a protocol reparable if the replacement of compromised keys is sufficient to restore security. They show that a protocol of Lu and Sundareshan does not have this property: if an opponent finds out a key shared by Alice with a server, he can use it to set up keys with other servers which survive the revocation of the compromised key. They also propose two reparable protocols, and ways in which key distribution can be safeguarded in a multiple domain network such as the Internet.

042410 'GSS-API Security for ONC RPC'
B Jaspan, *ISOC 94 pp 144–151*

The author describes a fix for Sun's 'secure' RPC mechanism whose 192-bit discrete log primitive was broken. It uses Kerberos techniques to add a data integrity wrapper for the arguments; sequence numbers in the headers prevent replay. Clients must establish a context, at which time servers recognize the security tokens.

042411 'A Pattern Matching Model for Misuse Intrusion Detection'
S Kumar, E Spafford, *NCSC 94 pp 11–21*

The authors provide a formal model of intrusion detection systems. This is based on coloured Petri nets and examines the paths which a system can detect between initial and final states.

042412 'An efficient password authentication scheme based on a unit circle'
HT Liaw, CL Lei, *Cryptologia v XIX no 2 (April 95) pp 198–208*

The authors propose a coding method for one-way encrypted passwords.

042413 'On the automation of GNY-logic'
A Mathuria, R Safavi-Naini, P Nickolas, *ACSC 95 pp 370–379*

This paper proposes a modified version of a logic due to Gong, Needham and Yahalom that allows it to be automated. The modification ensures that no useful inferences are lost and allow that the logical statements derivable from a given protocol to be deduced in a finite number of steps. Implementation of a protocol analysis tool based on this logic is described.

042414 'Some Remarks on the Logic of Gong, Needham and Yahalom'
A Mathuria, R Safavi-Naini, P Nickolas, *ISC 94 pp 303–308*

The authors point out a number of problems with the GNY logic; strange conclusions can be drawn from rules on recognisability and from various combinations of freshness rules. it also has difficulty verifying the Yahalom protocol. They suggest some possible solutions.

042415 'SESAME V2 Public Key and Authorisation Extensions to Kerberos'
P McMahon, *ISOC 94 pp 114–131*

The author describes SESAME, a Kerberos clone with added public key features. User data are (optionally) protected during transport; authorisation is privilege based; privileges are protected using digital signatures. Version 2 contains public key based distribution of inter-realm session keys (intra-realm works as in Kerberos), separate authentication and ticket verification keys, separate integrity and confidentiality keys, and secure transmission of PACs. Applications may access SESAME though the GSS-API, and different cryptographic algorithms may be installed.

042416 'A New Approach to the X.509 Framework: Allowing a Global Authentication Infrastructure Without a Global Trust Model'
S Mendes, C Huitema, *ISOC 94 pp 172–188*

This work reports on the PASSWORD Project, which did a test implementation of X.509 and X.400. It addressees deficiencies in X.509, for instance, in specifying attributes as well as names by using X.509 Version 3. Policy should specify quality of assurance, frequency of update, and intended use of the certificate (because of liability issues), and different infrastructures (PEM, ISO, PGP) must be supported.

042417 'A Key Distribution Protocol for Mobile Communication Systems'
C Park, K Kurosawa, S Tsujii, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 77–81*

This paper discusses the insecurity of the Tatebayashi Matsuzaki Newmann protocol, and presents two new distribution protocols that address security and efficiency.

042418 'Scaling the Web of Trust: Combining Kerberos and PGP to Provide Large Scale Authentication'
JI Schiller, D Atkins, *Usenix 95 pp 83–94*

The authors describe a scheme whereby kerberos can be used to create a service for signing PGP keys and thereby introducing people in an organisation who have no common acquaintances. They discuss the relative strengths and weakness of Kerberos and PGP and how their combination can be stronger than either alone, such as by enabling recovery from a compromise of the trusted centre.

042419 'Automatic Generation of High Security Guard Filters'
V Swarup, *NCSC 94 pp 123–137*

The author presents a security filter specification language, statements in which can be compiled into guard programs. Some of the nontrivial compiler algorithms have been formally verified.

042420 'IP spoofing and session hijacking'
D Thomsen, *Network Security (Mar 95) pp 6–11*

The author explains IP spoofing and session hijacking attacks, and discusses the effectiveness of countermeasures such as session encryption, IP sequence number encryption, and firewalls.

5 Secret Key Algorithms

042501 'An improved algorithm for computing the edit distance of run-length coded strings'
H Buhne, J Csirik, *Information Processing Letters v 54 no 2 (28/4/95) pp 93–96*

The authors examine the coding gains which can be realised when computing string edit distance. These amount to partitioning an n by m edit matrix into k by l bit blocks, which reduces the computation from $O(mn)$ to $O(ln + km)$.

042502 'Searching for the best linear approximation of DES-like cryptosystems'
L Buttyan, I Vajda, *Electronics Letters v 31 no 11 (25/5/95) pp 873–874*

Searching for the best linear characteristic is shown to be equivalent to searching for the maximal weight path in a digraph; it can be found in principle using the Viterbi algorithm, but the number of nodes needing to be stored would be large (2^{64} for DES). The search can be made feasible by assuming that only a subset of the S-boxes are active; with one active box, Matsui's expression is confirmed as optimal.

042503 'Frames: A Simple Characterisation of Permutations Realized by Frequently Used Networks'
H Cam, JAB Fortes, *IEEE transactions on Computers v 44 no 5 (May 95) pp 695–697*

The authors show how to reduce the time complexity of determining whether a permutation is realised by a k-stage Benes network of N inputs to $O(kN)$.

042504 'The Autoscritcher'
C Deavours, *Cryptologia v XIX no 2 (April 95) pp 137–148*

This article describes a family of keysearch machines fielded by the US Army in 1944/5 to solve Enigma traffic. They used a meet-in-the-middle technique to overcome the problem which rewirable reflector rotors caused the bombes.

042505 'New normal sequences of length 25'
M Gysin, J Seberry, *ACSC 95 pp 194–198*

An exhaustive search strategy for normal sequences is presented. It is shown that no new sequences of length 24 exist, and all the sequences of length 25 can be derived from Turyn sequences. The paper also mentions applications of binary sequences in data communications and security.

042506 'Known plaintext cryptanalysis of tree-structured block ciphers'
HM Heys, SE Tavares, *Electronics Letters v 31 no 10 (11/5/95) pp 784–785*

The authors extend their previous chosen-plaintext attack on tree-structured block ciphers to a known-plaintext attack using hypothesis testing techniques. It can be extended from an r-round SP network to a similar block cipher with $2r - 2$ rounds using a meet-in-the-middle approach. Expressions are derived for the amount of known plaintext required in either case.

042507 'Propagation Characteristics of Boolean Functions and their Balancedness'
S Hirose, K Ikeda, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 11–18*

This paper discusses Boolean functions that satisfy the propagation criterion and the balancedness of these functions.

042508 'On Random Generation of the Symmetric Group'
T Luczak, L Pyber, *Combinatorics, Probability and Computing v 2 no 4 (Dec 93) pp 503–512*

By considering the probability that a random permutation has an invariant subset of any given size, the authors prove that for every $\epsilon > 0$ there is a constant C such that

C randomly chosen permutations on n elements generate S_n with probability $> 1 - \epsilon$. They also confirm a conjecture of Cameron that only a small part of S_n can be covered by nontrivial transitive subgroups.

042509 'The Structure of the Abelian Groups Containing McFarland Difference Sets'
SL Ma, *Journal of Combinatorial Theory (series A) v 70 no 2 (May 95) pp 313–322*

The author studies the Sylow p-subgroups of Abelian groups admitting a McFarland difference set, and gets conditions under which their hyperplanes are normal subgroups. This technique is used to prove that there is no (320,88,24)-difference set in any Abelian group of exponent of 40 or more.

042510 'Bounding the expected size of irredundant forms'
L O'Connor, *ACSC 95 pp 412–422*

Irredundant forms of a Boolean function are defined and two new bounds on the expected size of minimal forms are derived.

042511 'On the Distribution of Characteristics in Bijective Mappings'
L O'Connor, *Journal of Cryptology v 8 no 2 (Spring 95) pp 67–86*

The author proves that the expected value of the largest entry in the XOR table of a bijective Boolean mapping on Z_2^m is bounded by $2m$, while the fraction of the table which is zero approaches $1/e$. He then develops probabilistic bounds on multiple round characteristics for both SP and Feistel networks.

042512 'Polynomial Splitting Ring and Root Representation of Linear Recurring Sequences over $Z/(p^e)^*$'
WF Qi, JJ Zhou, *Scientia Sinica (Series A) v 37 no 9 (September 1994) pp 1047–1052*

This paper discusses the splitting rings of polynomials over $Z(p^e)$; it discusses the factorisation of polynomials and the properties of their roots. Using these results and the structure of sequence families, the authors show how the terms of a linear recurring sequence over $Z/(p^e)$ may be represented by the roots of its characteristic polynomial, and that this representation is uniquely determined by the sequence.

042513 'Some concepts of stability analysis in combinatorial optimisation'
YN Sotskov, VK Leontev, EN Gardeev, *Discrete Applied Mathematics v 58 no 2 (24/3/95) pp 169–190*

The authors survey results in the stability of combinatorial problems. By how much can we perturb a guess at a shift register load in a correlation attack or a guess at a set of weights in a trapdoor knapsack before hill climbing techniques will take us into a different local optimum?

6 Public Key Algorithms

042601 'Electronic Cash on the Internet'
S Brands, *ISOC 94 pp 64–84*

This system features off-line operation, privacy, prior restraint on double spending, security in the face of broken cards, currency conversion, low transmission cost, and efficient computation. Banks, service providers, and customers, each have a computing device and network connection. Tamper resistant cards and blind signatures enhance security and privacy. The payment data structure is 125.5 bytes long; withdrawals require one small modular multiplication on-line for the bank and user; payments do not have to compute on-line, so they can easily be attached to e-mail.

042602 'Off-line electronic cash based on secret-key certificates'
S Brands, *LATIN 95 pp 131–166*

An off-line electronic coin system based on a recently proposed technique called secret-key certificates is presented. These are similar to public key certificates, except that anyone can produce a certificate on a public key which appears to be genuine; the control is that only if the certificate is genuine will there exist a corresponding secret key with which signatures can be created or messages decrypted. The derived cash system offers multi-party security and unconditional privacy of payments, and improves on previously known techniques.

042603 'Secure information broadcasting scheme using embedded locks'
JJR Chen, HKC Chang, *Computer Systems Science and Engineering v 10 no 2 (95) pp 92–99*

The authors propose a broadcast encryption scheme based on Rabin's method, and claim it involves fewer multiplcations than previous schemes.

042604 'One-Way Functions over Finite Near-Ring'
E Chida, H Shizuya, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 4–10*

This paper investigates one-way functions associated with finite near-rings. It shows that (i) if there exists a one-way group homomorphism, there exists a one-way non-ring near-ring homomorphism; (ii) if there exists a one-way ring homomorphism, there exists a one-way non-ring near-ring homomorphism. It also introduces a discrete logarithm problem over finite near-rings, and shows that integer factorisation is probabilistic polynomial time Turing equivalent to a modified version of this problem.

042605 'Severely Denting the Gabidulin Version of the McEliece Public Key Cryptosystem'
JK Gibson, *Designs, Codes and Cryptography v 6 no 1 (July 95) pp 37–45*

Gabidulin proposed a variant of McEliece in which maximum rank distance codes were used instead of Goppa codes, and claimed that it was more efficient. However, the author shows an attack whose effect is that larger parameters would have to be chosen, thus eliminating the claimed advantage in performance. In a postscript, he claims an attack on a modified version proposed by Gabidulin at Cirencester 93 (see **041611**).

042606 'Information Leakage Measurement in a Distributed Computation Protocol'
S Kawamura, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 59–66*

This paper deals with information leakage measurement in server aided secret computation. It shows that an RSA-based server aided protocol can leak information if the client which has the secret were to complain about the computation result.

042607 'A New RSA-Type Scheme Based on Singular Cubic Curves $y^2 \equiv x^3 + bx^2 \pmod n$'
H Kuwakado, K Koyama, Y Tsuruoka, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 27–33*

This paper proposes a new RSA-type scheme over the non-singular part of a singular cubic curve $E_n(0,b) : y^2 \equiv x^3+bx^2 \pmod n$. The authors prove that if b is a quadratic residue in Z_n, breaking this scheme over $E_n(0,b)$ is not easier than breaking the RSA scheme.

042608 'Use of RSA moduli with prespecified bits'
CH Lim, PJ Lee, *Electronics Letters v 31 no 10 (11/5/95) pp 785–786*

Vanstone and Zuccherato suggested using an RSA modulus made up of four primes of 256 bits but with a number of bits in their product fixed (below). It is shown that such a modulus can be factored in about 2^{45} operations, and an alternative approach to structuring moduli is suggested,

042609 'Les Réseaux de Neurones et leurs Applications Cryptographiques'
D Pointcheval, *Technical Report LIENS-95-2, Ecole Normale Supérieure, 2/95*

The author introduces a new public key primitive — the perceptron problem. This is NP-complete and comes from artificial intelligence work: given m binary vectors $X^i \in \{-1,1\}^n$, find a vector $V \in \{-1,1\}^n$ such that $X^iV \geq 0$ for all i. Zero knowledge identification schemes based on this are proposed; the author argues that with m and n greater than about 100 these schemes should be secure, and that they could be useful in smartcard applications.

042610 'A New Class of Non-interactive ID-Based Key Sharing Schemes and its Performances'
R Sakai, M Kasahara, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 51–58*

This paper proposes a new class of ID-based non-interactive key sharing scheme with a trusted centre which generates a common key on the basis of a linear combination of the centre secrets. It shows that these schemes prevent conventional collusion attacks. The authors also present a new type of statistical attack that is more suitable for the proposed schemes.

042611 'Short RSA Keys and Their Generation'
SA Vanstone, RJ Zuccherato, *Journal of Cryptology v 8 no 2 (Spring 95) pp 101–114*

The authors consider RSA moduli with a certain number of bits fixed in order to save on key storage. They argue, for example, that the first 296 bits of a 1024 bit modulus can be fixed without weakening the system.

042612 'Dynamic access control scheme based on the Chinese Remainder Theorem'
TC Wu, TS Wu, WH He, *Computer Systems Science and Engineering v 10 no 2 (95) pp 92–99*

The authors present an adaptation of the Akl-Taylor key assignment scheme to cope with dynamic access control in a lattice.

042613 'Fast Algorithms for LUC digital signature computation'
SM Yen, CS Laih, *IEE Proceedings on Computers and Digital Techniques v 142 no 2 (Mar 95) pp 165–169*

The authors show how to use the Lucas function's recurrence relation to speed up the computation of LUC signatures.

042614 'Improved Digital Signature Standard'
SM Yen, CS Laih, *IEEE Transactions on Computers v 44 no 5 (May 95) pp 729–730*

The authors propose a variant of DSA, in which the second component of the signature is not $(rx + h(m))/k$ but $(rk - h(m))/x$; this would allow x^{-1} to be precomputed.

7 Computational Number Theory

042701 'Algorithmic Number Theory — The Complexity Contribution'
LM Adleman, *FOCS 94 pp 88–113*

The author traces the relationship between number theoretic and complexity theoretic ideas from Gauss through the advances of the 1970's to the present day. The Solovay-Strassen proof that compositeness is in R made randomness a central feature of complexity theory, while Miller's proof that on ERH primality is in P brought more modern techniques into algorithmic number theory. There follows an extensive discussion of primality proving, and the results due to Pratt, Kilian, Goldwasser, Adleman and Huang which showed that primality is in R; a discussion of modern factoring algorithms from Gauss to the number field sieve; and the latest version of the Adleman/McCurley list of open problems.

042702 'Fast Combinatorial RNS Processors for DSP Applications'
ED Di Claudio, F Piazza, G Orlandi, *IEEE Transactions on Computers v 44 no 5 (May 95) pp 624–633*

The authors describe hardware approaches to parallelising multiplication using residue number systems and the Chinese Remainder Theorem. These improve on previous techniques where varying moduli are involved.

042703 'Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics'
V Dimitrov, T Cooklev, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 82–87*

Two new algorithms for performing modular exponentiation are suggested. They use non-standard number systems: the first one is based on the Zeckendorf representation, and the second on the hybrid binary-ternary number system.

042704 'Gauss periods and fast exponentiation in finite fields'
S Gao, J von zur Gathen, *LATIN 95 pp 311–322*

The authors show that exponentiation of an arbitrary element in $GF(p^n)$ can be performed with $O(n^2 \log\log n)$ operations for small p and infinitely many integers n.

042705 'Almost Primes in Short Intervals'
HZ Li, *Scientia Sinica (Series A) v 37 no 12 (December 1994) pp 1428–1441*

This paper proves that for sufficiently large x, there exists a number with at most two prime factors in the interval $(x - x^{0.4386}, x)$.

042706 'A Survey of Modern Integer Factorization Algorithms'
PL Montgomery, *CWI Quarterly v 7 no 4 (Dec 94) pp 337–366*

This is an extensive survey of modern factoring algorithms, written at the level of the bright undergraduate and illustrated with plentiful numerical examples. After number theory basics, the author explains Pollard's rho, $p-1$ and $p+1$ methods and gives a short account of elliptic curve factoring; he then treats the variants of the quadratic sieve at some length, including the large prime and multiple polynomial variants. Finally, there is a short section on the number field sieve.

042707 'Algorithms for Quantum Computers'
PW Shor, *FOCS 94 pp 124–134*

The author gives Las Vegas algorithms for factoring integers and extracting discrete logarithms on a quantum computer that take a number of steps which is polynomial in the input size. The basic idea behind factoring is to find the least x such that $g^x \equiv 1 \pmod{n}$; this is done by calculating g^a for a superposition of states representing possible a's, and then observing the machine. Discrete log is similar but more complicated.

042708 'Computational Number Theory at CWI in 1970–1994'
HJJ te Riele, J van der Lune, *CWI Quarterly v 7 no 4 (Dec 94) pp 285–335*

The authors survey a quarter of a century of research into computational number theory at CWI; they include performance figures for quadratic sieve implementations on a number of vector supercomputers, plus some preliminary results for the special number field sieve.

042709 'Comment: Fast square-and-multiply exponentiation for RSA'
SM Yen, *Electronics Letters v 31 no 9 (27/4/95) p 712*

The author remarks that the modular multiplcation algorithm proposed in **034706** had already appeared in the literature, and comments on its performance.

8 Theoretical Cryptology

042801 'New Bounds on the Information Rate of Secret Sharing Schemes'
C Blundo, A De Santis, AG Gaggia, U Vaccaro, *IEEE Transactions on Information Theory v 41 no 2 (Mar 95) pp 549–552*

The authors derive new bounds on the information rate and the average information rate of an access structure. They use a substitution technique in which a participant in a scheme is replaced with another scheme.

042802 'Some democratic secret sharing schemes'
M Carpentieri, *Discrete Applied Mathematics v 59 no 3 (26/5/95) pp 293–298*

The author considers how to construct secret sharing schemes using Shamir's method which do not need a dealer and which do not need larger secrets than would be the case if a dealer were present.

042803 'Generalised Cumulative arrays and their application to secret sharing schemes'
C Charnes, J Pieprzyk, *ACSC 95 pp 61–65*

This paper describes some modifications of cumulative arrays that allow realisation of a generalised Shamir scheme with a good information rate. It is shown that an optimal information rate can be achieved for access structures on four participants.

042804 'Private computations over the integers'
B Chor, M Geréb-Graus, E Kushilevitz, *SIAM Journal of Computing v 24 no 2 (April 95) pp 376–386*

A function of n arguments is t-private if there is a protocol for computing it which gives no additional information to a coalition of t participants. It was known that over private domains, every function is $\lfloor (n-1)/2 \rfloor$-private; this is extended to infinite domains. It is shown, for example, that over a countable domain every boolean function is either n-private, 1-private or $\lfloor (n-1)/2 \rfloor$-private but not $\lceil n/2 \rceil$-private.

042805 'On Monotone Formula Closure of SZK'
A De Santis, G Di Crescenzo, G Persiano, M Yung, *FOCS 94 pp 454–465*

The authors show that random-self-reducible (and co-random-self-reducible) languages of statistical zero knowledge proofs are closed under monotone boolean operations; all previously known statistical zero knowledge languages are in these classes. They also discuss some extensions.

042806 'Alternative Necessary and Sufficient Conditions for Collision Intractable Hashing'
T Itoh, K Hayashi, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 19–26*

This paper shows a necessary and sufficient condition for the existence of a collection of collision intractable hash functions. There exists a collection of (separated) collision intractable hash functions if and only if there exists a collection of distinction intractable pseudo-permutations (polarised permutations).

042807 'On Quantum Neural Computing'
S Kak, *Information Sciences v 83 no 3–4 (Mar 95) pp 143–160*

The author examines how quantum computation might be extended to neural networks. He argues that such networks could be trained rapidly, and that the information in them is not locally additive.

042808 'On the Complexity of Bounded-Interaction and Noninteractive Zero-knowledge Proofs'
J Kilian, *FOCS 94 pp 466–477*

The author shows how to prove assertions about committed bits in a number of ways and using much less interaction than was previously required.

042809 '4-Move Perfect ZKIP for Some Promise Problems'
K Kurosawa, W Ogata, S Tsujii, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E78-A no 1 (1995), pp 34–41*

This paper considers ZKIPs for promise problems. It shows a "4-move" perfect ZKIP (black-box simulation) for a promise problem of Quadratic Residuosity and that of Blum Numbers under no cryptographic assumption.

042810 'Reducibility and Completeness in Multi-Party Private Computations'
E Kushilevitz, S Micali, R Ostrovsky, *FOCS 94 pp 478–489*

The authors call f reducible to g in a multiparty private computation if n honest but curious players can compute f privately given oracles for g, and that it is complete if all f are reducible to it. They show that f is complete if and only if it cannot be computed n-privately; however, this complementarity between completeness and private computability breaks down for non-boolean functions. The result is presented as a generalisation of oblivious transfer.

042811 'CS Proofs'
S Micali, *FOCS 94 pp 436–453*

The author defines computationally sound proofs as 'false CS proofs may exist, but they will "never" be found'. He shows that these proofs can be constructed given a random oracale or a cryptographically strong pseudorandom function.

042812 'Necessary and Sufficient Conditions for Collision-Free Hashing'
A Russell, *Journal of Cryptology v 8 no 2 (Spring 95) pp 87–99*

The author defines a pseudopermutation as being computationally indistinguishable from a permutation — that is, that it be infeasible to compute quickly a proof of noninjectivity ($x \neq y$, $f(x) = f(y)$). He then shows that claw-free pseudopermutations exist if and only if collision free hash functions do.

042813 'On the Power of Quantum Computation'
DR Simon, *FOCS 94 pp 116–123*

The author shows that a quantum computer is exponentially faster than a deterministic one at solving the problem of whether a function is invariant under a given xor-mask. Thus provided P $\neq$ PSPACE, quantum computers have greater complexity theoretic power.

042814 'The Parallel Complexity of Propagation in Boolean Circuits'
A Subrahmanian, *Information and Computation v 117 no 2 (Mar 95) pp 266–275*

The problem of deciding whether the output of a Boolean circuit is determined by a partial assignment to its inputs is known to be NP-complete; however many of the consequences of partial input assignment can be determined in linear time by propagating output values. The various cases of this problem are classified in this paper.

042815 'Authentication from Linear Codes'
C Wu, X Wang, *Chinese Journal of Electronics, v 4 no 1 (January 1995) pp 96–98*

This paper proposes an unconditionally secure authentication system using the coset decomposition of a linear code, and discusses the protection which it provides against impersonation and substitution attacks.

9 Book Reviews

'SELF DEFENCE IN OPEN SYSTEMS: PROTECTING AND SHARING RESOURCES IN A DISTRIBUTED OPEN ENVIRONMENT'
MR Low
PhD Thesis, University of Hertfordshire, 1994

This thesis investigates how open distributed systems can be built using self authenticating proxies. These are digitally signed tokens giving access to a specific amount of a resource; unlike Neumann's proxies, they carry both the certificate of the key with which they were signed, and relevant accounting information. Thus their function is somewhat between that of capabilities and that of cheques.

A number of different mechanisms can be based on them, including delegation and endorsement; freshness can be provided where needed in protocols by a specific freshness certificate. Possible applications include electronic publishing, banking, and general access control; and performance figures for a test implementation are given. The conclusion is that the proxy mechanism is well suited to provide a general purpose protection mechanism in heterogeneous distributed systems.

'CIPHER AND HASH FUNCTION DESIGN'
J Daemen
Doctoral Thesis, Katholieke Universiteit Leuven, March 1995

The author develops a unified approach to linear and differential cryptanalysis based on Walsh transform techniques. Providing resistance against both types of attack then becomes a matter of preventing low-weight trails — whether linear or differential — combining to produce something nasty, such as where rounds having few active S-boxes alternate with rounds having many.

He then investigates ways of combining computational primitives in ways which may give systematic bounds on attack propagation, and proposes a number of designs for block ciphers, stream ciphers and hash functions. One feature is a discussion of self-synchronising stream ciphers, for which a novel recursive architecture is proposed.

Finally, there are a number of cryptanalytic results on stream ciphers, including active attacks based on forcing the target machines to resynchronise, a collision for a hash function of Damgård, and a family of weak keys for IDEA.

'LA SÉCURITÉ DES PRIMITIVES CRYPTOGRAPHIQUES'
S Vaudenay
Doctoral Thesis, Laboratoire d'Informatique de l'Ecole Normale Supérieure, April 1995 (in French)

Over the last few years, Serge Vaudenay has obtained a number of cryptanalytic results, primarily against hash functions. These are set out in a systematic way in his thesis.

Firstly, he considers the graph of a calculation — the way in which which its lower level primitives are combined into a round function. SP networks, Feistel networks and IDEA are familiar; but many hash functions use more complicated arrangements in the search for performance, and some of these possess structures which can be exploited in various ways. For example, spectral techniques can be used to search for fixed points. This section contains his attack on FFT-hash II.

He then goes down a level to look at the S-boxes or other lower level primitives. It starts off with his attack on two-round MD4 and proceeds to the development of a theory of multipermutations, which can be used to protect against both structure-level and primitive-level attacks; as an example, he considers how SAFER could be broken if its S-box were replaced with a random function. Finally, there is a discussion of nonlinearity and its role in preventing statistical attacks.

‘VERSCHLÜSSELT: DER FALL HANS BÜHLER’

R Strehle

Werd Verlag, 1994; ISBN 3-85932-141-2 (in German)

Hans Bühler was a salesman for Swiss crypto equipment supplier Crypto AG. He was arrested by the Iranian government and spent some time in prison before his employers bailed him out at great expense. On his return from Teheran, he was dismissed from the company, and in this book he tells his story.

Apparently the Iranian authorities believed that Crypto AG's products had been deliberately weakened in order to facilitate eavesdropping by the NSA. Was this true, or was it just an American ploy to discredit one of the third world's few sources of cryptographic equipment?

The answer will not be found directly in these pages. However they provide a number of insights into the company, the client, and the technology as perceived by a sales engineer. There is also a lot of material on the Iranian prison system.

‘COMPUTER SECURITY BASICS’

D Russell, GT Gangemi

O'Reilly and Associates, Inc, 1991; republished 1993; ISBN 0-937175-71-4

The turnover of computer security managers in US government is seven months, and it is probably just as bad in the private sector; after all, the job involves obstructing other managers' goals. So there is a steady market for books and courses from which the latest victims can learn the basics, and this book by Russell and Gangemi is one of the better ones.

It covers the motherhood-and-apple pie topics of physical, logical and communications security; there is no great depth, but unlike in many books of this type there are no really serious mistakes we could find. Coverage is broad, from Tempest through biometrics and access control models to audit, and there are extensive appendices covering US government standards and requirements.

‘PRACTICAL UNIX SECURITY’

S Garfinkel, G Spafford

O'Reilly and Associates, Inc, 1991; republished 1994; ISBN 0-937175-72-2

The move from mainframe to client-server systems has dispersed the system administration function. Previously this was handled by a central team of experts; now most administrators are part-timers looking after a local LAN. However, managing Unix security is a fairly complicated task, and there are many pitfalls for the unwary. How is this gap to be bridged?

Garfinkel and Spafford's book provides part of the answer. It starts off at an easy pace, explaining the basic mechanisms of passwords, groups, file permissions, logs and backups; the level gradually becomes more technical, and the weaknesses of suid, rsh and so on prepare the reader for the more complex security problems introduced by networking. These take up the last half of the book, and culminate in a brief discussion of firewalls.

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 1995 (volume 4) plus a set of the remaining back numbers (currently v 2 no 1, 3 and 4 and all of v 3) 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 1995 - Please debit my VISA/MasterCard £60 ☐ I enclose a cheque for £60 ☐ / US$90 ☐

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

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

Corporate subscription for all 1993, 1994 and 1995 issues - Please debit my VISA/MasterCard £145 ☐ I enclose a purchase order / cheque for £145 ☐ / US$212.50 ☐

Name: ....

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

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

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

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