Computer and Communications
Security Reviews

Volume 5 Number 2 (June 1996) ISSN 1352-6278

CONTENTS

Editor: Ross Anderson *Cambridge*

Contributing Editors:

Mike Burmester *London*
Dieter Gollmann *London*
Richard Graveman *Bellcore*
Sushil Jajodia *George Mason*
Heather Hinton *Toronto*
Kwok-Yan Lam *Singapore*
Ira Moskowitz *US Naval Labs*
Rei Safavi-Naini *Wollongong*
Pierangela Samarati *Milan*
Bruce Schneier *Counterpane*

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

'Computer and Communications Security Reviews' is published quarterly by, and is copyright, of Northgate Consultants Ltd. Subscription rates, conditions and ordering details are on the inside back cover.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by June 1996; and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Boppard 95: 5th annual Boppard workshop of the BSI on technology assessment, June 13–14 1995, Federal Academy of Public Administration, Germany; *proceedings published by SecuMedia Verlags GmbH, ISBN 3-922746-27-6*

Database 95: 9th annual IFIP TC11 Working Conference on Database Security, August 13–15 1995, Rensselaerville, NY, USA; *proceedings published by Chapman & Hall ISBN 0-412-72920-2*

Apps 95: 11th Annual Computer Security Applications Conference, December 11-15 1995, New Orleans, Louisiana; *proceedings published by the IEEE, ISBN 0-8186-7159-9*

NISSC 95: 18th National Information Systems Security Conference (formerly the National Computer Security Conference), October 10–13 1995, Baltimore, Maryland; *proceedings published by NIST*

FSE 96: 3rd International Workshop on Fast Software Encryption, February 21–23 1996, Cambridge, UK; *proceedings published by Springer as Lecture Notes in Computer Science vol. 1039*

ACM 96: 3rd ACM Conference on Computer and Communications Security, March 14–16 1996, New Delhi, India; *proceedings published by ACM, ISBN 0-89791-829-0*

Canada 96: 8th Annual Canadian Computer Security Symposium, "Business and Security in an Electronic World", April 29 – May 3 1996, Ottawa, Canada; *proceedings published by Communications Security Establishment of Canada; no ISBN number*

Oakland 96: 1996 IEEE Symposium on Security and Privacy, May 6–8, Oakland, California; *proceedings published by the IEEE, ISBN 0-8186-7417-2*

The first volume of the NISSC 95 proceedings were abstracted in volume 5 number 1; the abstracts here are of papers in the second volume.

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

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

or

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

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

1 Applications and Engineering

052101 'A Security Policy Model for Clinical Information Systems'
RJ Anderson, *Oakland 96 pp 30–43*

This article sets out a security policy model which aims to do for medical systems what Bell-LaPadula did for military systems and Clark-Wilson for banking systems: to reduce the protection goals to a small number of rules that can form a basis for communication between users and system builders, and also a foundation for more formal security models. The model encapsulates the principle that patients must consent to the sharing of their personal health information, and sets out nine access control rules that express this while taking into account the relevant features of medical privacy. The model is one of the first to tackle personal rather than institutional confidentiality concerns in a systematic way.

052102 'Industrial cryptography'
R Anderson, *IEE Review v 42 no 3 (May 1996) pp 118–120*

Applications that use embedded cryptography as an aid to crime prevention of various kinds have come to outnumber the more classical secrecy-oriented systems. This article discusses a number of them, including pay-TV, prepayment utility meters, burglar alarm signalling and automatic teller machines. It describes a number of ways in which banking, metering and pay-TV system security has failed, and points out that systems which are to provide evidence in court must be designed to withstand review by hostile expert witnesses.

052103 'On the Reliability of Electronic Payment Systems'
RJ Anderson, SJ Bezuidenhoudt, *IEEE Transactions on Software Engineering v 22 no 5 (May 96) pp 294–301*

In this journal version of **043102**, the authors describe the introduction of prepayment electricity meters to South Africa and the various security and reliability problems that were encountered. The security problems that caused actual losses all resulted from the opportunistic exploitation of blunders in design, implementation and operation. The lessons that security engineers should learn include the desirability of using multiple evaluators and the value of field trials. The experience also highlights the difficulty of trusting third parties, such as banks, not to sell meter tokens and then lose evidence of the sale.

052104 'Keeping it simple'
D Austin, *Banking Technology v 13 no 3 (Apr 96) p 16*

This article reports an attack by a senior banking IT figure on the fashionable sentiment that credit card transactions over the Internet should be encrypted. He dismisses this as hype and points out that the great majority of 'card not present' fraud involves dishonest retailers; thus protocols such as SET are in his opinion solving the wrong problem.

052105 'Lotus Notes - a New Security Paradigm'
I Beale, *Computer Law and Security Report v 12 no 2 (Mar/Apr 96) pp 112–114*

This article discusses the security features of Lotus Notes, and lists some of the questions that an auditor, user, manager or attacker should ask about its configuration.

052106 'Secured by Software'
N Blackman, *Security Gazette (May 96) pp 14–15*

The author predicts that the next generation of site security systems will be integrated with corporate systems generally, so that security managers will be able to watch closed circuit TV pictures in a corner of their PC screen rather than having to go down to a special room in the basement.

052107 'Perils and Pitfalls of Practical Cybercommerce'

NS Borenstein, *Communications of the ACM v 39 no 6 (June 96) pp 36–44*

This article describes a number of the problems experienced by customers of First Virtual's Internet payment system. Many of them had to do incompatible implementations of Internet protocols causing obscure problems — of a kind whose solution is not currently among the core competences of financial institutions. In addition to bugs and configuration problems, users made many mistakes typing email addresses. Things are made more complex still by the international nature of internet business, which leads to language problems. Finally, the role and limitations of cryptography are discussed, together with the threats against electronic payment systems.

052108 'The world is your oyster'

JC Broustra, *Cards International no 151 (12/3/96) p IV*

The CEO of Gemplus, a leading smartcard maker, says in this interview that his company plans to get into the US market by buying a share in DataCard, and into China via Golden Card, a combined ID/health/banking card.

052109 'ATM use grows at home and abroad, but never on Sundays'

Card World Independent (Mar 96) p 3

This article presents the latest figures for the number of ATMs and volumes of transactions for VISA/Plus, Europay and Mastercard/Cirrus, plus a breakdown of transactions by age group.

052110 'Europay launches reloadable, EMV compatible, multi-currency purse card'

Card World Independent (June 96) pp 4–5

An electronic purse smartcard called CLIP has been launched by Europay and will be tested in Iceland, Italy and the Czech Republic.

052111 'Planning for an immovable deadline'

Card World Independent (June 96) p 3

This article describes how VISA, Mastercard and Amex plan to deal with the Millenium bug on their international card payment networks.

052112 'Stock market fiasco over biometrics contract'

Card World Independent (May 96) pp 1–2

A US biometric company's shares leapt almost 30 times in value on the false rumour that it had secured a contract with Mastercard for fingerprint verification on payment cards. The actual contract was for a card with a built in fingerprint scanner that will be used to control access by the organisation's employees and visitors.

052113 'Visual card displays personalised messages'

Card World Independent (May 96) p 8

A new card technology has a visible message that can be rewritten by a terminal. It has embedded magnetic particles that can be rearranged by a write head to display non-volatile visible characters or graphics.

'E-commerce strides into Asia'

ComputerWorld v 2 no 19 (22-28/3/96) pp 223–228

This article gives an overview of the current progress of electronic commerce in several Asian countries including Singapore, Japan and Thailand. It observes that electronic commerce appears to be making slow but steady progress in the Asia-Pacific region as organisations there start to develop and implement secure transactions over the Internet.

052114 'Defending a Computer System using Autonomous Agents'
M Crosbie, EH Spafford, *NISSC 95 pp 549–558*

The authors propose using a number of simple 'intelligent agent' programs to detect intrusions. Each of them would look out for some particular symptom of hostile presence and they would confer about their suspicions. The idea is that this could be cheaper, more resilient, more scalable and degrade more gracefully than a traditional intrusion detection system.

052115 'Java Security: From HotJava to Netscape and Beyond'
D Dean, EW Felten, DS Wallach, *Oakland 96 pp 190–200*

The authors describe a number of flaws that they have discovered in various implementations of Java. In addition to the specific problems — which involved buffer overflows, loaders, pathnames, pointer forgery and public proxy variables — there are more general problems. Java has no security policy, and its implementations lack the basic features of a secure operating system, such as a TCB and an audit trail. They conclude that in its current form, Java cannot easily be made secure.

052116 'An Immunological Approach to Change Detection: Algorithms, Analysis and Implications'
P D'haeseleer, S Forrest, P Helman, *Oakland 96 pp 110–119*

The authors present improved algorithms for generating detector sets for use in the virus detection systems they constructed inspired by the immune system (**032116**). They present theoretical and simulation results for different parameters such as string length and the number of detectors.

052117 'Component architectures for Trusted NetWare'
J Epstein, G Grossman, R Schell, *NISSC 95 pp 455–463*

The authors describe the first two components being evaluated under the Trusted NetWare architecture — a PC based server, and a standalone client consisting of a PC with an add-on board to provide secure booting, encryption, and access to both the hard disk and the ethernet.

052118 'Electronic Commerce and Payment Mechanisms'
D Everett, *Smart Card News part 1: Mar 96 pp 56–59; part 2: Apr 96 pp 76–78; part 3: May 96 pp 96–99; part 4: June 96 pp 118–119*

These articles describe the basic mechanisms of electronic payment systems, such as encryption, card verification values and public key certificates.

052119 'Lessons Learned During the Life Cycle of an MLS Guard Deployed at Multiple Sites'
T Fiorino, P Casey, M Easley, R Jordan, *Apps 95 pp 99–107*

The paper describes the functional architecture of the Command and Control Guard (C2G), which allows two way automated transfer of data files between computing systems at high and low classifications. It provides an overview of its certification, accreditation and deployment process, and concludes with a review of the lessons learned during various phases of the project.

052120 'Electric Money'
U Flohr, *Byte Magazine v 21 no 6 (June 96) pp 74–84*

This article surveys a number of the better known electronic payment systems including DigiCash, NetCheque, NetBill and SET.

052121 'A Sense of Self for Unix Processes"
S Forrest, SA Hofmeyr, A Somayaji, TA Longstaff, *Oakland 96 pp 120–128*

The authors develop a novel intrusion detection system inspired by their previous work on antiviral software inspired by the immune system (**032116**). They monitor short sequences of system calls, and raise an alarm when a new sequence is encountered. Experiments show that after a few thousand calls have been monitored, few new patterns are observed until the underlying use changes. Rather than just detecting unauthorised programs, this technique can detect abnormal use of authorised programs such as sendmail, which play a part in many known kinds of attack. Furthermore, as it is local and adaptive, the defences of an organisation's machines would not be all the same and thus they would hopefully not all fall to the same attack.

052122 'The learning curve'

T George, *Banking Technology v 13 no 4 (May 96) pp 26–30*

This article surveys the latest self-service banking technology products such as automated loan machines and interactive video terminals, which facilitate unmanned microbranches. However, recent research shows that 60% of bank income comes from the 40% who do not use self service machines, which questions the wisdom of this investment.

052123 'An Open Trusted Network Architecture'

G Grossman, J Epstien, R Schell, *NISSC 95 pp 447–454*

The authors describe Trusted NetWare, an architecture developed by Novell and aimed at C2 under TNI. Its core is a security protocol implemented in several layers using active components embedded in clients and servers.

052124 'Medical Records Security'

EB Heinlein, *Computers and Security v 15 no 2 (96) pp 100–102*

The author talks about some existing and proposed regulations for medical record privacy in the USA and compares them unfavourably with Europe.

052125 'What's Up Doc?'

S Hinde, *Computer Audit Update (May 96) pp 2–4*

The author mentions the dispute between the British Medical Association and the health service on the security of a new national network, and argues that since most attacks are local, the emphasis should be on securing end systems.

052126 'SAP: Changing Risks, Internal Controls and Fraud Prevention'

N Iyer, *Computer Audit Update (May 96) pp 19–22*

This article discusses the particular problems and risks associated with implementing systems in SAP R/3.

052127 'A hierarchic neural network for human face detection'

P Juell, R March, *Pattern Recognition v 29 no 5 (96) pp 781–787*

The authors built a system to find human faces in images, as a front end for facial identification systems in law enforcement. They use contour enhancement plus four neural networks; there is one each for eyes, nose and mouth and these drive a 'parent' net which searches for possible faces.

052128 'User-Identifikation bei der Online-Dokumentation im Krankenhaus'

R Kaiser, *Datenschutz und Datensicherheit v 20 no 3 (Mar 96) pp 142–146*

Hospital records are often required to settle legal actions, but the electronic records that are becoming widespread in Germany have little legal standing, as they could have been created by any one of a number of users. In response to this and to general security concerns, the university clinic at Tübingen is installing a C2 evaluated hospital information system that will use Windows PCs as terminals.

052129 'A Design of Secure EDI Systems'

CG Kang, EJ Yoon, DH Kim, DK Lee, *Canada 96 pp 397–416*

This paper describes several threats to security encountered with Electronic Data Interchange (EDI) systems and the services required to implement Secure EDI (SEDI), as developed for Korea Telecom.

052130 'A DSS-Model for attack detection'
D Karafiannis, R Telesko, C Mayr, *Apps 95 pp 133–141*

This paper describes a model for using Decision Support Systems (DSS) in attack detection and classification, and presents an implementation of the model within SECURENET II project. The model consists of a number of modules: monitoring modules gather information from the network, and deliver it to three kinds of detection modules (expert system, neural network, and user intention and identification). The first of these detects well-known attacks, while the others analyse behaviour and look for anomalies. Alarms are then passed to a decision module.

052131 'Authorship Analysis: Identifying the Author of a Program'
I Krsul, EH Spafford, *NISSC 95 pp 514–524*

An attempt is reported to classify the authorship of 88 programs written by 29 different authors. The overall success rate was 73% but this varied widely; 17 were always correctly identified, and two never. The difficulties stem from code reuse, programming teams, software engineering methodologies, formatting tools and compilers.

052132 'Locating and extracting the eye in human face images'
KM Lam, H Yan, *Pattern Recognition v 29 no 5 (96) pp 771–779*

The eye is the most important feature that facial recognition systems must extract, but the traditional dynamic template algorithms for this are computation intensive. The authors show that a speedup of about 40% can be obtained by first locating the head boundary, then estimating the eye location, finding the eye corners, and finally using these to set initial parameters for the templates. They suggest that their approach could also be adapted to find the eyebrows and the mouth.

052133 'A Multivariate Data Analysis Software for Enhancing System Security'
KY Lam, L Hui, SL Chung, *Journal of Systems & Software v 31 no 3 pp 267–275*

This paper presents a multivariate data analysis technique for the analysis of user behaviour patterns in intrusion detection. Data analysis involves two steps: analysis of correlations, which is based on standardized principal components analysis, and classification of behaviour patterns, which is automated by a cluster recognition technique.

052134 'SATAN and Friends / SATAN et ses amis'
N Legault, R MacLean, *Canada 96 pp 41–67*

Three well-known software security tools (COPS, ISS and SATAN) were used to test a simple network system for vulnerabilities. The services that each tool provides are described in far more detail than are the results that each tool achieves during testing. All three tools were found to satisfy their stated objectives, and their features are tabulated.

052135 'Card fraud drops 14%'
R Martin, *Cards International no 152 (26/3/96) p 4*

According to APACS figures, payment card fraud in the UK fell from £96.8 million in 1994 to £83.3 million in 1995, despite a growth in total credit and debit card transaction values of 11% and 25% respectively. Cross-border fraud, at £20 million, is a growing component of the total.

052136 'Building a Firewall'
V McCarthy, *Datamation (15/5/96) pp 74–76*

The author discusses the pros and cons of firewalls, mentions ten products, and talks about configuration problems.

052137 'A Network of Firewalls: An Implementation Example'
B McKenney, D Woycke, W Lazear, *Apps 95 pp 3–13*

This paper describes a network firewall used to protect nodes of the Open System

Information System (OSIS), an information system used by US Intelligence Community to share unclassified information over Internet. It describes the operating environment, security policy and architecture of OSIS and discusses issues and lessons learned through implementation of the firewall. It covers issues common in implementation of firewalls, such as DNS and sendmail, together with issues unique to a network of firewalls, such as proxy to proxy compatibility.

052138 'A Systematic Methodology for Firewall Penetration Testing'
PR Moyer, EE Schultz, *Network Security (Mar 96) pp 11–18*

This article discusses how SRI goes about testing firewalls: with a combination of design review, policy evaluation and penetration tests. The tests first try to identify hosts and services behind the firewall, to find configuration errors and exploit known weaknesses, both in attacking the firewall machine itself and the hosts behind it.

052139 'Monitoring and Controlling Suspicious Activity in Real-time With IP-Watcher'
M Neuman, *Apps 95 pp 114–122*

IP-Watcher is a network monitoring program with graphical and text interfaces. It can be installed on a SUN (where it requires root privilege); it monitors logons in real time, reads relevant streams of data, and controls intruders by terminating or taking over their sessions. The paper describes its defensive and offensive uses and concludes with possible future extensions.

052140 'Money in Electronic Commerce: Digital Cash, Electronic Funds Transfer, and Ecash'
P Panurach, *Communications of the ACM v 39 no 6 (June 96) pp 45–50*

The author describes the broad functionality of electronic cheque systems, prepaid cards and a Digicash scheme currently being implemented by a bank in Missouri. He also discusses policy implications such as the increased velocity of money and regulatory lag.

052141 'The UBI Project: Securing a Residential Electronic Highway'
S Ratajczak, *Canada 96 pp 87–105*

This paper introduces the Universal, Bi-directional and Interactive (UBI) television project, designed to implement a set of multimedia services in homes throughout the province of Quebec. The technology and security requirements of the UBI network are discussed; the consortium partners include Groupe Videotron, Canada Post, Hydro-Quebec, National Bank of Canada, a smart card firm, the provincial lottery and Hearst.

052142 'Practical Security Solutions Using ENTRUST'
T Reinhardt, *Canada 96 pp 29–40*

This paper discusses how to use the NorTel cryptographic product, Entrust, to build low-cost customized security applications for a distributed system. It includes several "examples" of how to use it, including how to implement it and some pitfalls to avoid.

052143 'A Systems Engineering Approach to Security Engineering'
J Robbins, D Weiss, B Cornish, *Canada 96 pp 333–350*

This paper discusses issues related to the MIL-STD-499B (and similar) standards for security systems engineering. A complex information architecture must be separated into an "Information Domain" (information assets) and an "Information System" (the physical network systems) and can be modelled using the Hatley and Pirhbai modelling approach.

052144 'Building the Right Firewall'
EE Schultz, *Network Security (June 96) pp 13–17*

The quality of available firewalls varies greatly, and their common failure modes are discussed, as are the design tradeoffs and the question of whether an organisation should buy or build.

052145 'Seeing Red?'
S Scott, *Security Surveyor v 26 no 3 (Mar 96) pp 9–10*

The manager of the UK's largest burglar alarm service explains the measures his company has taken to reduce false alarms due to line and other failures, which if persistent can result in the police withdrawing cover from affected sites.

052146 'An Analysis of the Intel 80x86 Security Architecture and Implementations'
O Sibert, PA Porras, R Lindell, *IEEE Transactions on Software Engineering v 22 no 5 (May 96) pp 283–293*

In this journal version of **043152**, the authors report an examination of the Intel 80x86 family of microprocessors for security relevant bugs. A number of documented and undocumented features were found that could introduce covert channels, only some of which could be blocked by a knowledgeable TCB designer. In addition, no less than 117 implementation errors affecting various versions of the processors have been reported, and seven of these (in the 386 and 486) could violate protection directly.

052147 'Electronic Purses: A Comparative Review'
Smart Card News part 8: Mar 96 pp 46–49; part 9: Apr 96 pp 66–69

These articles continue **044147** and **051145** with details of a number of electronic purse trials and a discussion of the lessons learned from them.

052148 'Lufthansa Introduces Ticketless Travel'
Smart Card News (May 96) pp 81–83

Lufthansa has introduced smartcards for 600 frequent fliers on the Frankfurt to Berlin route; they combine booking, ticketing and boarding control functions. They will be extended shortly to all domestic flights.

052149 'A confidentiality system for ISDN inter-PC high-speed file transfer'
K Tanaka, H Matsumoto, I Oyaisu, *Computers and Security v 15 no 2 (96) pp 141–155*

The authors describe an NTT product for encrypting file transfer and telephone traffic between PCs over an ISDN line. The encryption is FEAL in appropriate modes, while the key management is a variant of Otway-Rees. They give performance figures for the end systems and for the key distribution centre.

052150 'Using Multi-Vendor Products to Support the Department of National Defence Strategic Security Architecture'
JH Weigelt, C Clupp, B Hunter, M Murray, D Wiener, *Canada 96 pp 257–268*

This paper describes the Canadian Department of National Defence IT security architecture and security architecture implementation plan, which incorporates multiple products from multiple vendors.

052151 'Beyond the fire-walls'
M Whybrow, *Banking Technology v 13 no 3 (Apr 96) p 18*

Hewlett Packard has acquired a company called Secure Ware with a view to supplying MLS operating systems, firewalls and encryption to banks and other companies wishing to do business on the net.

2 Operating System and Database Security

052201 'Ensuring Atomicity of Multilevel Transactions'
P Ammann, S Jajodia, I Ray, *Oakland 96 pp 74–84*

The authors tackle the problem of atomicity in MLS databases by defining a notion of 'semantic atomicity': this means that either all or none of the sections of a transaction are present in any history. Correctness is measured by the maintenance of integrity constraints rather than by serialisability.

052202 'Providing Different Degrees of Recency Options to Transactions in Multilevel Secure Databases'
V Atluri, E Bertino, S Jajodia, *Database 95 pp 211–247*

The authors propose a multilevel concurrency control model, based on use of timestamps and multiple versions, that provides different recency options to transactions: each transaction can choose the desired degree of recency for low data, and retrieving less recent data implies a shorter waiting time. Transactions can thus trade off recency for performance, and four different degrees of recency are possible. The protocols to assign timestamps to transactions in each of the four cases are presented, and a proof that the protocols produce one-copy serializable schedules is given.

052203 'Approach to object security in Distributed SOM'
M Benantar, B Blakley, AJ Nadalin, *IBM Systems Journal v 35 no 2 pp 192–203*

The authors describe the security mechanisms in IBM's Object Model, which is consistent with CORBA. An authentication such as Kerberos (or a user password) establishes a security context between client and server DSOM applications, and access to DSOM objects can be controlled at the server. The system is based on GSS/API and contains both policy and persona objects.

052204 'Supporting Multiple Access Control Policies in Database Systems'
E Bertino, S Jajodia, P Samarati, *Oakland 96 pp 94–107*

The authors discuss how to cope with conflicts between positive and negative authorisations that propagate down directories or other access structures. Their model is based on making some authorisations stronger than others, so that a strong positive authorisation that an object inherits from one structure will override a weak negative authorisation it gets from another. This allows a large number of different policies to be expressed, and holds out the prospect of access control mechanisms that can support multiple policies at the same time.

052205 'A Toolset for Multilevel Database Design'
R Burns, Y Koh, *Apps 95 pp 42–51*

The lack of computer aided engineering tools to support design of secure multilevel secure database has motivated development of a tool that is the subject of this paper. It is based on SRI Database Inference System Security Tool (DISSECT) and a commercial product Software through Pictures (StP), extended to support security labels. Its usefulness was validated by employing it in the design of a database.

052206 'Inference Analysis During Multilevel Database Design'
RK Burns, *Database 95 pp 301–316*

The author presents an approach to multilevel database design that combines two existing tools: a prototype inference analysis tool that identifies possible inference problems in multilevel schemas, and a commercial Entity Relationship diagramming tool that creates normalized relational database schemas from conceptual schemas. Combining the two tools helps a designer create multilevel relational schemas free from inference channels.

052207 'Solution to the On-Line Image Downgrading Problem'
S Cha, G Park, H Lee, *Apps 95 pp 108–112*

It has been shown that images can easily be contaminated with other information and even other images by embedding them in the low order bits. This causes problems when downgrading image data, as the presence or absence of embedded data is not readily visible, and detecting it is much harder than for text. The paper argues that the problem exists as long as images are represented in "raw" format and argues that palettisation could provide a solution to the problem.

052208 'Modeling a Multilevel Database with Temporal Downgrading Functionalities'
F Cuppens, A Gabillon, *Database 95 pp 145–164*

The sensitivity level of a piece of information may decrease with time or upon the occurrence of certain events. This paper discusses the problem of how to automatically enforce downgrading; rules are discussed which allow downgrading to occur at a specific time, upon the occurrence of certain events, or upon explicit requests by users. This is formalised in a language based on a temporal multilevel model; a logical interpretation of the entity-relationship approach is expressed in first order logic and extended with security levels, time concepts and mechanisms for specifying different downgrading rules.

052209 'Multilevel Security Issues in Real-Time Embedded Systems'
T Darr, *Apps 95 pp 80–86*

A typical real-time embedded system consists of a manager, an application domain and bulk storage. The system manager is similar in function to an operating system; it defines and enforces the global system security policy. The application domain performs the operational mission and the storage system stores classified data in an encrypted form. Questions such as scope of the security policy, its impact with other disciplines such as safety or reliability, and where and when a rigorous policy is needed are discussed. The paper concludes by suggesting areas of research and development.

052210 'User-Role Based Security Enforcement Mechanisms for Object-Oriented Systems and Applications'
SA Demurjian, TA Daggett, TC Ting, MY Hu, *Database 95 pp 79–94*

This paper discusses the implementation of role-base access control mechanisms, and in particular the problem of automatically generating applications embedding security specifications starting from text and form-based input. The authors discuss how ADAM, a system developed by them for the automatic generation of object-oriented applications, can be extended to include security specifications. Three possible approaches to generating code are presented, and their extensibility, flexibility, encapsulation, and reusability are described.

052211 'Umsetzung von IT-Sicherheitsanforderungen in UNIX-Umgebungen'
W Dinkelsbach, M Hübner, *Datenschutz und Datensicherheit v 20 no 3 (Mar 96) pp 159–166*

The spread of open systems has caused problems in the German banking industry, where people are not yet sure how to bring Unix systems up to banking security standards. Perceived problems include the large number of applications that must run as root (leading to poor separation of duties), poor scalability of security management, inflexible and over-simplified access control structures, and network security holes. For the most part, pragmatic solutions involve configuration management and procedural controls to compensate for these weaknesses; but this ad-hoc approach runs into problems in large installations. A number of Unix security tools developed for the German market are mentioned.

052212 'Messages, Communications, Information Security: Protecting the User from the Data"

JE Dobson, MJ Martin, *Database 95 pp 8–23*

The paper discusses the effects that incorrect information can have on the real-world. Different kind of failures that can result in compromised integrity of data or misinterpretation of data are discussed. The novel idea is to analyse database security in terms of message passing; many failures can be seen as a mismatch of sender and receiver (in some sense). A modeling method for analyzing failures and their effects on the system is presented.

052213 'Object-Oriented Modeling of Security Semantics'

E Ellmer, G Pernul, G Kappel, *Apps 95 pp 52–61*

This paper proposes an object oriented modeling technique for designing multilevel secure database applications. The technique uses three models of an object — static functional and behavioural — reflecting data structures, methods and life-cycle respectively. To develop a conceptual schema for a multilevel secure application, it uses an integrated data definition and behaviour modeling technique based on alternating refinement of each of the three models, and classification constraints help assign security labels to modeling concepts.

052214 'A Formal Specification of an Authorization Model for Object-Oriented Databases'

EB Fernandez, RB France, D Wei, *Database 95 pp 95–110*

The authors present the formal specification of an authorization model they had previously proposed for the protection of object-oriented systems and which considers authorizations for users to execute methods on classes. These authorizations are specified by the administrator; they can be positive or negative and explicit or implicit. Implicit authorizations are authorizations derived from those specified according to predefined rules and to the relationships among object classes. The formalization expresses, by using the formal language Z, the constraints that must be satisfied on the set of authorizations and the rules for the derivation of implicit authorizations with respect to the composite, aggregation, and generalization hierarchies among object classes.

052215 'A Security Model of Dynamic Labeling Providing a Tiered Approach to Verification'

SN Foley, L Gong, XL Qian, *Oakland 96 pp 142–153*

The authors propose a mandatory access control model that can support multilevel, Chinese Wall and separation of duty policies. The idea is that a TCB, once evaluated, could be used in a number of different environments. The central idea is control of dynamic label changing.

052216 'Improving Inter-Enclave Information Flow for a Secure Strike Planning Application'

J Froscher, D Goldschlag, M Kang, C Landwehr, A Moore, I Moskowitz, C Payne, *Apps 95 pp 89–98*

This paper describes the security requirements of some military intelligence systems that consist of many enclaves with limited information flow between them. This results in duplication of operation, and inconsistent and untimely data at different sites. Next it describes a system that uses reliable one-way flow from low to high that permits timely use of low results while limiting leaks of high information. The framework isolates security critical functions and allows analysis of information flows.

052217 'MISSI Compliance for Commercial-Off-The-Shelf Firewalls'

M Hale, T Mannarino, *Canada 96 pp 15–27*

This paper describes the National Security Agency's Multilevel Information System Security Initiative (MISSI) attempt to define standards for compliance with a minimal set of security and interoperability standards for commercial firewalls as used within a defence information security structure. It describes at a high level the security requirements for MISSI-compliant firewalls.

052218 'ILIAD: An Integrated Laboratory for Inference Analysis and Detection'

TH Hinke, HS Delugach, RP Wolf, *Database 95 pp 333–348*

The authors present a system to detect inference channels in multilevel databases. It is based on two main components: an inference detection tool and a database generator tool. The former retrieves inference channels in multilevel databases by operating on conceptual graphs derived from a semi-automated analysis of multilevel relation schemas, relation instances, and external knowledge. The latter produces multilevel databases against which the former can be tested, and uses a simulator to check whether the resulting database contains actual inference channels.

052219 'A Security Design Method for Information Exchange In and Between Organizations'

R Holbein, S Teufel, K Bauknecht, *Database 95 pp 267–285*

This paper presents an approach to security specification design, based on the use of a transaction based business process model of an organization's activities. From this, the authorizations each role needs in order to carry out its tasks are derived. It discusses grouping subjects, objects, and operations to limit the number of authorizations that must be considered.

052220 'An access control scheme based on Chinese remainder theorem and time stamp concept'

MS Hwang, WG Tzeng, WP Yang, *Computers and Security v 15 no 1 (96) pp 73–81*

The authors add timestamps to an access control scheme in which access rights are encoded using divisibility of labels modulo small prime numbers.

052221 'Argos — A Configurable Access Control Subsystem Which Can Propagate Access Rights'

D Jonscher, KR Dittrich, *Database 95 pp 43–60*

The authors present a system for enforcing access control in distributed federated database systems based on a general discretionary access control model with concepts such as positive/negative, implicit/explicit, and role-based authorizations. Administration can be decentralized and different protection policies can be enforced at the users' discretion. Each policy is implemented by a particular reference monitor which mediates all accesses to objects regulated by it. Requests submitted to the federation are checked first at the federation level and then at the site where the data to be accessed are stored. Two different degrees of local autonomy, corresponding to different local controls to be executed, are supported.

052222 'A Network Pump'

MH Kang, IS Moskowitz, DC Lee, *IEEE Transactions on Software Engineering v 22 no 5 (May 96) pp 329–338*

In this journal version of **043216**, the authors discuss how to extend the NRL data pump to networks in which there are multiple 'high' and 'low' participants. The goals are to balance congestion control, fairness, reliability, performance and resistance to both covert channel and service denial attacks. They discuss the buffer management techniques they use, which include a randomised delay in acknowledgement messages and buffer size allocation using a moving average of previous transactions. Finally they report the results of simulating the performance under various possible attacks.

052223 'Data security equals graph connectivity'

MY Kao, *SIAM Journal of Discrete Mathematics v 9 no 1 (Feb 96) pp 87–100*

The effectiveness of cell suppression techniques in statistical security applications had previously been shown by Gusfield to depend on the properties of the 'suppressed graph' of the database, in which vertices correspond to rows and columns, and edges to individual cells. This model is significantly extended in this article. It is shown for example that a cell is protected if and only if it lies in a suitable cycle, and all suppressed cells are protected if and only if each component of the graph is strongly connected and bridge free. Equivalences are shown between the protection of cells, columns and larger structures, and NP completeness results are proved: for example, finding the optimal set of cells to suppress for a given protection property is NP complete.

052224 'Security and Data Mining'
TY Lin, TH Hinke, DG Marks, B Thuraisingham, *Database 95 pp 391–399*

Insofar as data mining and knowledge discovery techniques can find previously unknown relationships in large databases, they have potentially profound implications for the world of multilevel security. They might detect new intrusion patterns; but by searching for new rules relating low and high data, they could also open up new inference channels. The theory of rough sets is suggested as a possible framework for investigating these problems.

052225 'Storage Jamming'
J McDermott, D Goldschlag, *Database 95 pp 365–381*

The authors define storage jamming as the malicious unauthorized modification of data for the purpose of disrupting real-world operations that depend on the data correctness. Several jamming strategies are discussed. Some approaches existing in the literature to safeguard information integrity are illustrated; the authors claim that they are of little assistance against jamming attacks. The authors then present a mechanism to detect such attacks, based on the use of detection objects that appear to be part of an applications but are not used. Changes to these objects are considered symptomatic of jamming.

052226 'An Analysis of the Timed Z-channel'
IS Moskowitz, SJ Greenwald, MH Kang, *Oakland 96 pp 2–11*

The authors develop an information theoretic model that corresponds to many real life covert channels: it is a modification of Golomb's Z-channel in which the output symbol transmission times are different, and possesses an algebraic solution. They apply this technique to a CPU timing channel and an MLS token ring.

052227 'The Modulated Input Modulated Output Model'
IS Moskowitz, MH Kang, *Database 95 pp 61–75*

This paper elaborates on the pump, an approach previously proposed by the authors to interface communication in a multilevel database with a replicated architecture. The pump modulates the communication of acknowledgment messages in response to write-up operations to avoid covert channels. The authors compare their approach with an alternative based on big buffers with no acknowledgment messages, and discuss extensions to the pump for dealing with bursty communication.

052228 'A Secure Concurrency Control Protocol for Real-Time Databases'
R Mukkamala, SH Son, *Database 95 pp 215–230*

This paper presents a concurrency control protocol for multilevel real-time database systems built on the two-phase locking approach. To stop high level transactions being delayed by concurrent low level ones, a secondary copy of each object for is maintained. Each transaction can update and read the primary copy of objects at its own level, and read the secondary copies of objects at lower levels. Updates enforced on primary copies are asynchronously propagated to the secondary copies. The serializability and non-blocking properties of the protocol are discussed.

052229 'Modeling Mandatory Access Control in Role-Based Security Systems'
M Nyanchama, SL Osborn, *Database 95 pp 129–144*

The authors propose an access model combining role-based and flow controls. Access authorizations are specified for roles, which users can impersonate. A role context is defined as the part of the system accessible through a given role. Information flow is controlled on the basis of the Bell-LaPadula model. These principles are expressed by constraints on the authorizations assigned to roles and on roles assigned to users to ensure that information is not leaked to unauthorized contexts.

052230 'Self-Protecting Objects in a Secure Federated Database'
MS Olivier, *Database 95 pp 27–42*

The paper presents an access control mechanism for protecting information in distributed federated object systems. It is based on self-protecting objects: each object includes methods, called its trusted extensions, which provide access control. When an object is relocated, its trusted extension is too. There are three different categories of security code: the Trusted Common Extension enforcing the federal security policy; the Trusted Local Extensions enforcing the sites' security policies, and Trusted Extensions enforcing the objects' security policy.

052231 'Locking Protocol for Multilevel Secure Databases Providing Support for Long Transactions'
S Pal, *Database 95 pp 183–198*

This paper presents a concurrency control protocol for multilevel databases, based on the use of two versions of each object: a current version and a snapshot. Each transaction can write and read the current version of objects at its own level and read the snapshot of objects at levels below. Snapshots are periodically updated to the current versions. A longer version period allows the execution of long read-only transactions to complete, while a shorter one lets users retrieve more recent values. The proof that the protocol produces one-copy serializable schedules is given.

052232 'Towards a MAC Policy Framework'
XL Qian, TF Lunt, *Database 95 pp 165–180*

The authors discuss the different aspects to be considered in applying a mandatory policy in relational database systems. Their framework is based on three main policies: interpretation, view, and update. The interpretation policy maps a multilevel database to a multilevel theory which lets us interpret the semantics of data classification. The view policy specifies the requirements that must be satisfied with respect to information flow from lower to higher levels. The update policy regulates the update operations on the basis of constraints which must be satisfied to ensure that update execution does not introduce downward information flows. Some earlier proposals are briefly discussed with respect to how they address the different policies.

052233 'View-Based Access Control with High Assurance'
XL Qian, *Oakland 96 pp 85–93*

The view-based access control model is an attempt to move from container-based to context-based control of object oriented systems, and is especially relevant where there are overlapping contexts and shared address space. An algorithm is provided that finds the lowest set of labels for database entries given the constraints on the views. Sometimes there is no safe solution, and the problem is in any case NP-complete; but the algorithm is usually practical and can be used at compile time to transform view-based into tuple-based labelling.

052234 'A Tool for Inference Detection and Knowledge Discovery in Databases'

S Rath, D Jones, J Hale, S Shenoi, *Database 95 pp 317–333*

This paper presents a tool to identify inference channels in multilevel databases. Three types of channel are discussed: precise and imprecise inference channels due to functional dependencies, and the inference based on external knowledge. The proposed approach evaluates multilevel relations on the basis of functional dependencies between attributes and imprecise relations capturing external knowledge to discover possible inference channels. A tool implementing the proposed approach for an Oracle database is described.

052235 'Multilevel Data Model for the Trusted ONTOS Prototype'

M Schaefer, R Martel, T Kanawati, V Lyons, *Database 95 pp 111–126*

The paper presents a security model for a multilevel object database system based on a client/server architecture. The model is illustrated and properties that must be satisfied in the objects' classification are given. Issues concerning aggregate objects are also discussed.

052236 'Assured Discretionary Access Control for Trusted RDBMS'

M Schaefer, G Smith, *Database 95 pp 251–266*

The paper addresses the problem of providing discretionary access control with high levels of assurance in multilevel relational databases. Three possible discretionary access control policies are presented, which are then discussed in the context of the TCSEC requirements.

052237 'The Triad Systems: the Design of a Distributed, Real-Time, Trusted System'

E Sebes, T Benzel, M Barnett, *Apps 95 pp 63–74*

Triad is a prototype distributed operating system providing a high assurance platform for real-time distributed multilevel applications. It is based on Trusted Mach which meets B3 requirements for security functionality and assurance and adds distributed real-time functionality to it. The paper explains the design by decomposing it into kernel level and server level components, and describes a framework for applications using the system.

052238 'Run-Time Security Evaluation (RTSE) for Distributed Applications'

C Serban, B McMillin, *Oakland 96 pp 222–232*

The authors describe a system for doing security checking at runtime. The desired control properties are expressed in formal logic, and then the program traces are evaluated for compliance with this. This is suggested as a useful aid to evaluating distributed applications.

052239 'An Adaptive Policy for Improved Timeliness in Secure Database Systems'

SH Son, R David, B Thuraisingham, *Database 95 pp 199–214*

The authors discuss the problem of enforcing multilevel security policies in real-time databases. To prevent downward flows of information, multilevel concurrency protocols may delay high level transactions whenever resource locking would introduce a downward channel. However, in real-time databases, security may be sacrificed to meet deadlines, and the trade offs are discussed. The authors then propose an adaptive version of the two phase locking protocol that trades off security for timeliness, depending on the state of the system, and illustrate its performance considerations.

052240 'Sidewinder: Combining Type Enforcement and Unix'

D Thomsen, *Apps 95 pp 14–20*

Sidewinder is designed to be an Internet firewall, which adds some interesting features to BSDi Unix: two kernels, type enforcement, triggers and controlled system calls. Using an administrative kernel separate from the operational kernel limits the critical value of the root account. Enforcing types is by using a Domain Definition Table that specifies which process can access which file type. By putting triggers on specific files that a legitimate user normally does not use, malicious behaviour can be detected. A series of flags in each domain indicate the calls that can be made from it.

052241 'Secure Network Objects'

L van Doorn, M Abadi, M Burrows, E Wobber, *Oakland 96 pp 211–221*

The authors propose an architecture for secure distributed object-oriented systems. It is based on an application programming interface that supports both access control lists an capabilities. It extends Modula-3 and can support both Kerberos and Sun's secure RPC; some performance measurements of a test implementation are given.

052242 'Database Design with Secure DBMS Products'

S Wiseman, S Lewis, *Apps 95 pp 32–41*

This paper proposes a new approach to the design of multilevel databases using labels. A database system is considered to consists of a collection of tables, rows, fields and processes that act as database clients. All of these are labeled with a classification, and the main rule of mandatory access control is that no operation is allowed that causes information flow from a high label to a low label. The paper shows that labeling rule affects the way databases are designed and simple schema designs are possible with suitable field labeling. Row labeling, however, requires more complex design.

3 Security Management and Policy

052301 'Faded Lustre: Vatican cryptography, 1815–1920'
D Alvarez, *Cryptologia v XX no 2 (Apr 96) pp 97–131*

Although the Vatican led the cryptographic art from the fourteenth century to the sixteenth, it fell behind after the Napoleonic war. While other states developed code books, the church still used nomenclators, with occasional experiments with polyalphabetics. Users such as Pope Leo XII did not trust their cipher bureau; they used cover addresses and clandestine mail routes as well. By World War 1, the papacy was using a fourteen page code book, while other nations' books ran to over a thousand pages. Codes were improved in 1916, but it was only when superencipherment was introduced in 1918 that the traffic became hard for the Italians to read.

052302 'IT-Sicherheit im Spiegel der aktuellen Risikodiskussion'
G Banse, *Boppard 95 pp 128–146*

The novel aspects of system risk come from the fact that causal chains often lie beyond our everyday experience. Unintended consequences are common, and design decisions taken today may have security consequences in the distant future. Risk assessment lies uncomfortably between fact and hypothesis, and what we do know falls between the domains of practical and theoretical knowledge.

052303 'On the Development of the Russian Federal Legislation in the Field of Information Security'
IL Batchilo, *Datenschutz und Datensicherheit v 20 no 3 (Mar 96) pp 167–170*

The author describes recent draft legislation on information in Russia which tackles data protection, state security, commercial confidence, copyright and patent. It also mentions some existing laws from constitutional provisions through the recent civil code to problems with regulating the mass media.

052304 'Laptops: The new target of the cyber-criminal'
A Bequai, *Computer Audit Update (June 96) pp 22–26*

Organisations should respond to the current wave of laptop theft by labelling, tight stock control and check-out procedures, encryption of proprietary data and rules for employees — such as that laptops should always be carried on to aircraft rather than checked as baggage.

052305 'Prosecuting cyber-crimes'
A Bequai, *Computer Audit Update (Apr 96) pp 22–27*

This article describes a number of US state and federal laws that can be used to prosecute electronic crimes, and 1994 guidelines from the US Sentencing Commission under which the penetrators of properly protected systems should get tougher sentences.

052306 'The Embattled Internet'
A Bequai, *Computer Audit Update (May 96) pp 23–26*

The author talks about Internet security problems.

052307 'Securing the Commercial Internet'
A Bhimani, *Communications of the ACM v 39 no 6 (June 96) pp 29–35*

The author talks about threats to internet users and about a number of initiatives including SSL, SHTTP and SET.

052308 'Sicherheit und Risiko — philosophische Reflexionen'
D Birnbacher, *Boppard 95 pp 19–37*

Assessing security risks is a slippery business; even expert opinions depend on norms and standards that can be questioned on a number of grounds. We lack an ethic of risks that would enable us to deal with historic, cultural and socioeconomic questions such as whether a risk is undergone freely, whether it is understood, whether it is a long established feature of society, and the personal priorities of individuals.

052309 'Measuring Security: What Can We Learn From Other Fields?'
DT Bodeau, *NISSC 95 pp 414–423*

This article reviews systems engineering metrics and discusses their relevance to security engineering. One problem is that one must incorporate a threat model, whether explicit or implicit; another is that the use of metrics tends to imply a claim of impartiality. Above all, one must know one's audience, and know one's metric.

052310 'Emerging law regarding computers, communications and software'
JS Bradish, *NISSC 95 pp 525–533*

The author talks about contracts, crypto export and some other US legal issues.

'Internet Security: How Much is Enough?'
L Bruno, *Data Communications International (4/96) pp 60–72*

This article surveys Internet security problems and discusses security products such as firewalls and encryption systems; a list of suppliers is provided.

052311 'The Spook Solution — Now Open for Business'
M Buckwell, *Computers and Security v 15 no 1 (96) pp 17–26*

The author tells a number of war stories about corporate computer security failures and draws a number of conclusions.

052312 'IT-Sicherheit: Management zwischen Technik, Recht und Gesellschaft'
A Büllesbach, *Boppard 95 pp 60–70*

The view of IT security as a collective good provided by the state is not consistent with the broader political picture of deregulation, privatisation and the rollback of the state. Developments in this regard in Eastern Europe are bound to have an effect on the west, but whose precise nature we cannot yet predict.

052313 'Asset Identification and Valuation'
J Clayton, *Canada 96 pp 211–235*

This paper addresses the need for a comprehensive taxonomy of assets and briefly addresses issues surrounding asset identification and valuation.

052314 'A Note of Distributed Coordinated Attacks'
FB Cohen, *Computers and Security v 15 no 2 (96) pp 103–121*

A malicious web page was set up which caused some machines whose users viewed it to attempt to telnet to a given site, causing congestion. The victim of this attack provides some details and remarks that similar attacks could also be used to guess passwords or exploit other vulnerabilities. Possible defensive measures are discussed.

052315 'Sicherheitswissenschaft — eine Wissenschaft zur Sicherheit in der Informationstechnik'
PC Compes, *Boppard 95 pp 71–77*

The author discusses the extent to which IT security has developed into a science, and sets out to clarify German security terminology.

052316 'ISS taps threat from network intruders'
Computer Business Review v 4 no 5 (May 96) p 38

This article describes the growth of Internet Security Systems, a company that sells network auditing services and penetration testing tools.

052317 'United States pushes key escrow, security in OECD'
Computer Fraud and Security Bulletin (Mar 96) pp 7–9

The USA is pushing the OECD to adopt their idea of commercial key escrow via trusted third parties, and wants a group of experts from friendly countries' SIGINT agencies to drive the agenda in secret.

052318 'The Trust Technology Assessment Program and the Benefits to US Evaluations'

J Connoly, B Abramowitz, *Apps 95 pp 157–161*

The Trust Technology Assessment Program (TTAP) is a joint NSA-NIST effort to commercialize INFOSEC product evaluations. Initially, TTAP will evaluate against the DoD's TCSEC but the intention is transition to the Common Criteria. The paper describes TTAP's goals, implementation plan, and current status; it focuses on its benefits to US evaluations.

052319 'Personal Computers — more power, more risks'

D Davies, *Computer Law and Security Report v 12 no 2 (Mar/Apr 96) pp 110–111*

The decentralisation of computing has made many security assumptions outdated. In addition, many security policies are not followed in practice — which can invalidate insurance claims.

052320 'The New Face of the Virus Threat'

J David, *Computers and Security v 15 no 1 (96) pp 13–16*

The author lists the top ten viruses for last year and talks about a number of antivirus products.

052321 'Critical factors of key escrow encryption systems'

DE Denning, *NISSC 95 pp 384–394*

The author tabulates some possible key escrow features and their effect on a scheme's marketability to various interest groups.

052322 'Security classification for documents'

JHP Eloff, R Holbein, S Teufel, *Computers and Security v 15 no 1 (96) pp 55–71*

The authors argue that commercial organisations should set up systems for the classification of paper documents similar to that used by military and intelligence organisations.

052323 'Distinguishing Security Engineering Process Areas by Maturity Levels'

K Ferraiolo, JE Sachs, *Canada 96 pp 135–149*

This paper describes a delineated set of maturity levels for a security engineering process. These levels are classified according to a defined set of security engineering process areas.

052324 'Decline in UK card fraud as banks prepare for national chip trials'

Financial Technology International Bulletin v 13 no 7 (Mar 96) pp 4–5

This article analyses 1995 UK card fraud losses by card type, circumstances of loss and place of misuse. It also reports disagreement among EU bodies about whether prepayment cards should have to be issued by banks.

052325 'Psychologists and banks clash over merits of photographs on cards'

Financial Technology International Bulletin v 13 no 5 (Jan 96) pp 2–3

A recent study by psychologists at the University of Westminster concluded that supermarket checkout staff could not tell effectively whether photographs on cards corresponded to cardholders in front of them. This was established in a controlled trial where 44 undergraduates tested experienced cashiers by presenting cards with four different photographs on them: genuine and bogus photos that were both good and poor matches. Banks who issue photocards responded that they experienced real savings, so photos must have at least a deterrent effect.

052326 ‘RNIB urges smart card agenda for the disabled’
Financial Technology International Bulletin v 13 no 7 (Mar 96) pp 6–7

Britain’s Royal National Institute for the Blind has presented recommendations for making card-based payment systems easier for the visually disabled to use. These include a standardised interface, the ability to differentiate cards by touch, lighter keyboards with tactile feedback, larger characters on screen, speech prompts and output, and user profiles that enable the presentation details to be customised to the user’s disability.

052327 ‘Understanding and Managing Risk in Software Systems’
S Fletcher, R Jansma, J Lim, M Murphy, G Wyys, *Apps 95 pp 162–171*

This paper describes a methodology for assessing the surety (including security, safety and dependability) of a software based system and presents an automated tool to support it. The framework uses a risk identification matrix to define risks, a risk mitigation matrix to model the possible barriers, and a system risk model to explore their effectiveness and interaction. The analyst uses them to build a system risk model; then a barrier and a threat analysis for each threat is performed; finally, an analysis engine is run to evaluate any residual risks in the system. The result is a risk management strategy for the system. A feature is considering safety, security and dependability within a single context.

052328 ‘Panel: Information Warfare: Attacks on Personal Information’
B Foran, *Canada 96 pp 85–86*

The author discusses the privacy of personal information held on Canadian citizens by government bodies and the perceptions that Canadians have of information privacy. He also discusses information warfare and the threat posed by hackers information and very briefly mentions the conflict between privacy of individual information, the obligations of organisations, and protection the required and afforded.

052329 ‘Chip cards reduce fraud in France’
Fraud Watch (96) no 1 p 8

Chip cards cut card fraud in France from 0.269% of turnover in 1987 to 0.028% in 1995, according to Carte Bleu. However, there is now an increasing amount of cross-border fraud in which magnetic stripe cards — particularly from the UK — are used.

052330 ‘Counterfeit and cross border fraud on increase warning’
Fraud Watch (96) no 1 pp 6–7

This article provides figures for card fraud and forgery in nine countries, broken down by the issuing and acquiring country. Card verification values are being harvested by crooks who skim genuine cards, and it appears that most of the counterfeiting operations are linked with the UK.

052331 ‘Finger minutiae system leaps the 1:100,000 false refusal barrier’
Fraud Watch (96) no 2 pp 6–9

This article surveys some biometric products and relates a claim by a supplier that their product can meet the banks’ requirement of a 1 in 100,000 insult rate.

052332 ‘Fraud beyond the forecourt’
Fraud Watch (96) no 2 pp 8–9

Two systems — Cardcast and Card Clear — are offered to petrol station owners in the UK to cut card fraud losses. They broadcast real-time hot card updates using spare bandwidth in TV transmissions.

052333 ‘US government pilots Crypto-SmartDisk’
Fraud Watch (96) no 1 p 10

A number of US government departments are piloting the use of a security processor that is packaged inside a 3.5 inch diskette; it contains a smartcard chip, an arithmetic coprocessor, and circuitry to detect and generate the magnetic fields needed for the device to emulate a diskette drive.

052334 'The use of generic architectures in system integration'
D Gambel, J Hemenway, *NISSC 95 pp 432–446*

The authors discuss some of the trade-offs commonly encountered in secure systems integration and describe a methodology they have developed based on product profiles, composition analysis and compliance testing.

052335 'Internet: juristische probleme und kein Ende?'
RW Gerling, *Datenschutz und Datensicherheit v 20 no 4 (Apr 96) pp 218–223*

The author talks about some of the legal problems with the Internet, with particular reference to newsgroups and anonymous ftp.

052336 'IT-Sicherheit aus Sicht des Datenschutzbeauftragten'
H Gliss, *Datenschutz-Berater v 20 no 5 (May 96) pp 1–10*

This article presents the detailed results of a recent computer security survey of German businesses. The main causes of loss were fire, burglary, human error, breakdown and corruption; many respondents thought that high-tech attacks and evidential reliability problems could become serious in future, though they account for only a small proportion of incidents at present. The survey also highlighted a disparity in perception between senior management and data protection officers over responsibilities and priorities.

052337 'Sicherheitslage: Management-Defizite — Handelsblatt-Enquête zeigt Handlungsbedarf'
H Gliss, *Datenschutz-Berater v 20 no 4 (Apr 96) pp 8–9*

According to a recent survey by a German newspaper, 78% of 408 business had security standards or strategies, but 61% admitted that these were only partially effective and 16.5% that there was no control over PC applications. When asked who was responsible for finding security holes, 64% named the company's data protection officer, 14% the external auditors and 19% failed to answer.

052338 'Wovor der Bürger am meisten Angst hat: Dantenmißbrauch durch Adreßverlage'
H Gliss, *Datenschutz-Berater v 20 no 6 (June 96) pp 7–8*

A survey has shown that German citizens are more concerned about misuse of personal data, and in particular about the disclosure of their private address, than about burglary, pollution, assault or road accidents.

052339 'Telearbeit in virtuellen Unternehmen'
P Gola, *Datenschutz-Berater v 20 no 4 (Apr 96) pp 1–6*

This article looks at the data protection implications in Germany of 'virtual' companies involving many home workers and freelances. It discusses the postal workers' contract, under which sensitive information can only be shared with people who retain their employee status.

052340 'Disaster recovery under the microscope'
S Gold, *Information Security Monitor v 11 no 4 (Mar 96) pp 5–8*

The recent IRA docklands bomb showed that UK corporate disaster recovery programmes are by now generally reliable. However, the same cannot be said for all other countries; a number of problems and plans in Canada, Hong Kong, the USA and elsewhere are described.

052341 'Ask and Ye Shall Receive: A Study in Social Engineering'
T Greening, *SIGSAC Review v 14 no 2 (Apr 96) pp 9–14*

336 computer science students at the University of Sydney were sent an email

message asking them to supply their password to 'validate' the password database after a suspected breakin. 138 of them returned a valid password; 30 returned a plausible looking but invalid password; and over 200 changed their passwords without official prompting in the two weeks following the experiment. However, very few attempts were made to report the message to the university authorities.

052342 'Communications Surveillance and its Implications in an Electronic World'
D Guinier, *Canada 96 pp 269–298 (in French)*

This paper examines the Clipper chip and Skipjack algorithms and offers some enhancements. The author proposes a Smartcard based "SGP - Smart Key Escrow and Good Privacy".

052343 'A business approach to effective information technology risk analysis and management'
S Halliday, K Badenhorst, R von Solms, *Information Management and Computer Security v 4 no 1 (96) pp 19–31*

The authors propose a risk assessment system that is driven by the business's perception of what its essential processes are rather than by lists of threats or vulnerabilities. The idea is to prioritise risks.

052344 'Sicherungsinfrastrukturen und rechtliche Rahmenbedingungen'
V Hammer, *Datenschutz und Datensicherheit v 20 no 3 (Mar 96) pp 147–158*

The author discusses the legal situation for public key cryptography and the proposed public key infrastructures in Germany. He proposes three principles: that the infrastructures must be extensible to new applications; that different 'trust instances' should be interoperable and compatible; and that the effectiveness of all structures on which people are compelled to depend should be subject to legal regulation which sets out responsibilities clearly.

052345 'Can You Social Engineer Your Way Into Your Network?'
W Hancock, *Network Security (Apr 96) pp 14–15*

The author describes some techniques he has used when carrying out trial attacks on client sites. These include making passable imitations of ID badges using a colour copier, and borrowing a desk for a few hours by pretending to be from Head Office; a laptop with a promiscuous ethernet connection does the rest.

052346 'Assumptions, Perceptions and False Reassurances'
S Hinde, *Computer Audit Update (June 96) pp 2–4*

The author issued a negative audit report on the fire protection of a client's computer room. This was disputed, as the Fire Brigade had certified the premises only a few weeks previously. It turned out that the brigade were only interested in the threat to life, not to the computers; they were satisfied because the single computer operator had two exit routes.

052347 'Been there and got the same tee shirt'
S Hinde, *Computer Audit Update (Apr 96) pp 2–4*

The author talks about two recent surveys of computer security failures in the UK and about recent government guidelines.

052348 'Changing Policies Towards Encryption and Internet Security'
P Hook, *Computer Fraud and Security Bulletin (une 96) pp 12–14*

The author talks about Internet security, encryption and trusted third parties.

052349 'Security Needs Identification'
JP Hopkinson, *Canada 96 pp 123–134*

This paper describes four types of organisation culture towards security: threat adverse, vulnerability adverse, impact adverse and risk adverse. The author then classifies the types of safeguards that tend to be employed by each type of culture. The author argues that organisations need to implement all (identified) types of safeguard, instead of relying on those safeguards that most easily fit with their cultural bias.

052350 'Information Warfare: A Front Line Perspective'
MD Jibbs, *NISSC 95 pp 543–548*

This article provides a US Air Force perspective on the tools needed for defensive information warfare. Most of them concern security management; they range from training and auditing through a 24 hour response centre.

052351 'A New Perspective on Combining Assurance Evidence'
J Kahn, *Apps 95 pp 172–181*

This paper considers the integration of trusted components with commercial off-the-shelf components. To convince evaluators that the resulting system is sound, the system integrator must produce evidence. Evidence can also be needed to substantiate performance, functional correctness, resilience, and many other system characteristics. The paper discusses creating and using such evidence and proposes a framework for integrating evidence from component systems.

052352 'Contingency planning: what to do when bad things happen to good systems'
JJ Kahn, MD Abrams, *NISSC 95 pp 474–479*

The authors discuss contingency planning from the viewpoint of recovering from failures caused by the inevitable bugs in security systems. The spread of systems for which manual recovery is no longer an option means that more development effort should be aimed at this problem.

052353 'Der IT-Sicherheitsprozess: Fiktion und Realität'
H Kersten, *Boppard 95 pp 53–59*

Three things are needed for secure systems — building in protection at the R&D stage, third party evaluation of the resulting products, and awareness training of users.

052354 'Konzeptionelle Strategien aus sicherheitstechnischer Sicht'
D Kruse, *Boppard 95 pp 81–91*

The next century's complex applications will only be secured by a complex combination of technical and legal measures; the former are already to hand, but the combination must take into account the social context of each application.

052355 'Information Security Design Principles for Adaptive Organisations'
S Lichtenstein, *Computer Audit Update (June 96) pp 7–15*

The author discusses the effect on information security of moving to more flexible and decentralised organisational structures. She argues for simple controls that default to human involvement, while still separating those who perform a control function from those regulated by it.

052356 'Commercial security on the Internet'
C Liddy, *Information Management and Computer Security v 4 no 1 (96) pp 47–49*

The author discusses the factors likely to affect the rate of uptake and acceptance of public key technology in various sectors of the economy.

052357 'Contingency Planning — Data Processing'
AL Lyons, *Computer Fraud and Security Bulletin (May 96) pp 12–16*

The author presents a series of checklists for writers of contingency plans.

052358 'Moves to protect Proprietary Data'
W Madsen, *Computer Fraud and Security Bulletin (May 96) pp 10–11*

The US Department of Justice proposes to introduce a bill making electronic espionage a specific offence that would have extraterritorial application and allow asset seizure.

052359 'The Sherlock Holmes Hotline'
M McCormack, *Computer Fraud and Security Bulletin (June 96) p 19*

Microsoft has launched a hotline for users to report unlicensed copies of software they have purchased; in return for evidence they get a free legal replacement.

052360 'What Every Information Systems Security Professional Should Know About Electronic Records Management'
JS McEwen, *NISSC 95 pp 480–486*

It is pointless to protect the wrong records, or to be unable to find the right ones; so security people should have a working knowledge of electronic records management techniques.

052361 'Adventures in Cryptoland'
G Mellen, *Cryptologia v XX no 2 (Apr 96) pp 155-164*

The author describes working at Bell Labs in the 1950's on a secure teleprinter and on documenting a radar with a covert communication feature.

052362 'A Probabilistic Flaw in PGP Design?'
T Moreau, *Computers and Security v 15 no 1 (96) pp 39–43*

The author suggests that the file randseed.bin used in PGP key generation could be a weakness if a backup became available to an opponent.

052363 'The Quite Jemmy'
N Morris-Cotterill, *Computer Fraud and Security Bulletin (Mar 96) pp 11–14*

The world wide web makes is easy for villains to steal the identity of others, which makes it harder for firms to check out employees and contract staff.

052364 'INFOSEC Systems Evaluation and Risk Assessment (IERA) National Master Supply Arrangement (NMSA)'
D Morrison, *Canada 96 pp 107–122*

This paper describes the criteria set by the Canadian government for acceptable levels of IT Security expertise and the process of evaluating and awarding IERA NMSA status to private sector firms.

052365 'Automating the Assessment of Risk in IT Systems'
C Morton, M Froh, *Canada 96 pp 181–199*

The authors argue that risk assessment must be considered throughout the life cycle of an IT system, and propose a risk assessment method based on threat scenarios that will form the basis of a future risk assessment automated tool.

052366 'Protection of computer programs in Ireland'
K Murray, *Computer Law and Security Report v 12 no 3 (May/June 96) pp 57–59*

News Datacom tried to sue an Irish manufacturer of pirate satellite decoding systems for breach of copyright, claiming that their encryption algorithm was so complex that the code in their smartcard must have been copied. They failed; the defendant successfully claimed to have reverse engineered the algorithm and produced a different but compatible implementation. In a similar US case, SEGA failed to prevent a clone maker from selling game cartridges compatible with their system.

052367 'Bad News for Bulletin Boards'
J Osen, *Network Security (Apr 96) pp 11–13*

This article discusses the Stratton Oakmont versus Prodigy case in which a bulletin board operator was held liable for defamation after an unidentified user posted to a moderated newsgroup it operated; and a case in which the Church of Scientology sued and ISP for breach of copyright after a former adherent posted some of their 'scripture'.

052368 'The Amateur Action Case'
J Osen, *Computer Fraud and Security Bulletin (Apr 96) pp 10–18*

This article describes in detail the Thomas case, in which the operator of an 'adult' bulletin board in California was extradited to Tennessee and tried according to the decency standards prevalent there.

052369 'The Freedom of Information Act and the 2600 Club'
J Osen, *Network Security (June 96) pp 17–19*

The author discusses the CPSR's unsuccessful attempt to obtain documents under the Freedom of Information Act about a US Secret Service raid on a hackers' meeting in a shopping mall.

052370 'The State of Cryptography in Global Communications'
T Parker, *Network Security (May 96) pp 13–17*

This article talks about PGP, PEM, SET, IPv6 and SESAME.

052371 'Email Security — An Oxymoron?'
AP Peterson, *Network Security (June 96) pp 10–13*

The author points out that many features of email, such as remailers, user customisable return addresses, mailing lists and attachments, create security problems.

052372 'Computer forensics: an approach to evidence in cyberspace'
MM Pollitt, *NISSC 95 pp 487–491*

The author discusses techniques for seizing computer evidence and securing its admissibility in US courts.

052373 'Be prepared'
C Pounder, *Computer Audit Update (May 96) pp 29–30*

The author discusses the differing criteria for the jurisdiction of data protection laws in the UK, France and the Netherlands.

052374 'Regina v Brown: A Snooper's Charter?'
M Rebeiro, *Computer Audit Update (May 96) pp 33–35*

A Kent policeman who accessed the Police National Computer to help a friend's debt collection agency was convicted of an offence under the Data Protection Act, but acquitted on appeal on the grounds that he had not personally used the data. This might open up a loophole for abuse.

052375 'Information Technology Security Requirements Model'
A Robinson, *Canada 96 pp 311–320*

This paper presents layered model of security that simultaneously addresses network and computer security: the layout of this model is based on the OSI network model.

052376 'Security and Software Reuse'
GW Rogers, JC Crabb, *NISSC 95 pp 424–431'*

The authors discuss the evaluation effort that the US Army could save by having government-developed standard software, and argue that software reuse implies central evaluation.

052377 'Konzeptionelle Strategien aus juristischer Sicht'
A Roßnagel, *Boppard 95 pp 99–113*

This article discusses what the state's role in IT security should be, and traces the development of German legislation on topics such as data protection and wiretapping. He then asks what regulatory strategies could be adopted for the 21st century. One would be to go for deregulation, in which case the state should guard against abuse of market power; another would be self-regulation (e.g. by professional groups such as doctors and lawyers), in which case the state should stop powerful groups acting at the expense of 'outsiders'; and the third is centralised regulation, as with traffic safety.

052378 'Multimediadienste und Datenschutz'
A Roßnagel, J Bizer, *Datenschutz und Datensicherheit v 20 no 4 (Apr 96) pp 209–217*
the authors discuss a number of applications from the point of view of German data protection law. These include video-on-demand, distance learning, teleshopping and telework.

052379 'Information security in business environments'
E Sanderson, KA Forcht, *Information Management and Computer Security v 4 no 1 (96) pp 32–37*
The authors talk about Internet security, encryption, viruses and so on.

052380 'Authentication, Access Control and Audit'
R Sandhu, P Samarati, *Computing Surveys v 28 no 1 (Mar 96) pp 241–243*
The authors provide a top level overview of authentication, access control and audit technologies.

052381 'Datenschutrechtliche Probleme von Online-Dienste'
P Schaar, *Datenschutz und Datensicherheit v 20 no 3 (Mar 96) pp 134–138*
The growth of online services presents serious jurisdictional problems; a German might use a service based in the USA, which has completely different data protection laws. Clarification of the legal situation would be desirable.

052382 'Testing times for the LPCB'
Security Surveyor v 27 no 2 (July 96) p 11
This article reports a public row over the costs of evaluations carried out by the UK insurance industry's Loss Prevention Certification Board, which range from £3000 for a simple burglar alarm to £6000 for a passive infrared unit. The LPCB maintains that its evaluations are tightly operated and costed.

052383 'Software piracy: prevention, detection and liability avoidance'
MJ Shaw, *NISSC 95 pp 492–513*
The author describes US laws relating to software piracy and makes recommendations for organisations that wish to avoid liability.

052384 'Achieving Interoperable Security Services in Open Systems Products'
P Smith, *Computers and Security v 15 no 1 (96) pp 27–37*
This paper describes a UK Ministry of Defence programme to demonstrate security in open systems in the hope of getting commercial software firms to provide a series of interfaces on which crypto and other security features can be hung.

052385 'Imaged Documents Code'
P Sommer, *Computer Fraud and Security Bulletin (Apr 96) p 5*
A new UK Civil Evidence Act will remove the requirement that a computer be certified to be working before its output can be admissible in civil cases. The emphasis will shift instead to the weight of evidence, and this will facilitate the introduction of document image processing systems. The British Standards Institute has produced a code of practice for this.

052386 'IT security in Dutch practice'
MEM Spruit, M Looijen, *Computers and Security v 15 no 2 (96) pp 157–170*
The authors report a survey of IT security incidents at 391 organisations in the Netherlands. In centralised IT systems, unintentional user errors were the main cause

of failure, while in distributed sites the two main causes were the use of equipment for private purposes and hardware malfunction.

052387 'Telework Security'

A Sturgeon, *Canada 96 pp 151–179*

This paper discusses at a very high level several security issues surrounding home offices and telecommuting.

052388 'Making the Right Risk Decision'

M Tipman, CK Hastings, *Canada 96 pp 201–209*

This paper discusses some future challenges in the area of risk assessment and risk management.

052389 'Eigenverantwortung und Marktwitschaft als Steuerungsimpulse det IT-Sicherheit'

R Voßbein, *Boppard 95 pp 92–98*

The extent to which security services can be provided by market forces alone will depend on whether competition works in a positive or negative way.

052390 'A retrospective of the criteria movement'

WH Ware, *NISSC 95 pp 582–588*

The author tells the story of the Orange Book, its successors, its overseas imitators, and the common criteria that are pulling all these together.

052391 'Social enginering: the only real test of information systems security plans'

IS Winkler, *NISSC 95 pp 464–469*

Social engineering attacks weaknesses in 'commonsense'; for example, security professional often think that users understand the importance of choosing good passwords. Such wrong assumptions are so pervasive that the only way to test one's own organisational security is by attacking it.

052392 'A route to security'

M Whybrow, *Banking Technology v 13 no 4 (May 96) p 20*

X/Open is about to launch a Unix security branding programme based on XBSS that is about comparable to C2 but oriented to commercial concerns.

052393 'Constructing difficult-to-guess passwords'

CC Wood, *Information Management and Computer Security v 4 no 1 (96) pp 43–44*

The author lists a number of tricks for constructing hard-to-guess passwords.

052394 'A community response to CMM-based security engineering process improvement'

MW Zior, *NISSC 95 pp 404–413*

The NSA surveyed the opinions of 22 security engineering organisations on the use of SEI's capability maturity model. Most of them already used it in other contexts. and seventeen thought it could be very useful in security.

4 Formal Methods and Protocols

052401 'A Secure Voting Protocol Using Threshold Schemes'
A Baraani-Dastjerdi, J Pieprzyk, R Safavi-Naini, *Apps 95 pp 143–148*

This paper presents an electronic voting scheme for large-scale elections. It uses threshold encryption to preserve the privacy and accuracy of votes against dishonest participants, and is based on a scheme of Fujioka, Okamoto, and Ohta (**021611**). The original scheme required all the registered voters to cast their votes; the failure of a single voter would disrupt the whole election. The modified scheme overcomes this drawback; it provides resilience while retaining all the other properties of the original scheme.

052402 'Secure Remote Control and Administration of Uninterruptable Power Supply Systems with SNMP'
N Berg, G Enste, D Kraus, *Apps 95 pp 21–30*

This paper describes a modification of SNMP used to control an uninterruptable power supply system. The modification uses monotonous counters instead of synchronised clocks and employs DES in CBC mode to produce a message authentication code for providing message integrity. The paper also describes requirements of secure key distribution for the system and proposes a a system for this.

052403 'Decentralized Trust Management'
M Blaze, J Feigenbaum, J Lacy, *Oakland 96 pp 164–173*

The authors present a system for mapping public key certificates to access decisions. Policy is expressed in a series of assertions about the rights attaching to certain public key certificates, and the system processes queries as to whether a given collection of public keys is permitted to authorise a given action according to local policy. The idea is to make the policy mechanism independent of the particular certificate mechanism, such as X.509 or PGP, that might be in use. A test implementation is reported.

052404 'High-Bandwidth Encryption with Low-Bandwidth Smartcards'
M Blaze, *FSE 96 pp 33–40*

The author presents RKEP (Remotely Keyed Encryption Protocol) which enables a low-bandwidth processor such as a smartcard to manage keys used for bulk encryption in software. To encrypt a file, the plaintext is first hashed into the first block. This is then encrypted by the card to generate the first block of ciphertext, and encrypted again to get a message key that is passed to the host software to bulk encrypt the rest of the file. To decrypt, the card generates the message key, the bulk decryption is performed, and the hashing repeated to finally extract the first plaintext block.

052405 'Modelling Firewall Security Policies'
RJ Bottomly, RK Britton, *Canada 96 pp 299–310*

Firewalls are not readily modelled using Orange Book definitions of subjects. The authors redefine these terms given the characteristics of firewalls and define a set of access rules to govern the behaviour of these firewall subjects and objects.

052406 'Internet Holes — Part 7: The Human Side'
F Cohen, *Network Security (Mar 96) pp 7–10*

The author recounts one incident in which two Internet security probing systems attacked each other, and another indicating that the best way to route attacks is through small ISPs who, unlike universities and defence establishments, do not have sufficient staff to follow up incidents. The lesson learned is that sites should combine zero tolerance of attack with polite followup.

052407 'Internet Holes — Part 8: Spam'
F Cohen, *Network Security (Apr 96) pp 8–10*

The author argues that spamming is essentially an authentication problem, since it is the ability to masquerade as other email users that enables bad people to subscribe their targets to thousands of mailing lists. In the absence of decent authentication, one can fall back on protocols to filter the hosts from which email is accepted.

052408 'Internet Holes — Part 9: IP Address Forgery and How to Eliminate it'
F Cohen, *Network Security (May 96) pp 5–12*

The author describes IP and how IP address forgery can be used in a number of attacks. He suggests packet filtering as the first choice of defence, and provides source code for a sample implementation.

052409 'Internet Holes — Part 10: UDP Viruses'
F Cohen, *Network Security (June 96) pp 7–10*

The author describes how to construct UDP packets that reproduce. For example, with a source address of 127.0.0.1 and source and destination ports 7, the receiving machine will be sent into an infinite loop. Similar effects can be achieved using a number of other services; they are described as 'protocol level viruses'.

052410 'Non-Repudiation with Mandatory Proof of Receipt'
T Coffey, P Saidha, *Computer Communications Review v 26 no 1 (Jan 96) pp 6–17*

The authors propose a protocol for a trusted third party which would accumulate proofs of origin and receipt of a message. Once it has both, it will send the former to the recipient and the latter to the sender. In this way, any party that fails to complete its part of the protocol can gain nothing from the message.

052411 'Adopting the Message Security Protocol for Use in Canada'
J Detombe, G Gill, J Weigelt, Y Theriault, *Canada 96 pp 241–255*

This paper describes and rationalizes the modifications to the Secure Data Network System (SDNS) Message Security Protocol for use by the Department of National Defence in Canada. Changes made to permit this U.S. developed standard to be used in Canada include changing the encryption algorithms, from KEA and Skipjack to DES and RSA (for compatibility with the Nortel Entrust crypto-kernel). Changes were also required to the security label header information, to disallow changes to the label when messages are forwarded.

052412 'Why the Kuperee authentication system fails'
Y Ding, P Horster, *Operating Systems Review v 30 n0 2 (Apr 96) pp 42–51*

An authentication system proposed in **041213**, that provided the same general functions as Kerberos but using a Diffie-Hellman variant, is shown to be vulnerable to a number of impersonation attacks. Some possible fixes are described.

052413 'Comparing Information Without Leaking It'
R Fagin, M Naor, P Winkler, *Communications of the ACM v 39 no 5 (May 96) pp 77–85*

This article surveys a number of protocols that enable two players to find out whether they possess the same piece of secret information, without either of them leaking information if not. Practical protocols can be constructed using the Unix 'passwd' command, airline reservation systems, and decks of cards. Some of the protocols were already in the literature; some are new.

052414 'Defining Noninterference in the Temporal Logic of Actions'
T Fine, *Oakland 96 pp 12–21*

The author mixes CSP and state machine approaches to modelling noninterference, which he defines between processes rather than levels. The result is that in his logic, it is not a property but a condition (a property of properties) — that for all behaviours, there exists another behaviour with no high-level transitions but the same low-level output. This is argued to conform more closely to the informal definition of noninterference. Nonetheless, the problems with nondeterminism remain.

052415 'The Design and Implementation of a Secure Auction Service'
MK Franklin, MK Reiter, *IEEE Transactions on Software Engineering v 22 no 5 (May 96) pp 302–312*

In this journal version of **043412**, the authors report building a secure auction application using their Rampart protocol suite (which uses threshold signature and Byzantine agreement techniques to create a virtual secure processor out of a set of less trusted machines, up to one third of which may be taken over by an opponent at any time without loss of security). This auction service lets users submit sealed bids during an auction period; once it is over, it opens the bids, determines the winner, banks her electronic cash and sends her a certificate with which she can collect her goods.

052416 'What do we mean by entity authentication?'
D Gollmann, *Oakland 96 pp 46–54*

The author argues that many of the errors in authentication protocols come from using anthropocentric language, by describing the participants as 'Alice' and 'Bob' and using words such as 'talks to'. This is not a good model of wide area computer communications, in which messages may easily pass through a dozen machines en route. Five of the possible goals of an authentication protocol are given, and attacks which frustrate only a subset of these goals are discussed. The conclusion is that authentication goals should be expressed at a level of abstraction that is fit for the purpose in hand.

052417 'Immediacy in Distributed Trusted Systems'
G Grossman, *Apps 95 pp 75–79*

Every trusted system maintains a database of protection-critical information, such as a list of userids, ACLs and passwords. The latency between the time at which an administrator initiates a modification to this information and the time at which the modification takes place is of security concern. In TCSEC the concern is mainly considered in the context of systems in which TCB consists of a single body of co-located hardware and software. This paper explores complications that arise in the context of distributed systems and proposes a new definition of "immediate" for such systems.

052418 'Improving Network Security Through Port Switching'
W Hancock, *Network Security (Apr 96) pp 7–8*

The author discusses how switching bridges can be used to reduce network vulnerabilities, and discusses the possible costs.

052419 'Single sign-on: Holy Grail or graveyard of security?'
P Hunter, *Information Security Monitor v 11 no 7 (June 96) pp 5–7*

This article discusses the pros and cons of single sign-on systems and mentions a number of fielded products. It also discusses XSSO, the standard being promoted by the Open Group, which will be independent of the underlying authentication technology.

052420 'Accountability in Electronic Commerce Protocols'
R Kailar, *IEEE Transactions on Software Engineering v 22 no 5 (May 96) pp 313–328*

In this journal version of **043419**, the author presents a protocol verification logic that takes no account of freshness; its concern is accountability, and in particular whether a party ever (whether directly or through a delegation chain) signed or otherwise authenticated a given message. Another way of looking at this is the question of who can prove what on the completion of a protocol run. Despite its limited assumptions, this logic turns out to have significant analytic power, and its usefulness is demonstrated by exhibiting attacks on a number of electronic commerce protocols.

052421 'Replay tolerance of authentication protocols'
KY Lam, *Computer Communications v 18 no 12 (Dec 95) pp 988–993*
This paper studies the problem of message replay in distributed authentication, and presents a practical implementation of the message logging replay-tolerance approach.

052422 'A simple scheme to make passwords based on one-way functions harder to crack'
U Manber, *Computers and Security v 15 no 2 (96) pp 171–176*
The author proposes adding a second salt to the Unix password scheme of perhaps eight bits that would be randomly generated when the password was first encrypted, and then discarded. This would make password checking about a hundred times harder but would have a similar effect on password cracking.

052423 'On Two Proposals for On-line Bankcard Payments using Open Networks: Problems and Solutions'
WB Mao, *Oakland 96 pp 201–210*
The author criticises the STT and SEPP protocols for electronic commerce and suggests some possible modifications. There are places where non-repudiation services might beneficially be employed, and others where public key encryption could be replaced by DES (for example, between the merchant and the gateway that acquires his transactions).

052424 'Addressing Threats in World Wide Web Technology'
K Meyer, S Schaeffer, D Baker, *Apps 95 pp 123–132*
The paper reviews the threats to web-based systems and explores the possible protections, including authentication, access control, object reuse, auditing and encryption. The particular technologies discussed are SHTTP, SSL and DCE; their applicability to different services and different threats is discussed.

052425 'Internet Attack Mechanisms'
AP Peterson, *Network Security (May 96) pp 17–19*
The author describes in some detail how to go about attacking a target company network. He suggests finding target hosts by NIC searches, mapping their network using PING, using a socket opener to identify web, mail and news hosts, finding valid usernames using Altavista or other web search engines, and then trying passwords.

052426 'A Communication Agreement Framework for Access/Action Control'
M Röscheisen, T Winograd, *Oakland 96 pp 154–163*
The authors introduce a new model of security for networked environments with multiple authorities and 'trusted proxies'. It is based on communication pacts or 'commpacts' which provide a language in which expectations can be coordinated; for example, a household could use them (together with Caller ID) to enforce an access policy of 'no telephone calls during the evening other than from friends'. It turns out that they are also powerful enough to express conventional access controls. It is argued that the commpact model is transparent to the user and fits easily into existing institutional structures.

052427 'Security properties and CSP'
S Schneider, *Oakland 96 pp 174–187*
This article applies CSP to the analysis of cryptographic protocols. Definitions of confidentiality and authentication are given and a model of the enemy is sketched.

052428 'Internet Sniffer Attacks'
EE Schultz, TA Longstaff, *NISSC 95 pp 534–542*

A number of recent promiscuous monitoring attacks are reported. Attackers are starting to target network control information rather than just IDs and passwords.

052429 'An Authentication and Key Distribution System for Open Network Systems'
SP Shieh, WH Yang, *Operating Systems Review v 30 n0 2 (Apr 96) pp 32–41*

The authors describe an authentication system that they have fielded on the campus of the National Chiao Tung University, Taiwan, as a competitor to Kerberos. The underlying protocol is similar to Otway-Rees in consisting of nested remote procedure calls (client to server to authentication server); the innovation is that the server does not retain the session key once set up, but rather passes it to the client in a ticket that is timestamped and encrypted with the server's own long term key. In this way, key storage is pushed out to the clients.

052430 'Limitations on Design Principles for Public Key Protocols'
P Syverson, *Oakland 96 pp 62–72*

The author discusses the robustness principles proposed in **032401** and **044403** for public key protocols, and in particular the principle that messages should be signed first and encrypted afterwards. He points out that in protocols where public key encryption is used to define the addressee implicitly, the addressee can decrypt the message and then re-encrypt it to someone else.

052431 'Formal language for security services based on modelling analysis'
D Trcek, J Blazic, *Computer Communications v 18 no 12 (dec 95) pp 921–928*
This paper presents a language for modelling the security services base, defined according to the OSI security framework. Elements of this base are modelled with corresponding channels; for each channel, a set of productions is introduced which forms the grammar of a language.

052432 'Encryption Alternatives for Network Security'
MA Wright, *Computer Fraud and Security Bulletin (Mar 96) pp 15–17*

The author discusses the relative merits of encryption at different levels in the protocol stack.

052433 'Remote login authentication scheme based on a geometric approach'
TC Wu, *Computer Communications v 18 no 12 (Dec 95) pp 959–963*

This paper presents a login authentication scheme based on the use of smart cards and the properties of Euclidean geometry. Impersonation and replay attacks on it are discussed.

052434 'Cryptovirology: Extortion-Based Security threats and Countermeasures'
A Young, M Yung, *Oakland 96 pp 129–140*

The authors describe how cryptographic techniques can be used offensively by virus writers. For example, a virus can encrypt data on a target machine so that only the virus writer can decrypt it; this might be used for extortion. Secret sharing techniques can be used to distribute the private key around the network. A test implementation using RSA and triple-TEA is reported.

052435 'A Fair Non-repudiation Protocol'
JY Zhou, D Gollmann, *Oakland 96 pp 55–61*

The authors present a protocol that provides non-repudiation of both origin and receipt using a trusted third party. It is fair in the sense that it does not give either the sender or receiver an advantage at any point in the protocol run.

5 Secret Key Algorithms

052501 'Tiger: A Fast New Hash Function'
R Anderson, E Biham, *FSE 96 pp 89–97*

The authors propose a fast new hash function optimised for 64 bit processors such as the DEC Alpha series, but that still runs reasonably fast on 32 bit machines. It is based on three rounds of a block cipher that operates on 192 bit blocks with a 512 bit key; each round consists of eight passes. Pseudorandom 8-to-64 bit S-boxes are used, their values being exclusive or'ed together. Source code for the compression function is supplied.

052502 'Two Practical and Provably Secure Block Ciphers: BEAR and LION'
R Anderson, E Biham, *FSE 96 pp 113–120*

Two block ciphers are presented, based on the Luby-Rackoff construction but with one large and one small 'half' block. The first uses a keyed hash function then a stream cipher and then another keyed hash function, while the second uses a stream cipher, a hash function and finally another stream cipher. The constructions are provably secure, in the sense that a key recovery oracle would enable one to find both preimages and collisions for the hash function, and the seed of the stream cipher. This construction not only completes the set of reductions between block ciphers, stream ciphers and hash functions; it is also practical where a block cipher of variable length is required.

052503 'Formulas of general solutions of Boolean equations'
D Banković, *Discrete Mathematics v 152 (20/5/96) pp 25–32*

The author develops a decomposition technique for finding parametrised solutions of general Boolean equations.

052504 'Cellular automata based scheme for solution of Boolean equations'
S Bhattacharjee, S Sinha, C Chattopadhyay, P Chaudhuri, *IEE Proceedings on Computers and Digital techniques v 143 no 3 (May 96) pp 174–180*

This article presents a technique for solving Boolean equations using cellular automata; it turns out to be faster than traditional methods when xors make up over two thirds of the operators.

052505 'On a Conjecture of Helleseth Regarding Pairs of Binary m-Sequences'
AR Calderbank, B McGuire, B Poonen, M Rubinstein, *IEEE Transactions on Information Theory v 42 no 3 (May 96) pp 988–990*

The authors prove a conjecture of Helleseth, namely that there are no pairs of binary m-sequences with a 3-valued crosscorrelation function where m is a power of 2.

052506 'A Comparison of Fast Correlation Attacks'
A Clark, JD Golić, E Dawson, *FSE 96 pp 145–157*

The authors compare the performance of fast correlation attacks based on iterative probabilistic decoding with the newer techniques based on free energy minimisation. They show that by further optimising the traditional algorithms –e.g., by using fast resetting — their performance can be brought up to the level of the free energy algorithm and in some cases beyond.

052507 'A Combined Approach to the Construction of Hadamard Matrices'
R Craigen, H Kharagani, *Australasian Journal of Combinatorics v 13 (Mar 96) pp 89–107*

The second author's previous techniques is generalised to construct Hadamard matrices of new orders. For example, if $2^{t+1} \mid m^2n^2/4$, then there is one of order $4m^2n^2(13^t m^2n^2/4 + m^2n^2 + 1)$.

052508 'Bounds on the number of functions satisfying the Strict Avalanche Criterion'

TW Cusick, *Information Processing Letters v 57 no 5 (11/3/96) pp 261–293*

The author provides asymptotic formulae for the number of Boolean functions satisfying the strict avalanche criterion of orders one and two, and gives a construction for $2^{2^{n-2}}$ balanced Boolean functions of n variables that satisfy the first order criterion. He also states two conjectures that if proved would enable the existing bounds to be tightened.

052509 'Quasigroups, Isotopisms and Authentication Schemes'

E Dawson, D Donovan, A Offer, *Australasian Journal of Combinatorics v 13 (Mar 96) pp 75–88*

The authors show that the Denés-Keedwell authentication scheme becomes weak with long enough messages; enough of the key can be recovered for a message to be forged. They present work factors for the attack, and establish conditions under which the scheme remains sound.

052510 'Automated cryptanalysis of xor plaintext strings'

E Dawson, L Nielsen, *Cryptologia v XX no 2 (Apr 96) pp 165–181*

When an analyst obtains a depth of two messages encrypted with the same stream cipher, he can combine them to get the xor of two plaintext strings. The authors have written software to extract the plantext from such combinations; the describe the routines used; the get over 60% of letters by naive analysis and over three quarters once they use spaces. analysis in a number of contexts.

052511 'Cryptanalysis of MD4'

H Dobbertin, *FSE 96 pp 53–69*

The author shows how to find collisions for MD4 at a cost of about 2^{20} computations of its compress function. The basic idea is that a small difference in inputs can be controlled in such a way that the resulting differences in output cancel out. An example is given in which the message "At the price of $176,495 Alf Blowfish sells his house..." with a prefix including twenty random looking bytes, hashes to the same value as the same message with the sum changed to $276,495.

052512 'RIPEMD-160: A Strengthened Version of RIPEMD'

H Dobbertin, A Bosselaers, B Preneel, *FSE 96 pp 71–82*

Following attacks by Dobbertin on MD4 and on two rounds of REPIMD, an improved hash algorithm called RIPEMD-160 is presented. The number of rounds is increased from three to five; the two lines are made more different; and the hash output is increased to 160 bits. Optional extensions to 256 and 512 bit hashes are given, as are performance figures for the 160-bit version. It is slightly slower than SHA1.

052513 'Pseudorandom vector generation by the compound inversive method'

F Emmerich, *Mathematics of Computation v 65 no 214 (4/96) pp 749–760*

This articles analyses the discrepancy of a k-dimensional inversive congruential generator, and establishes the discrepancy of successive s-tuples from the output sequence. It turns out that the statistical properties are attractive up to $k = 4$.

052514 'On pattern occurrences in a random text'

I Fudos, E Pitoura, W Szpankowski, *Information Processing Letters v 57 no 6 (25/3/96) pp 307–312*

The authors derive the generating function for the probability that a certain pattern will occur a given number of times in a text whose symbols occur independently but with different probabilities.

052515 'A Note on the Hash Function of Tillich and Zëmor'
W Geiselmann, *FSE 96 pp 51–52*

This is a shortened version of **051511**.

052516 'On the Security of Nonlinear Filter Generators'
JD Golić, *FSE 96 pp 173–188*

The author investigates attacks on nonlinear filter generators based on the augmented filter function as introduced in **044502**. He points out that such attacks can be made difficult by spacing the filter inputs so that they constitute a full positive difference set. He proposes a related attack in which one guesses a possibly degenerate subset of the shift register states and computes further bits from the keystream. He argues that the complexity of this attack is exponential in the number of filter function inputs rather than the number of stages of the shift register.

052517 'Correlation Attacks on Clock-Controlled Shift Registers in Keystream Generators'
JD Golić, SV Petrović, *IEEE Transactions on Computers v 45 no 4 (Apr 96) pp 482–486*

The authors show how to use many-to-one edit distances in attacking clock controlled shift registers, and how these attacks can be implemented using recursive algorithms. Where the combining function of a number of outputs from a clock controlled cascade in m-th order correlation immune, the Levenshtein distance measure has to be generalised into a many-to-one function. This may give a divide-and-conquer attack on the underlying shift register state, in which only states that are near the minimum edit distance are considered.

052518 'ISAAC'
RJ Jenkins, *FSE 96 pp 41–49*

This article suggests a series of pseudorandom generators similar to RC4 but designed for high speed in software on 32-bit machines. They use different combinations of indirection, shifting, addition and accumulation and are presented in C source code form.

052519 'The serial test for a nonlinear pseudorandom number generator'
T Kato, LM Wu, N Yanagihara, *Mathematics of Computation v 65 no 214 (4/96) pp 761–769*

The generator $y_{n+1} = ay_n^{-1} + b + cy_n \pmod{2^w}$ has maximal length 2^{w-1} if and only if $a + c \equiv 1 \pmod 4$, $b \equiv 2 \pmod 4$ and $y_0 \neq 2$; and in this case there is a bound on the discrepancy of the sequence.

052520 'Large Families of Sequences with Near-Optimal Correlations and Large Linear Span'
A Klapper, *IEEE Transactions on Information Theory v 42 no 4 (July 96) pp 1241–1247*

The author introduces quadratic form ('QF') sequences — a family of $2^n + 1$ sequences of period $2^n - 1$. Some of them have maximum correlations slightly greater that $2^{n/2} - 1$ and linear spans that are exponentially larger than Gold, Kasami or GMW sequences. They are generated by applying a suitable quadratic form to the i-th power of a primitive root, raising the result to a suitable power, and taking the trace.

052521 'Truncated Differentials of SAFER'
LR Knudsen, TA Berson, *FSE 96 pp 15–26*

A differential attack on five-round SAFER is described that requires only about 2^{45} chosen plaintexts. The key idea is the truncated differential, which predicts only part of an n-bit value. An attack on five-round 32-bit block SAFER was carried out with ten structures of 2^{16} texts to confirm the theory; 17 right pairs were obtained.

The attack does not appear to work on six-round SAFER, but it does go across to five round SAFER K-128 where it can find 64 keybits.

052522 'Attacks on the HKM/HFX Cryptosystem'
XJ Lai, RA Rueppel, *FSE 96 pp 1–14*

The authors present a number of attacks on a cryptosystem proposed to provide confidentiality and authenticity for fax messages.

052523 'Faster Luby-Rackoff Ciphers'
S Lucks, *FSE 96 pp 189–203*

The author discusses a number of ways in which hash functions can be used in variants of the Luby-Rackoff construction to construct block ciphers with moderately large blocks that are secure against adaptively chosen plaintext attacks.

052524 'New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis'
M Matsui, *FSE 96 pp 205–218*

A 64 bit block cipher can be made more secure against both linear and differential cryptanalysis if its S-boxes are of different sizes. There are also structures other than the classical Feistel one that give advantages. Combining these ideas with recursive round functions, the author proposes two new block ciphers that are provably secure against differential and linear cryptanalysis, and are also fast in practice.

052525 'Pseudo noise sequences for engineers'
RN Mutagi, *Electronics and Communication Engineering Journal v 8 no 2 (apr 96) pp 79–87*

The author surveys ways of generating shift register sequences, and in particular ways of generating them using a number of low-speed devices in parallel, each of which generates a decimated sequence at a lower rate. He also describes hardware configurations for synchronising on an acquired signal.

052526 'Fast Accumulated Hashing'
K Nyberg, *FSE 96 pp 83–87*

The author presents a commutative hash function based on taking the coordinate-wise product modulo 2 of one-way hashes of the input, and calculates the probability of a successful forgery.

052527 'Correlation Attacks on Stream Ciphers: Computing Low-Weight Parity Checks Based on Error-Correcting Codes'
WT Penzhorn, *FSE 96 pp 159–172*

The author applies ideas from maximal-length codes to produce an algorithm for finding weight 4 multiples of polynomials over $GF(2)$. Its worst case complexity is $O(2^{2k/3}$, and in general it is suitable for shift registers up to about 100 bits. Its effect is to cut the overall complexity of the Meier Staffelbach algorithm.

052528 'The Cipher SHARK'
V Rijmen, J Daemen, B Preneel, A Bosselaers, E De Win, *FSE 96 pp 99–111*

The authors present a new block cipher. It is an SP-network, like SAFER, but it is about five times faster in software. It combines highly nonlinear S-boxes with maximum distance separable codes to guarantee good diffusion. As a result, it resists both linear and differential cryptanalysis after only a few rounds.

052529 'Learning Sparse Multivariate Polynomials over a Field with Queries and Counterexamples'
RE Schapire, LM Sellie, *Journal of Computer and System Sciences v 52 no 2 (April 96) pp 201–221*

The authors present the first provably effective algorithm to learn a sparse Boolean function. If there are n variables and t nonzero terms, it takes $nt+2$ equivalence queries and $(nt+1)(t^2+3t)/2$ membership queries.

052530 'Unbalanced Feistel Networks and Block Cipher Design'
B Schneier, J Kelsey, *FSE 96 pp 121–144*

The authors generalise the Feistel construction to networks where the source and the target of the autoclave function are of different sizes. They deduce some results for the rates of confusion and diffusion and suggest a taxonomy which they apply to McGuffin, BEAR, LION, MD4, GDES, Khufu, Khafre, REDOC and nonlinear feedback shift registers. The implications for linear and differential analysis are discussed.

052531 'Reihenschreiber'
M van der Meulen, *Cryptologia v XX no 2 (Apr 96) pp 141–154*

In 1958, the German army and intelligence agencies introduced a hand cipher based on a special slide rule. Its main role was use by soldiers in the field, but it was authorised for all levels of classification. The slide contains two fixed and ten (out of 26 possible) movable bars with digits on them; the movable bars can each be locked in one of ten possible positions, and a slide with a mask is used to select digits to form a decimal keystream. The masks were changed every ten days, the bar selection every day, and the bar positions by a message key. Finally, tables for applying the keystream digits to plaintext letters were changed every month. The cipher proved too complex for field use and was withdrawn in 1962.

052532 'On the Weak Keys of Blowfish'
S Vaudenay, *FSE 96 pp 27–32*

If the S-boxes in Blowfish are disclosed, and the number of rounds reduced to eight, then the rest of the key can be recovered with 248 chosen plaintexts. Where an S-box has a collision, this complexity falls to 2^{23} after eight rounds and 3.2^{51} after sixteen rounds. If the S boxes remain secret then one can test whether or not a collision exists with 2^{22} plaintexts.

6 Public Key Algorithms

052601 'Remote scheme for password authentication based on theory of quadratic residues'
CC Chang, SM Tsu, CY Chen, *Computer Communications v 18 no 12 (Dec 95) pp 936–942*

This paper proposes a remote password authentication scheme based on quadratic residue.

052602 'Efficient blind signature scheme based on quadratic residues'
CI Fan, CL Lei, *Electronics Letters v 32 no 9 (25/4/96) pp 811–813*

The authors propose a blind signature scheme based on quadratic forms modulo the product of four large primes.

052603 'Blind multisignature schemes and their relevance for electronic voting'
P Horster, M Michels, H Petersen, *Apps 95 pp 149–155*

In a multisignature scheme, members of a group of signers produce partial signatures that are individually checked and then combined by a clerk to produce a final signed message. In a blind multisignature, we want to get a signature from a group of signers without any signer knowing the relationship between the blinded and unblinded messages, and the signature parameters. The paper proposes a blind multisignature scheme based on a variant of El Gamal. Its security against outsiders and insiders (whether colluding insiders, or a signer bypassing other signers) is discussed. It scheme is used as the blinding element in an electronic voting protocol.

052604 'On the security of Wu and Yeh's conference key distribution scheme'
T Hwang, NY Lee, CH Wang, MY Ko, *Computer Communications v 18 no 12 (Dec 95) pp 978–981*

This paper shows that, in the Wu and Yeh conference key distribution system, an opponent who knows the ID of a member in the conference can compute the conference key without knowing any secret from the system.

052605 'Modified Harn digital signature scheme based on factorising and discrete logarithms'
NY Lee, T Hwang, *IEE Proceedings on Computers and Digital techniques v 143 no 3 (May 96) pp 196–198*

A signature scheme of Harn had been claimed secure so long as both factoring and discrete log remained difficult; it worked mod p where the factors of $(p-1)/2$ were secret. In this paper, it is shown that the ability to calculate discrete logs mod p is sufficient to forge a signature.

052606 'Online multiple secret sharing'
RGE Pinch, *Electronics Letters v 32 no 12 (6/6/96) pp 1087–1088*

This paper generalises Cachin's secret sharing scheme (**051804**) to one that, assuming the intractability of Diffie-Hellman, allows shares to be reused and membership to be changed dynamically.

7 Computational Number Theory

052701 'Perfect power testing'
R Balasubramanian, SV Nagaraj, *Information Processing Letters v 58 no 2 (22/4/96) pp 59–63*

The authors present a slight improvement on an algorithm by Bach and Sorensen for testing whether an integer is a perfect square.

052702 'GF(2^n) Multiplication and Division over the Dual Basis'
STJ Fenn, M Benaissa, D Taylor, *IEEE Transactions on Computers v 53 no 3 (Mar 96) pp 319–327*

A GF(2^n) multiplier is presented that uses a general linear function, rather than the trace function, to define duality and has thus greater flexibility in the choice of 'normal' bases. The Berlekamp bit-serial multiplier is shown to be a special case of a more general design, and efficient designs are given for parallel multipliers, constant multipliers and a systolic divider that is independent of the defining irreducible polynomial.

052703 'A new algorithm for constructing large Carmichael numbers'
G Löh, W Niebuhr, *Mathematics of Computation v 65 no 214 (4/96) pp 823–826*

The authors give an algorithm for constructing Carmichael numbers with very large numbers of prime factors.

052704 'Fast exponentiation method obtained by folding the exponent in half'
DC Lou, CC Chang, *Electronics Letters v 32 no 11 (23/5/96) pp 984–985*

The authors propose to speed up exponentiation by extracting common substrings from the exponent.

052705 'On finding primitive roots in finite fields'
I Shparlinski, *Theoretical Computer Science v 157 (3/5/96) pp 273–275*

In any given finite field, a primitive root can be found in time $O(q^{1/4+\epsilon})$. The technique is to construct a polynomial with a known root and then find the isomorphism.

8 Theoretical Cryptology

052801 'The CEO Problem'
T Berger, Z Zhang, H Viswanathan, *IEEE Transactions on Information Theory v 42 no 3 (May 96) pp 887–902*

The authors look at a new problem in the area of multiterminal source coding. Consider the Chief Executive Officer (CEO) of a company who has L agents that independently observe corrupted versions of a data sequence. The agents send, the information they observe to the CEO. The fidelity with which he can reconstruct the data depends on the bandwidth that the agents have to confer among themselves. If they cannot confer, then even with infinitely many agents, the CEO cannot eliminate all the errors.

052802 'A Short Note on Shor's Factoring Algorithm'
H Buhrman, *SIGACT News v 27 no 1 (Mar 96) pp 89–90*

The author points out that Shor's algorithm for factoring numbers with a bounded error probability can be made to work with zero probability by adding a primality proving stage.

052803 'ID-based non-interactive zero-knowledge proof system based on one-out-of-two non-interactive oblivious transfer'
YH Chen, T Hwang, *Computer Communications v 18 no 12 (Dec 95) pp 993–996*

This paper proposes an ID-based non-interactive zero-knowledge proof system based on a 1-out-of-2 non-interactive oblivious transfer protocol.

052804 'Cryptographic Redundancy and Mixing Functions'
O Collins, *IEEE Transactions on Communications v 44 no 4 (4/96) pp 423–426*

Error correcting codes can be used to combine multiple semi-secure channels into a single channel with greater security. With an (n, k) MDS code, we can force the enemy to intercept k channels to get anywhere. A similar result can be obtained with mixing functions modelled on the fast Fourier transform.

052805 'Evaluating the strength of ciphers'
JC Higgins, *NISSC 95 pp 395–403*

The author points out that the problem of evaluating cipher strength is under reasonable assumptions undecidable.

052806 'Randomized Algorithms'
R Motwani, P Raghavan, *Computing Surveys v 28 no 1 (Mar 96) pp 33–37*

This article surveys the uses of randomness in computer science; a number of these uses are security related.

052807 'Efficient Perfectly Secure Message Transmission in Synchronous Networks'
HM Sayeed, *Information and Computation v 126 no 1 (10/4/96) pp 53–61*

The author improves on Dolev's algorithms for secure communications in the presence of Byzantine failure. Assuming only one adversary who controls a number of nodes, the two phase protocol proposed is in the worst case linear in the diameter of the network, and polynomial in the number of wires connecting the sender and receiver.

9 Book Reviews

'SECURITY IN CLINICAL INFORMATION SYSTEMS'
Ross Anderson
British Medical Association, 0-7279-1048-5

This book (a shortened version of which appeared as **052101 ???** above, sets out a security policy model commissioned by the British Medical Association for the security of clinical information systems. This aims to do for medical computing what Bell-LaPadula did for the military; namely, to express the most important goals of security policy in a compact set of rules that can not only serve as a basis for formal models, but also facilitate discussion between system builders and users.

There are nine principles, which collectively enforce the principle — drawn from both medical ethics and European data protection law — that personal health information must not be disclosed by healthcare professionals without the patient's consent. The nub of this is an access control list for each logical record, and a provision that patients shall be notified of all additions to the access control list; their consent must also be sought except in case of emergence or statutory exemptions such as court ordered access. Information may only flow between records where the destination's access control list is contained in the source's.

These principles provide an alternative view of the world; existing models — such as Bell-LaPadula, Clark-Wilson and the Chinese Wall model — are all oriented to institutional security concerns. Here is a model whose concern is firmly that of personal privacy. It may have much more general application than healthcare.

'PRACTICAL UNIX AND INTERNET SECURITY
S Garfinkel, G Spafford
O'Reilly and Associates, Inc, 1996; ISBN 1-56592-148-8

This is a greatly expanded version of the authors' 'Practical Unix Security', which we reviewed in v 4 no 2. The new book is twice the size, and it is more useful to people whose knowledge of Unix internals is patchy. This is welcome given the large number of people who are now working part-time as system administrators without very much in the way of formal training.

This does not mean that this book is any less useful to the professional, as the authors use the accelerating lecture technique. Topics, and their treatment, become steadily more detailed. On page 6 we find a section on 'What is an operating system?'; by page 40 we have graduated to 'The problem with security through obscurity' but towards the end of the book (on page 716) we find 'Tips on writing SUID/SGID programs'.

The scope is encyclopaedic, ranging from information on how to get and use a number of the security resources that are freely available on the net to tips on handling incidents. This volume will be a useful reference on any system administrator's or security manager's shelf.

How to Subscribe

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

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

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

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

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

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

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

Name: ....

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

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint `E5C7 93BE 379D 2842 49DC A809 A147 05F6` can be fetched from `http://www.cl.cam.ac.uk/users/rja14`. You can also fax this order form to us on +44 1223 334678, or mail it to us at:

Northgate Consultants Ltd., 10 Water End, Wrestlingworth, Sandy, Beds SG19 2HA, United Kingdom