



Card Issuers Reveal They Knew of Security Flaw

Major card issuers, Visa and Mondex (and presumably chip manufacturers and card fabricators) say they have known for over a year about a security weakness in Smart Cards, publicly revealed this month by The Australian Financial Review.

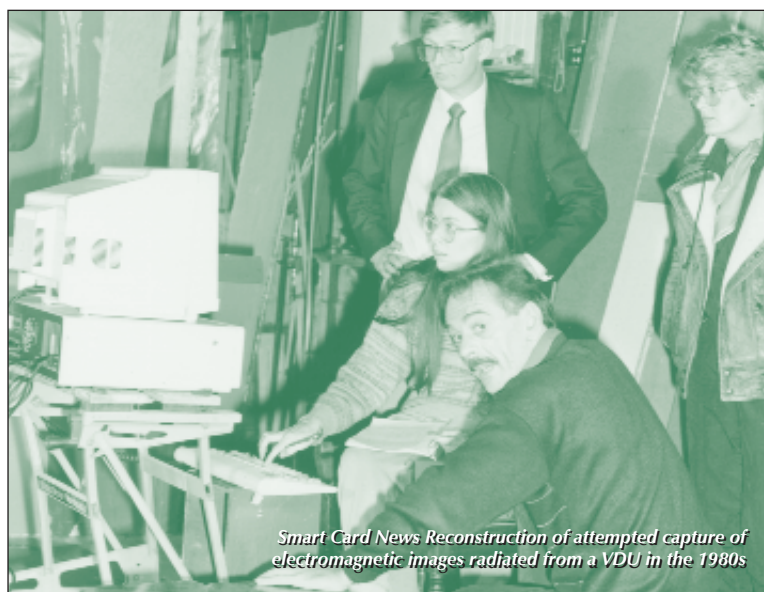


The attack technique involves monitoring the Smart Card's power consumption to break the secret security codes. Experts say that silicon chips use more power to process a 1 than an 0 - the two characters used in binary language - and it is possible to read confidential information using equipment that can cost as little as US \$500.

Both Visa and Mondex say they have no knowledge of any successful attacks on their cards and have taken interim steps to address the issue. The longer term solution is expected to come from hardware modifications to the chip.



(See Smart Cards and Information Leakage - page 116)





June 1998

News

- 103-115** *Smart Security Intercity Trains
Shanghai Metro Goes Contactless
Patient Card for Florida Practice
Smart Cards in Western Europe
Bank in Your Pocket
Largest Loyalty Program in Brazil
Proton Launched in Mexico
Turnover Rises with Smart Cards
Electronic Voting System
Smart US Retailers Sideline Banks
Combined Card for Transit Project*
- 119-120** *Other News
Nationwide EasyPark in Israel*

Interview

- 114-116** *The Sunflower Heads for Nasdaq*

Smart Card Tutorial

- 117-118** *Smart Cards and Information Leakage*

Cards on the Cover
*AOM's Smart Card
Frequent Flyer Program
Successfully Launched*
Page 118
Gemplus Sunflowers
Page 114
**Standard Chartered (Visa
International's Open
Platform User's Group)**
Page 107
Russia's Golden Crown Card
Page 120

Main Photograph
*Smart Card News
Reconstruction*
[Smart Card News Ltd]

How to Subscribe
If you wish to subscribe
to Smart Card News
please complete the
form on page 119

Don't Forget!
Our On-Line Websites,
containing a Library of
Smart Cards and information
about the full range of SCN
services, can be found at
the following addresses:
<http://www.smartcard.co.uk>

On-Line News:
<http://news.smartcard.co.uk>

*Smart Card News is published monthly by Smart Card News Ltd PO BOX 1383 Rottingdean Brighton East Sussex BN2 8WX England
Telephone : + 44 (0) 1273 236677 / 626677 • Facsimile : + 44 (0) 1273 624433 / 300991 • e-mail : scn@pavilion.co.uk ISSN 0967 196X*

*North American Sales Office : Richard T Hauge 256 El Portal Way San Jose CA 95119-1413 USA
Telephone : +1 408 225 8074 • e-mail : richard_hauge@msn.com*

*Managing Director Patsy Everett Editor Jack Smith Technical Advisor Dr David B Everett
Graphic Designer David Lavelle*

*Editorial Consultants Dr Donald W Davies CBE FRS, Independent Security Consultant
Peter Hawkes, Principal Executive Electronics & Information Technology Division, British Technology Group Ltd
Simon Reed, Head of Strategic Marketing for the Orga Group
Robin Townend, SVP World-wide Smart Card Strategy, Intellect Electronics, Inc.*

Printed by Design and Print (Sussex) Ltd. Telephone : +44 (0) 1273 430430

Thai Oil Companies Launch Card

Three of Thailand's leading petrol retailers have launched nationwide Smart Card schemes to enable fleet and transport operators to monitor and control costs and enjoy the benefit of loyalty discounts.

The first scheme was set up in February 1997 by all 600 Caltex stations and now about one third of the 2,000 Esso and PTT (Petroleum Authority of Thailand) outlets are joining forces to launch a similar, but separate, scheme.

The cards used combine magnetic stripe and Smart Card technology, the magnetic stripe enabling the Thai Military Bank - the bank involved in the scheme - to handle payment through its existing credit card network, while the chip generates and stores the data used to monitor transport-related expenses.

Details of the fleet owner, driver, services allowed and maximum transaction amount, are shown on the card or held in the chip. Fleet owners can then monitor all petrol-related expenses accumulated by their vehicle fleet each month; the expenses of each driver and each car can be checked. Drivers benefit from the security of not having to carry significant amounts of cash.

All payments are approved and recorded on-line, but the fleet expense control and customer profile are operated off-line. Transactions are stored locally at the point-of-sale terminal in the petrol station and downloaded to the oil company at the end of the day. A monthly financial statement summarising goods and services used, and discount accumulated, is sent to the fleet owner.

Dr Phornchai Sripraphal, Director of Brand and Retail Marketing at Caltex, said: "Caltex corporate customers can now be in full control of their fleet fuel usage. It not only provides our customers with detailed information on their transport-related transactions, but also protects them from fraud."

Schlumberger, working with Posnet, a subsidiary of Smart Telecom, has provided the Smart Cards and Smart 1000 EFTPOS terminals to handle both payment and allocation of loyalty discounts. In addition to handling both magnetic stripe and Smart Card transactions, the terminals have a dual-language function, enabling the display and printing of Thai characters.

The separate transaction terminal is portable so that it can be taken to the driver in the car.

Contact

■ **Sally Chew** Schlumberger Industries International SA
☎ +65 746 9676 ✉ schew@singapore.asia.slb.com

Smart Security Intercity Trains

Amtrak is to introduce contactless Smart Card technology for security on its new high-speed intercity trains when they start service next year.

The \$2.4 billion rail programme, funded jointly by the federal government and the private sector, will bring 150 mph passenger rail services to North America by the turn of the century. Up to 18 new trains will operate routes between Washington, DC and New York City and between New York and Boston.

The security key card system consists of customised contactless Smart Cards and readers installed in the trains. Train crews will be granted varying levels of access and authorisation for specific operations by the system and the train computer network. Giesecke & Devrient America supplied the contactless Smart Cards and teamed with Productivity Enhancement Products (PEP) to design and manufacture card readers to operate in a railroad environment.

Contact

■ **Claudia Watson** G&D America
☎ +1 703 620 8843 ✉ c_watson@ix.netcom.com

Intellect Alliance with Retail Logic

Intellect, of Australia, has announced a joint venture agreement with UK based Retail Logic, a developer of payment card processing software. They plan to develop a Smart Card solution for handling multiple electronic cash schemes and loyalty cards. The teaming will enable Retail Logic's client base to upgrade from magnetic stripe to Smart Card capable devices - significant in that Retail Logic's payment software is currently provided to 80 per cent of the large UK retailers.

Contact

■ **Geoff Gander** Intellect
☎ +61 8 9472 2222 ✉ geoff.gander@intellect.com.au

Shanghai Metro Goes Contactless

Shanghai Metro is currently trialing contactless Smart Cards for automatic fare collection.

The first field trials started last September by Cubic Transportation Systems and their Australian-based subcontractor VFJ.

Shanghai Metro Line 1 is scheduled for completion in December of this year and Metro Line 2 in 1999. When the scheme is rolled out it is expected that over 200,000 MIFARE contactless Smart Cards from Philips Semiconductors and 700 readers will be in use on these two lines. The potential for all five metro lines in Shanghai amounts to more than 3,000 readers in the short term. The scheme may be extended to Shanghai bus companies in a move to integrate all of the mass transit contactless Smart Card systems into one multi-modal system.

Road toll in Guangxi

VFJ is also using MIFARE-based touch-and-go technology in an electronic toll collection scheme in Guangxi with some 10,000 cards issued and 40 readers installed since last January. In a second phase it is planned to extend the scheme to 100,000 cards and 2000 readers within this year.

Hong Kong Cargo Terminal Card

Personnel at the Hong Kong Air Cargo Terminal are to be issued with MIFARE contactless Smart Cards in a company ID scheme being installed by VFG. Some 4,000 personalised cards with photograph will be issued and 700 readers installed for staff access and vehicle control.

Contact

■ **Peter Gasteiner**

☎ +43 3124 299250

✉ peter.gasteiner@at.ccmil.philips.com

College Access/Attendance Card

As the British government launches a campaign to clamp down on truants and grapples with the problems of keeping intruders out of schools, Hoofdstad College in Amsterdam in The Netherlands has introduced a contactless student card to keep track of student attendance at mandatory classes and to secure access to college buildings.

The system developed by Iolan, a specialist in building management systems and access control, is being trialed with 5,000 students and teachers out of a total of some 25,000. Iolan opted for Philips Semiconductors' MIFARE contactless technology, which makes the scheme unusual because of the contactless implementation of an administration system, but is apparently raising national and international interest.

Registration is necessary as subsidies awarded depend on the number of students attending classes and, of course, non-attendance has legal ramifications for minors and must be tracked. At the same time, accurate registration provides useful data for administrators such as interest in certain subjects or particular classes.

In September last year, Iolan introduced an access control system in four of the college's 100 buildings. Each building entrance and classroom is equipped with a MIFARE reader connected to a communications bus, with a total of 150 readers. The contactless cards are used by teachers and students to access the buildings and to check in (once an hour) in the classroom, eliminating tedious pen and paper records for teachers and administrators. The data is sent via the bus to an automatic student administration network and immediately entered into the database. The scheme will later include building management tasks such as heating or lighting control.

Contact

■ **Peter Gasteiner**

☎ +43 3124 299250

✉ peter.gasteiner@at.ccmil.philips.com

BT Joins Chipcard Alliance

BT, the British telecommunications giant, has joined the Global Chipcard Alliance bringing membership up to 27 companies. The Alliance was formed to create an open infrastructure for chip cards and achieve global interoperability for multiple application Smart Cards.

Welcoming BT, Gerard Ketelaar, GCA Vice President, said BT had significant experience in developing Eurochip Smart Cards used in public payphones and would bring its world-renowned development expertise to the Alliance.

Patient Card for Florida Practice

A private medical practice in Orlando, Florida, is to introduce a Smart Card system for patients.

Leapfrog Smart Products Inc., a Smart Card application development company, has signed a contract with RDV Sportsplex Family Practice in Orlando.

Dr Richard Baxley, owner of the practice, said: "We have always been committed to give our patients the very best health care possible. Utilising technology is just one more way to insure that our patients can benefit from the latest advances in the healthcare industry."

The patient card will contain relevant medical history and insurance information. When a patient checks-in, the card will be read and the patient will authenticate himself via a PIN or biometric. Data from the visit will be gathered to integrate into an electronic bill for the insurance carriers.

"Patient authentication will cut down on fraud and misuse of insurance cards," said Dale Grogan, President of Leapfrog.

Contact

- **Leslie Dukker Doty** Leapfrog Smart Products Inc.
☎ +1 407 872 1161 📠 +1 407 872 0508.

SecuraCard Smart Card Reader

SecuraCard, developed by California-based Kopel Inc., is a wallet that contains a Smart Card reader, allowing owners to have access to their remaining balances and transaction logs without extra accessories, and incorporates a "beeping" function for credit card protection.

The leather wallet and document holders use a miniature digital screen. Sliding a Smart Card into the designated slot in the wallet provides instant access to information. The read-only operation ensures no changes or damage to the card. The wallet also alerts the owner of lost or stolen cards through a series of timed beeps. A useful feature too if you forget to pick up your card at a point of payment!

Contact

- **Audrey Hiraki** Sales and Marketing Manager, Kopel
☎ +1 818 991 6255 📠 +1 818 991 6298

Satellite Terminal Security by ORGA

ORGA Card Systems is to provide an advanced, fraud-resistant chip card solution for the QUALCOMM-manufactured Globalstar User Terminals utilised in the digital-based mobile satellite communications system. This innovation will enable subscribers to easily and securely access a comprehensive range of voice, messaging, facsimile and data services available on the network.

The Globalstar worldwide communications network will consist of 56 low-earth orbiting satellites, 48 of which will be operational, with eight in-orbit spares. This placement pattern offers high-quality communications to millions of individuals in virtually every populated area in the world. Services will be accessible through conventional fixed and cellular networks and also through the Globalstar communications system network using the Globalstar new fixed-site satellite telephones and hand-held or mobile mounted terminals.

Contact

- **Gerry Smith** ORGA, USA
☎ +1 610 993 9810
- **Keriann Hartman** QUALCOMM
☎ +1 619 658 2768
🌐 www.qualcomm.com • www.orga.com

Visa Korea launches SET Pilot

Visa Korea announced its Electronic Commerce (EC) pilot launch utilising the SET 1.0 (Secure Electronic Transaction) for the first time in Korea.

The company demonstrated SET 1.0 transactions to representatives of the Ministry of Industry & Energy, and Visa's main membership holders, including IBM Korea, Dacom, Metaland, Bara International and Cybertech Holdings. In order to enable its cardholders to pay in a more secure way in an open network environment such as the Internet.

Participating in the pilot program are the six major card members and other membership holders, including Korea Exchange Bank Credit Card Co., Kookmin Card, BC Card, Korea Long Term Credit Card, Shinhan Bank and Koram Bank.

Contact

- **Colin Baptie** Visa International
☎ +44 (0)171 937 8111 📠 +44 (0)171 9370977

Smart Cards in Western Europe

Smart Card technology is one of the fastest growing and dynamic branches of the IT industry in Western Europe today, according to new research from International Data Corporation (IDC).

The European Smart Card Market: Review and Forecast 1996 - 2001 reveals that the main vendors in Western Europe expect their turnover to grow by more than 56% in 1998 and of these cards the microprocessor based cards are expected to top 308 million.

During the last 20 years, Smart Cards have evolved from a leading edge technology to a mass-market medium with worldwide applications in such fields as banking, mobile telephones and security access. The market has grown from straightforward memory applications to truly interactive application devices where the microprocessor carries the 'client' application.

IDC believes the potential offered by Smart Cards will trigger significant opportunity for IT vendors for the next few years. With over 1 billion microprocessor Smart Cards forecasted to be circulating at the turn of the century, they are regarded by the vendors as the fastest and most efficient way to secure electronic commerce, web, intranet, extranet and workgroup applications and to generate associated revenues.

Points from the report:

- Rapid growth of the microprocessor market has attracted newcomers, such as IT vendors and microprocessor vendors, who see this technology as one of the best ways to boost electronic commerce and secure computer access.
- Java Cards procure several benefits for end-users: cheaper costs of development, easy downloading, and multi-application cards. However, by letting issuers choose between several suppliers they may reinforce the competition.
- Contactless cards, though still in their infancy, eliminate current problems associated with contact Smart Cards and will also provide opportunities for newcomers.

The report analyses the three major technology trends (microprocessor, contactless and Java Cards) in the UK, France and Germany.

The study gives a comprehensive analysis of the different market inhibitors and drivers, trends and applications for each segment as well as vendor positioning with local market development in the three countries.

The report is priced at \$6,500 and is available from IDC offices. IDC's Web site: www.idc.com

Contact

■ **Annabelle Ducellier** IDC

☎ +33 (0)1 49 04 80 02 ✉ aducellieridc.com

SingTel and GPT joint venture

Singapore Telecommunications (SingTel) and UK payphone and phonecard supplier GPT International are to invest 15 million Singapore dollars to set up a phonecard-manufacturing facility in Singapore.

The two companies signed a memorandum of understanding to form a joint venture company to undertake the project.

GPT General Manager, Paul Seward, said they expect the facility to be operational by end-1998. An initial 60 million cards a year would be produced for the Asia-Pacific market. GPT currently produces 30 to 40 million cards a year for SingTel. The MoU also calls for establishing a SingTel-GPT Card Technology Center in Singapore bringing together GPT's technical know-how and SingTel's marketing and systems integration strengths. This will enable new microprocessor card-based applications to be developed quickly for the region.

"With GPT's expertise and our experience in managing payphone services in Singapore, SingTel is well poised to meet the demands for Smart Cards not only locally but within the region," said Tan Kee Joo, SingTel's Chief Executive of Consumer Sales. Singapore Telecom is one of the leading telecommunications companies in Asia and the largest listed company on the Singapore Stock Exchange.

Contact

■ **Ms Foo Kim Leng** Singapore Telecom

☎ +65 838 2011 ✉ +65 733 1350

Bank in Your Pocket

Visa International and Standard Chartered Bank have launched a new multifunction Smart Card based on Visa's Open Platform and the Java Card specification.

The new card, supplied by Gemplus, was used to make an Internet purchase from a kiosk in Singapore, the first real-world test of the card. A transaction including credit payment and loyalty applications was also conducted on a traditional terminal to illustrate that the new card is compatible with existing point-of-sale terminals.

Edmund P. Jensen, President and CEO of Visa International, said: "The card literally creates a new global medium of payment and information exchange that replaces the consumer's wallet - in effect, giving consumers a bank in their pocket."

The Standard Chartered/Visa multifunction card will initially be tested among staff of the two companies in Singapore and will be available to cardholders in Singapore beginning the third quarter of 1998. It will be rolled out in Taiwan, Hong Kong and elsewhere in Asia next year.

In addition to a credit payment application, the card includes a loyalty program, a relationship application and a security function for shopping on the Internet, employing a SET Secure Electronic Transaction application. As the pilot program advances, Standard Chartered will be able to load functions on each card, with the bank's customers having the option to customise the card to their specific needs.

Contact

■ **Ryan Mikolasik** Visa International
 ☎ +1 650 432 5769 ✉ rmikolas@visa.com

Open Platform Users' Group

More than 20 Financial Institutions have joined Visa's Open Platform Users' Group, driving development of multifunction Smart Card programs based on open technology

Visa International last month announced the formation of a users' group for financial institutions interested in using Visa's Open Platform based on Java.

Members of the Users' Group include some of the world's leading banks and financial institutions which intend to use the Open Platform specifications to create multifunction Smart Card products that provide consumers with an expanding array of services and benefits, including payment, identification, physical access, network access and loyalty programs.

To date, more than 20 financial institutions have joined the Users' Group worldwide. Charter Members of the Users' Group plan to use the Open Platform to launch multifunction Smart Cards within the next 24 months, with a number of those financial institutions committed to doing so in the next year.

Participants will share information and discuss multifunction implementation issues, and will have access to early and ongoing global information on opportunities and advances in this area. Members will be able to exchange experiences and communicate with vendors about common requirements.

Visa International Open Platform Users' Group

Asia Pacific

Standard Chartered Bank

Australia

Commonwealth Bank of Australia, St George Bank, Westpac Banking Corporation

Japan

DC Card, The Sumitomo Credit Service

Korea

BC Card, KLB Credit Card, Kookmin Credit Card; Korea Exchange Bank Credit Service, LG Credit Card, Samsung Card

Singapore

Network for Electronic Transfers (Singapore)

Taiwan

ChinaTrust Commercial Bank, Financial Information System Center

Canada

Scotiabank

Central Eastern Europe, Middle East, Africa, South Africa
 First National Bank of Southern Africa, Nedcor Bank

European Union

France: Carte Bleue; Spain: Visa Espana; UK: Barclays Bank

Latin America and Caribbean

Citibank Latin America

USA

Bank of America, Citibank, First Union, NationsBank

Largest Loyalty Program in Brazil

Gemplus has announced that it is providing 2 million Smart Cards for the Smart Club do Brasil loyalty program that will be rolled out in August of this year starting in the city of Rio de Janeiro.

Companies partnering to issue the loyalty card are Banco Bradesco, Brazil's largest bank; Shell Brasil, with more than 4,000 service stations in the country; TAM, a Brazilian airline; Lojas Americanas, one of the largest Brazilian retailers; and Rede Globo, the largest telecommunications company in Brazil. RDS, a Rede Globo partner in southern Brazil, is also participating.

The loyalty solution will enable consumers to earn points for purchases made at participating companies, which can then be redeemed for gifts, discounts, and other special privileges.

The loyalty application will use a Gemplus GPM896 memory card.

In the third quarter of 1998, the loyalty solution will be rolled out to other cities in Brazil. Gemplus expects to deliver 5 million Smart Cards in 1998 in conjunction with the project.

"We are pleased to be participating in this important loyalty program in Brazil," said Donna Jeker, Vice President of Strategic Marketing and Partnerships for North and Latin America. "Our third-party partners are key to implementing our strategy of providing Smart Card solutions that will make a difference in how people live and work."

Contact

■ Dr Patricia Neptune

Neptune Group International Inc. (for Gemplus)

☎ +1 203 221 2820

Taiwan Bank to Utilise VeriSmart

Chia Hsin, an electronic commerce solution provider in Taiwan, will be first to utilise VeriFone's VeriSmart to deliver secure Internet-based Smart Card applications to its customers.

VeriFone announced that its VeriSmart architecture now allows the delivery of secure consumer Smart Card applications for the Internet. The capability is enabled through the flexible VeriSmart architecture

Financial institutions, telecommunications companies and other Smart Card service providers using the VeriSmart architecture can now deliver secure services to consumers utilising the Internet.

The new PayPort appliance is a low-cost peripheral that incorporates the Smart Card capability into a consumer's personal computer. With the PayPort appliance, a consumer's PC becomes enabled for a new set of applications that range from electronic cash to Smart Card security for Internet-based and other applications.

"Smart Card technology provides an additional level of security for applications running over the Internet, including financial applications such as electronic cash loading and purchasing, home banking and stock trading," said Nelson An-Ping Chang, President, Chia Hsin Corporation.

"These are just some of the applications that Chia Hsin is developing for customers through our VeriSmart-based Smart Card solutions."

Flexible architecture

"VeriSmart is a flexible architecture that lets telcos, banks, or other Smart Card service providers deliver a wide range of applications to consumers using the most effective delivery methods," said Thomas J. Kilcoyne, Vice President and General Manager, Consumer Systems Division, VeriFone, Inc.

"With the surge in the number of consumers connected to the Internet, this is a valuable new capability for the VeriSmart system, and the PayPort appliance provides a simple, inexpensive means to Smart Card enable consumer Personal Computers."

The PayPort is a palm-sized Smart Card reader/writer appliance, like VeriFone's Personal ATM device, that offers consumers the ability to access Smart Card-based services in the convenience of their home or office. Where the Personal ATM connects through a phone line, the PayPort product plugs into a personal computer's serial port.

Contact

■ Dan Toporek VeriFone, Inc.

☎ +1 408 919 5524 ✉ dan_t1@verifone.com

Proton Launched in Mexico

Proton, the Mexican Smart Card payment system, was officially launched in Mexico City early this month and it is estimated that initially some three million cards will be put into circulation before the system is extended throughout the country at the beginning of next year.

The Inbursa financial group acquired an exclusive license to operate the Proton electronic purse system in Mexico from Banksys, the Belgian developer of the system. Inbursa and Telmex (the Mexican telephone operator) have installed a network of 150,000 public telephones at which the cards can be used and the network is set to double in size between now and the end of 1999. Armand Linkens, Managing Director and Director of marketing and sales at Banksys, said: "Mexico will very quickly figure among the largest and most dynamic Proton-based payment systems in the world."

Contacts

- **Juan B Mesa Iturbide**
☎ +52 5 514 9367 📠 +52 5 514 0692
✉ jmesa@mex1.uninet.net.mx
- **Youri Tolmatchov** Banksys
☎ +32 2 727 6666 📠 +32 2 727 2727
✉ tolmatchov.y@banksys.be

BT Joins Leeds Visa Cash Pilot

BT has announced that it is to join the Visa Cash electronic purse project in Leeds in the UK with the introduction of over 100 new payphones which will accept the Visa Cash card.

The new payphones, manufactured by Schlumberger working with the British telecommunications company, will only accept Visa Cash as payment and are being installed at convenient locations such as the University of Leeds, Leeds Metropolitan University, the railway station and in leisure centres, restaurants and city centre shopping precincts. Since the Leeds pilot was launched last October, 55,000 cards have been issued by the six banks involved - Abbey National, Barclays/Barclaycard, The Co-operative Bank, The Halifax, Lloyds/TSB and The Royal Bank of Scotland.

Contact

- **Colin Baptie** Visa International
☎ +44 (0)171 937 8111 📠 +44 (0)171 9370977

Burger King Pilots Mondex

Burger King is piloting Mondex electronic cash in four of its fast-food restaurants in the Long Island area of New York.

Carrying the BK brand, the cards combine a payment function and a loyalty program. Customers will receive one loyalty point for every dollar spent and can redeem them against BK food. The Mondex Smart Cards are being supplied and personalised by Gemplus. De La Rue is providing the point-of-sale terminals with Smart Card readers, and Giesecke & Devrient America is supplying Smart Card dispensing machines for use inside the restaurants.

Chase Manhattan Bank, already participating in the New York City Mondex trial, has upgraded seven of its ATMs in the area to load Mondex value.

Gemplus Introduces GemSAFE

Gemplus has introduced GemSAFE to provide a portable, Smart Card-based solution to secure access to corporate intranets, Web sites and e-mail systems.

GemSAFE stores a user's digital identity on a Smart Card. The user simply inserts the card into the reader, types in the PIN for identification and allows the chip on the card to carry out user authentication. Compatible with Microsoft Corporation and Netscape Communications browser software suites, individual GemSAFE kits are priced under US \$100 with volume discounts.

Contact

- **Lisa Colley** Gemplus
☎ +44 (0)1705 488037 ✉ lisa.colley@cmail.edt.fr

e-COMM Pilot in France

Secure Internet transactions using a Carte Bleue Visa chip card and the SET (Secure Electronic Transaction) specification marked the launch last month of a pilot in France by the e-COMM Consortium of BNP, Société Générale, Crédit Lyonnais, France Télécom, Gemplus and Visa.

Contact

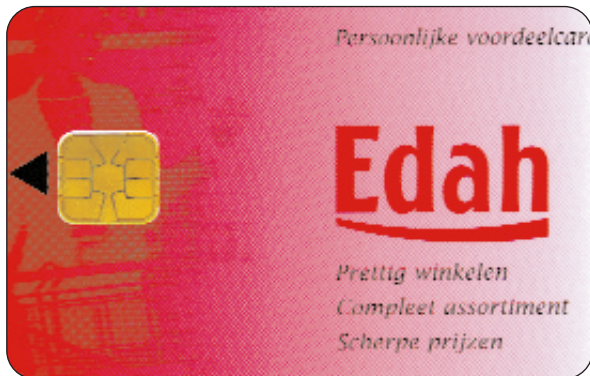
- **Catherine Hamon-Goudey** e-COMM
☎ +33 (0)1 41 86 76 76

Turnover Rises with Smart Cards

Right:
Edah Smart Card
Loyalty Scheme
[Schlumberger]

Below Left:
In-store multi-media
terminals for the Edah
Loyalty Scheme
[PH Design]

Below Right:
Tesco's Cashless
Vending Machine
[Gemplus]



Leading Dutch supermarket chain, Edah, reports that initial results from its Smart Card loyalty scheme show that turnover has increased, typically about 5 per cent on monthly figures compared with last year's trading. Edah has rolled out over 1.6 million cards through its nationwide network of 315 stores.

"The initial results from our Smart loyalty scheme are extremely encouraging," says Edah's Marketing Manager Jaap Rieter. "The technology of Smart Cards is helping us to establish a much more personal relationship with our customers, to our mutual benefit. We have already seen a marked improvement in sales, and as our database improves, we expect this to increase even further."

The scheme was developed by retail systems integrator, Riva Systems, using Smart Cards from Schlumberger. Each card stores a shopper's points so that the user can check them at any time while shopping, and provides the means to deliver special offers which are targeted at the individual's buying preferences and patterns.



The system has four main elements: the cards, a multi-media terminal where users can check their rewards and display and print targeted offers, point-of-sale terminals equipped with Smart Card readers, and a buying behaviour database.

Sales information is uploaded from the check-outs using the stores' existing management information network. Purchasing data is extracted and fed into a new database which profile users into a number of behaviour groups. The store's database then matches these behaviour groups against a constantly changing range of special offers created by the marketing department. Also, as five offers are typically provided, the store can also complement targeted rewards with incentives to try new lines. These special offers are downloaded overnight to the store's multi-media kiosks via the public switched telephone network, ready for the next day's trading.

Contact

- **Geert-Peter van Asperen** Riva Systems
☎ +31 33 434 1400
- **Isabelle Marand** Schlumberger
☎ +33 (0)1 47 46 55 42
✉ marand@montrouge.ts.slb.com

Cashless Vending for Tesco Staff

Cardinal, a Gemplus Value Added Reseller, has developed a Smart Card-based payment system to be installed in drinks vending machines at more than 400 Tesco stores throughout the UK.

Tesco plans to provide more than 130,000 staff with a wide selection of meals, snacks and drinks from vending machines, not only during store opening hours but also throughout the night when deliveries are received and shelves stacked.



A major advantage of the system is elimination of the need for money to be collected, says a Tesco spokesperson. Also, vending machine availability is improved by doing away with coin mechanisms and the problems of jammed coins or full coin boxes.

Contact

- **Lisa Colley** Gemplus
☎ +44 (0)1705 488037
✉ lisa.colley@ccmail.edt.fr

Electronic Voting System



Omron Electronics has developed an electronic voting system using Smart Cards which has been successfully trialed in Portugal.

The prototype SVE (Sistema de Voto Electrónico) was trialed in Portugal recently during a municipal election in Lisbon. Electronic voting booths were used in parallel with the traditional paper-based ballot procedure.

A further trial in April of this year during the Annual Congress of the Portuguese Social Democrat Party, saw the system working live without a paper-based back-up system.

With the electronic voting system, votes cannot be deposited unless they are valid, eliminating the problem of spoiled papers or attempts at fraud, Omron explained. The system also speeds the ballot process as counting of the votes is automated, enabling the rapid calculation of the final results and providing statistical analysis at any time during voting.

Each voter is identified on entering the polling station and issued with a Smart Card. The voter then goes to the voting booth to select his preferred candidate on an Omron touch screen terminal equipped with a Smart Card reader.

After voting, the Card is inserted into an electronic deposit box on exit from the polling station.

The system enables the transmission of the election data from the host terminal to a central computer via the telephone network.

Contact

- **Guy Boxall** Omron Europe
☎ +44 (0)181 450 4646 📠 +44 (0)181 450 8087

Mondex Launch in Costa Rica

Mondex electronic cash has been launched in Costa Rica by Credomatic International Corporation, the major issuer, acquirer and processing agent of credit and debit cards in Central America.

Left:
Portuguese President Jorge Sampaio prepares to use the new electronic voting system at a municipal election in Lisbon [Omron]

Credomatic acquired the first Mondex franchise rights to be sold in Latin America in June 1997 and has exclusive rights to commercially develop the system in seven countries - Costa Rica, Guatemala, Nicaragua, Panama, Honduras, El Salvador and Belize, which collectively represent a marketplace of over 30 million people.

Some 10,000 Mondex cards will be issued in the first launch phase and it is forecast that more than 3,000 merchants will be able to accept Mondex payments by the end of this year.

Importantly, more than 7,500 of the cards will offer both the MasterCard credit function on the magnetic stripe and the Mondex electronic cash function on the chip.

Mondex International is a subsidiary of MasterCard and Richard Child, President for MasterCard Latin America and the Caribbean, said: "The combination of MasterCard credit and Mondex electronic cash on a single card is a world first, and is an important step in the future of the payments industry in Central America." Credomatic demonstrated Mondex's multi-currency capability with the first ever telephone transfer of Mondex electronic cash from the United States to Costa Rica (between San Francisco and San Jose) in US dollars. The card issuer intends to include Costa Rican Colones and other Central American currencies as well as US dollars on the card.

Contacts

- **Juan Carlos Páez** Smart Card Project Manager,
Credomatic International Corporation
☎ +506 256 6954
- **Tim Stewart** Executive Vice President Americas Region,
Mondex International
☎ +1 973 660 4101.

Russian Order for Bull

Bull Smart Cards and Terminals division has won a contract to supply 1,300 Smart Card terminals to the Russian Credit Bank

Smart US Retailers Sideline Banks

Leading retailers in the US are using Smart Cards to boost customer loyalty, generate new sales and reduce cash handling and other costs while the banks are being left behind, according to a new study from Killen & Associates.

“Forward thinking retailers are forging ahead to deliver Smart Card-based solutions and the public is responding eagerly,” says Michael Killen, President of Killen & Associates.

“Smart Cards are increasingly finding uses in stand-alone, controlled applications. Mobil Oil, Safeway, Peete’s Coffee, K Mart and other market leaders have found the value proposition and are committed. They see customer traffic and sales increasing and costs decreasing. Meanwhile,” he added, “most banks are still waiting on the side lines, missing fee and transaction-based revenue streams while their retail business clients find more and more golden nuggets of opportunity.”

The new study, Retailers’ Smart Card Strategies: New Business Opportunities and the Disintermediation of Banks, includes an examination of winning retail strategies for the use and deployment of Smart Cards, the impact of Smart Cards on retailing and merchant financial services, and key opportunities arising for telephone companies and phone card issuers.

Contact

■ **Jules Street** Killen & Associates
☎ +1 650 617 6130 ✉ jules@killen.com

TownCard Smart Card Scheme

TownCard, a multi-retailer, multi-function Smart Card-based loyalty scheme has been announced by Scotcomms Partnership.

Scotcomms says the aim is to stimulate active participation by residents and visitors in local commerce and civic amenities through a Smart Card incentive scheme.

The system uses Gemplus GPM2K Smart Cards and Dione CPT500 card reader terminals. The programmable card enables users to collect loyalty points and other benefits such as discounts and the opportunity to take part in prize draws.

Scotcomms has won a contract for Club Scotland, a rugby supporters scheme that is being developed in conjunction with the Scottish Rugby Union. Club members will receive a Smart Card for use in terminals installed at participating rugby clubs. Points accumulated can be used to obtain priority access to designated tickets and certain discounts. Members will also receive reduced rates on travel and hotel accommodation and enter prize draws.

Scotcomms has also developed the football-based TeamCard which is expected to be adopted by several Premier League clubs.

Contact

■ **Lisa Colley** Gemplus
☎ +44 (0)1705 455037 ✉ lisa.colley@ccmail.edt.fr

SET Too Complicated and Expensive

The financial services sector is finding the secure electronic transactions (SET) protocol too complicated and too expensive, according to a new report from strategic analysts Datamonitor.

As a result, says the report, E-commerce Payment Strategies: Competitors Profiles, the SET protocol will develop much slower than forecast by IT vendors and the financial services sector alike and will not reach the consumer market until late 1999.

Datamonitor says most financial services institutions are delaying roll-out to the mass market because of the substantial investment required from the credit card issuer. The most expensive components are the purchase and systems integration of the SET infrastructure and the payment gateway in particular; and constructing a digital certificate authority and managing the certificate database.

“The problem for the financial services sector is that the small scale of on-line shopping does not justify the extensive investment in SET,” says the report.

“The SET protocol appears to place the cart before the horse: the technology exists but there is insufficient demand for on-line shopping. SET must be more user-friendly and less expensive to draw consumers to the Internet market.”

Contact

■ **Russ Milburn** Datamonitor
☎ +44(0)171 316 0001 ✉ rmlburn@datamonitor.com

Combined Card for Transit Project

A microprocessor card with both contact and contactless interfaces is the “primary card requirement” for a public transit fare collection system in a four-county area surrounding Seattle, Washington. Called the Central Puget Sound Regional Fare Co-ordination Project, it brings together seven public transportation agencies operating 2,200 buses, passenger and vehicle ferry service at 13 terminals, and commuter and light rail. About 500,000 to one million Smart Cards will be issued for transportation-related purposes.

A Request For Proposals (RFP) from King County Metro, which is acting on behalf of the seven agency partners, says the primary business objective is to increase travel and revenues and enhance customer convenience. Interested parties are encouraged to propose added value to the system in areas such as revaluing, marketing and non-transit applications such as retail electronic purse, telecom or banking applications. The system should also be capable of accommodating future multiple applications for municipal and commercial purposes.

Contact

- **Candace Carlson** Project Manager
 ☎ +1 206 684 1562 ✉ candace.carlson@metrokc.gov

City Card for Nottingham

Nottingham, in England, is to launch a City Card in September of this year. It will be issued free to all city residents. Participating retailers can choose the level of reward points they offer shoppers, but no retailer will offer less than a 2 per cent rate of return. The cardholder can redeem the points at a retailer of their choice.

The contract for the City Card has been awarded to TOUCH, Ambient’s wholly-owned subsidiary, which will be responsible for implementing and running the scheme. It is working with technology partners, Saunders Jefferies, VeriFone and GPT.

Contacts

- **Tim Jones** Nottingham City Council
 ☎ +44 (0)1159 154368
- **Vincent Isaacs** Chairman, Ambient
 ☎ +44 (0)171 428 3200

China’s Cashless Payment System

Competition to win a share of the orders for China’s national Smart Card-based cashless payment system is hotting up with Schlumberger claiming it is the first company to offer a complete solution meeting the specification drawn up by the People’s Bank of China (PBOC).

The announcement comes after Giesecke & Devrient said it had developed the first Smart Cards which satisfy the PBOC standards and had obtained bank certification (SCN May 1998). Other industry heavyweights in the scene are Bull which expects to take part in the trials scheduled to start in October of this year, and Gemplus.

Schlumberger is offering its new Qianflex (Qian means money in Chinese) product range which includes Smart Cards, point-of-sale terminals, Security Access Module (SAM) and personalisation services.

The Qianflex cards are available with 1K of field-reprogrammable memory, or optionally, with 2K to provide storage for additional applications. The POS terminals are a variant of Schlumberger’s Smart 1000 terminals which display instructions in Chinese and English and use infra-red technology for portability. Its plug-in SAM uses triple-DES encryption and a dynamic session key for secure transactions off-line. Qianflex functions as a debit payment card and as an electronic purse for small transactions and can be reloaded at bank ATMs. The card is compatible with the IC cards issued by commercial banks in China and EMV (Europay/MasterCard/Visa) allowing global interoperability for China’s financial cards. It also has the ability to operate as a multi-application card providing a growth path for new services.

Jack Liu, President of Schlumberger Test and Transactions Asia, said: “This is the largest Smart bank card project in the world, and one of the most ambitious. Qianflex will play a key role in modernising China’s financial infrastructure. Our focus now is to support the trials.”

Contact

- **Patricia Ng** Schlumberger Industries International, Asia
 ☎ +65 746 9676 ✉ patricia @singapore.asia.slb.com

The Sunflower Heads for Nasdaq



In this exclusive interview, SCN's Severine Percetti asks Marc Lassus to unveil what could be the future of Gemplus...

With a production capacity of 900 million cards, an international presence in 27 countries, and applications supplied to 85 countries, the group currently estimates that it holds around 41% of the world-wide Smart Card market. In 1997 the company, again experienced an impressive 40% growth.

This success illustrates the spectacular growth Gemplus has experienced since its creation in Gémenos (France) by Marc Lassus ten years ago. The competitiveness of Gemplus lies in its effort to offer a constantly expanding range of services and applications for its Smart Cards. These include telecommunications (payphone cards and GSM), banking (credit, debit cards, loyalty) and pay-TV but also electronic commerce (electronic purses, payment over the internet), transportation, education, access control, health care and identity.

Gemplus is constantly striving to expand its market share of the international Smart Card market which is still in its infancy. According to a market study the company conducted, the real boom is predicted for the beginning of the 3rd millennium when there will be 1 card for each inhabitant in 2003, compared with 1 card for each 10 inhabitants in 1996¹.

The Smart Card market is indeed young, booming and, is increasingly competitive. As Gemplus retains the world leadership in the design, manufacture and marketing of both plastic and Smart Cards, Schlumberger Electronic Transactions, its main competitor is not far behind: it holds a solid 35% to 40% of the market leaving Giesecke & Devrient GmbH with 13 to 15%.

Since 1996 the market has gone through a major restructuring. Schlumberger grew by acquiring Solaic; NEC and Motorola announced a year ago their entrance into the market; the latter, is interested

in contactless technologies as Sony is, and both have since directed their R&D team this way.

No doubt this fast growing industry arouses the covetousness of industrial giants and it could well see the arrival of newcomers such as Microsoft, IBM, EDS and Intel. Asked in a previous interview if he feared the competition of Microsoft, IBM and EDS, Lassus pointed out that: "Bill Gates (Microsoft) only addresses 1% of the world's population-those who are computer literate. We address 100% including the 60% in Africa and other places who have never used a telephone. Companies like IBM and EDS must integrate Smart Cards into their systems. But they can't be a competitive manufacturer because you have to build volume to do that- and I doubt if they'd ever go into the phonecard business."²

From a volume strategy...

So what is the strategy Gemplus will use to evolve and dominate a continuing and increasingly competitive market environment?

Lassus is not at ease in his new fortune-teller role: when asked what his plans are, he answers with modesty and realism: "we intend to stick to our plans and simply do better".

High production volumes make the strength of the company. This "big thinking" strategy consists of a marginally profitable phonecard business, eroded by a continuing fall in prices. Indeed, as Lassus recognised a year ago³: "The market pressure has resulted in the falling of the price of cards by 15 to 20% every year from FRF 12 per card in 1990 to FRF 2 in 1997".

Building volume is achieved by creating and developing vertically integrated markets in every country. This gradual process is backed up by a constantly upgraded technological choice, from the cheapest electronic tag or phone card, to ultra-sophisticated Smart Cards. This step-by-step pattern lies at the heart of the company's "sunflower strategy".

High production volumes and the subsequent creation of new markets for different ranges of products and services demonstrate the intention of the group to lead on every front.

But maintaining and sustaining an ever-larger market share requires a sizeable manufacturing capability: "The Smart Card market demands the building of a production plant in the distribution area. It is a must," insists Lassus. Hence the high level of capital expenditure spent in 1997: FRF 470 million were spent to increase the manufacturing capacity through the completion of a new plant in France, new manufacturing facilities in Mexico and China and the opening of new Research and Development centres in Asia and North-America. Consequently "Cash requirements significantly increased. In response the company has restructured its capital ownership bringing on board new shareholders⁴. And partly because of these imperatives "for the first time ever, the group's net income decreased, from FRF 140 million in 1996 to FRF 14 million in 1997."⁵

The investment has been substantial and financially heavy. It will enable Gemplus to increase the 1997's capacity of 50 million modules a month. 1.6 million Smart Cards are now manufactured every day of the year in 12 factories as well as 1 million magnetic stripe cards per day.

Yet this additional capacity could well be insufficient to sustain a growing market share. In order to build volume further, Gemplus is also developing tags, a market that could ultimately overshadow Smart Cards, and Lassus predicts a "future made of smart objects". New manufacturing facilities worth US\$50 million in Singapore (including a clean room), India and China have already been planned.

Besides, the logistics might slow down such deployment: chip supplies have already been a source of concern and penalised the 1995-1996 sales: "our sales were US\$460 million, with enough chips, we could have exceeded US\$500 million." declared Lassus in a previous interview⁶.

The "building" volume strategy relies on low margin products: essentially the phonecards and the electronic tags. But microprocessor cards and more particularly SIM cards boosted the sales in 1997 growing by over 57%. In total: "Revenues in 1997 for Smart Cards increased 41% to reach FRF 3.454 billion, while volumes increased 28%"⁷.

Phonecards, GSM and electronic tags will carry on creating volumes and Paul Naldrett, general manager of Gemplus UK, couldn't envisage the telecomms market becoming saturated⁸. However the competition in this field is increasingly strong with Motorola's increased interest in GSM,

Schlumberger and Landis & Gyr both offering payphones, and of course the continuing process of partnerships.

...To a vertical market strategy

If Gemplus builds on volume with low margin products, it is also working at offering a wider range of high, added value applications. More sophisticated applications will certainly grow in the next five years⁹, but they won't generate the same volume on which Gemplus bases its global strategy. Their roll out is slower than expected and consequently the price erosion is likely to carry on.

Their development coincides with a profound transformation of the industry with the shift from proprietary systems to open ones resulting in more competition between card manufacturers, software vendors and system integrators. Asked how he viewed the interest of Microsoft in developing operating systems for Smart Cards, Marc Lassus answers back: "we are aware of this. But we are well positioned to understand the market, particularly in terms of applications. It is up to us to move faster". As for IBM, Lassus is not convinced that the industrial giant wants to develop the market. Anyhow he believes that Gemplus could be "the link to these big USA companies".

Does Gemplus have any choice but to ally itself with software vendors to play an active role in the international standards? Are Java or Multos a source of concern? "These are trends to follow" he says, pointing out that he "keeps his options open" and that "the game is still being played".

Gemplus, on the other hand has to move into software and become a system integrator offering total solutions. "It is a must," emphasises Lassus "and this is what the Sunflower strategy is about: the sunflower, it is Gemplus: the seeds or layers forming the heart of the plant, represent its products (Smart Cards, personalisation services, securisation, hardware, derived products and integrators turnkey products); the petals symbolise the applications in services. Every pound in revenue made at the heart of the flower produces 30 times more in the petals". The stake is important: to remain in control of a versatile market.

Asked what Gemplus' core business will be in 5 years time, Paul Naldrett confirmed Marc Lassus' vision of the future:

Interview

“Still a big part of our core business will be our industrial strength: manufacturing. On top of that a much greater input will be on total solutions, software development, product development for customers. One may even see Gemplus operating applications ourselves”

How long is it going to take Gemplus to break away from a ‘volume strategy’? “It is a gradual pattern,” says Marc Lassus. “It requires changing the culture of the company. 50% of our business is in tools. Our challenge is to make 50% of it in the layers around the heart of the sunflower. In 10 years time it could be 80%. Such change of culture could be coming from the USA market. This explains our intention to enter the Nasdaq market”.

Footnotes

- ¹ See table 2
- ² European Card Review p12 (01/02/1997)
- ³ Les Echos (20/05/97)
- ⁴ New shareholders now include GE Capital (USA) with 5% of the capital, NTT Data Corporation (Japan) with 1%, the Dassault group (France) with 10%, BIA (Saudi Arabia) with 8%, Finno SA (France) (12%), Verpex (Singapore Government) (4%). They join existing shareholders, KDD Corporation (Japan) holding 1%, the Quandt group (Germany) with 33%, Singapore Technologies with 2% and Fleming Ventures Ltd (UK) with 5%. 20% of the capital remains in the hands of employees and founders.
- ⁵ 1997 Annual Report, p 32.
- ⁶ European Card Review p12 (01/02/97)
- ⁷ 1997 Annual Report, p 30.
- ⁸ See table 2
- ⁹ See table 2

Right:
Table 1
[1997 Gemplus
Annual Report p30]

Year ending December 31	1992	1993	1994	1995	1995 Pro forma	1996	1997
Memory cards	357	507	659	627	627	741	885
Microprocessor cards	85	167	324	559	559	1,001	1,573
Contactless cards	-	-	-	13	13	61	67
Magnetic-stripe and other plastic cards	-	-	-	159	440	399	378
Hardware	28	45	60	73	73	75	126
Other	21	33	41	51	51	28	425
Total	491	752	1,084	1,482	1,763	2,305	3,454

Below Right:
Table 2
[Card Forum International
March / April 1998]

Gemplus: Smart Card Market Forecast 2003

Market Segment	1997 million units	2003 million units	Average yearly growth
Phonecards	684	3,270	30%
GSM	69	760	49%
Banking	49	690	55%
Loyalty	22	320	56%
Healthcare	16	210	54%
Pay-TV	12	150	52%
Ticketing	8	240	77%
Gaming	2	70	78%
Access Control	10	260	72%
Identity	2	50	71%
Information technology	1	120	142%
Other	24	170	38%
Total	900	6,310	38%
Comparison with Earth Population	1989:	1 card per 100 people	
+ 7 Years	1996:	1 card per 10 people	
+ 7 Years	2003:	1 card per 1 people	

Smart Cards and Information Leakage

The media has been full of discussions on Differential Power Analysis (DPA) this month for which claims have varied from it doesn't matter through to predictions of the end for Smart Cards. The truth, of course, always lies somewhere in between these extreme views and so this month we will explore the subject and attempt to balance these views.

The story starts with TEMPEST (Transient Electromagnetic Pulse Emanation Standard) a U.S government code word that defines a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. Microprocessors, computers, VDU's in fact all electronic devices emanate radiation through the ether or through electrical conductors. In the early 50's the U.S government became concerned that such radiation patterns may be collected and analysed by an enemy. The use of cryptography could effectively be thwarted if the appropriate information could be successfully reconstructed. Research in the laboratory showed that such signals could be collected at some considerable distance from the source of the emanations and accordingly the Tempest program was started.

Although the subject of Tempest was well known in the defence world it entered the wider public domain with the publication of a land mark paper in 1985 entitled "Electronic Radiation from Video Display Units: An eavesdropping Risk" by Win van Eck of the Netherland's PTT Research Laboratories. His paper showed the successful reconstruction of the image displayed on the target VDU captured at some distance away, even outside the building. It is the use of square wave signals and high switching frequencies in digital equipment that leads to the radiation of electromagnetic fields with frequency components extending into hundreds of megahertz. It is important to note here that although the spectral power of these signals decreases with increasing frequency, that the radiation effectiveness increases with increasing frequency.

The solution to this problem is equally well known and relates to the screening of the equipment by creating an effective Faraday Cage and the filtering of the signal and power cables to reduce their radiating capability. The levels required for such screening and filtering are part of the classified Tempest standard. In this particular case the designer

of equipment receives expert advice on the level of protection required. The designer of cryptographic equipment needs similar advice from experts on the appropriate algorithms and the necessary key lengths.

In the world of cryptographic security another seminal paper was published in 1996 by Paul Kocher entitled "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and other Systems". In this paper he was able to show that by measuring the amount of time required to perform private key operations, that attackers could, in principle, find the key exponents and thereby potentially break the cryptographic system. Although such attacks are in practice somewhat difficult and adequate defences fairly straightforward, the issues raised have none the less much wider implications.

Two years ago Dan Boneh and colleagues from Bellcore highlighted the vulnerability of Smart Card cryptographic implementations to Differential Fault Analysis (DFA). They showed in their paper ("On the Importance of Checking Calculations") how you could take advantage of induced random hardware faults. In particular they showed how you could theoretically break the Chinese Remainder Theorem by such techniques. Again the ideas were not new and in practice are not only difficult to create but are also relatively easy to protect against.

The main point about all these attacks is that the principles are well known. The difficulty for the designer is to ensure that adequate controls are applied to the particular implementation, to ensure that his system is not vulnerable to a low work function attack. Protection controls by their very nature are an overhead and perfect security can never be achieved. Security is an all pervasive subject where one is not only concerned about the strengths of the front door but also whether there is an unattended back door, and in particular, has some new tool been invented that can effortlessly bore a hole in the door.

And now we come to the new paper "Introduction to Differential Power Analysis and Related Attacks" by Paul Kocher, Joshua Jaffe and Benjamin Jun from the U.S consultancy company Cryptography Research. This paper describes a class of attacks against Smart Cards and secure cryptographic tokens based on the analysis of the device's power signal. This involves the use of advanced statistical techniques to reconstruct the processor tasks thereby determining the secret information such as cryptographic keys and PINs stored in the card.

Smart Card Tutorial

As we have already discussed, the concept of information leakage is not new, it is the success that Paul Kocher and his colleagues have demonstrated in applying their new tools to break existing Smart Card implementation that has raised concern.

The monitoring of power consumption to identify cryptographic operation in Smart Cards was first reported by Ernst Bovenlander of TNO at the 1997 Eurocrypt Conference, where he was able to identify the regular structure of the DES cryptographic algorithm. The work of Kocher, Jaffe and Jun takes this much further by being able to determine the actual keys used in the cryptographic algorithms. They show that the operation of the transistors within the Smart Card chip produces observable electronic behaviour. Because the operation of the logic is regularly being synchronised to a deterministic clock pattern, it is possible to identify macro characteristics of the microprocessor operation just by simple monitoring of the power consumption.

So just how practical are these attacks? In their paper Kocher et al first define the concept of simple power analysis (SPA). Here they discuss the monitoring of the power signal using, say an oscilloscope, where they point out that it may be possible, for instance, to visually observe the difference between the squaring and multiply operations commonly used in the implementation of the RSA (or other public key) algorithm. As they point out it is not particularly difficult to protect against this type of attack.

The thrust of their paper is aimed at Differential Power Analysis (DPA) where they use statistical analysis and error correction techniques to extract information correlated to secret keys. The attack requires two phases, the collection of power signal data followed by the data analysis.

In their paper they give an example of a DPA attack on the DES algorithm. As they point out such techniques require a detailed knowledge of the target algorithm and its likely implementation. In the example quoted 1000 samples of the DES operation are stored for analysis where each sample consists of 100,000 data points. The attacker is also assumed to have the relevant 1000 ciphertxts.

A third analysis tool is described as High-Order Differential Power Analysis (HO-DPA). This is described as an extension of the DPA technique where sample data is collected from multiple cryptographic suboperations. Here it may be data from multiple sources (e.g. different Smart Cards doing the same

operation), correlated signals stored using different measurement techniques (e.g. power signal and EMR signal) or signals with different temporal offsets. Clearly such analysis requires an even deeper understanding of the underlying mechanisms. As the authors point out they are not aware of any actual systems that are vulnerable to HO-DPA that are not also vulnerable to DPA.

Cryptography Research is currently licensing their technology to implementers that is resistant to these attacks. Whilst it is possible to modify the hardware of the processor to help mask these unwanted signals it is clear that the actual implementation of the cryptographic algorithms is fundamental to an adequate protection profile. The authors of the paper should be complimented for the success of their research and for bringing it into the public domain because it helps focus the designers of such systems to ensure that adequate protection mechanisms are employed. As history shows the battle will continue but there seems every reason to believe that the seesaw is tipped to the advantage of the designer. New attack methods will always appear but good security designs continuously employ change to ensure that the economics of an attack remain with the defenders. Well implemented Smart Card devices present a formidable tamper resistant barrier, with what should we compare them ?

David B Everett

■ According to a Visa spokesperson, chip technology is the most secure technology available today. HO-DPA was discovered by Visa during due diligence which was being carried out by a third party security laboratory under contract to Visa. There is no economic case for breaking chip technology, no chip is 100% secure but Visa intends to stay several steps ahead of the attackers.

Visa believes the problem to be a security systems issue. Visa has 9 million chip cards in the market place and there has not been a case of any cards being compromised. Visa cash is fully accountable and has an audit trail.

Other News

VeriFone Inc., has signed a licensing agreement with Banksys to integrate the Proton chip technology into its Smart Card payment terminals.

Contact

- **Youri Tolmatchov** Banksys
☎ +32 2 727 6666 ✉ tolmatchov.y@banksys.be

American Banknote Corporation has announced its agreement to acquire 12.5 per cent of Ambient Corporation. ABN Chairman Morris Weissman, says they are excited about Ambient's close-coupled contactless Smart Card technology.

Smart Card International, a Gemplus Value Added Reseller, has introduced a new standalone Smart Card loyalty terminal which can link into the Windows 95-based solution designed for small to medium retailers. Called Gemini, the package costs under £2,500 and includes the stand-alone Gemplus GCR500 Smart Card reader/writer, software and a marketing starter pack of 100 loyalty Smart Cards and leaflets.

Contact

- **Lisa Colley** Gemplus
☎ +44 (0)1705 488037 ✉ lisa.colley@ccmail.edt.fr

Sun Microsystems and over 20 leading retail and technology companies including IBM, Siemens Nixdorf, Telxon and Datafit, have announced the JavaPOS universal software platform - the first Java-enabled specification for point-of-sale devices. JavaPOS enables hand-held scanners, stock taking equipment, kiosks for customer information and checkout tills to interoperate. JavaPOS is available for review on the Web at www.javapos.com

Contact

- **Ann French** Sun Microsystems
☎ +44 (0)1276 416941 ✉ ann.french@uk.sun.com

Gemplus and RS Components are working together to deliver Smart Cards and card readers. Selected Gemplus products are now included in the RS Components catalogue which is also available on web site: rswww.com. Initially customers will be able to order the Gemplus GFM2K, GPM2K and GPM8K memory cards and the GCR410, GC1400 and GPR400 card readers.

Contact

- **Lisa Colley** Gemplus
☎ +44 (0)1705 488037 ✉ lisa.colley@ccmail.edt.fr

Oberthur Smart Cards has joined the MULTOS global supplier network. MULTOS is a multi-application operating system which enables different applications, such as credit/debit, electronic purse and loyalty schemes, to be held securely and independently on a single Smart Card..

Contact

- **Emmanuel Lequenne** Oberthur Smart Cards
☎ +1 310 884 7995



Subscribe to Smart Card News

I wish to subscribe to **Smart Card News**, which will entitle me to buy the **International Smart Card Industry Guide** at the discount price of £70

- UK : £375**
- International : £395**

Please send me _____ copies of the **International Smart Card Industry Guide 1997/8:**

- subscriber : £70 per copy**
 - non-subscriber : £125 per copy**
- Shipping : £7 UK, £10 Europe, £15 Rest of the World

Please send me _____ copies of the **Smart Card Technology in the Asia Pacific Rim 1998 Special Report :**

- subscriber : £80 per copy**
 - non-subscriber : £100 per copy**
- Shipping : £5 UK, £7 Europe, £10.50 Rest of the World

Please send me _____ copies of the **Smart Card Tutorials CD : £150 per copy in the following format (PC Formatted Discs only) :**

- Word 6** **PDF (Adobe Acrobat)** **HTML**
- [Updates October - October upon request]
Shipping: £2 UK, £4 Europe, £7 Rest of the World

Name

Position

Company

Address

Telephone

Facsimile

- Please invoice my company
- Cheque enclosed
- Visa/Mastercard/Eurocard/Access/Amex

Card No.

Expiry Date

Signature

Please return to:

Smart Card News Ltd. PO BOX 1383, Rottingdean, Brighton, East Sussex BN2 8WX United Kingdom
or facsimile : + 44 (0) 1273 624433 / 300991
or e-mail : scn@pavilion.co.uk

Smart Card News carries an unconditional refund guarantee. Should you wish to cancel your subscription at any time then we will refund all unmailed issues.

Smart Card News Technical Services

I would like information about:

- SCN Market Intelligence**
- SCN Website Design Service**
- Advertising in SCN Publications / Website**

Please complete the form opposite

Nationwide EasyPark in Israel

Right:
Hand Held Terminal
[Easy Park]

Below Right:
Golden Crown Smart Card
Payment System
[FTC]



Israel is planning the world's first nationwide electronic parking system which will include 25 cities and over 1.3 million drivers.

EasyPark has signed an agreement with the Israeli Local Government Economic Services (LGES) to implement the scheme using pocket-sized contactless Smart Cards which operate as in-vehicle parking meters.

Motorists will pay for parking throughout the country with a single card and pay only for the time they actually park.

"We expect to provide complete national coverage for the EasyPark program by the end of 1999, with over 500,000 cards by the year 2001," said EasyPark's General Manager, Moshe Mishal. "Our goal is to place tens of thousands of cards in the field during the first months of the program."

The in-vehicle parking meter uses microprocessor-based contactless Smart card technology developed by EasyPark's parent company, On Track Innovations.

Parking inspectors will be equipped with hand-held terminals to check cards through the windcreens of vehicles.

Contact

- **Moshe Mishal** EasyPark
☎ +972 6693 8884 ✉ easypark@oti.co.il

Russia's Golden Crown Card

Zolotaya Korona, Russia's Golden Crown Smart Card payment system has become the largest in Russia, linking over 130 issuing banks and covering most of the country from Kaliningrad to Vladivostok and including Moscow and St Petersburg. So far, over 450,000 ZK cards have been issued (as of 1 May 1998).

The system has 64 processing centres and transaction volume is currently running at 688,000 per month through over 5,000 point-of-sale terminals in shops, petrol stations, hotels, airports and pharmacies, and more than 130 ATMs.

The system software was developed by a partner company, Financial Technologies Center (Novosibirsk, Russia) which has also implemented a number of national payment system projects in some states of the CIS (former USSR), including TurkmenCard (Turkmenistan), AlayCard (Kyrgyzstan) and BaayCard (Yakutia-Sakha Republic, Russia) payment systems. Another ZK card-based payment system is being created in the Mordovian Republic (Russia).

FTC uses point-of-sale terminals from VeriFone (USA), DataCard (USA), Ingenico (France); ATMs from Bull (France), Olivetti (Italy), Siemens (Germany), IBM (USA), NCR (USA), and Solaic E3744 and Gemplus MPCOS-EMV Smart Cards.



Contact

- **Yaroslav Gorbachov** FTC
☎ +7 383 2 399243 ✉ +7 383 2 325019
✉ yg@ftc.ru