

# PISEC '99

## A success at the first attempt

*The Barcelona Hilton was the venue for the recent World Product & Image Security Convention, otherwise known as PISEC '99. John Carson presents an overview of the event.*

**'As an anti-fraud solution provider we found PISEC '99 very informative. From our perspective, we believe that a quality show that highlights the problems of the brand owner is what motivates us to spend our resources on developing new solutions.'**

So said George Phillips of Verify First Technologies, summing up the enthusiastic response from delegates to PISEC '99 organised by Tarsus Conferences in association with LTSI and *Product & Image Security* magazine. With 194 delegates, 55 speakers and 22 exhibitors over the three days of the conference, it's fair to say that the first attempt at a world security convention was a success.

Michael Fairley, the managing director of Tarsus Publishing and Conference Group, opened proceedings by stating that despite 17 security-related conferences and the launch of *Product & Image Security* magazine, the problems of counterfeiting, fraud and brand protection continue to grow.

PISEC '99 highlighted a different subject every day – Government (day one), Branded Goods (day two) and Commerce (day three), with keynote speakers presenting papers in the morning and breakout sessions in the afternoon. The number of delegates attending each afternoon session were roughly equal, but the branded goods presentations were particularly popular.

Sir James Sharples, ex-chief constable of Merseyside and former president of the Association of Chief Police Officers, was the chairman for the first day. In his introduction he said that 'in 35 years I've seen a lot of crudity in criminal activity and I'm not sure that the papers presented will impact on the

daily lives of police constables and customs officers. Much remains to be done in co-operation so this convention is very timely, but should incorporate other interested parties in time to come'.

Sir James was followed by Patrick Ravillard, an administrator in the European Union Commission, Belgium,

**'Enough cigarettes were being supplied to Andorra for every man, woman, child and dog to be smoking 500 a day!'**

who gave delegates the background to the EU stand on product piracy and the EU response to the fight against counterfeiting in the single market. He explained that a Green Paper on Combating Counterfeiting and Piracy

development of information technologies equals the progressive decrease of traditional security documents. This would include the transition from physical currency to plastic money, credit and pre-payment cards and electronic purse.

Ian Walton carried on the European theme in his capacity as head of the VAT Team in the European Commission's Task Force for Anti-Fraud Co-ordination (UCLAF) in Brussels. He asked what can be done to reduce cross border fraud and other illegal trade, and who shoulders the responsibility: Customs & Excise or manufacturers?

'We have to identify fraud and irregularities at the earliest possible stage,' he said. 'The Community's fiscal systems are under attack and it is not a 'corner shop' operation. Imports and exports are difficult to detect and take action against because of the differing jurisdictions of Member States. Huge amounts of goods disappear and end up on the black market.

'For example, enough cigarettes were being supplied to Andorra for

every man, woman, child and dog to be smoking 500 a day!'

Sara Church of the United States Treasury Department offered an insight on counterfeit deterrence technology in US currency. She admitted that an initial error in production was eventually kept as a feature, when nylon fibres that should have been registered were actually randomly dispersed – which makes it harder to counterfeit. The main point Sara made was that public education was the key to eliminating counterfeiting in currency.

Are biometrics an answer to the problems faced? That was the ques-



*Delegates packed the hall for the keynote speakers*

was adopted by the Commission on 15th October 1998, but that 'the phenomenon is significant and on the increase'.

Because of this, Patrick said that a follow-up Communication is taking stock of the consultation process and presenting an action plan for the future, which he envisaged to include legislative measures.

Juan Diaz Lopez of Fabrica Nacional de Moneda Y Timbre, Spain, presented a paper on the role of the security printer in the future and equated security printing to be 'the technical revolution versus the established techniques'. He said that the



tion posed by Dr Stewart Hefferman of TSSI/Association for Biometrics in the first Government breakout session of the afternoon. He stated: 'The document, and its usage, is under attack. The magnetic stripe is very weak in security – the document might be genuine but it's not the legitimate person using that document. Document security does little to protect against fraudulent usage.'

He also explained that adding a biometric template (e.g. name, address, date of birth etc) is very simple and can be applied at one point via standard equipment available in the printer's factory. Regardless of the size of the template, an amount of textual information can easily be accommodated by existing technologies such as magnetic inks and barcodes.

Mark Dikken of Rotaform, The Netherlands, addressed the Commerce breakout session with a talk about papers containing machine-readable features that can be used to detect alterations. He mentioned a paper that is specially made with a patented active and non-active side. On the active side is a special coating that works with laser printing – in fact, the toner adhesion of the coating is stronger than the adhesion of the paper.

This means that if you remove the toner, you will automatically remove the coating which makes the paper active. So in this way alteration with chemicals or mechanical attacks will be highlighted such as cut and paste attacks.

The Branded Goods session included a paper by Ingvar Lamperth of MoDo Paper, Sweden, who started by saying: 'We consider that many anti-counterfeiting solutions are complicated, expensive and difficult to integrate with product graphics and design features.'

'We think many devices can be intrusive, and while they offer much to the manufacturer, they offer little to the customer who cannot see or appreciate the benefits. KISS – Keep It Simple, Stupid!'

He then described the Silverseal security paper which can carry bespoke images in the coating. These images are made in a patented process using raised and recessed images in the backing roll to produce variations in the depth of the coating. The recessed areas result in a thicker coating that appear dark when held up to the light, and under UV light it appears brighter than the surrounding area because there are more optical brighteners present.

Ingvar said that this process is more secure than watermarking for a variety of reasons, one being that conventional watermarks are available from many sources; Silverseal images are produced under a patented process and manufactured only at MoDo Paper's mill.

Day Two was kicked off by Tony Swaffield of the Overland Group, UK,

fended her country's poor record with counterfeit products. She explained: 'China is like a window – open it and western fresh air goes in ... but also mosquitoes and flies that come back out.'

China is an attractive market for counterfeiters to attack, with ten billion people there. Yang said that every company and organisation in China



*Sara Church makes her point*

a brand acquisition company whose main global licence is the brand 'Caterpillar' in respect of footwear. Tony had also spent 15 years with the Trading Standards Service where he took the lead role in major anti-counterfeiting and piracy operations.

'I've been there, done it and bought the fake T-shirt,' he said to laughs from delegates. He told how counterfeits are now made to order in large warehouses, and every footwear manufacturer has problems with China. 'Russia is also a nightmare – it's difficult to convince authorities to chase counterfeiters when there are murders to investigate,' he added.

This was followed by Mark Lange, corporate attorney for Microsoft based in Paris, who defined the different types of software piracy: Counterfeit – unauthorised copies of software and/or documentation; Reseller Piracy – unauthorised copying of software onto computer hard disks; End User Piracy – copying software onto more computers than the number authorised; Internet Piracy – unauthorised reproduction and distribution by electronic means.

He added: 'The good news is we're catching more ... the bad news is there's more to catch.'

The next speaker was Yang Chen, a consultant at the China Trade Association of Fake Prevention, who de-

has a seal which is like the president's signature of a western company. Now counterfeit seals are appearing, even though major anti-counterfeit devices like holograms have been used in China since 1990.

Tony Bol of General Motors, USA, presented a paper on countering the global unauthorised replacement part problem (US\$12 billion lost annually), and said that 'in the automobile industry there is a tendency to believe that the duplication of specific parts by the counterfeiter is not possible because of the high-tech research, development and manufacturing processes required.'

'It is felt that these requirements are too complex and therefore too costly for the counterfeiter. This is not true and is a costly mistake. The counterfeiter does not need to manufacture a quality product; in most cases they will purchase the least costly material or part available and pass it off as the genuine article.'

'The replacement cost of a faulty part, warranty work, loss of market share and reputation is borne by the legitimate trademark holder, not the counterfeiter.'

He added with a wry smile: 'We can't compete with our own trademarks because the counterfeit stuff is being sold cheaper!'

*continued on page 34*



## PISEC '99

### A success at the first attempt

continued from page 33

Dr Peter Harrop from PINACL, UK, spoke about low cost RFID tagging. He said that it differs from EAS in that the latter is just an anti-theft tag that does

into the UK, where fraud increased there!

Dorothy Higginson of the Smart Card Club, UK, talked about citizen cards and Government Strategic Directions for smart cards. She defined a citizens' card as a multi-application platform which allows a mixture of public and private sector applications to co-reside in one card. People may use it for parking, bus travel, shopping and many other activities.

evening around 160 delegates attended an informal dinner at Barcelona's Olympic Port where three awards were presented by Mike Fairley and Jeremy Plimmer.

The PISEC '99 World Product & Image Security Award for Product Authentication went to MoDo Paper for Silverseal. Barco Graphics won the Counterfeit Deterrence award for its Fortuna system, and Portals (Bathford) picked up the Brand Protection award for ThermoText.

The delegates were 'roughed up' on the third day by Guy Johnson, former head of the largest cheque and credit card fraud squad in the UK. He criticised a lot of the technologies on show by saying that this was not the only answer: 'You can change the data on a credit card even though a hologram is there - so it technically looks like a credit card, but with someone else's name.'

'The criminal has not got brand loyalty ... he will attack anyone. Bank products such as cheques and cards do have built within them security features that deter counterfeiters. That is not to say that these documents are not counterfeited, but it is far easier for the criminal to circumvent the system of how they are issued, and therefore devaluing its integral security.'



Above: The team from Barco Graphics receive their award for Counterfeit Deterrence for their Fortuna system from Jeremy Plimmer and Mike Fairley

Below: Tony Swaffield, Overland Group; Mark Lange, Microsoft and Jeremy Plimmer, LTSI

not provide ID, it just says it's there, whereas RFID uses data.

He mentioned that prices are coming down and devices are getting smaller. Some new ones are like tiny silver dots or postage stamps, which means that for the first time the technology can be useful in security printing and jewellery.

Brand protection with low cost RFID can take many forms: a tag hidden in a designer product during manufacture can help control counterfeits and grey markets; electronics can automatically monitor whether the right labels are on the right pharmaceuticals and so on. This is all becoming more affordable.

In his presentation, Ed White of Thorn Secure Science International, UK, quoted Brian Bayliss of MasterCard who said: 'Things move so slowly - we wish the fraudster moved as slowly as us and then we might have a chance!'

Ed also explained how the French had introduced chips onto cards which decreased fraud. This was not due to less criminal activity, but because the fraudsters moved over the 'border'



Obviously with a project like that, security becomes an issue, and Dorothy said that her organisation had to seek sign-off from the Data Protection Registrar to ensure that individuals' rights are not being contravened.

It wasn't all work and no play. In the

Lewis Endlar of Manchester Metropolitan University, UK, gave a worrying paper about the threat of electronic crime in the workplace. He mentioned eavesdropping as the collection and interception of data, especially on the Internet; people who assume another's identity to purchase goods online and



never pay and Trojan Horse software in the form of a computer virus that is installed on a server for the purpose of accruing information about transactions.

He said that technology can also be used to fight back. A number of photocopyers such as those produced by Canon include a specially programmed microchip that recognises currencies – if someone attempts to copy

## **'We can't compete with our own trademarks because the counterfeit stuff is being sold cheaper!'**

the currency, the copier prints a black sheet of paper.

Other techniques employed to fight electronic crime include encryption, authentication using a digital certificate and secured electronic transaction.

Pharmaceutically secure? That was the question posed by Keith Barnes of Packform, UK, who mentioned a toiletries company that produces a third more stock than needed just to account for 'lost product'. Tagging is not always the answer.

He recalled a case in Canada of a pair of shoplifters working together. The woman would put twelve tagged items in her bag, whilst her male friend carried one item. They would both walk through the exit at the same time thus setting off the alarm. 'Oh dear,' says the man attracting attention, 'did I forget to pay?' He would walk back to the checkout and pay whilst his accomplice just kept on going with their haul.

The next speaker was Dirk Schuurman, a chief inspector in Interpol, The Netherlands, who gave delegates a comprehensive history of counterfeit currency and mentioned the problems of producing the Euro in different locations. He said: 'It is to be expected that organised crime will be focusing on the new Euro notes in order to make exceptionally good counterfeits.'

'Harmonisation of the laws and legislation in the various countries is necessary. Issues, such as copyright in banknotes and coins, must also be settled so as to give the police adequate legal tools to take effective action. A coin with two national sides gives many legal problems.'

Quite a technical paper followed, presented by Hiroyuki Matsumoto of NHK Spring Company, Japan, in which he talked about document protection by micro-fibres and crypto-

graphy. He made two points: that experienced techniques and/or expensive facilities are not enough for anti-counterfeiting; and there is a necessity for authentication systems which are equipped with higher security.

His solution was FibeCrypt, a machine-readable authentication system that combines magnetic micro-fibres and cryptography. At an issuing procedure of a medium, a micro-fibres detector scans a pattern of micro-fibres which are distributed throughout the medium.

The signal is processed and transformed into a reference data and is then recorded on a storage unit with a read/write head. For authentication purposes, the pattern of micro-fibres is transformed into a target data by a similar procedure as the reference data. The two sets of data are compared with a pattern matching scheme, and the system decides whether the medium is valid or not by a degree of similarity.

Anti-counterfeiting strategies for alcoholic beverages was discussed in

## **'I've been there, done it and bought the fake T-shirt'**

the final paper by Laurie Sherwood of Diageo. It is a serious problem, with around US\$14 billion lost every year to activity of this type.

Laurie recounted a story in Guatemala where a man died after drinking fake spirit. At his funeral, 29 guests drunk from the same stock and died themselves! Counterfeiters don't care who owns the brand, but just how successful it is. She said that in some countries the counterfeiters even buy tax stamps from the authorities, which shows just how widespread corruption is. If the authorities won't co-operate in stamping out counterfeiting, then who can?

This was a worrying note for a very successful conference to finish on, but the signs are that new technologies and solutions are being developed every day to beat fraud and counterfeiting, and eventually the good guys might just win the war, if not the battle.

- Due to space limitations we can only cover a selection of the 55 speakers at PISEC '99, but a full set of conference papers can be obtained for £500 from Carrie Jones at Tarsus Conferences on 01707 653389, fax 01707 654550, e-mail [carrie.jones@tarsus-publishing.com](mailto:carrie.jones@tarsus-publishing.com).

Reader enquiry 45

## **Some quotes about PISEC '99**

'Well attended – well done. The Branded Goods day, in particular, had several good papers.'

**Lew Kontnik,  
Reconnaissance International**

'From the outset I was impressed with the convention/exhibition – not only with planning and attendance, but also with the timeliness and relevancy. It was a good example of government agencies and the security industry coming together to discuss, resolve and disseminate the threats facing the business. I am sure the convention will go from strength to strength.'

**Sir James Sharples**

'This was the first event where (in this segment of business) MoDo Paper attended and exhibited at the same time. Due to the 'young and unique' product we found it very useful, and developed some very good contacts during the three days.'

**Ingvar Lamperth, MoDo Paper**

'The conference was a good opportunity to obtain information on the wide variety of security technologies on offer for product security and brand protection.'

**Elke Leidl, Giesecke & Devrient**

'The conference provided a useful opportunity to see first hand latest developments in document security, and to make contact with industry specialists. Some of the presentations were extremely interesting, and I especially welcomed the provision of detailed notes of the more technical papers. Overall, the conference was definitely worthwhile.'

**Mandie Campbell,  
National Forgery Section,  
UK Immigration Service**

'Congratulations on a successful show. A professionally organised and extremely well attended conference and exhibition which was an eye-opener for myself who has always previously attended and exhibited solely at holography-related conferences and shows: To talk and listen to both potential and existing high level users of holograms that one would not normally meet was both interesting and very good exposure for my company and our products. The quality of papers and discussions was also of the highest level and certainly educational for myself.'

**Steve Kyle,  
Westmead Technology**