Featured this month

Online banking - catch 22

UK bank, HSBC, will not give up pushing online banking, despite the threats from organized gangs against Internet users, said the banks' Group Operating Officer, Alan Jebson, at the recent E-Crime Congress in London.

"We want to see as many customers as possible using online banking," said Jebson. "Going online has increased productivity," he said. However, the bank is engaged in a constant cat and mouse game to stop electronic fraudsters exploiting the new system loopholes to steal money.

HSBC has 18.9 million Internet registered users to safeguard, some of which have already been tricked into exposing their account details to phishers, said Jebson. "Customers are no longer sure that emails sent from banks are genuine."

In fact consumer mistrust is directly affecting the takeup of online banking services according to analyst firm, Forrester. To combat phishing and other threats HSBC is in daily contact with law enforcement to get dubious sites closed down.

Also, in an industry response the financial services sector as a whole is moving towards two-factor and three-factor authentication.

"But the harder we make it for criminals, the more inconvenient it is for customers," said Jebson.

Two-layers of biometric measurements to ensure security

One biometric can’t do it all...

Biometric technology is being embraced by Governments as the way to fight identity theft and potentially shield us from terrorist attacks. The UK Government is likely to push through an Identity Card Bill, that would insist on all UK citizens having biometric-based ID cards. The US is calling for all visitors to the country to have biometric-based passports. Demand for biometrics is growing whether the technology is ready or not.

Professor Richard Walton, former director of the CESG analyses the pitfalls of biometrics. He examines whether the use of one biometric measurement is enough for many applications. He delves into the probabilities of false positives arising as well false negatives. He sets out why the combination of different biometrics is a good option. The author also examines how biometrics based on behavioural measurements can complement physiological biometrics. Turn to page 6...
Online banking: catch 22

Continued from page 1...

But even after technical systems are in place to identify criminals, they can still escape said Jebson. Money mules, recruited by criminal gangs are a key link for the transfer of money in online frauds. The mules are enlisted through websites, where job descriptions request the applicant to have a bank account. HSBC has introduced a new fraud detection system to cope. But catching the money mules doesn’t solve the problem as they are hard to prosecute, said Jebson.

"Banks and government need to work together to get better legal support.”

Trojans are another worry for HSBC, said Jebson as they don’t rely on users to give away data.

In response, “customers will have to play more significant roles,” in securing their data.

Already they “are becoming wiser to PC security issues,” he said, “But some still don’t have firewalls or anti-virus.”

Last year HSBC faced 100,000 virus attacks in one day alone but Jebson did not highlight this as the bank’s biggest IT security risk. "The primary e-threat used to be hackers," he said, "but it no longer keeps us awake at night.”

2.4 billion lost to hi-tech crime

Brian McKenna

Last year British business lost £2.4 billion to electronically-enabled crime, the National Hi-Tech Crime Unit has said.

The Unit made the claim at its E-Crime Congress in London on 5 April. According to a survey conducted by NOP, 89% of a sample group of 200 companies said that they had experienced some form of hi-tech crime during 2004.

Highlights of the report:
• 90% of the 200 companies suffered unauthorized penetration of company systems.
• 89% suffered theft of information or data.
• 97% were hit by virus attacks which had cost them £71.
• financial fraud had cost nine per cent at £68k.

The survey also found that more than a quarter of companies failed to undertake regular security audits.

Detective Superintendent Mick Deats, deputy head of the Unit said: “Over the past year, we have seen a sustained increase in the professionalism of cyber-criminals scope of the problem that we will be able to build effective strategies to deal with it.”

Trevor Pearce, director-general of the National Crime Squad, told delegates at the congress that “thirty five per cent of the companies surveyed have no crisis management procedures, which are, as we know from long experience in the off-line world, essential in extortion situations”.

He went on to confirm that the Serious and Organised Crime Agency (SOCA), planned by the outgoing Labour government, will take on responsibility for the “international and organised end of hi-tech crime” from the Unit, when it is launched.

Firearms expert in charge of National Hi-Tech Crime Unit

The former head of Firearms at the National Crime Squad has been appointed to the top position in the UK’s National Hi-Tech Crime Unit. Detective Chief Superintendent Sharon Lemon replaces Len Hynds, who has been promoted to Assistant Chief Constable with the National Crime Squad as Business Change and Transition Director.

Sharon Lemon started her career with the Metropolitan Police, and served at many busy inner London divisions at all ranks, until she joined the National Crime Squad (NCS) in 1999. As the Head of Firearms she is recognized as transforming the armed capability to one
where the NCS is seen as good practice nationally.

She was head of the Paedophile On-Line Investigation Team (POLIT), the national and international single point of contact for child abuse on-line investigations. She also played a key role in the formation of the Virtual Global Taskforce (VGT), an international law enforcement collaboration comprising Australia, Canada, Interpol, the UK and the USA.

Lemon said, in a statement: "I am relishing the challenge of managing the Unit which tackles all aspects of hi-tech crime and criminality .... During its first four years, the Unit has established a clear presence in this field and built an outstanding profile nationally and internationally. I am keen to build on this excellent start."

Citibank call centre fraud reveals Indian data protection deficit

Brian McKenna

The Indian business process outsourcing industry fears a Western backlash in the wake of a fraud incident that targeted Citibank. Three former employees of Mphasis, a Bangalore-based outsourcing company, and nine accomplices allegedly stole more than $350,000 from Citibank account holders in New York. The would-be fraudsters were arrested by Pune police after an alert by a Citibank official.

Nasscom, India’s IT industry lobby group, has moved to set up a national employee registry dubbed ‘Fortress India’. This voluntary register will be in operation before the end of May, and will enrol the 350,000 Indians who work in BPO.

Industry commentator Krishnan Thiagarajan, writing in the Hindu Group Publications’ eWeek, said that while US protests over jobs lost to outsourcing died down after the presidential elections, the ‘key issues relating to data security and privacy [have been] left unaddressed by the Indian government’.

“[T]he latest fraud exposes the soft underbelly of data security in BPO outsourcing”, he said, and called for Nasscom and the Indian government to act to put in place a ‘comprehensive data protection law’ as well as screen candidates.

Meanwhile, the Indian Express sought to downplay the significance of the fraud, citing the US investor site, The Motley Fool’s observation that ‘the facts of the Mphasis case suggest that in some cases, data may be safer once sent abroad. Reflect for a moment on how quickly the alleged criminals in Pune were caught’.

Reuters IM service shut down by worm

Financial news provider Reuters was forced to shut down its instant messaging service on Thursday 14 April to stop the spread of a back-door installing worm.

The service, which has 60,000 users, was the victim of Kelvir-U. Reuters offers the IM service to financial clients along with its news and information services. It said that the worm was not specifically designed to attack the service, which is based on Microsoft’s Windows Messenger client.

The Reuters service was back in action by 7am on Friday 15 April. Francis DeSouza, chief executive of IMlogic, an instant messaging security and management company told Internet Week that “the Kelvir worm attacked only version 3.1 client of the Reuters client, not version 4.0. Large customers, who had mostly upgraded, were okay.”

IMlogic has also said this was the first instance where a virus has targeted a privately controlled user community.

The Kelvir-U worm sends an IM to contacts on an infected user’s contact list, encouraging recipients to click on a hyper-link that invokes a back-door installing worm, Spybot.

The Kelvir worm that knocked out Reuters is only the most recent in a long line of variants that have appeared in the last six weeks. Symantec says that two dozen different Kelvir worms have cropped up, all of which target Microsoft’s MSN Messenger and Windows Messenger.

Please turn over...

In brief

Ralph Lauren shoppers get more than they thought

Customers who have used their GM branded MasterCard in Ralph Lauren recently might well be contacted by their card provider. Not to tell them of a special deal, but to break the bad news that they are one of 180,000 customers whose credit card information has been accessed by criminals, stolen from Ralph Lauren Polo Corp.

HSBC North America has been contacting owners of the card to warn them that their data may have been stolen. While Ralph Lauren has not yet admitted liability, The Wall Street Journal has quoted an insider saying that the information was stolen from the famous purveyor of American casual wear.

Microsoft’s April patches

April showers rained down on patch management teams thanks to Microsoft’s latest update. Consisting of eight patches for twelve vulnerabilities, five of which were classed as critical, the update contained patches for problems in Internet Explorer, Word and MSN Messenger as well as for Microsoft’s TCP/IP stack.

Banks fight the Phishers

Facing losses of up to $500m a year, banks are finally starting to invest in technology that is fighting the war against phishers. Phishing, the creation of websites masquerading as legitimate banking sites, is responsible for an increasing amount of fraud and thefts from banks and customers.

Technologies being implemented include software that enables a bank to tell if someone is ‘casing’ its site in order to replicate it for a phishing site.

CAN-Spam used against gang of four

Four US citizens are being prosecuted using the recent CAN-Spam legislation, after allegedly sending hundreds of thousands of emails offering weight-loss programmes. Over 10,000 complaints were received about the defendants use of email.

US federal employees get chip ID

Biometric information is going to play an integral part of the ID badges that all US federal employees will receive later this year. In another attempt to increase security in the US, staff’s ID badges will contain information such as digital fingerprints stored in a chip. The badges will also have the facility to add different levels of security clearance and enable employees to access government buildings other than their own.
In brief

**Research network used for file sharing**
Internet2, the superfast version of the internet being used and tested by US universities, is apparently being used for illegal file sharing of music and films.

The Recording Industry Association of America has said that it intends to file over 400 lawsuits against students using the network for file sharing and illegal downloads of pirated material.

**Cops bust Estonian for ebank theft**
Estonian police arrested a 24-year-old man they suspect stole millions from online accounts across Europe using a virus that deleted itself once it had done its job.

The alleged thief wrote seemingly genuine letters from government institutions, banks and investment firms, but which actually contained a link to a page that uploaded the virus. The virus then transmitted their personal information, including internet banking account numbers and passwords, back to him and deleted itself after emptying the accounts. The man faces five years’ prison.

**eBay scammer get six years**
A federal judge sentenced Charles Stergios, 21, to more than six years for scams on internet auction site eBay that cheated 321 people out of $421,000. The judge earlier rejected a plea bargain after Stergios threw a jug of water across the courtroom at a prosecutor who called him a thief.

**Phishermen take up pharming**
Pharming is a new scam that secretly directs computer users from a legitimate, free, blogging site, hackers are able to fill their page with keylogging software or malicious code. They then send out their blog address via spam or through an instant messaging service, even targeting particular individuals - and as soon as someone visits the page, they are infected, or spied on.

Websense Security Labs have released details of toxic blogs to warn consumers of the "hundreds" of occurrences on the Internet. Given that most blog sites do not have protection for the files that they host, it is an easy way for hackers to disseminate their wares, requiring only social engineering to get people to look at their pages. And the popularity of blogs is such that this is getting easier.

**Welcome to the toxic blog**
The accessibility of Web logs, their anonymous nature and potential global readership has long been a draw for aspiring writers, lobbyists, pained teenagers and angry workers. Add to that the large storage capacity, and it is no surprise as to why blogs have become such a phenomenon. Unfortunately, the hackers have noticed this too. Welcome to the toxic blog.

By creating a blog from a legitimate, free, blogging site, hackers are able to fill their page with keylogging software or malicious code. They then send out their blog address via spam or through an instant messaging service, even targeting particular individuals - and as soon as someone visits the page, they are infected, or spied on.

**Disclosure — time to ask the users**

Eric Doyle
The circular debate around the ethics of vulnerability disclosure needs customer input

Vulnerability disclosures hit the headlines in April when Sybase appeared to threaten UK security research firm Next Generation Systems Software (NGS) with legal action. NGS found eight security holes in Sybase’s Adaptive Server Enterprise (ASE) database last year and reported them to Sybase. After fixes were released in February and time had been allowed for customers to apply them, NGS said it would publicly release details of the flaws.

The database company took exception, and argued that security bug hunting comes under the banner of database performance testing and benchmarking. Publishing the results from such tests without permission is specifically prohibited under the licensing agreement for Sybase ASE.

Several days later, NGS was allowed to co-publish edited details with Sybase. Sherief Hammad, a founding director of NGS, said that it was an amicable agreement. He added that this would not change the way NGS works in the future as he feels the company always acts responsibly.

Sybase insists it was all a misunderstanding and is now reviewing its policies regarding vulnerability research. Kathleen Schaub, vice president of marketing at Sybase, says it will work more proactively and co-operatively with researchers in the future.

The incident underlines the uneasy relationship between researchers and software vendors. This is rooted in the belief that researchers are little better than hackers. Though some people are willing to give researchers credibility, this is not the view of Marcus Ranum, a security advisor He disputes the term ‘researcher’ and regards those who claim the term as self-seeking opportunists at best.
ChoicePoint saga repercussions

Not an information security breach?

Philip Hunter

Fall out from the ChoicePoint debacle in the US continues to reverberate around the IT security world and beyond. The case surfaced in February 2005 when the company revealed it had fallen victim to a major scam allowing identity thieves access to personal data on at least 145,000 consumers and possibly as many as 500,000. This has stoked the smouldering debate over the relative rights of individuals and agencies over control of personal information and over who is responsible for monitoring access to it. It has also called into question the boundary between strict technical IT security and the broader issues of identity fraud.

Disaster for entire information brokerage industry

In many respects it was a disaster not just for ChoicePoint and potentially many of its customers, but also the whole information brokerage industry that has mushroomed during the last decade, especially in the US. The case highlights how vulnerable our identities have become and the lack of regulation over the agencies entrusted with it. And it is at least stimulating healthy debate over how to protect personal information without constricting the electronic commerce and financial sectors that have become utterly dependent on real-time access to such data.

Who ever heard of Choicepoint?

ChoicePoint, based in Georgia, is one of the world’s largest data brokers or aggregators. Only a tiny minority of consumers whose data is held by it had heard of the company until it disclosed the security breach in February four months after it had been discovered. Equally, few of the consumers were aware that so much personal information had been concentrated in a single data repository comprising 19 billion records. This extends well beyond credit reports and includes:

- Court records.
- Bankruptcy proceedings.
- Driving records.
- Consumer demographics.
- Lifestyle data.
- Employment background checks.
- Tenant rental history.
- Insurance claims.
- Social security numbers.
- Dates of birth.

In short, ChoicePoint collates just about all personal information that is in the public domain and a good deal that is not so readily available. In Europe the information brokerage business is not quite so well advanced, with no single repository with as comprehensive a data set as ChoicePoint. But many of the same issues apply, and the ChoicePoint case is just as pertinent in highlighting the growing risks involved in the personal information trade.

That hurt!

The impact of the breach on ChoicePoint itself was all too obvious. The disclosure was followed by a 20% fall in its share price, and then there are the huge costs of having to alert initially 145,000 Californian customers, plus 110,000 more in other states, that their personal records had been compromised. On top of that there are lawsuits to defend, and possible damages to pay. A number of lawsuits are pending, involving class actions on behalf of consumers whose identities have been compromised, arguing negligence on ChoicePoint’s part.

Response

Most serious of all is the longer-term loss of confidence in ChoicePoint’s ability to manage and protect so much data. The company has been quick to respond in several ways. ChoicePoint has stopped selling personal information, except when this is clearly for the benefit of consumers, for example to a well established bank seeking a credit reference. It has also appointed Carol DiBattiste, formerly deputy administrator of the US Transportation Security Administration, to look after privacy and authorisation of access. This was more to regain trust by having an external security advisor removed from the company’s day-to-day running, than to beef up security.

No IT security breach?

Indeed a bizarre aspect of the case is ChoicePoint’s assertion that there had
been no information security breach, that instead it was a conventional fraud of the kind that happens every day. This is extremely disingenuous, and not helpful to the cause of information security. It is true that there was no hack in the technical sense. A group of thieves registered 50 fake companies as ChoicePoint customers, and from that point on were able to help themselves legitimately to almost all the data they wanted. No amount of encryption or authentication would have helped at that stage.

But technology these days is only the tip of the information security iceberg. It is easy enough to make a system totally impregnable in theory, but the much harder task of the real world involves allowing legitimate users to go about their business relatively unimpeded while detecting and combating abuses. This involves procedures and policies beyond technology, and ChoicePoint has tacitly admitted culpability on these fronts through moves such as DiBattiste’s appointment.

### ID theft opportunities

However the information security issues go beyond ChoicePoint to the whole basis of modern commerce, highlighting the growing problem of identity theft. According to the UK consumer group Which, identity theft now costs the UK economy £1.3 billion annually and is rising fast, having so far afflicted one in four adults one way or another. One problem is that identity data such as dates of birth and national insurance numbers cannot be changed, unlike passwords. This is why there has been so much concern among the consumers affected by the ChoicePoint case, who fear they could fall victim to a variety of frauds for years to come.

Identity fraud can take various forms. It can lead to obtaining of credit cards, bank accounts or telephone service in the name of the victim, or it can involve taking over someone’s existing account by fraudulently executing a change of address. It can even result in a complete identity take over for fraudulent assumption of financial and other benefits. These may include renting property and obtaining benefits such as free dentistry or medicines normally only available to people on low incomes. Another problem is that theft of identities, unlike say credit cards, often goes undetected for a long time, sometimes over a year. This increases the exposure of the liable parties, whether this is a bank, insurance company, or in some cases the customers themselves. Therefore banks and others are striving to improve detection rates by various means, for example through identification of unusual transaction patterns or other anomalies.

The most common identity frauds so far have involved simple theft of personal details for withdrawing cash from victims’ bank accounts, or making purchases on their credit cards. But this can be readily stopped by issuing new PINs and account numbers to customers in the event of a large-scale breach such as the ChoicePoint fraud. For ChoicePoint victims, the greater risks involve accessing of credit status reports for various motives including obtaining basic credit.

### Freezing

This however can be stemmed at least temporarily by imposing a security freeze on specified consumers, prohibiting any third party from accessing certain personal details on them.

In California, and also Texas, consumers have the right to freeze their credit reports at any time in this way, and then lift the freeze when they are applying for credit themselves. Consumers therefore can exert some control over their credit reports and ensure they are available to a bank to which they are applying for a new credit card, but not to any third party without their knowledge.

In the long term however security freezes if widely deployed would impede the processing of applications and references for credit that often take place in the background without consumers’ knowledge. Civil libertarians though would no doubt consider this a price worth paying. In this case, ChoicePoint has imposed its own security freeze by suspending the sale of information products that contain sensitive consumer data, and estimates it will lose $15 to $20 million revenue in 2005 as a result.

### Security freezes could impede identity fraud

#### The pain of the Choicepoint fraud debacle:
- The shareprice of the data aggregator plunged by 20%.
- Shareholders file a class-action suit against the company and its executives.
- Company executives are being investigated by the Securities and Exchange Commission for hasty share deals.

#### Making it up:
- Choicepoint has withdrawn the sale of citizen information that contains sensitive data.
- The company has created an independent office of Credentialing, Compliance and Privacy.

### Bankruptcy

But the case has also stimulated debate over longer-term issues surrounding identity. In particular it has focused attention on the relative ease with which personal information can now be gathered and then sold. One loophole likely to be closed in the US is the lucrative and freely available personal information about people who have
Security concepts for biometric measurements

There are four security concepts that are important for this discussion. These are the False Acceptance Rate (FAR), the False Rejection Rate (FRR), Entropy, and Secret Data. In this section I shall define these four concepts and make general remarks about their relevance to biometric security mechanisms.

FAR

The FAR is the probability that a biometric system will accept a measurement as genuine when it is in fact not. It is typically presented either as a percentage value or as a probability in the range 0 to 1. A typical biometric system based on a single measurement (for example measuring a single fingerprint) will have a FAR between 0.1% and 2% (i.e. probability between 0.001 and 0.02). For most applications the FAR is the key element in providing security. However, FAR does not give the whole picture and sometimes it is necessary to consider other factors.

No consumer control

Another loophole, in this case shielding the information brokers themselves, is the lack of a business relationship with the consumers whose data they hold. Apart from the security freeze option in Texas and California, consumers have no control over the gathering or sale of that information, providing basic data protection guidelines are adhered to, and yet can suffer when breaches occur. Furthermore they often lack the legal rights they would have if they were customers. For these reasons one proposal is to give the brokers an economic incentive to maintain tight security by imposing fines when breaches occur. Brokers are also likely to be required to disclose when breaches occur, as they are already in California. These two measures would give brokers the incentives often lacking at present to be secure and be seen to be secure.

More questionable are plans to give consumers greater control over their personal records. In practice few would exercise such rights to their advantage and there is also the danger of introducing an administrative quagmire. Giving consumers too many rights can be counterproductive, as has been shown in the case of general compensation claims where about two thirds fail even in a relatively favourable litigation climate, because so many are frivolous or wildly over optimistic. The result is a huge waste of public money. However, the ChoicePoint case does suggest that allowing consumers to impose security freezes could significantly impede identity fraud without too much inconvenience if they are applied sparingly and only when risk of fraud has been identified.

The ChoicePoint fraud has also been valuable in another sense, by highlighting how we now have very little control over who does have access to personal information that may not facilitate identity theft but can compromise what services we may be granted and on what terms. At present medical records remain largely outside the grasp of information brokers, in the UK at least, being still paper based to the extent that they are not always even available to health practitioners when required. Now is perhaps the time to ensure that our medical records are not made available for sale in the same way as our credit status to potential insurers or whoever might want to access them.

Combining biometric measurements for security applications

Professor Richard Walton CB

In the current security environment Governments and others are looking to Biometric technology to improve identification processes. Some of the potential applications have significant implications for civil liberties. There is legitimate concern about the efficacy of the technology and of the decision-making processes resulting from interpretation of biometric measurements. Claims are often exaggerated; by technology vendors and by both advocates and opponents of the use of biometrics for such purposes. This paper examines some of the issues arising from the application of biometric measurements for security applications. Specifically there is concern that use of a single biometric measure is inadequate for many potential applications. Important questions considered include the use of Entropy to compare the security properties of a biometric system with a traditional password system based on secret data and the use of statistical models to underpin security claims. The paper is based on a report commissioned by Senselect Ltd to examine the effects of using two or more biometric measurements for security applications.

Security concepts for biometric measurements

There are four security concepts that are important for this discussion. These are the False Acceptance Rate (FAR), the False Rejection Rate (FRR), Entropy, and Secret Data. In this section I shall define these four concepts and make general remarks about their relevance to biometric security mechanisms.

FAR

The FAR is the probability that a biometric system will accept a measurement as genuine when it is in fact not. It is typically presented either as a percentage value or as a probability in the range 0 to 1. A typical biometric system based on a single measurement (for example measuring a single fingerprint) will have a FAR between 0.1% and 2% (i.e. probability between 0.001 and 0.02). For most applications the FAR is the key element in providing security. However, FAR does not give the whole picture and sometimes it is necessary to consider other factors.
consider the statistical distribution of the false acceptances in greater detail. Much of the literature makes no explicit mention of this statistical distribution but assumes an underlying random model based on a normal distribution. For many current purposes this is good enough but there could be problems with large-scale operations. In any application it is also necessary to consider detailed attack scenarios which will depend on the implementation of the biometric system, the environment in which it operates and the capabilities of the potential attacker.

**FRR**

The FRR is the probability that a measurement of the biometric from a genuine source is rejected by the system as false. Like the FAR, the FRR usually is reported as either a percentage or as a probability between 0 and 1. Biometric systems tend to be set up with an FRR larger than the FAR. A typical range might be 1-10%. For most applications the FRR does not directly affect the security offered but is a hygiene factor affecting the cost and acceptability of the system. For this reason in [2] CESG ignores the FRR in making recommendations on the security offered by a biometric system. For the applications that would have been foremost in mind when [2] was written, this is understandable. However it is actually wrong for the general case. As we shall see in section 5.4 of this report, there are important applications where the FRR is the crucial security parameter and the FAR provides the hygiene factor. The remarks made in 2.1 about measuring FAR apply equally to FRR.

**ENTROPY**

The entropy of a biometric system is a measure of the uncertainty of the outcome of a random measurement, given the prior knowledge available to the observer. Thus entropy is not a function of the system alone but also factors in the observer). If the observer knows a measurement has n possible outcomes with probabilities $p_1, p_2, \ldots, p_n$ respectively the associated entropy measured in bits (binary digits) is given by:

$$E = \sum_{i=1}^{n} q_i \log_2 1/\pi_i.$$  

For example for a single throw of a fair die the entropy is $\log_2 6 = 2.585$ bits.

This is all very well as far as it goes but often we are looking at a slightly different scenario where we are not concerned so much with the outcome of the measurement but with the measurement giving a specific (acceptable) value. This requires a slightly more complicated model. Suppose the observer can divide the measurements into n categories for the category i (1 < i < n). Suppose also that from the point of view of the observer the probability of the measurement being in category i is $q_i$. Then the entropy would be given by:

$$E = \sum_{i=1}^{n} q_i \log_2 1/\pi_i.$$  

To illustrate the concept, let us now consider the situation for a single biometric measurement with FAR = $p_A$ and FRR = $p_R$. We are concerned with the biometric measurement being accepted as genuine rather than the value of the measurement. Thus, assuming that the distributions of false rejections and acceptances are random (normal model) the entropy from the points of view of a genuine subject ($E_G$) and an impostor ($E_I$) would be:

$$E_G = \log_2 1/(1-p_R)$$

$$E_I = \log_2 1/p_A.$$

An FAR of 1% and FRR of 5% would yield $E_G = 0.074$ bits and $E_I = 6.64$ bits. An independent observer who believed a genuine person or an impostor to be equally likely would see a different entropy:

$$E = \frac{1}{2} \log_2 1/(1-p_R) + \frac{1}{2} \log_2 1/p_A,$$

(which in the above example would be 3.69 bits).

The importance of entropy is that it allows us to compare the strength of different systems against random attacks, which in turn gives us a baseline for comparisons between dissimilar security mechanisms. For example, entropy can be used to compare multi-fingerprint biometric systems with traditional passwords. On the other hand it can be seen from the above that entropy is highly dependent on the specific scenario envisaged and a great deal of care must be taken when making calculations. It is sometimes helpful to think of the entropy as a measurement of the gap in an attacker’s
knowledge. The attacker then fills the gap either with more information or with extra work or accepts a (high) probability that the attack will fail.

Secret data
Secret data is information known only to the legitimate user(s) of a security system and which is crucial to the security of the mechanisms. Most information security mechanisms rely on some secret data to keep out the attackers. In some cases the secret data has to be known (by which I mean available for use) by many/all users of the system (shared) whereas in other cases knowledge of the secret data may be confined to a single entity (private). For example in a traditional symmetric cryptographic system the key or cryptovariable must be known to all users, whereas in an asymmetric (public key) system the private keys of individual users are only known to them. Secret data may need to be stored securely (possibly for a long time) or may be ephemeral and only required during the computation surrounding a particular transaction and may then be destroyed. For example in the RSA public key system the private keys are permanent and if compromised the whole public/private key set has to be changed whereas in the Diffie-Hellman system the private keys are ephemeral with new ones being generated for each use. In general a security system will use a mixture of shared and private, ephemeral and non-ephemeral secret data. The important thing is that the security of the system is dependent on secret data remaining secret.

Secret data is a source of entropy - in many cases the only source of entropy to be overcome by the attacker. Traditionally, cryptographic security is measured purely in terms of the entropy provided by the secret data. General attack scenarios include the assumption that all non-secret data is known and available for use by the attacker. This is the fail-safe assumption whenever the attack environment cannot be controlled. However there are occasions (especially with biometric security systems) when the attack environment can be partially controlled and it can make sense to relax the fail-safe assumption. On such occasions it is legitimate to consider the non-secret sources of entropy.

Applications of single biometrics
Most current applications of biometrics are concerned with identity verification for a relatively small population. This provides a benign environment in which the technology can perform very well. There are always specific security and acceptability issues but by-and-large the technology copes with the demands on it. The scenario is that subjects have been enrolled in the system co-operatively by providing one or more measurements of the biometric from which a template is computed and stored - either in the system or on a token under the control of the subject. Then in operational circumstances the subject claims an identity and submits to the appropriate biometric measurement. The system checks the new measurement against the template and issues a pass/fail decision. If the result is a fail it is usual for some kind of further examination to be conducted. In this scenario the important parameters are the FAR and FRR. If the FAR is too high the subject might be ineffective (insecure) while if the FRR is too high the burden of secondary examination can become intolerable. As long as the number of false claimants is relatively small and the security requirement is low enough the system can work well.

If the system is stressed with a large number of false claimants the danger of false acceptance can be too great. Such verification systems are most effective when the operational environment is such as to exclude presentation of false credentials. For example if a human guard is present who can ensure that the subject actually does present the appropriate biometric measurement and is not able to fool the system with a fake or bypass the sensor with an electronic replay.

However if the biometric system is unsupervised or can otherwise be fooled or bypassed without triggering an alert, the security will be ineffective because as it states in [2], the biometric template and algorithm is not secret (I will look at one exception later in this paper. One problem with mechanical devices is that when an attacker works out how to spoof them the trick can keep on working and this is much more dangerous than with human operatives who might be less alert but are unpredictable. In applications with inadequate supervision or other protection a biometric will need to be complemented with a source of additional entropy to block such attacks - for example by involving secret data, or possibly by use of additional non-secret mechanisms that cannot be attacked in the same way.

As operations increase in scale or when more complex applications are required, the problems of too high FAR and/or FRR can become unacceptable. Now there are some biometric measures that reportedly do have very low FAR values (for example Retinal Scanning, DNA matching) and sometimes the solution to larger-scale issues will be to select one of these measures. But sometimes these solutions will be unappealing and the possibility of combining measurements from different biometric sources could be attractive. This is the main point of this paper and will be the subject of the next section. But first I want to give one example calculation by way of warning of some of the dangers of interpreting biometric measurements.
A messy example

I shall be concerned with the following situation. We have a set of subjects on whom we will perform a biometric measurement which we want to compare with one specific template (we might, for example, be looking for a criminal). We don’t know whether or not the wanted individual is present. What can we infer from the measurements. Suppose there are \( n \) people to be measured and that the FAR and FRR of the system are \( p \) and \( r \) respectively. Suppose also that our prior belief is that the probability of the genuine subject being present is \( q \). We get \( m \) matches. What is the probability that the genuine subject is among the matches?

The algebra involved is a bit messy to perform although it is relatively straightforward so I will just state the answer, which is:

\[
mq(1-r)^2(1-p) + (n-m+1)(1-q+rq)(1+rq)p
\]

As it stands this doesn’t convey much to most of us but if we plug in some figures we can see some implications.

If \( q=1 \) and \( r=0 \), we are in a state where the genuine subject is tested and (because FRR is zero) will definitely prove positive so if \( m=1 \) we would require the result to be certain, i.e. the expression should equal 1, which it does. Similarly if \( q=0 \) the genuine subject isn’t tested so the expression must evaluate to 0, which again it does. So far so good!

Now suppose that \( q=\frac{1}{2} \) and \( m=1 \) and \( r=0 \) (so we are bound to get the target if he’s present!). Now the probability evaluates to

\[
\frac{1-p}{1+p+pn}
\]

But even so, if \( n \) is large enough this probability can be much less than 1. For example if FAR is 1% (reasonable for some fingerprint measurements) and the number being tested is 50, the probability of a single positive result being the right one (even with no FRR) will be:

\[
\frac{0.99/(0.99+0.5)}{0.99/1.49} \approx 0.99/1.49 \text{ which is close to } 2/3.
\]

Although this might be enough to convict on the balance of probabilities it is far from being beyond all reasonable doubt. Yet what might a mathematically illiterate Prosecution, Jury and Judge make of it?

The moral of this is that inferences based on biometrics are not all that simple and that care needs to be taken in selecting applications.

Combining biometrics

For many of the applications now under consideration it appears that most single biometric measurements are not up to the job. A natural question to ask is whether or not something can be gained by combining different biometrics. There are indeed a number of good reasons why such a step is worth taking. The most obvious reason for combining two or more biometric measurements is to reduce the overall FAR. Many of the problems of scale are occasioned by the size of FAR or FRR or both. If we take measurements from two independent biometrics, the combined FAR will be the product of the two independent FARs. Thus using both a fingerprint and a face scan (for example), each with a FAR of 1%, will result in a combined FAR of 0.01%. For more than two independent biometrics the combined FAR will again be the product of all the individual FARs. Thus using a suitable combination of biometrics can enable us to drive down the FAR as much as we want. The assumption of independence is important, but for most biometrics being considered this should not prove to be a problem. In cases where there is any doubt it will be important to conduct trials to establish the true position. An example of common biometric measurements that would not be independent is height and weight. These are not usually used for identification purposes because of high FAR and in the case of weight, instability over time (although height used to appear on passports).

So consider two biometrics (which we will assume to be independent) with FAR and FRR \( p_1, p_2 \) and \( r_1, r_2 \) respectively. The combined system has

\[
FAR = p_1p_2 \text{ and } FRR = 1 - (1-r_1)(1-r_2)
\]

(This latter is approximately \( FRR = r_1 + r_2 \)). So although we get an improvement in FAR, the FRR gets worse. However the improvement from multiplication of 2 small numbers (FAR) is much greater than the worsening by addition of 2 small numbers (FRR) so it is possible to achieve a significant overall improvement by resetting thresholds to keep the FRR manageable while benefiting from a good reduction in FAR.

We have seen in 2.3 that when looking at the defence against attacks on a biometric security system we need to consider the entropy faced by the attacker. In many cases, subject to the extent to which the attacker is able to harness knowledge of the biometric details, the FAR will provide the main source of entropy (as \( \log_2 1/FAR \)). In those cases where the attacker is able to exploit some of the biometric knowledge to spoof the system the involvement of more than one biometric might still leave some protection to fill the gap and thereby perform better than any of the individual component biometrics.

There is a further major advantage to be expected from combining different biometrics. Recall that in 2.1 I said that we really ought to consider the statistical distribution of false acceptances more carefully and that the random model on which we (and most others) rely is not necessarily valid. In fact it is almost certainly invalid. In reality when considering a particular biometric measure we would expect to find false acceptances to cluster among a set of individuals who have similar characteristics. So there will be some individuals who are never mistaken for a particular target while others may be mistaken regularly. This is far from random. However if we are using two or more truly independent biometrics there is no obvious reason for the same individuals to cluster with respect
to different biometrics, so the reality will be closer to the random model which we can analyse. The more independent biometrics that are used the closer to the random model will be the result and security will be greater. For large-scale applications this could be extremely important.

**Further applications**

The range of applications for which biometrics are now being considered has grown beyond the simple identity verification considered in section 3. Especially with the desire to use biometrics to assist in the war against terrorism, the fight against crime and the policing of borders, the scale and type of operations has changed. As we have seen, scale alone is a major factor requiring much lower values of FAR to maintain acceptable security, but there are other issues involved that cannot be remedied simply by improving the value of the FAR.

To help in the descriptions that follow I shall consider the set of all potential subjects (S) to be partitioned into 5 categories:

a. V:
VIPs, individuals who may need special treatment. V will necessarily be small and individuals in V will always be assumed to have been registered with great care. In many circumstances attempted matches will be against a single template - i.e. we know we are trying to verify a particular individual which makes V look much like R (below) and the only effect is that the system would issue some form of VIP alert. The more interesting case is when the VIP identity is not claimed and the system has to match against all the templates in V.

b. R:
Registered users, individuals who are already in the system having co-operated in the registration process.

c. N:
Unregistered users, individuals appearing for the first time, who are expected to be co-operative but about whom nothing is known.

d. T:
Known targets, individuals whose biometric details are on the system (although they may not have been obtained co-operatively) - the associated identity may or may not be known.

e. U:
Unknown targets, individuals whose biometric details are not on the system, but whom we wish to catch.

**Standard identity verification**

This process is only concerned with individuals in R or (possibly) V. All subjects must claim to be a particular registered individual and a match against the stored template is attempted to verify the claim. This is a good application for biometrics.

**Unclaimed identity verification**

Some applications do not require the identity to be claimed (for example some fingerprint operated locks). This means that matches must be attempted against all templates in the system. In such systems we consider all the subjects to be in V. Biometrics will only be useful if V is small. Such applications are always going to be less secure than the standard process and should be avoided if possible.

**Open identification**

By an open identification system I mean one where subjects may or may not already be on the system. If they are on the system (R or V) all that is required is a standard verification. But if they claim not to be on the system (N) we need to verify that this is indeed the case and then they must be registered. Because of the different nature of the two tasks it is sensible to think of them (and implement them) separately. Thus for an immigration system (for example) the sensible solution would be to have a standard verification system at the point of entry and refuse entry to all who fail to make a valid identity claim. Normally the registration process will be undertaken elsewhere in advance.

**Avoidance of duplicate identities**

This is the other half of open identification although it may also be a freestanding application. A subject claims to be in N and it is necessary to ensure this is so by checking against all the stored identities of members of R. Unless the potential size of R is small the use of the common biometrics is likely to be inadequate. There is potential here for the use of several independent biometric measurements depending on the size of population and the dangers of failure. For an immigration system the potential size of population is the whole world. However there is another issue here. Usually the parameter that is important for security is the FAR, but in this case the security failure arises from a failure to match a biometric in the genuine case and the incorrect match to a false identity is the inconvenience to the user. This will limit the utility of biometrics. Fortunately it is usually possible to afford more time and computation in the registration process than in an access control situation so a layered approach is both possible and necessary. Initially a search against templates should be made with a threshold yielding a low FRR. Scores against all biometrics should be stored and all single matches should be subjected to secondary testing - if necessary re-measurement. There will be a need for a much deeper understanding of the underlying biometric technology and more rigorous trials than is the case with standard verification applications. This will be expensive but necessary to achieve the benefits of the application. At the verification stage (see section Open Identification) it may be possible to use fewer biometrics (and different thresholds) than are actually stored in the registration process reserving the other biometrics for use in the event of failing the primary test, thereby reaping the benefits of simplicity most of the time with low overall FAR through secondary testing. Where more than one biometric is used it could enhance security by varying the order of testing. For example if several fingerprints and a face
scan are available the subject would not know in advance which test is to be used at a particular time so as to reduce the possibility of a successful masquerade.

**Crime fishing**

There are two flavours to crime fishing. One is the technique either of trawling through a data base of people’s biometric measurements to match biometric evidence from a particular crime and the other is of searching a data base of biometrics associated with various crimes and then trying to match a particular individual. As indicated by the calculation in 3.1 this is fraught with problems. If the database is small (as compared to 1/FAR) and there is good reason to believe the guilty party is there, a fishing expedition can be effective. Otherwise the danger of a miscarriage of justice is high. There will also often be concerns about the quality of biometric data taken uncooperatively (e.g. lifted from the scene of a crime). Multiple biometrics could help because of the much reduced value of the FAR and also the improved randomness of false matches - but the chances of multiple biometric data being available from a particular crime scene is also much reduced. Crime fishing is not the same as using biometric evidence to clinch cases where there is a substantial body of circumstantial or other evidence to support a suspicion. In such cases the population being tested is small (often 1) and the probability that the guilty party is among those being tested is reasonably substantial.

**Watch list**

The watch list is seen as a potential weapon in the war against terrorism. The idea is to have a database of the details (in this case biometrics) of the known or suspected terrorists and to search this database for matches. So when an individual in N is registered we search for matches against details of members of T. We also (at least on a random basis) search for matches between individuals in R and those in T. The points to make here are:

a. The search at registration time is not too bad being just a minor addition to the existing search for duplication (see section: avoidance of duplicate identities).

b. Searching at point of entry will be a burden and ineffective if T is too large.

c. As with the search for duplication, the critical security parameter here is the FRR and not the FAR.

d. Unless T is very small we will need multiple biometrics to be effective.

e. Normally, members of T will not have been cooperative in providing biometric samples, so there will be doubts about quality.²

f. The most important terrorists will be in U and we won’t have anything to match against. This underlines the importance of vigilance in the registration process - trying to identify supposed members of N who are really in U. Biometrics won’t help us do this.

As a final remark in this section, among the advantages of fingerprints and face scans is the possibility of obtaining some uncooperative measurements. So, despite their high values of FAR and FRR they still have a role to play in these more challenging applications.

**Non-biometric biometrics**

When we think about biometrics most of us take the term literally and consider physiological measurements like height, weight, fingerprints, face scans, hand geometry, iris scans, retinal images, DNA etc. However, there is another class of measurement that are also considered to be ‘biometric’. These are measurements of learned behaviour that can also characterise an individual. These non-biometric biometrics have their own characteristics that can be complementary to those of other biometrics. In this section I will consider just a few of the more important aspects.

An important set of non-biometric biometrics is to do with how we write and includes handwriting, signatures and dynamic signatures. The most useful of these for security purposes is the dynamic signature. The dynamic signature captures not only the form in which you sign your name but also the dynamics of the action. The dynamic signature has been found to be characteristic of the individual and hard to forge. There are products available to implement the technology. The main drawback today is that there has been little (if any) independent research to verify vendor claims as to the effectiveness of the technology. Properties include:

a. Very low values of FAR are reported, Good.

b. Variation of performance does depend on the individual subject, with consequently variable values of FRR, Bad - although overall, the vendors claim acceptable values of FRR.

c. The subject has to cooperate; it is possible to fail deliberately unlike a physical biometric; this makes it unsuitable for some purposes but ideal for others, for example a duress signal.

d. The dynamic signature involves secret information (captured in the FAR - so entropy is easy to calculate) that cannot be forgotten and cannot be taught to anyone else, Magic for security purposes.

e. An individual can develop several signatures for different purposes, Opens up a number of possibilities.

f. The signature can vary slowly with time, Bad but manageable.

g. Injury can affect the signature temporarily or permanently, Bad but manageable.
h. Signatures are culturally acceptable, Good.

Combining a technology like dynamic signature with a physiological biometric can result in an overall system that can combine the advantages of both. This can be especially valuable for high security applications because of the entropy characteristics of the dynamic signature and the ability to pass a duress signal, while the physiological biometric can provide both some assurance against deliberate falsification and secondary testing to reduce the FRR. (For example allow an extra go at signing if the fingerprint or whatever matches up). To keep a good FAR it is important to ensure that eventually a pass is obtained against both measurements.

Conclusions
The security of biometrics is characterised by two quantities, the FAR and the FRR. Unfortunately it is difficult to obtain valid estimates for these quantities because large-scale trials are expensive and the underlying statistical models are often inadequate to support smaller-scale trials.

The use of single biometric measurements is generally good enough for small-scale verification of a claimed identity but is less good for large-scale applications and those requiring matches against a number of templates. Many applications now being considered fall into these categories. Improvements can be made by combining independent biometrics. The FAR of a combination is the product of the individual component biometrics. This leads to significant reduction in system FAR and hence to increased security. Moreover the errors arising from combined independent biometrics are will be more random than for each component and thus the random statistical models underlying the security calculations will be a better approximation to the true picture.

There is also potential for the different biometrics to complement each other in resistance to differing attack scenarios, thereby compensating to some extent for the inherent lack of secret data in a biometric template.

In some potential applications, the critical security parameter is the FRR rather than the FAR. This needs to be handled with care but it is also helpful to combine independent biometrics.

Biometrics based on behavioural measurements can complement physiological biometrics extremely well. Dynamic signatures, in particular, offer a way of benefiting from increased entropy and when used in combination with physiological biometrics can be very powerful.

References:


Notes
1 This is a subtle point, if we were only concerned with the value of the measurement the entropy would turn out low from the point of view of either a genuine subject or an impostor as in each case the likely result is nearly predictable - acceptance in the one case and rejection in the other.

2 Of course as time goes on it is possible that individuals will have been registered before they start their terrorist career, so what is a major problem today may lessen considerably in the future.

About the author:
Professor Richard Walton CB B.Sc. Ph.D. (Nottingham) B.A. (O.U.) C.Math. FIMA MBCS as appointed to in January 1999 to the UK GCHQ Board as Director CESG, the National Technical Authority for Information Assurance. He held this post until October 2002 when he was seconded to the Cabinet Office to initiate work on the production of a National Strategy on Information Assurance. His earlier posts included Head of the Division employing most of the GCHQ Mathematicians (1996-99) and Head of the Mathematical Services Group in CESG (1985-91). He was appointed Companion of the order of the Bath (CB) in the 2003 New Year Honours. He retired from the Civil Service in May 2003 and is now an independent consultant (own company, Walton-Mackenzie Ltd) and visiting Professor in the Information Security Group at Royal Holloway University of London. He was appointed as an independent member of the Defence Scientific Advisory Council in April 2004.

Contact:
Email: Richard@walton-mackenzie.com


<table>
<thead>
<tr>
<th>Year</th>
<th>Revenue(US$ million)</th>
<th>Growth Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>52.9</td>
<td></td>
</tr>
<tr>
<td>1999</td>
<td>98.3</td>
<td>86%</td>
</tr>
<tr>
<td>2000</td>
<td>120.0</td>
<td>22%</td>
</tr>
<tr>
<td>2001</td>
<td>160.4</td>
<td>34%</td>
</tr>
<tr>
<td>2002</td>
<td>260.1</td>
<td>62%</td>
</tr>
<tr>
<td>2003</td>
<td>423.6</td>
<td>63%</td>
</tr>
<tr>
<td>2004</td>
<td>707.3</td>
<td>67%</td>
</tr>
<tr>
<td>2005</td>
<td>1131.6</td>
<td>60%</td>
</tr>
<tr>
<td>2006</td>
<td>1867.2</td>
<td>65%</td>
</tr>
</tbody>
</table>
Managing Intellectual Property

Peter Stephenson

Over the past couple of years we have discussed a number of techniques for managing risk, conducting investigations and other proactive and reactive approaches to some of the tougher problems of information security. Now we take up what is, arguably, the most difficult and potentially expensive information security problem of all: protection of intellectual property. The difficulties associated with IP protection are significant. And they are matched directly by the impact of IP compromise.

Consider the entertainment industry. I was told by a security executive of one of the United States’ largest entertainment companies that one particular animated film cost over $7 million and took over ten years to produce due to the need to evolve entirely new technologies in order to make the production. Weeks before the film was to appear in distribution it was leaked somehow to the Internet underground.

The entertainment industry, though perhaps the most visible, is by no means the only high profile industry that exists largely based upon unique intellectual property. The pharmaceutical industry spends billions of dollars every year to research and develop new drugs. If the formula for a new drug is leaked prior to approval by government agencies, all of the development investment may be wasted on a product that a competitor may bring a clone of to market faster.

The bottom line is that IP management has become business’s biggest nightmare. Over the next few columns we will take up the topic of protecting and managing IP. We will begin this month with an overview of the problem and some representative cases. Next, we will discuss strategies and tools for protecting IP proactively. We’ll end with some innovative techniques for tracking IP leakage and gaining convictions when IP is stolen. We begin with some background on the problem.

Background

According to US Deputy Assistant Attorney General John G. Malcolm, intellectual property crime consists mainly of “…copyright piracy, trademark counterfeiting, and theft of trade secrets.” In his testimony Mr. Malcolm pointed out some significant and troubling issues. For example, he describes in detail the relationships between various types of organized crime and piracy. In one case, pirated copies of Microsoft and Symantec software brought the pirates over $9 Million.

Mr. Malcolm describes the organization of a typical high level software piracy, or , warez group:

“Like legitimate companies, “top-tier” warez groups have clear hierarchies and divisions of labor. Rank and position within warez groups are based on a variety of factors, including special skills, length and quality of service to the group, and reputation within the warez scene. A typical group - which can consist of people all over the world who may know each other only through their screen names - will consist of one or possibly two leaders, two or three high level individuals known as “Council,” twelve to fifteen Staff members, and a general Membership comprising anywhere from twenty to eighty individuals. The Leader has ultimate authority over all aspects of the group and its activities. Council members are primarily responsible for the group’s day-to-day operations, including preparation of new releases, recruitment, and security issues. Staff members are typically the most active individuals in preparing a group’s new releases for distribution, or in maintaining the group’s “File Transfer Protocol” (FTP) sites from which the pirated software is distributed. Finally, the general Members contribute to the group in a variety of ways, including acting as occasional suppliers of new software, hosting the groups FTP servers, or providing hardware (e.g., laptops, hard drives, routers, other computer equipment) to other group members for use in their warez activities. The more work someone does for the group, the higher up the organization that person will move, and the greater the access that person will have to pirated products.”

An example of such a group was ShadowCrew, a group consisting of over 4,000 members world wide that was described as an on-line one stop shop for identity theft. While not dealing directly in intellectual property, ShadowCrew followed the same sophisticated organizational scheme as top-tier warez groups and, through a combination of sophisticated organization and strong disciplinary measures against members, the group cleared tens of millions of dollars through identity theft, document forgery and other similar illegal enterprises. The danger here is that such groups are highly organized, very structured, almost completely anonymous and, therefore, extremely effective.

Former Attorney General Janet Reno expressed concern as early as 2000. In an article prepared for theStandard.com she stated:
"...economic espionage – unlawful practices engaged in by private companies and sometimes by foreign governments aimed at stealing assets such as formulas, blueprints or marketing strategies – is on the rise. The FBI estimates that a significant number of countries are targeting US firms, with high-tech companies the most frequent targets."

With that pronouncement the Attorney General moved IP theft into the arena of international economic espionage. The bottom line is that IP theft is a real and increasing issue and information security professionals are being asked to step up to the problem and solve it.

But solving the problem of IP management is not a trivial task. It requires a solid combination of good security policy, solid implementation and several things that organizations outside of the government have been reluctant to do, most especially information classification. Information classification is the core of any effort to protect IP because without such classification it may be difficult to determine what does or does not need to be protected. Also, without formal information classification, an employee leaking intellectual property outside of the organization may claim ignorance of the IP’s value.

A framework for IP management

Over the past decade we have developed and expanded upon a framework for protecting intellectual property. That framework needs to address three important aspects of IP management:

- Policy foundation.
- Proactive management.
- Discovery, tracing and recovery of leaked intellectual property.

To address these we will adapt a simple, but extremely effective, framework I developed nearly ten years ago called Intrusion Management to the task of managing intellectual property. The Intrusion Management Framework consists of five layers:

**AVOIDANCE:** Everything you do to avoid the consequences of an intrusion

**ASSURANCE:** Everything you do to ensure that the measures you took in Avoidance are working correctly and effectively

**DETECTION:** Everything you do to detect an intrusion attempt

**RESPONSE:** Everything you do when the first three layers fail

**RECOVERY:** Restoring the target system to its pre-incident state

Adapting this framework to our needs, we get a new Intellectual Property Management Framework:

**AVOIDANCE:** Everything you do to proactively protect your intellectual property

**ASSURANCE:** Those tests and audits you perform to ensure that your protection measures are effective

**DETECTION:** All measures you take to detect, report, contain and track attempts to alter, destroy, access, or otherwise compromise your IP

**RESPONSE:** Those measures used to trace leaked intellectual property, identify the sources of the leak and take action against those sources

**RECOVERY:** Measures taken to interdict and manage the consequences of an IP leak and to ensure that the source and enabling root cause(s) of the leak are removed and appropriate countermeasures implemented.

Over the course of the next several columns we will discuss each of the layers of the framework in detail. To set the stage, however, we offer some brief discussion of the layers here.

The Avoidance Layer

Avoidance, as with any information protecting model, is arguably the most important set of tasks that you can perform. Not only is it far less expensive to implement good avoidance measures than it is to recover after the fact, good avoidance, assurance, and detection measures lower the cost and impact of the inevitable successful attempt at IP theft.

The application of avoidance measures follows a detailed risk analysis of the IP environment. We have discussed risk management in depth here and we introduced you to the FARES (now called Formal Analysis of Risk in Enterprise Systems) process. FARES or other risk management methodologies (FARES is preferred, of course, due to its highly structured and reliably provable approach) must be applied to your IP environment so that you can understand the threats against your intellectual property and the vulnerabilities that would allow a threat to produce an impact successfully. You also need to know what that impact will be so that you can craft an appropriate, cost-effective, response.

There is a class of IP protection tools emerging in both hardware and software environments. For example, the application of secure vaults allows the implementation of specialized encrypted storage containers that both protect and help track IP stored as files. Watermarking and other identification measures also are becoming more mature.

Of course, before tools can be applied, the results of the risk analysis need to be transformed into a clear set of policies governing IP management. From those policies you will develop a set of standards and practices to implement them.

The Assurance layer

We will discuss the assurance layer much more completely in future columns, however we should mention here that the testing and auditing of avoidance measures is critical. Knowing that the measures you are taking to protect your IP is one of the most important proactive aspects of IP management. Additionally, these measures should work together with detection measures to enable you to identify, rapidly, attempts to compromise intellectual property. IP leakage takes very little
time and effective containment often is dependant upon how rapidly the event is detected.

The Detection Layer
The Detection Layer is one of the most difficult to implement. It begins, of course, with procedures dictated by policies and standards. However, IP is characterized by the fact that, to a computer, it is no different from any other file. If an intruder can access it, the intruder can steal it and may not ever be detected in the act. For that reason, special precautions need to be in place to monitor all access to IP. A key aspect of detection is the ability to contain the leak once it is identified. Timely containment may mean the difference between a costly leak and no incident at all.

These precautions depend upon classification and isolation of intellectual property such that it is treated specially. Restriction of access is, as well, very important. We will discuss some ways to control access to IP files in an upcoming column.

The Response Layer
The Response layer assumes that all else has, at least in part, failed. If the response layer is to be useful, however, certain functions in the upper three layers need to be effective. For example, we need to know what IP was involved, how the leakage occurred and who was involved. Given that information we can begin to take appropriate reactive measures. The Detection Layer needs to provide a reliable audit trail that we can use to recreate the event.

Response to an IP incident usually is a formal investigation and the evidence collected in that investigation needs to be managed as we have discussed in our columns on end-to-end digital investigation. There are some very sophisticated tracing mechanisms required as well. These tracing mechanisms will be a topic in themselves.

The Recovery Layer
Recovery from an IP incident requires that you understand fully what has occurred and what the consequences of the event are. Often part of recovery, more than with any other type of system breach, involves legal action. Thus, legal counsel must be involved from the first knowledge that a leak has occurred. To this end, a solid relationship with counsel prior to an event is a must. In addition you will need to know what law enforcement agency to call when an event occurs and who within that agency is your optimum point of contact.

Recovery also may include the need for communications to the public. Corporate communications staff needs to understand how to handle the media and how to understand and communicate the magnitude of the event. This requires training and close communication.

Conclusions
The process of managing intellectual property is a very complicated one. It is pervasive and global. It is pervasive in the sense that protective measures, while focused upon the IP itself, need to permeate the enterprise in a layered protection scheme typical of good security defense in depth. It is global in the sense that IP management may apply not only to the hosting enterprise, but to connected enterprises and, even, to the Internet. Ability to operate effectively within these disparate and often unmanageable (by the owner of the IP) environment requires careful planning and execution.

Over the next several months we will address each layer in the model in detail. We will offer policy suggestions, we will examine tools and we will develop processes that can help protect your IP while it is contained and recover from a breach if containment fails. We will begin next time by expanding and extending the framework into a working model that you can use to verify your IP management plan.

References:
1 Statement of John G. Malcolm Deputy Assistant Attorney General For The Criminal Division United States Department of Justice Before the Subcommittee on Courts, the Internet, and Intellectual Property Committee on the Judiciary, United States House of Representatives Concerning Copyright Piracy and Links to Crime and Terrorism Presented on March 13, 2003
From incidents to disasters

Stephen Hinde

Just under a half of businesses have not developed corporate recovery plans to deal with catastrophic events according to a report issued by the UK Chartered Management Institute (CMI) in March 2005. The survey of 440 managers, conducted by the Continuity Forum and Veritas Software, ranged from sole traders to companies employing more than 10,000 employees. The Survey found that just over three-quarters of financial institutions have business continuity plans – twice as many as retail companies. The lessons of the terrorist attacks on the New York World Trade Center and the IRA bombs that devastated parts of the City of London in the 1990s are apparently still not learned.

But it is not just good business sense to have business resumption planning it has become a regulatory requirement in the UK for financial years beginning after April 2005. Companies will be required to publish separate operating and financial reviews warning investors of business risks, including possible details of business recovery plans.

The fear of loss of IT systems topped the list of worries with nearly three-quarters of respondents listing it as number one, followed by loss of skills. Despite an increase to 41% in the proportion of events involving loss of key personnel last year, only a handful of business continuity plans covered staff loss. As I write this, a large British law firm has just lost an entire 40 plus strong specialist group to a competitor firm.

All the pain: none of the gain

One of the more disquieting findings is that although organisations have experienced disruptions over the past 12 months ranging from floods to loss of staff to terrorist damage in other countries, they have not updated the business continuity plans to reflect the incidents. They are as vulnerable now as they were prior to the incident. No lessons have been learned. All the pain: none of the gain to misquote a former Chancellor of the Exchequer.

Even when organizations have prepared a plan business continuity plan, many have no idea whether it will work in anger because they do not bother to test it. A fifth never tested and just over a half only rehearsed the plans once a year. And one in eight organizations that uncovered a problem during a test did not update the business continuity plan to reflect the problem. An excellent example of testing of plans and of test evacuation drills was demonstrated during the terrorist attack on the World Trade Centers when all but a few of Morgan Stanley’s 3,700 employees successfully evacuated from the second Tower. Dean Witter, a brokerage that is now part of Morgan Stanley, was one of the organizations that was affected by the 1993 bomb attack. Management decided there and then that should the unthinkable happen again, staff would be trained to evacuate. The staff, who were involved mainly in processing trades for retail investors or handling administrative matters, were trained and organized to evacuate floor by floor.

After the first airplane crashed into the North Tower, Morgan Stanley’s staff quickly and efficiently evacuated from their 22 floors (53rd to 74th) of the South Tower. Their plans were to evacuate irrespective of the building management’s decision as to whether to evacuate or not. When the second airplane hit the Twin Towers just above the Morgan Stanley floors, the evacuation by Morgan Stanley personnel was well under way.

Where this model evacuation went awry was in the ticking off of names after the evacuation. Staff just went home, turned off their telephones and avoided contact. It took two and a half days of telephoning and home visits before Morgan Stanley was able to account for all bar 15 employees, some of whom had stayed inside the building to help colleagues down. Good planning and luck helped to contribute to this success story. Others were not so fortunate. Investment bank, Keefe Bruyette Woods, situated in the South Tower, lost 69 of its 172 staff, and Cantor Fitzgerald lost 700 of its 1,000 staff.

A separate survey in March based on 250 companies conducted by the Business continuity Institute found that organizations have contingency plans for dealing with terrorist attacks, but are failing to plan for disruption caused by more mundane events such as telecommunications and power failures, which are more likely to cause disruption. Just over a quarter of respondents regard terrorism and war as their biggest threat, followed by natural disasters, fire and floods. And yet a fifth of businesses do not have disaster recovery plans for their IT systems. And a third do not have general business resumption plans. This survey found a similar level of non-testing (25%) to the CMI survey.

One of the main failures of the plans surveyed was that they failed to plan for potential telecommunications failures. Nearly three-quarters of the companies surveyed recognized that the failure of telecommunications would damage the reputation of their businesses, but most relied on business resumption plans that assumed telecommunications would be working. Only an eighth of organization had second-tier telecommunications in place and less than a tenth had a third-party recovery site.

The survey also found weaknesses in businesses’ supply chains. Nearly a fifth said they were happy to rely on a statement from the supplier that they had business resumption plans in place. A third had asked to read the supplier’s business resumption plan, and another 27% did not know how suppliers’ business resumption plans were verified.
The disaster of the red chillies

The contamination of food with an illegal dye which triggered the UK’s biggest ever recall of products last February is a good case study for business continuity planning. Sudan 1 is a synthetically produced red dye normally used for colouring solvents, oils, waxes, petrol and shoe and floor polishes. It is also used to colour some chilli powders produced in India and exported around the world. It is rated a “class three” carcinogen, or cancer-causing agent, by the International Agency for Research on Cancer and has been banned from use as a food additive in Britain and the rest of the European Union since 1995. America banned its use in 1918.

There is a concern that the dye, Sudan 1, has the potential to cause cancer. However, the Food Standards Agency has said the risk is very low. Professor Alan Boobis, an expert in toxicology at Imperial College, London said “Sudan 1 was banned from use in food products following experiments on rats, which suggested that the chemical could trigger the formation of malignant tumours. There is little reason for the public to be alarmed. People should not be unduly concerned about the health effects. It is a good idea to remove this substance from the food chain, but this is being done simply as a precaution, not because there is an immediate impact on health.”

Since July 2003 — following the discovery of traces of Sudan 1 in chilli powder samples in France — all dried and crushed or ground chilli coming into the EU must be accompanied by a certificate showing that it has been tested and found to be free of the illegal dye. Any consignment that does not have a certificate is detained for tests and destroyed if it contains Sudan 1. But chilli powder has a long shelf life and some of the batches now in Britain arrived before the testing regime was introduced, as did the batch at the centre of this scandal.

The contaminated batch of chilli powder passed through at least two suppliers in Britain before ending up with Premier Foods, a large food manufacturer which inadvertently used the chilli powder to produce a batch of Crosse & Blackwell Worcester sauce. This sauce, in turn, was used as an ingredient in a wide range of other products. More than 600 different products manufactured by over 60 different producers contained the illegal powder. Many are ready-made meals such as shepherd’s pie, pasta bake, chicken wings, sausage casserole, pizza and chilli con carne. It is really staggering what products actually contain Worcestershire sauce.

The scandal prompted the largest recall of food products in British history. Retailers were instructed to remove all affected items. Supermarket shelves and catering establishments were similarly instructed. The UK Food Standards Agency worked with the food industry and local authorities to trace any other products which might be contaminated. Local authorities were faced with a massive task: not only was there a list of over 600 affected products, which took a long time in compilation; but also in identifying shops, restaurants and other catering establishments – unbelievably, there was no list. The task was carried out by telephone, letter or face-to-face visits.

David Statham, Director of Enforcement at the Food Standards Agency, said: “This has been an enormous undertaking. Hundreds of products have been affected in thousands of shops. The vast majority of contaminated foods have been removed providing some reassurance to consumers. However, there may be some products remaining both in shops and in the catering sector and we will continue to work with local authorities to remove them as far as is practical and achievable.”

The slow reaction

Concerns have been raised about why the public was alerted to the problem some weeks after the Food Standards Agency knew that Sudan 1 may have entered the food chain after routine tests by an Italian company on a batch of Crosse & Blackwell Worcester sauce. This slow disclosure by the Agency, which was set up after the BSE food scare of the 1990s to stop a repetition of a food scare, helped to feed a media frenzy, thereby exacerbating the impact and moving it from a very low risk incident to a major cancer scare.

It took the Agency a very long time to establish the list of affected foods. It is perhaps a sign of how far society has moved into eating processed food that the authorities had no comprehension as to just how many foods contain Worcestershire sauce. The fact that the contaminated product was used as an ingredient in so many processed foods introduced additional layers into product recall – with some of the 60 plus producers not having product recall systems. Product recall was thought of in linear terms as exemplified by the Perrier Water recall in the early 1990s – a single, discrete product that was easy to identify. The lack of a definitive list of catering establishments and food shops also hampered the product recall.

It was fortuitous that the risk to human health was very low bearing in mind the time taken to respond; the slowness in identifying the products affected; and the incomplete list of catering establishments and food shops. All these lessons that will need to be addressed by the FSA before a really serious food incident happens.

The punishment of the innocent?

When I conduct physical security audits, I always look at the neighbouring businesses to see whether there are dangerous substances stored or risky processes that increase the risks posed to the computer centre or the likelihood of an incident or disaster. For instance, a site near an airport runway,
or next door to a gasometer, or adja-
cent to a munitions factory, or a labor-
atory conducting vivisection experi-
ments. To ignore them and to assume
that you can look at the risks facing the
computer centre in isolation from the
neighbouring environment is risky to
the point of foolhardiness. But what
about neighbouring products?
In the case above, the contaminated
chilli powder was used as an ingredi-
ent in Worcester Sauce – Crosse & Blackwell’s
Worcester Sauce. But to most Britons
Worcestershire Sauce is synonymous with
Lea & Perrins. For most consumers Worcester
SAUCE sold in the UK is Lea &
Perrins. In fact, over 90% of
Worcester sauce sold in the UK is Lea &
Perrins. For most consumers Worcester
sausage is Lea & Perrins and Lea & Perrins
is Worcester sauce. So any scare story
about contaminated Worcester sauce
automatically implicated Lea & Perrins
in many consumer’s minds – a thought
process encouraged by the media incor-
rectly showing a bottle of Lea & Perrins
to illustrate their story of the contamina-
tion. Thus Lea & Perrin, a brand owned
by HP Foods, was a blameless brand
cought up in the crossfire.
Lea & Perrins had an established cri-
sis team that was activated when the
disaster struck. The team included the
board of directors, key officials and the
regulatory and external affairs manager.
On a typical day the company receives
50 calls at its customer service tele-
phone line. After the story broke that
became over 5,000 in a week. The
company used an external company to
field the large increase in telephone
calls and replaced its usual week-end
recorded message service with staff
working 10 hour shifts.

There is no easy answer to how to
defend a product that was not affected.
You can not reassure the public by very
public pictures of products being with-
drawn from shelves, as we saw with
Perrier and other products in the past,
because there is no product to withdraw.
You can not be seen to benefit from
knocking the affected competing prod-
uct. The company depended heavily on
public relations and getting its officials
in front of the cameras. It is also lucky in
that a bottle lasts a long time so the pur-
chase of the next bottle is likely to be
well after the scare is over, unlike, say,
bread or meat or eggs.
The important lesson is that Lea &
Perrins was prepared – it had plans and
they were activated quickly. So many
incidents become disasters because of
the poor response by management.

From SATAN to OVAL: the
evolution of vulnerability
assessment

By Dr. Gerhard Eschelbeck, CTO & VP Engineering, Qualys

With the growing reliance and dependence on our inter-connected
world, security vulnerabilities are a real world issue requiring focus
and attention. Security vulnerabilities are the path to security breach-
es and originate from many different areas - incorrectly configured
systems, unchanged default passwords, product flaws, or missing
security patches to name a few. The comprehensive and accurate
identification and remediation of security vulnerabilities is a key
requirement to mitigate security risk for enterprises.

Vulnerability assessment technology has evolved significantly since the initial
release of SATAN1 about a decade ago. SATAN was a dictionary based UNIX
security testing tool designed to help system administrators identify common
security problems. Second generation vulnerability scanners built upon hard-
coded decision trees followed shortly. Predefined decision trees allowed mini-
mization of the necessary probes depending on operating system and
application. Their lack of flexibility however made them quickly obsolete.

Modern scanner architectures are built as inference-based systems, which don’t
require any agent software on the target systems. They learn about each target sys-
tem individually while selective probes are being exchanged with the target sys-
tem. The inference-based architecture is centred around highly multi-threaded
engines for scanning thousands of vulner-
abilities simultaneously on any system on
a network. Modern scanner architectures
also support multiple levels (trusted and
un-trusted) of vulnerability assessment
against any given target system.

Untrusted vulnerability assessments simula-
te the scenario of an attacker without prior knowledge about the target system,
while trusted assessments leverage creden-
tials to log into the target systems for
auditing configuration and patch infor-
mation. An important criterion for mea-
suring the effectiveness of a vulnerability
canner is the comprehensiveness and
accuracy of its vulnerability knowledge
base. Also, the ability to report and com-
municate vulnerability findings in a stan-
dardized manner from the vulnerability
canner to other applications (i.e. patch
distribution or configuration manage-
ment) is a critical requirement.

The OVAL2 (Open Vulnerability
Assessment Language) project is an
effort to develop a standardized process
for checking, reporting, and remediation
of configuration as well as vulnerability
issues. OVAL is being developed as an
international effort under the leadership of
MITRE with support from industry,
government, academia, and the security
community. XML based OVAL provides
a definition schema for various plat-
forms (Windows, Linux, Solaris …). It
allows defined standardized probes
and criteria to test a system for a partic-
ular vulnerability. The OVAL effort
involves development and standardiza-
OVAL aims to standardize and define a structured process for identifying and communicating vulnerability and configuration information from the point of knowledge of a vulnerability to the point of action. Vulnerability Assessment has matured over the past years, and to standardize the information exchange during the full vulnerability lifecycle makes OVAL a significant contribution to the security industry. Multiple security vendors have committed support for OVAL in their upcoming product releases. Enterprises will benefit from OVAL compliant tools to integrate and improve the flow of information from vulnerability alert, to vulnerability detection as well as remediation.

About the Author
Gerhard Eschelbeck is chief technology officer and vice president of engineering for Qualys, Inc. He published the industry’s first research derived from a statistical analysis of millions of critical vulnerabilities over a multi-year period. Eschelbeck presented his findings before Congress, and is a significant contributor to the SANS Top 20 expert consensus identifying the most critical security vulnerabilities. He holds several patents in the field of managed network security and earned Masters and Ph.D. degrees in computer science from the University of Linz, Austria. Eschelbeck can be reached at ge@qualys.com.

1 “Info about SATAN”, CERIAS Purdue, http://www.cerias.purdue.edu/about/history/coast/satan.php

British IT directors fail to make strategic case for IAM

Brian McKenna

Identity and Access Management is being misunderstood and badly positioned by UK IT directors, says a research report from RSA Security. As a consequence British boards are failing to get the strategic point of the technology.

The research found that 27% of the 101 IT directors canvassed stated that lack of buy-in from senior management was the main obstruction to implementing identity and access management. This is despite the fact that 52% of the respondents believe it would save their companies money.

The researchers found that while 76% recognised IAM as a priority, only eight per cent had a good understanding, and 34% had not much understanding at all.

British IT directors fail to make strategic case for IAM

Brian McKenna

Identity and Access Management is being misunderstood and badly positioned by UK IT directors, says a research report from RSA Security. As a consequence British boards are failing to get the strategic point of the technology.

The research found that 27% of the 101 IT directors canvassed stated that lack of buy-in from senior management was the main obstruction to implementing identity and access management. This is despite the fact that 52% of the respondents believe it would save their companies money.

The researchers found that while 76% recognised IAM as a priority, only eight per cent had a good understanding, and 34% had not much understanding at all.