14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Criminals using Cryptography, Reasonable Precaution or Convenient Smokescreen?

S Doogan

Abstract

An analysis of the role of cryptography to date as used in the commission of crime. This paper will discuss the current regulatory framework and examine whether the proposals emanating mainly from various national law enforcement bodies for tighter national controls of Internet service provision and cryptography are justifiable in the light of the expanding role of e-commerce. The paper will also scrutinise the current case law and other evidence to discover whether the criminal activities which the proposals seek to restrict can, on the available evidence, be minimised by this method, or whether they will have an entirely different outcome.

Introduction

Almost since the first computers were linked together with handmade connections system security has been a major issue for anyone involved with computer networks. However there are two separate though related areas of security involved here which are often either ignored or misunderstood. The first, and perhaps the most obvious, is system integrity itself which is in essence, the keeping out of unwanted intruders. This is achieved to a greater or lesser degree by the use of passwords, unique logins and "secure" software. In the U.K., as in most western legal systems, break-ins can be dealt with though the invocation of computer misuse legislation. For a more detailed analysis of this see my previous paper "liability of Internet service providers to hacker attacks".

The second aspect of computer security can be seen as the validation and ensuring of the integrity of the data transmitted or stored on computer networks. It is on the regulations and laws surrounding this second aspect that I wish to concentrate. Equally important, and perhaps often more important is ensuring that the law as it stands is actually workable and that it achieves what its originators set out to do.

The uses and importance of cryptography are well documented within military archives, and even in the occasional television program, however, they often miss the point that traders and business, merchants and tradesmen, especially those involved in international business also used codes and encrypted messages to protect their interests and have been doing so for many years. Electronic commerce and privacy advocates are merely raising the profile of cryptography in a civilian context

Recognising, or at least acknowledging the importance of the issues implicit in this technology, especially security for commercial applications and individual privacy, most western governments (and many others) are adapting existing legislation, or are adopting new regulatory frameworks. However formulated, most of these proposals incorporate very similar goals in that they seek to create a regulated, and safe environment where national and international electronic commerce may develop together with attendant legitimate concern that National Security be maintained and that electronic criminal activity be minimised, if not eliminated. This paper will (hopefully) assess whether the criminal activity which the proposals seek to purge can, on the available evidence, be thwarted by this method, or whether it will have an entirely different outcome.

What is cryptography actually used for

The first and most obvious use of cryptographic systems is to keep private information private. There is however, a second equally important use, the validation of information and who has sent that information. This clearly has an application in modern society in terms of banking and business, as well as for individual privacy.

When an encrypted message is received by the intended recipient, probably the most fundamental question which they must answer is how they can be sure that the message which they have received is what it actually purports to be and that it actually comes from the person that they think it does and has not been altered en-route. As any competent user will verify, it is a trivial matter to make electronic mail appear to have come from a source other than it appears, it is therefore essential that there be a method of verification, where person to person verification is not possible, cryptography can be used to provide a reasonable certainty that the message has in fact come unaltered from its purported sender. The concept of a "digital signature", while related to this application is a lesser standard being put forward as the means of verifying the validity of electronic contracts, which appears to be of more concern to politicians and lawyers than to the userbase, its strengths and weaknesses will be discussed later in this paper.

Validation and integrity checking of data can be performed in many different ways, from simply lifting the phone and asking the producer/publisher of the data whether the information is valid, to highly complex techniques involving multiple algorithms, unique one time session keys and similar methods, most of which are mystifying to a non-technical user. At the risk of offending cryptography purists, however, the key to security in systems utilised by non computer scientists is ease of use. This issue is being addressed by software houses such as Microsoft and Lotus in that cryptographic software is being incorporated directly into their products, however the same reasons which are encouraging the software companies to improve their software are also attracting the attention of governmental bodies, especially the security services. Legislative attitudes vary widely from one jurisdiction to another with security agencies putting the case that increases in police powers to conduct electronic surveillance and interception of communications are necessary if the police are not to be at a disadvantage in the fight against criminals. This pressure has had varied results with a very noticeable discrepancy arising between the attitude of the United States and that of the European Union.

Even today, not all encryption is clearly visible to the naive user, sandwiched between the pretty applications which are visible on the desktop, and the actual TCP/IP or X.25 connection which provides access to the network is what is called the sockets layer. Very little attention was paid to this layer until it was realised that it could itself provide one of the main keys to the creation of a secure electronic environment. In the light of this realisation, what is now known as S.S.L. (Secure Sockets Layer) and several variations of it were developed. This is an area which is sometimes forgotten by those seeking to regulate the use of encryption technology since most applications level software , and therefore most users are unaware of the nature of the Sockets layer which they are in fact using. This seemingly over pedantic differentiation is important for those concerned with the legal regulation of electronic networks since it could in fact mean that someone using an application over a strong S.S.L. layer would potentially be in breach of their national legislation, if their country forbids the use of encryption over a certain strength, for example the U.S, and does not make a specific exclusion for sockets connections over which the user has little or no choice, or knowledge.

Cryptographic Methods Commonly Used on the Internet

There are primarily two cryptographic techniques in use by "normal users" today, symmetric and asymmetric key cryptography with by far the more popular being asymmetric. The technical differences between them however are of little interest in this context, except in so far as while both employ pairs of keys, symmetric key cryptography which uses two identical keys for decoding and encoding messages, is primarily of use in a closed system whereas asymmetric or public key cryptography is more suitable for use in a Wide area network context (such as the Internet. This paper concentrates on the regulations surrounding Public key asymmetric cryptography, but it should be remembered that this is not the only method available.

The Regulatory Regime

Since Cryptography is a discipline which produces applications of interest to both the civil and military authorities it is perhaps unsurprising that there are, in many countries, very strict regulations governing the use and export of cryptographic products. In the U.K. we have the somewhat surprising reality that the same regulations which were breached in the infamous "Iraqi Supergun" affair are in fact the same ones which are used to control the export of cryptography and cryptographic products. These regulations are developed from an International agreement called the "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies". As the name implies, these are items, usually of a tangible kind which are capable of being put two different use,. depending on the wishes of the user. The difficulties in deciding precisely which dual use technologies should be controlled are clear when questions such as "when is a big pipe not just a big pipe" are considered. The situation is further complicated when it is realised that the same surgical instruments which are used to perform keyhole surgery in the U.K. can with relative ease be adapted to function as the laser guidance system on a "smart missile", and the same computer used as the Amnesty International web server could just as easily be a system used for setting ballistic missile trajectories and targeting, it is all merely a question of application. This agreement, which has recently been renewed (at the end of 1998) remains substantially the same as its predecessor COCOM which was originally intended to block technology passing from the western powers to the east during the Cold War.

Within the U.K. there are as yet few restrictions on the use or export of encryption products, and apart from the specific instances included in the Wassennar agreement (to which neither the U.K. nor the U.S. strictly adhere having negotiated some derogations in the interests of "National Security). There is however a quasi governmental agency called the "Certification Body of the UK IT Security Evaluation and certification Scheme" which appears under the auspices of CESG (the Communications Electronics Security Scheme which is itself closely related to GCHQ).

ITSEC, which is, unsurprisingly, based in Cheltenham, together with the Department of Trade and Industry’s "Information Security Policy Group" jointly administer this scheme whereby security certificates are granted for so called secure software products. These licenses do not guarantee that the product is free from defects, nor do they necessarily mean that the system on which the software is operating is in fact secure, all that the certificate certifies is that the particular version of the particular product performed to a satisfactory level in a controlled environment on a set batch of tests. Certain products are restricted by CESG for use only by UK governmental or quasi governmental departments, while others are available on a case by case basis to foreign governments and certain U.K. businesses. The algorithms, or mathematical models used in these products are not made public, however, by a process of reverse engineering it is possible to approximate with a fair degree of certainty how these systems function, and what methods they utilise. At least in part because of this ability to in some measure analyse the systems, there has been much criticism of the U.K. governments refusal to open the software to a wider analysis by outside cryptography professionals, notably from certain of those cryptographers who were involved in the certification. While these products are mainly used in governmental inter-departmental data transfers or military purposes, it would be a mistake to assume that these information transfers are of little interest since the content of the transfers is often data referring to individuals and may be of a highly sensitive nature. While there are very legitimate concerns about the security and also about the content of these data transfers, of equal (and growing) importance are those which do not (as yet) directly involve governmental regulation. These non governmental aspects can for convenience sake be divided into two main categories, individual privacy and business confidentiality issues. There are of course major areas of overlap both in these areas which any proposals for regulation or legislation must take into account.

Personal Privacy Issues

Personal privacy for the individual is rated highly on every report on consumer concerns in the information age, with worries about information mining - that is the correlation of multiple databases, from various sources creating a profile of the Individual from disparate pieces of information. This aspect of Privacy is itself he subject of many papers and books and insofar as the data is stored securely, collected and processed fairly is outwith the scope of this paper. There is also however, concern about the privacy of email and other information which may become available about individuals through their use of the Internet either inadvertently or through deliberate collection by Web sites set up to interrogate visitors computers. While these are real concerns and of vital importance to the individual, the recent wave of legislation from such diverse sources and the U.K. U.S., China and the European Union has been prompted primarily, not by altruistic concerns for their citizens but by the hard headed realisation that the much vaunted electronic commerce revolution will simply not take place unless both business and consumers believe that it is secure. The important concept here unfortunately, is that the users *believe* that the system is secure, not that it fulfils any objective criteria showing demonstrable security . While this may seem to be a very cynical view of both the regulatory as well as the political situation it is not at all far fetched. If current personal banking procedures are considered, almost everyone today holds at least one credit card or cashcard. These can be used to withdraw cash on presentation of a four digit PIN number. The size of the PIN is selected so as to provide a number which is easily remembered, but also provides an obstacle to the casual thief. the data on the card itself can be read by any card reader (available for under £50 from electronics stores) and the PIN itself, can be discovered either by watching or by the use of a short-wave radio easily modified for the purpose (again available from the same electronics store). Credit cards used in transactions are even more vulnerable since the slips generated contain sufficient information for fraudulent transactions. If other standard banking procedures are examined, most exhibit similar weaknesses. Why are these systems not replaced with more secure ones, Customers perceive them as having an acceptable level of risk with an acceptable level of security. A trade-off is taking place, the bank and customer accept a lower level of security on the basis that the system provides a higher level of "user friendliness", which encourages the use of the system, thereby increasing the volume and value of transactions processed via the system which thereby becomes sufficiently accepted.

Business Use (Banking)

To continue with the example already mentioned, this time from the business perspective; banks, it might have been reasonably supposed, will be only too aware of the uses and therefore the regulations required to create a secure cryptographic environment. As trustees not only of individual but also often ultimately of national wealth, it might seem natural that they could employ some of the most widespread and advanced cryptographic systems in use today. Unfortunately this is not always the case, Their systems are indeed very well distributed, but not necessarily completely secure. There are many reasons for this, but perhaps the most important is that security, which incorporates their crypto systems is a non revenue producing expense. Since the bank makes no money from its security measures, they must therefore serve another purpose, or purposes. Customers of these institutions will be the first to recognise the need for security especially in its traditional guise of security staff and strong vaults, simply to stop the traditional masked raider. However, with the bulk of banking transactions, both corporate and private being conducted, at least partially electronically, the less obvious security of the computerised delivery and corollary systems together with the general tracability and accounting systems have become increasingly vital, to such an extent that it is today inconceivable that a bank could function for any prolonged period of time without them. This should imply that these systems be as near as robust as possible to the point of infallibility, as well as highly secure. Unfortunately this is not necessarily the case across the board. There are several reasons for this which include:

- Operator ignorance and laziness,
- a lack of understanding both as to how certain systems function as they do, and more importantly, why they function as they do, even at an executive/managerial level.
- Innate flaws in the system, perhaps caused either through faults in the implementation and design or simply through software flaws
- Older less secure systems being still being used (perhaps because of known reliability) despite having been superseded and compromised
- Intentionally designed levels of security, which are not completely secure (e.g. PIN numbers which are used as Key pairs with the second number lightly encrypted on the plastic card)

Why then do most, if not all, banks (and their customers) accept this relatively poor level of guardianship. The answer as with the original question has several facets, the first and perhaps the most obvious, is that most customers and more junior or non technical bank officials simply do not know that the systems are insecure, they simply use them.

The second and equally important reason is that security in the banking environment is a non-revenue producing activity, this for purely business reasons currently puts caps on the level of expenditure that the bank is willing to spend, since it is to be run as a business and not, despite the marketing, for the convenience of it's customers. The consequences of this economic reality is that for the bank to be profitable, and therefore "safe" it is not necessary that their computer systems be absolutely unassailable so long as they are secure in practice most of the time. Just as most businesses realise that certain level of what is often euphemistically called "shrinkage" is inevitable, and budget accordingly, so too the banks and other financial institutions realise that not everything they do will produce profit, and therefore take account of that fact. Built into the cost structure of the banking system as with all other types of business is a percentage allowable for fraud, theft, and procedures for forcing the reconciliation of the accounts whereby a strictly limited level of error is tolerated. The simple fact is, that even with it's known (and well documented, if not publicly recognised) failings, the banking systems in use today such as A.T.M.s are adequate most of the time, at least for the functions in which the banks in the U.K. actually employ them. To understand this fully it is helpful to look at both what a bank actually does, and if not Banking law, then at least banking practice in the U.K. re: their customers.

Banks, like any other business exist to make money for their owners, they do this by taking calculated risks, occasionally they take a seriously bad risk and lose, but most often they gain. Since the abolition of the "gold standard" much banking has been done on the "trust" system, embedded in what is essentially contractual relationships. Individuals and corporations deposit money "trusting" that the bank will keep it secure and return it on the presentation of a legitimate demand, usually with interest. The Banks then lend out the vast majority of that money to other individuals and businesses, again trusting that the demands of the loan contract will be honoured.

In the complex fast moving world of finance today, it is neither practicable nor desirable that the tonnes of paper which would be required to track this system be used, therefore, which the original contract is often in writing, the record keeping is largely done electronically, indeed the record keeping of smaller scale banking such as is done at A.T.M. machines is completely electronic, so what happens when things go wrong and what does this have to do with cryptography?

Answering these questions in reverse, It is cryptography, or rather a variant on an application of it which allows such systems to function. Although there are important operational differences in the application of these systems from institution to institution, in general each ATM has a card reader installed, when a card is inserted, it's validity is checked against a database stored in the memory of the ATM, a final check is then performed when the user is prompted for a four digit "P.I.N" number. At first glance this appears to be a relatively secure system, however on closer examination it has several areas of weakness.

The first and perhaps the most obvious is the duplication of the card itself. The plastic card is almost always of a standard size and thickness with standard data stored on a magnetic strip on the back , this allows for customers of one bank to conveniently use the machines of another, but it also allows for much easier duplication of the cards since the hardware and software to read an write the information stored on the cards is available for a minimal cost. Several devices such as holograph technology have been introduced in an effort to make the cards harder to copy, but they can all either be easily bypassed, e.g. by using a different model of ATM, or they are of an intrusive nature which operators in normal situations may ignore.

A second weakness is the database stored in the ATM itself, who has access to, controls, and operates it. Some systems are designed that the database is automatically erased if the ATM is opened , even in normal operation (this was introduced in the wake of concerns over bank staff having access to customer PIN codes) however, the system itself had at least one programmer and there are also staff employed to update and administer the system, all of whom could conceivably either deliberately or accidentally introduce flaws, such as duplicate entries or entries which access the wrong account.

Another very common point made against A.T.M.s is that a four digit PIN is not overly secure. In the Past this was true, since most machines allowed an unlimited number of attempts, however in almost all machines today, the user is allowed only two tries before being warned that the card will be destroyed by the ATM if another wrong PIN is entered. Of course none of this will in any way stop users from either disclosing voluntarily, or being forced to disclose their PIN thus allowing access (on production of a card carrying the correct data) to their account

It should be clear from the above account that the security arrangements for electronic and automated data and transaction processing are not as secure as might have been thought at first glance. And while there are exceptions to this in the details, in general, most systems have similar flaws and are vulnerable to several different types of attack both technological and physical.

What has been done about it

Proposals as to precisely how to ensure that electronic commerce is as secure (if not more so) in practice, than high street banking have come from several different sources. Unfortunately, there has been much misunderstanding both of the proposals being made and of the problems which are presented in the first place along with a bifurcation of the motives for both the solutions and the issues.

The United States first real attempt to deal with the issue of electronic security was the so caller

"Clipper Chip" initiative. This failed for several reasons, not the least of which was the weakness of the encryption to be employed and the possibility of abuse of the "Back door" which was to be introduced at the request of the law enforcement agencies. In the face of a public and commercial outcry this initiative has since been shelved, however the issues which it raised are those with which almost every government is being forced to deal. This has been an ongoing situation in the U.S., the "Land of the Free" which in 1994 made it law that all telephone exchanges have ports added to them to allow remote telephone tapping, and in 1995 an FBI/NSA sponsored Bill attempted to introduce automatic tapping of 1% of *all* inter-city telephone calls

In October 1996 the U.S. Vice President Al. Gore announced a relaxation in the United States export restrictions for one year (which has now been extended) for commercial software providers, from 40 bit encryption software to 56 bit. 128 Bit software could also be sold under licence on a case by case basis. While this was hailed as a move in the right direction in many quarters, the reality is somewhat more disappointing. As is easily inferred from the terminology, the length of the key is one of the most important factors in determining the strength of the encryption being employed. The Best current estimates put the length of time that it would take to "crack" a 40 bit encryption key using DES on a fairly standard desktop machine of today's standards would take between one and two weeks, on dedicated machines either or on parallel processing "farms" of networked machines, DES can with relative ease by decrypted real-time, it is not too much of a jump of the imagination to envisage that this would routinely be done by any security agency since the financial resources required are trivial. As the writer of PGP has written "Standard DES uses a 56 bit key which is too small by today's standards, and can now be broken….. DES has reached the end of its useful and so has any software package that relies on it.". This to a great extent shows the irrelevance of the American "relaxation" of the export controls.

The substantive reason behind the change had much more to with the powerful software lobbying from companies such as Lotus and Microsoft who wish to take advantage of the burgeoning e-commerce market and who were being put at a competitive disadvantage by controls on the export of cryptographic products.

The competitive disadvantage about which the American companies were complaining was largely as a result of most other developed countries, especially those in the European Union having a starkly different policy towards encryption.

The policy in the European countries, while not totally unified has, until now, with the exception of the French followed a "hands off" approach, and even the French have recently relaxed at least some of their restrictions. This approach has also been adopted in the O.E.C.D. guidelines, the European Commission document `Towards A European Framework for Digital Signatures And Encryption,' (October 1997), In general, in Europe a trend can be seen recognising the fast diminishing value of attempting to regulate the use of cryptography by the general public, this can be gleaned from the statement from the Council of Europe in its Recommendation R(95)13 Concerning Problems of Criminal Procedure Law Connected with Information Technology where it stated:

> *"measures should be considered to minimise the negative effects*
>
> *of the use of cryptography on the investigation of criminal offences,*
>
> *without affecting its legitimate use more than is strictly necessary"*

A similar theme recurs in both the Communication of the European Commission "Towards A European Framework for Digital Signatures And Encryption" and the House of Lords "Agenda for Action" which both urge a relaxation in the regulation of encryption products. Similarly, in it's pre-election policy document "Communicating Britain's Future" the British Labour Party, now the U.K Government, state:

"attempts to control the use of encryption technology

are wrong in principle, unworkable in practice, and damaging

to the long-term economic value of the information networks."

Unfortunately, this clear statement of intention has since been superseded by what is in essence a revised white paper of the Previous administration entitled "Licensing of Trusted Third Parties for the Provision of Encryption Services".

The UK

The legal situation in the U.K prior to the "Licensing of Trusted Third Parties for the Provision of Encryption Services", which will remain in force until the consultation paper (or some version of it) becomes law is that there are no specific restrictions on encryption products supplied outwith the E.U. as long as the export complies with the Wassenaar arrangement or a licence is obtained from the D.T.I.. Certain states both within and outwith the E.U. of course have their own regulatory framework which must be complied with. Perhaps one sign that the situation is considerably less clear than is desirable is the Department of Trade and Industry recommendation that even though a license may not strictly be required, it should be nevertheless be obtained, and a lawyer consulted.

The current U.K. regulatory regime is now in a state of great uncertainty. With the adoption of the "Licensing of Trusted Third Parties for the Provision of Encryption Services" White Paper came an outcry from Civil liberties groups and from businesses concerned that implicit in the paper was the idea that they would have to had over (or escrow) their encryption keys to a government nominated body.

Trusted? Third Parties

The policy statement from the U.K. Government given as a written answer in the house of commons in May 1998 unfortunately only lays open the idea of a system of TTPs it does not even attempt to answer many of the Key questions that such a regime poses, probably because of a lack of clarity both in the minds of the politicians as to precisely what form the infrastructure should take, and in the uncertainty as to how the electronic networks are developing.

There are many models of how TTPs should function, and just as many conflicts over their proposed shape, powers, duties and obligations, both to the public and the authorities. Currently most favoured by the U.K. legislature is a multi-functional "voluntary" system with TTPs being appointed via a license issued by the Department of trade and industry. One issue looms large over all the others with these proposals, the question as to what a multifunctional voluntary system actually is. This has yet to be clearly defined since all the current statements which I have seen contain either inaccuracies or vague assurances of propriety. Perhaps the best (if not the only) way to see what this phrase can mean is to look at what TTPs *could* do, then decide whether they *should* perform these functions and finally try to discern a clear and useful function (if any) for them, if needed.

- Trusted Third Parties, it is alleged, can provide a secure, efficient and economical method of ensuring that when two parties contract on-line with each other, both in the commercial and consumer sphere, that each is who the other thinks it is.
- They can provide escrow services for cryptographic keys which, it is submitted by supporters, may be useful in the event of an employee leaving and not surrendering their key. They can provide a convenient means for law enforcement agencies to gain access timeously to encrypted data in whatever form.
- They can provide disaster recovery and a range of other support services from a properly

accredited source.

Unfortunately there are difficulties with each of these proposals.

Starting with the idea of an employee leaving encrypted information behind them. Any organisation which gives its employees sufficient trust (and who have sufficient computer literacy skills) to use encryption, need not be overly concerned about a rogue employee. Quite apart from the implicit breach of the employment contract which can be enforced, any employee acting in this fashion can be charged under the computer misuse act, since a refusal to return the key, or destruction of it could easily be construed as unauthorised modification. Additionally, any commercial entity which today encourages it's employees to use encryption will be aware of the numerous methods which can be used to prevent precisely this situation, indeed, systems utilising anything other than the most basic password protection (such as that employed in MSWord) will have contingency plans, these of course may range from simply keeping copies of everyone's encryption key in the safe through periodical backups of crucial software to full fledged disaster recovery systems including real-time duplication of system events to a secure server with a valid firewall. Of course, should the employee choose to use non-approved software, or something such as PGP with a different private key from that used for normal work, only the most complex security systems will have a chance of retrieving this data. However since encryption of this level is already freely available, and the employee is intent on doing damage, it is highly unlikely that they would baulk at a minor misdemeanour like installing a non-approved package if they are willing to purposely conceal data. It this situation, the key held by the T.T.P. would be of absolutely no use whatsoever.

The same point hold true for the claims that TTPs will allow timeous decryption of criminal activity, at least in relation to computer systems. Just as a disgruntled employee could use non-approved encryption packages and keys to bypass company security policy, so too could anyone who was concerned that law enforcement not be able to access their files. Dorothy Denning, although a supporter of Key escrow makes precisely this point both in her paper Crime and Crypto on the Information Superhighway and in Codes, Keys and Conflicts: Issues in U.S. Crypto Policy

It should also be noted that key exchange can already be facilitated via several different systems e.g. the P.G.P. public key server networks which are available to anyone on the Internet free of charge. Disaster recovery is an entirely different issue, and one which has little or no bearing on cryptographic policy

Escrow

As has been noted, it has been suggested that one function of the proposed TTP system could be Key escrow, the handing over to a third party of the private key, or at least segments of it to various approved agencies. The purpose of this is apparently severalfold. The first, and perhaps most important purpose, is to stop wrongdoing, to prevent large-scale fraud and other criminal activity. The obvious difficulty with this is that criminal enterprises are hardly going to happily pass over the correct key, I find it difficult to imagine e.g. the Colombian Medelin Cartel handing over their organisations key (should such a thing exist how do they register it, perhaps as "Drugs"R"Us). Hardcore criminals are simply going to ignore any system which can in anyway compromise the integrity of their enterprises. Perhaps more likely is the use of an escrow system to discover large scale corporate fraud such as happened in the Robert Maxwell pension fund fraud. However I would suggest that anyone involved in such activities will either simply not keep the records on computers, or more likely will use a non-escrowed key. As the Law Society response to the DTI consultation document puts it:

> *"it seems obvious that "crooks and terrorists" will use "something else"*
>
> *to avoid handing over keys to anyone who might in turn hand them over to*

> *the law enforcement authorities and we do not see how the existence of the TTP regime will discourage, let alone prevent, it"*

The only circumstances in which a key escrow based TTP regime has an indisputably valid function technically is in the covert data surveillance of individuals under suspicion of criminal activity. The problem with this is succinctly, although implicitly accepted in the IHAC report:

> *"Historically, state intrusions on privacy in the form of search, seizure or electronic surveillance have been based on the justification that there are grounds to believe that the individual whose privacy the state seeks to invade is either involved in some form of wrongdoing, or has some concrete evidence of wrongdoing. These are the criteria applied by the courts in balancing individual privacy against state interests.*
>
> *The same principles would apply to encrypted information, but decrypting information is not identical to either of the existing precedents - seizing evidence with a search warrant or intercepting communications with a judicial authorization. If decryption requires access to the keys, seizing them with a conventional warrant would alert the recipient of the message that he or she was under investigation."*

The logic of this argument is irreproachable, that is, until the logical consequences of it's application are applied and the current Jurisdictional and statutory situation is considered. It is true that requiring keys be handed over to allow examination of encrypted data would warn even the most technically illiterate suspect that they are under scrutiny, however, requiring everyone that uses encryption to escrow their keys (or even a portion of them) merely alerts everyone to the lowered security of the system and encourages the use of "something else". It was recently reported that a version of the "Lotus Notes" suite of software was sold to the Belgian Government with 75% of its allegedly secure encryption algorithm compromised, having been escrowed to the U.S. government as a condition of allowing the sale of the product abroad under the "relaxation" of 1996. Since this software was intended for governmental use it is likely that at least some of the software was installed on systems where security is of vital importance, despite the official denials. Needless to say the Belgian government were very unhappy at the idea that their confidential information could be read with relative ease, even by a country which is supposedly regarded as an ally.

The argument that TTP's could provide a means of covert surveillance therefore fails on the basis that since the users are aware of the weaknesses in the system, the very people whom the enforcement agencies would wish to keep under surveillance will not use the system because of those very weaknesses. Those who would use the system are the normal naive honest companies and individuals in whom the security services would have no interest. It has of course been suggested, that this is precisely the reason that both the U.S. and U.K. governments favour a T.T.P./Escrow system given their joint interest in the "Echelon" surveillance and intelligence gathering system at RAF Menwith Hill.

> *The European Parliament is now asking whether the ECHELON communications interceptions*

> *violate the sovereignty and privacy of citizens in other countries. In some cases, such as the NSA's Menwith Hill station in England, surveillance is conducted against citizens on their own soil and with the full knowledge and cooperation of their government*

At least in theory, to gain access to the private information of an individual or a corporation, the security services must first obtain a Judicial warrant either requiring delivery or permitting seizure of the suspicious materials. For the warrant to be granted they must, in general, first convince a judge that they have cause to suspect something amiss. The grounds of suspicion of criminal activity which is presented as the "evidence" for the granting of the warrant while not necessarily of a very high level of proof, must have been obtained through other sources than the material to which the warrant pertains. Should encrypted data be subject to a lesser standard, which is itself even more open to abuse than the warrant system?

Digital Signatures

At the heart of any contract is the requirement that the terms of the contract be clearly understood, the most basic term to be agreed, of course, is the identity of the parties. There is no strict necessity for personal information as such to pass between the parties, as often such information is completely irrelevant, e.g. in a shop the customer need not know anything about the assistant or vice versa, for a contract to be formed in the shape of a sale of some good. In this case sufficient information has passed in the characterisation of the parties as customer and assistant. However, in many contract there can be a need for much more information. If engaging the services of a lawyer, it is vital that the person so employed actually be a member of the law society, if using a credit card it is vital that the signatory of the authorisation slip actually be the card holder, the same is true where cheques are to be used. Even in noncontractual relationships authenticity can be a problem issue. If for example an unauthorised person gives legal advice in the name of a qualified solicitor, or a stockbroker is induced to sell shares thinking he is doing the wishes of his client when in fact the message was false, or in error then a multitude of difficulties can arise, both legal and otherwise. In an electronic context where face to face communication is currently, and in all likelihood, will remain the exception rather than the rule, it becomes even more important that each party is as certain as possible of the identity of the other.

To satisfy this need, cryptographic software writers have come up with the concept of the unforgeable digital signature. This is an arrangement which is in many ways similar to the asymmetric public key model used by most heavy cryptographic systems. In fact often the same software , indeed the same keys, are used to generate both the digital signature and the encryption. The U.K. consultation document proposes that the "voluntary" TTP system which is to be instituted in Britain should be used not only as a key repository and recovery service, but also as a certifying authority for digital signatures and identification verification, again to ensure that the sender and recipient are actually who they claim to be. The main justification for this proposal, which is also used as an argument in favour of key escrow is that for the electronic markets to flourish, reasonable certainty of the status of electronic contracts and of the identity of the parties making them is essential. Earlier in this discussion I looked at the level of identification which was required for the formulation of a contract in a purchase of an item in a shop and found that it was not particularly high. What is being proposed here is that a far higher standard be imposed on electronic commerce to allow parties who are otherwise unknown to each other to conduct business over the electronic network on the basis that the certification and authentication provided by the TTP will be sufficient to create a form of "ring of trust" between otherwise unrelated companies and individuals.

This proposal, while apparently sensible in theory, surely runs contrary to accepted business practice in several areas, and is in reality quite unnecessary. Where one-off contracts are to be concluded at the consumer level, then the most appropriate method of contracting and payment is surely a secure S.S.L. server, perhaps backed up by the data sent by SSL being again encrypted using an asymmetric public key system. Where the contracts to be tendered are between businesses or are of a large scale, I would suggest that it is highly unlikely that these two entities would have no communication between them other than electronic contract making, there will, probably at a senior level be a meeting, at which keys and digital signatures could easily be exchanged.

Such meetings and exchanges, as well as serving a useful social function (since everyone likes to know with whom they are dealing) obviate the need to introduce a third party and therefore a third weakness into the security of the arrangement. This is explicitly acknowledged in the English Law Society response to the D.T.I. consultation document in it's section 1 comments:

> *"The Paper says (para.42) that "TTPs will allow UK Business to take advantage*
>
> *of; "secure electronic trading". We find it difficult to think*
>
> *of reasons why those who use encryption in the course of business*
>
> *would want to make use of TTPs services. To do so would create*
>
> *a security risk by giving the capacity to decrypt information to others*
>
> *outside the control of the sender and intended receiver, thereby increasing*
>
> *the number of those with access to it, without, as we see it, any material corresponding benefit. In our view. the very great majority of encryption users would not want*
>
> *to give any outsider information which could allow access to their encrypted*
>
> *material, however apparently trustworthy the outsider. They would rely*
>
> *on contractual arrangements with those with whom they wanted to communicate*
>
> *and which did not require the disclosure of their keys to anyone else."*

While the Law society is clearly thinking primarily of unauthorised disclosure by employees of the T.T.P. or accidental or negligent disclosure, there is also the issue of deliberate, unauthorised hacking of the T.T.P. to be considered. Anyone with reasonable computer skills and a working knowledge of system security can safely set up a simple server, joining it either to an existing network or a new one. It merely takes time and patience to test and re-test to iron out the inevitable bugs. However, it is an entirely different proposition to ask that person to set up a system with is absolutely secure. In reality, it is probably impossible. Every operating system ever written, indeed every computer program over a few lines long has some bugs in it. Therefore the communications protocols themselves have inherent bugs, as do both the client and server applications which are to be used. Native system vulnerabilities can to some extent be eliminated by careful configuration and use of monitoring and independent security systems. The difficulty is that these systems are not the most user friendly to use and can themselves introduce new vulnerabilities. For a simple server, it is enough that it works most of the time. The systems of the TTP on the other hand must be fully secure and operational at all time, otherwise there can be no viable justification of the TTPs to existence. Since 100% reliability and security are impossible goals, there must be an approximation of this through the use of backup systems and verification procedures, again time consuming and difficult to secure.

An added problem for anyone potentially interested in setting up as a T.T.P. is that the same requirement for security which will both permit the organisation to be certified as secure and also attract customers will also attract attention from hackers. There is nothing more appealing to a dedicated computer hacker than a public statement of security. To hackers it is the digital equivalent of a declaration of war. Sooner or later then hackers will break the system, either by replacing it via methods such as I.P. spoofing, or simply by hacking it in the "traditional" way. Once a TTP's system has been compromised once, irreparable damage may be done not only to it's own business interests through lack of customer confidence, but genuine harm can come to it's clients through their private keys and potentially other equally sensitive data being in the hands of unauthorised persons. Even if the hackers were to simply breach the defences of the TTP and the leave without even looking at any data, the very fact that the system had been compromised would both undermine confidence and result in expense and administrative difficulty in issuing new keys, replacing compromised and potentially compromised data, installing new security procedures (which may themselves introduce new bugs, and have to be tested) and generally attempting to repair damage which can never be totally undone since the "Trusted Third Party" has shown itself unworthy of the trust shown it by allowing it's systems to be vulnerable in the first place.

When is a signature not a signature

The proposals are also unnecessary in that they, by giving a special status to digital signatures which are certified by licensed TTPs (a rebuttable presumption of validity) are at the same time, in effect taking away that same presumption from the signatures of people who do not use the service. I can see no reason why it makes sense that the currently existing presumption of validity (which is used in thousands of transactions daily even now) should be de facto removed and replaced with a much more restrictive regime especially in the case of consumer contracts. In this situation, a credit card is the most common method of payment, as with the PIN and the cashcard, the weaknesses of this system are well known, but it still enjoys consumer confidence, and has a clear procedure where a dispute arises over a transaction. The current lack of consumer confidence over the use of the Internet an electronic commerce has far more to do with a lack of knowledge of how electronic security procedures work, and are implemented, than to do with a real need for tighter legal controls. What is in fact necessary is more publicity and a wider acceptance of the 99.9% of transactions which are processed without difficulty than a highlighting of the small number which do not.

TTP or not TTP

The difficulties which the introduction of a TTP based infrastructure would present have been to some extent recognised in the last month with the publication of the "Building Confidence in Electronic Commerce" DTI consultation document.

"We have listened to industry -- they have persuaded us that it (key Escrow)

might not be the best way forward,"

The biggest impact of this paper so far has been the governments insistence on a 3 week "consultation" period rather than the governments own guideline specified eight weeks. The twist in the tail is however that key escrow is "not dead and buried at all, Of course, it is still an option, and we'll have to see what else comes up" While official complaints have been lodged with the Parliamentary Ombudsman over the shortness of the consultation paper, it seems likely that the U.K. Government will adopt the second approach laid out in S18 of the document of passing enabling legislation so that such changes in the law as it deems necessary can be passed by Statutory Instrument, since to follow the first approach would take much longer and there is a desire in the legislature to move quickly on this issue. The second approach also has the benefit of allowing what might otherwise become issues of contentious public debate to be quietly passed into legislation.

Criminals using TTP Infrastructure?

In this paper as I originally envisaged it, this would be a long section ridiculing the idea that criminals would use a system whereby the encryption keys which could decode files which could send them to jail were placed in the trust of a government appointed agent. However, the publication of the DTI consultation document in March 1999 which acknowledges that this will be a problem and the recognition that there is no reason for criminals to use such a system, especially when there is in existence an alternative which does not involve escrow and which is not prohibitively expensive. The use of PGP or similar non-escrowed products is only one solution, although a very secure, and well known one, an equally simple alternative is that since key escrow and TTP licensing *must* be global to be effective where international trade or transactions are concerned, is for the criminal to move their electronic base of operations to somewhere which does not support this "standard"

The Weakness of Dennings and the Law Enforcement case

> *Criminals are lazy, greedy and they make mistakes....We are able to capitalise*
>
> *on this and we anticipate that a licensing scheme would allow us to have some*
>
> *successes....We would prefer to have a mandatory licensing system because*
>
> *that would be more inclusive"*
>
> John Abbott, National Criminal Intelligence Service Director

This statement, made without the backing of cases echoes the sentiments of Louis Freeh, current director of the F.B.I. who was also a strong supporter of the failed "Clipper initiative" and now supports mandatory Key escrow":

> *"Which, had the NSA not panicked at the AT&T crypto phone and*
> *persuaded them to incorporate it, the 3-DES version of the phone would*
> *have sold a few hundred units and then been abandoned. Crypto would*
> *still be an obscure subject of interest to a couple of hundred mathematicians"*

These two quotes, taken from people who gave evidence to the same committee on the same day shows the crux of the problem. Law enforcement, quite reasonably, wants tight regulation so that they can concentrate on catching criminals, unfortunately the regulations are coming too late to be effective and so would not fulfil their stated purpose.

The only database which I have been able to discover of any size of cases involving electronic encryption is that maintained by Dorothy Denning of Georgia University and William Baugh which had not been updated in almost two years. This material contains references to such terrorist attacks as the "Supreme Truth" nerve gas attacks on the Tokyo Subway and the World Trade Centre Bombing. However in these cases, either the Suspect was arrested and then supplied the Key (as part of a deal or by leaving it stored on a seized disk) or the suspect was arrested and the cryptography itself was broken. One terrorist case in particular is of interest, that of Leary, the New York Subway Bomber. This case is of interest not because the case itself, but because the encryption used by him *did* stand up to the best effort of "outside experts" but was eventually broken by an unnamed "federal agency" (the information found was of little or no use). This case implies that the U.S. government have a rather better ability to crack coded mail than exists in the public sector and must cast some doubt on the necessity of the law enforcement communities desire for stricter regulation, if such messages can be broken when necessary. The criminal cases cover such organisations as the Cali drugs cartel and Dutch organised crime. These sophisticated criminals have, it is claimed, been using several different forms of encryption in an attempt to cover their activities, however, there is still sufficient information on them that they can be tracked, identified and even convicted from other evidence with information coming from encrypted files providing little more than confirmation of what was already known. A thorough traffic analysis, will yield information about who is talking to whom and when, in many cases this is enough for law enforcement agencies to investigate further, and so discover more evidence which can then be backed up by decrypting computer files if necessary. Strict regulation of *all* traffic is not necessary for this, and may in fact serve to alert criminals to use other less obvious means of communicating.

Probably the most disturbing cases where any regulations are being revised are those which involve attacks on children in whatever form. Cryptography, and specifically PGP, it is claimed, is being used by organised groups of Paedophiles to trade indecent images of children and to store them securely on their computers, According to the Denning Datatabase the favouring of one particular package over other was because online paedophiles are "generally educated, technically knowledgeable, and heavy Internet users". While this is doubtless true, paedophiles are by their very nature secretive and will use the best available resources to hide their activities. This cannot be extrapolated to mean that cryptographic tools are to blame for the wrongdoing of a tiny minority of the users. There already exists strong legislation against child pornography and abuse. Introduction of regulations over the whole area of cryptographic policy is a "knee-jerk" response which more importantly will fulfil no useful function since paedophiles, like other criminals, are hardly going to respect regulations which could potentially lead to their capture and imprisonment.

Conclusion

It is clear from this paper and all the available that the availability of strong cryptography is a very mixed blessing, on the one hand it can be used in the development of electronic commerce and the maintenance of personal privacy, on the other it does provide a useful tool for the criminally minded. However, as to whether the arguments for criminals using cryptography is a reasonable justification for the introduction of heavy handed regulation which would attempt to limit the availability and use of such products - the conclusion is clear. While the law enforcement communities case does hold some water, it is simply not enough. It is true that if encryption was completely illegal, and unobtainable, it would in some cases make the conviction of the criminal somewhat easier, it might even mean that a few more were caught, but the price is simply too high. The infrastructure for strong encryption for the individual already exists on a transnational basis. If regulations are promulgated which require the use of Trusted Third Parties, lower strength encryption or even merely a heavy paperwork burden (which increases costs) what must happen is that those citizens who are law abiding in the first place will follow the new regulations, whereas those who are not will simply ignore then and continue to use the system which is currently in place anyway, of strong, virtually unbreakable encryption, unencumbered by any legal framework. The only way in which this could be made effective is to outlaw all non-regulated products and then trace any traffic which uses them. This is simply not technically feasible, and is also a great deal of effort when a)the number of cases which actually involve cryptography is still very small and b) the files which are eventually decrypted often have little or no bearing on the outcome of the case.

The reality of the U.K. proposals as they stand is that they may provide a placebo for non technical business and private users but will create a cumbersome system with very serious flaws which flies in the spirit, if not the letter of the directives which it seeks to implement, to say nothing of the desire of the majority of informed users. The reality is that strong encryption is available to the ordinary user, and any governmental attempt to successfully control it will have to be world wide, not simply national. This is of course ignoring any financial cost which the proposals will place on business, and the possible competitive disadvantage at which it will put them.

The reality is that misunderstanding (whether intentional or not) surrounding issues of how electronic networks function and the available security measures, has resulted in White papers being produced which merely show that there is confusion over many aspects of the situation. Unfortunately for us these white papers are very close to becoming law.

> *The spooks' underlying problem is that they have invested enormous amounts of time and effort persuading the pols that `something must be*

done' about cryptology. However all the practical proposals they have come up with just look set to make the problem worse.

Ross Anderson 1999