The Regulation of Investigatory Powers Bill –

Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses

by Ian Brown and Brian Gladman

Introduction

The Regulation of Investigatory Powers (RIP) Bill currently going through Parliament will introduce powers to allow a number of UK authorities to intercept Internet communications and to seize encryption keys used for the protection of such traffic and for the protection of stored computer data. Such powers are not limited in their application to those involved in criminal activities and this means that law abiding individuals and businesses may be subject to interception activities as well as demands to hand over their encryption keys. Although abuse of these powers may well be limited, there can be no doubt that this will sometimes occur and this means that honest computer and Internet users will bear increased risks to their privacy, safety and security once this legislation is enacted.

This paper aims to show that the envisaged powers for interception and for the seizure of encryption keys are technically inept. It also aims to offer honest computer and Internet users advice on the practical steps they can take to maintain their privacy, safety and security in the presence of the oppressive powers introduced by this legislation.

There are three areas of risk that will be covered separately:

- the interception of electronic mail;
- the seizure of information on a user's computer;
- the seizure of encryption keys.

Preventing Email Interception

In order to understand how to avoid the risks of email interception introduced by the RIP Bill it is necessary to understand in outline how the Internet works. This is covered in the next section, which can be skipped by those who already have this knowledge.

The Internet Protocol

The Internet is built on a simple but powerful way of moving data from one computer to another called the Internet Protocol (IP). In basic terms any data that needs to be exchanged is chopped up into small pieces called 'packets', these packets are marked so they can be checked and reassembled later, destination labels are added and they are then sent to the Internet for delivery. The packets then pass individually across the Internet and when they reach their destination they are checked and reassembled in the right order to recreate the original data item. Many different types of data can be handled in this way, for example, electronic mail messages, web pages or even direct voice and video messaging.

Most home users connect to the Internet using a telephone line and a computer fitted with a device called a modem. When a user wishes to connect to the Internet, their computer uses the modem to dial the access number of an 'Internet Service Provider' (ISP), after which it is given an 'IP address' which allows it to exchange data packets with any other computer that is also connected in the same way.

IP addresses are in a numeric form (e.g. 94.60.38.75) but there are special computers on the Internet running the Domain Name System (DNS) that act like telephone directories so that somewhat more meaningful names (e.g. www.parliament.uk) can be converted into the numeric addresses that computers need. Many sites have permanent IP addresses but users are often only given a temporary IP address when they are actually Internet connected (that is, when they are 'on-line').

Electronic Mail

Although two IP connected computers could exchange electronic mail (email) directly, such an approach would often be inconvenient because both computers would have to be on-line at the same time. To avoid this difficulty Internet users are provided with a 'post office box' in which their incoming email is stored for them until they next make a connection. In fact there will often be different servers for incoming and outgoing email. This approach is often referred to as 'store and forward'.

After a user connects to the Internet and starts their email software, the latter connects to the incoming and outgoing mail servers using IP connections. Once such connections are made, the server will then ask the user's computer to supply details of their account name and password in order to ensure that any email is accepted from a legitimate customer or correctly delivered to its intended recipient. After these account details have been checked, a prearranged set of messages (a protocol) is then used to manage the collection and delivery of each item of email. And when this has been completed the connections between the users' computer and the two servers are terminated.

Although it is normal for a customer to obtain their IP connection and their email service from the same service provider, such an arrangement is not necessary – the only essential service is an IP service since this can be used to access email servers anywhere on the Internet. In consequence once a user has such an IP service, they can then obtain their email service elsewhere they want. There are now a large number of independent email services available, very many of which are free.

The ability of UK users to obtain an email service that employs servers outside the UK has serious consequences for the interception of email messages. If, for example, such servers are located in a country where email interception is unlawful, a UK user's email cannot be intercepted while it is on these servers. However, a UK user's email still seems to be vulnerable to interception when they make a connection to their mail service from the UK. However, this turns out to be incorrect since these data exchanges can be encrypted and this can be done in a way that does not allow keys to be seized.

In practice there are several easy ways in which UK citizens can reduce or even eliminate the risk of email interception.

1. Choose a Small ISP

Firstly, since the Government has said that it only expects to implement email interception at a small number of ISPs, it is quite easy to reduce the risk of interception. For example, it is very unlikely that the Government will install interception equipment at the many small ISPs since the overall costs of doing this will be high and the gains involved will be very limited. It is very likely that any interception capability will be at larger ISPs and this means that using a small ISP can reduce the likelihood that email is vulnerable to interception. Some care would be needed in the choice because some small ISPs obtain services from larger ones and their email may still be subject to interception. In practice a user who employs this approach could not be certain that their email was safe, but the chances that it could be intercepted would be small. If they were really worried, they could use several different ISP accounts and alternate between them to increase the difficulties involved in intercepting their email.

2. Email Accounts Hosted Outside the UK

But there is a much better way of avoiding interception by setting up email accounts outside the UK. As indicated earlier, provided that the location of the mail servers have been chosen to be outside the jurisdiction in which RIP powers apply, any email stored on these servers cannot be read by UK authorities.

At first sight it might seem that email could be intercepted when a UK user connects to their overseas server to send or receive their email but this is incorrect. Using a technique called Diffie-Hellman key negotiation it is possible for the user's computer and a mail server to

negotiate, generate and use unique encryption keys to encrypt all data passing between them. And once such keys have been used they can be immediately destroyed so that they cannot be seized. The data exchanges required for a user to send and receive their email from an overseas mail server can hence be completely protected. As a result, the only place in the UK where the email could be obtained by UK authorities is on the user's own computer.

In fact many popular email applications already include facilities to encrypt these data exchanges with mail servers so all a UK user has to do to avoid email interception is to sign up with one of these services (many are completely free). Examples of electronic mail services that can be used to circumvent RIP email interception powers in this way include:

- http://www.messagerx.com
- http://www.mail2web.com

It will be important to use strong cryptography to protect email account access because the use of such accounts is likely to attract GCHQ interest using certificated warrants ("trawling warrants") targeted against encrypted traffic.

3. Direct Email Delivery

If most computers had permanent connections to the Internet any email could then be sent directly without the need for mail servers. While permanent connections are somewhat unusual at the moment, the introduction of ADSL and cable based Internet access will mean that many Internet users are likely to migrate to permanent Internet connections and this will mean that email packages will become available that can make use of direct connections for email delivery. This will mean that the success of interception based on the existence of email servers is certain to decline with time and seems likely to have a very limited useful life. In consequence it is very hard to see the implementation of such approaches as a good investment of taxpayers' money in the fight against criminals on the Internet.

4. Secure Internet Protocols

There is a powerful new Internet Protocol currently being introduced – IPv6 – that will allow two Internet connected computers to negotiate, use and destroy unique encryption keys for each data exchange. This will provide secure encryption using keys that cannot be seized and will protect all the traffic between the computer systems involved. This is now being progressively deployed and is likely to become the universal standard for IP data exchange well before the end of this decade. If implemented properly such secure IP services will protect ***all*** Internet services – email, voice, video and all other services – from attempts at interception. Again, therefore, investments in Internet interception will become completely ineffective as new Internet technologies are introduced.

Conclusions for Email Interception

From this analysis it can be seen that:

- RIP powers for email interception are already trivially easy to circumvent;
- The already questionable value of such powers will be completely undermined as new Internet technologies are introduced over the next few years.

Storing Data Securely on Computer Systems

Legislation already provides powers for law enforcement authorities to seize computer systems and the data they contain if they suspect owners of criminal wrongdoing. The RIP Bill extends these powers by allowing authorities faced with encrypted data to demand that it be decrypted or, in some circumstances, to demand copies of the encryption keys that have been used to protect it. One of the arguments used to support the RIP legislation has been that criminals will see the dangers of computer data being seized and will increasingly resort to the use of encryption. In practice this argument appears to be based more on fear than on

reality since there is very little evidence to suggest it is actually happening to any significant extent at the moment.

But RIP powers for key seizure are not limited to those suspected of criminal activity and this means that honest users who are concerned that their computer data might be seized need to understand how they can protect themselves from the risks to their privacy, security and safety that this would involve. In practice anyone who really wants to avoid their data being seized has many ways of doing this.

Effective Information Security

A key concept for effective information security is that of 'defence in depth' – information that needs to be highly secure should be given several layers and several different forms of protection. An analogy is that of the medieval castle:

- built on a hill to reduce the possibility of surprise attacks;
- surrounded by a wide moat;
- protected by a strong outer wall (with little ground between the wall and the moat);
- an inner walled area – for example, a keep – so that attackers who penetrate the outer defences have further hurdles to overcome;

where there are several layers of defence, each posing different problems for attackers and each arranged so that they are mutually reinforcing.

Exactly the same principles apply for protecting information stored on computer systems and some of techniques involved in building layers of protection will now be described. Used carefully and in combination these can provide barriers that are close to impregnable for stored data.

Data Storage on Computers

Most computer systems typically have a single large hard disc drive with space for several gigabytes of data. If there is sensitive data on such a drive it can be encrypted to protect it but it may still be vulnerable if the encryption keys used are not properly protected or if they cab be seized using RIP powers.

In fact, such storage is not very safe for many other reasons. For example deleted data will often be very easy to recover and, even when a considerable effort has been made to remove it, sophisticated techniques will sometimes be able to recover it.

For these reasons the most important first question to ask about storing critical secret information on any computer is 'does it really need to be there?'. Computers, especially ones that are used to connect to the Internet, are not very secure and this means that they should not be used to store secret information unless this is absolutely unavoidable.

Encryption

Encryption allows data to be scrambled in such a way that it can only be recovered by using special keys. It offers a powerful technique for protecting information but one that is subject to a number of risks including the following:

- if keys are lost the owners of encrypted information will no longer be able to access it;
- if keys are stolen (or seized) others may be able to access any of the information that they protect;
- encryption capabilities may not be properly engineered and there may be easy ways around the protection which they seem to provide;
- encryption software is often quite difficult to use and this will sometimes mean that users make mistakes that undermine the protection that is available.

In practice, these difficulties mean that encryption is much less valuable for protecting stored data than many people expect. While some of the above problems will eventually be overcome as the technology develops, relying on the use of encryption alone to protect stored computer data is not sensible at present. This will be especially true once the RIP powers are available since honest people may well be forced to give up the keys on which their privacy, safety and security depend.

Steganography

Steganography – information hiding – provides a powerful technique for protecting information simply by hiding its existence. With encryption data is scrambled but its existence is not hidden and this means that anyone who obtains scrambled data will know that there is a key to it somewhere. This is an immediate vulnerability that can be avoided by hiding the existence of the information in question.

Ross Anderson, Roger Needham and Adi Shamir[1] have described a powerful concept known as a 'Steganographic File System' (SFS) in which the filing system on a computer is set up in such a way that the existence of files can be hidden by a password. Importantly there can be several layers of protection so that, for example, revealing the password to the top layer does not reveal ***anything*** about lower layers. Faced with a demand for access to data held on such a system a user could hence provide passwords to several layers of files but not reveal the fact that more layers exist. Any authority that seized a computer with such a file system could never be certain that they had scanned all the data on the computer since there might be hidden layers that the owner has not revealed to them.

At the moment the availability of steganographic file systems is somewhat limited. Examples are available on Linux and Unix systems but users of the popular Microsoft Windows operating systems are less well served. But there can be little doubt that this will soon change.

Such file systems are more powerful than encryption for protecting stored data since they mean that anyone who gains access to a computer using such a system can never be sure that they have gained access to all of the information that it contains. Of course, encryption can be used in combination with steganography to provide a formidable challenge for anyone trying to access this information against the owner's wishes.

Physical Steganography

A major problem with the use of encryption or steganographic techniques to protect stored computer data is that law enforcement authorities will eventually wake up to the need to develop the expertise needed to overcome these types of protection. The possible law enforcement use of experts is the most powerful approach to combating criminals on the Internet. It is undoubtedly the right approach and will, hopefully, be limited to such ends but abuse cannot be ruled out so it is worth asking what honest owners of computer data can do to limit such risks.

If computer data is stored on a typical hard drive, expert examination of its contents is likely to reveal a lot about the data it holds. The best way of avoiding such vulnerabilities is not to store sensitive data on such discs but to rely instead on removable disc drives.

Disc drives that use removable disc cartridges are now quite inexpensive and have capacities ranging from 100 megabytes up to several gigabytes. By using such removable cartridges, critical data can be stored away from the computer when it is not in use and this greatly reduces its vulnerability. Moreover, if such a removable cartridge is not loaded on a computer when the latter is used for Internet access, the vulnerability of the data to access via the Internet is significantly reduced.

---

[1] The Steganographic File System, by Ross Anderson, Roger Needham and Adi Shamir, available at: http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.ps.gz

If a computer system is seized it is quite possible that an associated removable cartridge might not be found. Of course if the removable drive is present on the computer, the authorities will be looking for removable cartridges so it will be important to have some around that contain innocuous data that they can seize. But once removable cartridges are being used, any authority that seizes a computer can never be certain that they have gained access to all the data held by the owner since they cannot be sure how many cartridges are in use. Protection is limited only by the ingenuity of the owner in physically hiding disc cartridges and this means that this form of information hiding – physical steganography – provides a remarkably simple and yet extremely powerful technique for maintaining the secrecy of stored computer data. PACE and RIP are powerless against these techniques so there is no reason for any careful computer user who really needs to protect their critical data to worry about such laws. Of course it is best not to lie to law enforcement authorities so the question about how many removable cartridges are in use should simply not be answered!

There are many associated things that can be done to make it more difficult to find computer data stored on a removable hard disc system:

- As discussed already, if a removable disc drive is permanently fitted, several cartridges containing innocuous data can be stored near the computer to mask the possible existence of other more sensitive cartridges.
- some removable disc drives can be detached from the computer system when not in use so that law enforcement authorities would not even be aware that the computer can use removable cartridges (but care is needed to ensure that loaded software and drivers do not betray the existence of such a drive).
- The removable disc could use both data encryption and a steganographic file system to guard against the possibility that it may be found in a search.

Data Storage Outside the UK

The RIP legislation provides the power to seize the keys that protect data that has already itself been seized so an obvious step is to ensure that critical data is not subject to seizure, for example, by storing outside the jurisdiction of UK authorities. If data can be stored in this way, encryption can then be used, as discussed earlier, to protect access to it without using keys that can be seized.

Fortunately there are now many companies that offer users free disc space to store their computer data at remote locations so anyone who has data that they want to store in a way that UK authorities cannot seize has many easy options to choose from. One example of an organisation providing free disc space outside the UK is:

- http://www.freedrive.com

There are many organisations offering similar facilities. These not only store data beyond the reach of UK authorities but also make it very difficult to discover the full range of data available to anyone who uses such services.

Techniques That Criminals Will Use

The techniques discussed so far are those that it is sensible for honest people to use to protect their email and their stored computer data. Of course, all of these techniques are available to criminals as well but there are even more powerful ways in which criminals can create almost insuperable difficulties for law enforcement authorities when faced with stored computer data.

Quite a few of the sites that offer free disc space, also offer facilities that allow such space to be shared among a number of users. Some already offer fully anonymous access and those that do not can easily be accessed through services that provide anonymity. Services offering both shared access and anonymity seem ideal for use by paedophiles and others who want to store and share obscene material without taking the risks involved in storing

material on their own computer systems. It is hard to believe that such evil people are unaware of these capabilities but even if they are, the very existence of the RIP legislation seems certain to publicise their existence and their value in hiding criminal activities.

Many other techniques are available to criminals but will not be discussed here as they are unlikely to be worthwhile for honest computer users. But when combined with the approaches described here, these additional techniques (which criminals undoubtedly know about) will present law enforcement authorities with almost impregnable barriers that will consume enormous resources in efforts to overcome them.

Conclusions for Stored Data

The task faced by law enforcement in recovering protected stored computer data can be made very difficult by using steganography. While encryption and steganographic file systems offer extensive protection, the use of 'physical steganography' in the form of removable hard disc drives and cartridges is a simple and highly effective way of hiding critical data. Moreover, it is limited only by the ingenuity of a user in physically hiding the disc cartridges involved. If necessary any users who want to put their sensitive data beyond the reach of UK authorities can easy do so using the capabilities offered by the many organisations that now provide free disc storage space combined with anonymous Internet access.

In consequence PACE and RIP powers for access to stored computer data do not pose a threat to anyone who is prepared to be careful and well organised about the way in which they store and use their computer data.

Criminals who are careful and clever in their use of their computers and the Internet have many ways of ensuring that their data cannot be seized. In consequence, there is little reason to have any confidence that the measures introduced in the RIP Bill will be effective against them. Some less careful criminals may be caught but the detrimental impact of the legislation on the rights of honest computer and Internet users is a high price to pay when it seems most likely that such criminals would be caught without the need for such powers.

Minimising the Risks Posed by Government Access to Keys (GAK)

The powers in the RIP Bill providing for GAK pose serious threats to the privacy, safety and security of computer and Internet users. A basic and crucial principle that underpins the use of public key cryptography is that the private components of cryptographic key pairs should ***never*** be revealed under any circumstances but once GAK powers are in place honest key owners can never guarantee this. In significant measure the implementation of GAK powers in the UK will hence undermine confidence in cryptographic security and this in turn will undermine confidence in data confidentiality and in digital signatures.

Current cryptographic applications are designed around the principle that the private key components of key pairs are kept fully secure but once RIP powers come into play design changes will be needed to provide new approaches that are not so susceptible to being undermined by GAK.

Short Term Measures

An immediate change that can be made is to reduce the lifetime of public/private key pairs. Many users keep the same key pairs for years with the consequence that many messages will be encrypted using them. If such keys are seized, all items encrypted with them are vulnerable to exposure and this makes it sensible to change keys more frequently so that the damage done by the loss or seizure of any one key is limited.

The popular PGP encryption programme supports this approach by providing for a sequence of data confidentiality keys to be coupled to a single digital signature key. At the moment PGP does not securely wipe keys once they are no longer needed so the key owner has to arrange this manually but it would not be difficult to extend the software to automate this process

Another feature needed in PGP is the automatic revocation of any private key that is exported in plaintext form. The UK Government has said that key revocation is allowed in the event that a key is seized but there are ambiguities in their position so it would be better from a user's perspective to ensure that key revocation is completely automatic when a private key is exposed by plaintext export. Ian Brown, Adam Back and Ben Laurie have published proposals for such an extension to the open PGP standard[2].

Perfect Forward Secrecy

If two computers are on-line at the same time the Diffie-Hellman key negotiation technique discussed earlier can be used to obtain an encryption key that is used just once and then destroyed. Since such a key cannot be seized, this provides fully effective message security that is not in any way undermined by the GAK powers in the RIP Bill. The use of 'one-time' keys is sometimes referred to as 'perfect forward secrecy'.

But this approach is more difficult to arrange for email since the computers involved do not normally use the direct connection needed to negotiate a key at the time a message is sent. Instead of on-line key negotiation it is normal to use longer-term keys and this means that they become subject to possible seizure using GAK powers.

But the protocols used for secure email can be re-engineered to use one-time keys. Fortunately messages between correspondents tend to run in sequences of messages and responses and this means that it is possible to use each message in such a sequence to set up the key for the next message so that each key is used only once and then destroyed. There is a higher overhead in generating many more keys but ways exist to minimise this cost.

When two people want to exchange secure email messages, the originator of the correspondence generates a new initial key pair and sends the public key with the first message. The recipient then uses this public key to encrypt their response, which also contains a new public key. When the originator receives this message they use the initial private key to decrypt it and then immediately destroy this key. If they want to continue the exchange they use the public key in the message they have just decrypted to do this and send a new public key for use in the next response.

It can hence bee seen that even email can be engineered to use one-time keys. Provided that decryption with such one-time keys is always followed by immediate key deletion, GAK powers are of no use in decrypting any intercepted messages. This is more complex than current secure email approaches since users do have to store a number of 'one-time' private keys until they are used in message replies. These keys would be subject to seizure prior to their use but in this situation a user is free to revoke them and hence ensure that they are not used in protecting any future messages.

In fact this is one of several approaches that can be used to ensure that GAK powers are ineffective. The extension to RFC2440 to specify such new approaches has already been published and work is already being planned to add these capabilities to existing encryption applications. As in other areas, therefore, RIP Bill powers will be obsolete and ineffective almost as soon as they are introduced.

Conclusions

The technical thinking behind the Regulation of Investigatory Powers Bill is inept. Criminals can easily circumvent the measures envisaged and the ways in which they are likely to react will actually pose much more serious problems for UK law enforcement authorities than the problems the legislation is intended to solve. At the same time the measures will damage confidence in cryptography and this will be detrimental to the privacy, safety and security interests of honest individuals and businesses and to the UK's aspirations in e-commerce.

---

[2] Forward Secrecy Extensions for OpenPGP, by Ian Brown, Adam Back and Ben Laurie – a proposed update to RFC 2440.