Cryptography Policy: Overdue for Reform

Greg Taylor of Electronic Frontiers Australia looks at the regulation and policy surrounding cryptography and highlights the problems with current local export restrictions

Data encryption plays an essential role in secure transmission of commercial information over public networks, yet its widespread employment is being stifled by cold-war era regulations. Within the Defence Department in Canberra, the arcane science of cryptography is still being treated as if it were a military secret, despite having moved into the academic and commercial sectors over 20 years ago.

Cryptography is a technology used to "scramble" information into an unreadable form. Computers have revolutionised cryptography and have enabled incredibly powerful ciphers to be deployed. Computer ciphers have two chief components: a method (or algorithm) and a key. The two are used together to encrypt a message or file. The algorithm is generally public but the key is kept secret. Anyone who has the key can use the decryption algorithm for the cipher to unscramble a message or file. The key is usually just a large number.

DEVELOPMENTS IN CRYPTOGRAPHY

The two main developments of interest are:

- secret key cryptography, also called symmetric cryptography because the same key is used for encryption and decryption.
- public key cryptography, also called asymmetric cryptography because different keys are used for encryption and decryption. Public key systems usually rely on key pairs, one of which is a public key which can be given to anyone, while the other is a private key which must be kept secret by its owner.

Public key cryptography, invented in the late 1970s, has revolutionised the development of methods for secure transmission of information over public networks. It enables two computers to generate and exchange one-time keys in a way that is protected against interception.

Computer cryptography is already in widespread use, although unknown to many people. Common applications include:

- protection of information transmitted during electronic banking transactions, such as automatic teller machine transactions, EFTPOS purchases and Internet transactions.
- encryption of email sent over the Internet for confidentiality (using PGP or S/MIME)
- encryption of files stored on computers - again to protect their confidentiality.
- the use of digital signatures which are an essential part of the authentication process in electronic commerce transactions.

Cryptography is now an essential tool for many businesses and governments to protect valuable confidential information both when it is stored in their computer systems and when it is transmitted from one location to another over public networks. Without cryptography, it would be very difficult or expensive to protect this information. For individuals, it is an extremely valuable tool to protect private information or communications.

Sophisticated cryptographic software is readily available now to virtually anyone who wants it, and often at little or no cost, and is widely and legally available on the Internet. Much of this software is also extremely powerful - to the point where it would be impractical for governments or their defence agencies to attempt to 'break' the encryption.

However, the strength of cryptography is an issue that is surrounded by controversy. On one side of the debate is the argument that free access to cryptography by the general public enables them to fulfil their right to protect the privacy and security of their communications, including commercially valuable data. On the other side, the government argues that it needs to control the use of cryptography to enable eavesdropping on communications as part of its law enforcement activities.

THE US EXPORT RESTRICTIONS

With certain exceptions, all software originating in the USA has limited crypto strength because of export restrictions.

Examples include:

- The major Web browsers (Netscape Navigator/Communicator and Microsoft Internet Explorer), which are limited to 40-bit keys in the export version as opposed to 128-bit keys in the US domestic version.
- Some widely used 'office' software such as Lotus Notes, the export version of which is limited to an effective 40-bit key. (The actual key length is 64 bits but part of the key is escrowed in the USA.)

In September 1998 the US relaxed its export controls, but only for export to defined markets or industries, with more liberal exceptions being made available for licensed key recovery products (see below).

The US limits have obvious effects on Australia. Because of the large international market share held by some US software companies, many of the products of these firms have become defacto standards. Since cryptography requires both the sender and the receiver(s) to communicate using the same protocols (ie, standards), any US limits on cryptography can affect standards, which in turn affect the types or strength of encryption available to users in other countries.

THE AUSTRALIAN SITUATION

Within Australia, encryption software can still be freely used and exchanged within national boundaries. A number of local firms also produce cryptographic software

and hardware. Nevertheless, there are some restrictions in place.

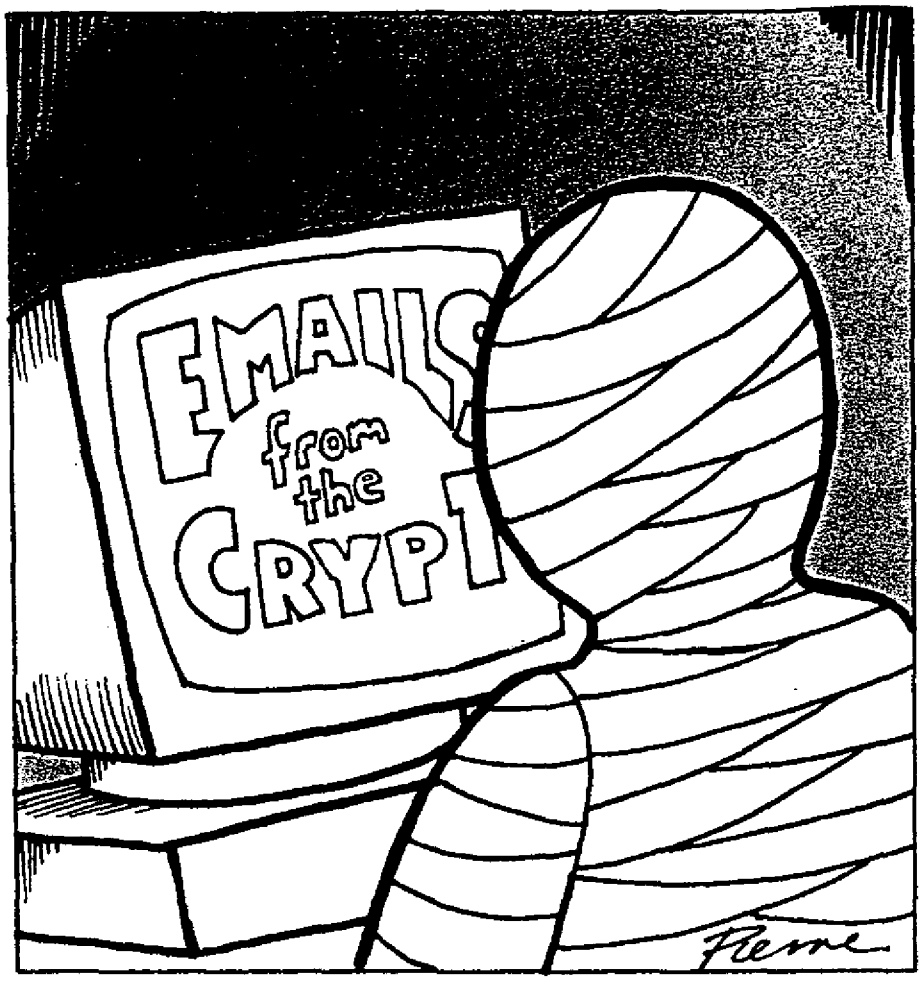
The *Telecommunications Legislation Amendment Bill* was passed by the Senate in November 1997. The purpose of the Bill is to amend several existing Acts including the *Telecommunications (Interception) Act* of 1979. The amendments will require carriage service providers (CSPs) to provide, at the CSP's expense, access to any data or communications which they transmit for their customers. CSPs include a wide range of telecommunications service providers including telephone service providers and most Internet service providers.

Importantly, the amendments require the CSP to decrypt any data which the CSP was responsible for encrypting for a customer. There is, however, apparently no requirement on the CSP to decrypt data or messages which the customer personally encrypted (ie. encryption which did not involve the CSP).

Prior to the November 1997 amendments, the government still had mechanisms for gaining access to the plain text of any data or messages encrypted by a CSP. For example the government could withhold the approval for any new telecommunications service which a CSP proposed to supply unless the service was capable of providing access for authorities to the plain text of any message. A recent example was the roll-out of Telstra's revamped ISDN OnRamp service in 1997. Availability of the new service was delayed until systems were in place for interception of any traffic transmitted using this service. A similar delay occurred with the introduction of GSM mobile phones.

AUSTRALIAN PUBLIC POLICY

There has been silence from the federal government for some time on broader cryptography policy. However, there have been some specific cryptography-related initiatives mainly related to the establishment of a legal regime for electronic commerce. Several expert working groups have been established - one by the Minister for Communication, the Arts and the Information Economy and another by the Attorney-General. The latter is dealing with the legal regime for online transactions and information exchange. Both working groups have released reports this year.



In 1996, the Federal Government made substantial steps towards developing a policy on the use of cryptography in Australia. A report was commissioned from Mr Gerard Walsh, a former deputy head of the Australian Security Intelligence Organisation (ASIO).

However, the Walsh Report was withheld by the Attorney-General's Department from publication. It was eventually obtained by EFA under the *Freedom of Information Act* and published on the EFA Web site (subject to the deletion of certain sections on grounds of national security under the Act).

The Walsh Report comes out in favour of free access to cryptography by the public. The conclusions in the report are especially interesting in view of Mr. Walsh's background with ASIO. Some commentators have suggested that the report was withheld because it did not reach the "right" conclusions (ie., that use of cryptography should be restricted). The status of current thinking in the government is unknown, although all major parties have published policies supporting relaxation of controls.

AUSTRALIA'S EXPORT CONTROLS

It is illegal to export any cryptographic software products from Australia without a license issued by the Department of Defence. Australia's export regulations are amongst the most stringent in the world, and closely parallel restrictions imposed in the USA, although all licence applications here are evaluated on a case-by-case basis, rather than in accord with any published guidelines.

The controls are administered by the Director, Strategic Trade Policy and Operations (STPO), a division of the Defence Acquisition Organisation. With one major exception (the General Software Note) the Australian controls are based on obligations under the international Wassenaar Arrangement, discussed below.

The Australian regulation of cryptographic export controls is set out in Schedule 13E of the *Customs (Prohibited Exports Regulations)* and Section 112 of the *Customs Act 1901* which deals with prohibited exports. Items prohibited under this legislation are

listed in the Defence and Strategic Goods List (DSGL) of the Australian Controls on the Export of Defence and Strategic Goods. Crypto software is identified under Part 3, Category 5/2 of the controlled goods list.

Under these regulations, all cryptography software requires a permit or a licence before it can be exported. Evaluation of licence applications is carried out by Defence Signals Directorate, the body responsible for Australia's external security.

An exception to the rules is the Personal Use Exemption, which allows encryption software to be taken out of the country without a permit under specified conditions for personnal use (eg., where installed on a notebook computer). There are also exemptions for authentication-only products and limited application devices such as ATMs and smartcard readers.

There is a major loophole in the Australian legislation in that the *Customs Act* applies only to physical goods. Intangible exports via electronic networks such as the Internet are not covered by the regulations. This has resulted in some controversial media coverage of late, particularly in regard to the availability on Australian websites of products such as Cryptozilla, a strong-crypto version of Netscape which used Australian-developed crypto software embedded in the open source code provided by Netscape Communications.

Although there have been hints that the *Customs Act* would be amended to cover intangible exports, there are no known moves at present to do so. In the meantime, the Defence Department is attempting to enforce export controls in the electronic medium by means of "moral suasion", a strategy that is not meeting with widespread support or success.

THE KEY RECOVERY CONTROVERSY

A number of governments, in particular the US and UK, have proposed key escrow or key recovery schemes. The aim of the schemes is to allow authorised officials to decrypt intercepted messages. Law enforcement and intelligence agencies argue that without this ability, criminals can abuse cryptography to conceal illegal activity from the law. Australian policy is to encourage key recovery products for export purposes, but no official policy on this matter has been published.

Under key escrow, it would be mandatory for everyone using encryption products to provide a copy of their key to the government for law enforcement access. Under key recovery, the key would be kept by a third-party, generally a commercial service provider. Both systems generally claim that keys and/or plain text would only be available to law enforcement with a court warrant.

The basis of key escrow and key recovery is that all encryption keys are stored in key repositories where government officials can obtain copies of them for use in decrypting messages. There are significant privacy concerns with this approach. There are also major risks in having large numbers of keys stored in central locations. Honest mistakes, corruption and criminal hacking all pose major threats.

THE WASSENAAR ARRANGEMENT

The basis for the export controls of most countries is a military treaty officially entitled *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* ('**Wassenaar Arrangement**') which is a protocol intended primarily to control weapons of mass destruction. There are currently 33 signatories to the Wassenaar Arrangement. The Dual-Use section of the Arrangement forms the basis for most national controls over the export of cryptography products.

The Wassenaar Arrangement is the successor regime to the Co-ordinating Committee for Multilateral Export Controls (COCOM) established by NATO in 1949 to control the export of military equipment and dual-use technologies to Warsaw Pact states. Negotiations to establish a successor regime to COCOM commenced in 1993 and COCOM was terminated in March 1994. The Arrangement was not intended to impede bona fide civil transactions.

There is a preamble to the Wassenaar Dual-Use list called the *General Software Note* (GSN), which was intended to exempt mass market and public domain software form the scope of the controls. However, Australia explicitly disallows this waiver in respect of encryption software. Four other countries, USA, New Zealand, France and Russia, also disallow the GSN waiver.

The reasoning behind this stance by Australia has never been explained, despite the fact that this policy position means that Australian crypto developers are at a severe disadvantage compared with their European counterparts.

There are now moves afoot to further tighten international restrictions on cryptography in a current review of the Wassenaar Arrangement. The Australian delegation is at the forefront of this movement, although their position is widely believed to be influenced by the US government's hardline stance. Amongst the proposals to be put forward are a plan to include intangible exports as controlled items, and removal of the GSN waiver.

CONCLUSION

Most technical and professional organisations involved in the development of network standards are opposed to the controls that are placed on cryptography, since they restrict the development of global standards, weaken security, encourage information warfare, and impose severe risks to human rights and privacy.

Campaigns involving both industry and civil liberties interests are active in many countries. There is now an international movement sponsored by the Global Internet Liberty Campaign (GILC) which has gained the support of many industry and civil liberties lobby groups, to call a halt to what are generally perceived as silly and unworkable restrictions. Strong cryptography is now widely available and is in the public domain. Export controls are starting to be routinely circumvented by developers moving offshore. It appears to be only a matter of time before the legislature and the bureaucracy wakes up to the obvious.

Greg Taylor is a board member of Electronic Frontiers Australia Inc. and chair of its cryptography committee. Further information is available from the EFA website: http://www.efa.org.au