Parliamentary Office of Science and Technology

postnote

October 2006 Number 270

DATA ENCRYPTION

Encryption is increasingly used to protect digital information, from personal details held on a computer to financial details transmitted over the Internet. Encryption has many benefits but can also be used to conceal criminal activity. This POSTnote outlines encryption techniques, their applications and their reliability. It also discusses controversial government proposals to give public authorities new powers under the Regulation of Investigatory Powers Act, relating to the handling of encrypted data in criminal investigations.[1]

What is encryption?

Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to 'decrypt' it to obtain the original message (Box 1). It is commonly used in connection with electronic data (Box 2), whether stored on a computer or transmitted over an unsecured network such as the Internet. Encryption tools (usually in the form of computer programs or software) are widely available and can be used to secure:

- stored data, from single files to entire hard disks;
- computer code such as computer operating systems;
- information transmitted over the Internet, including e-mails and internet telephony (Voice over Internet Protocol or VoIP);
- entire communications infrastructures, such as wireless networks (including mobile telephony).

Public key cryptography

Until the 1970s, all encryption was **symmetric**, like the example in Box 1: anyone who knew how to encrypt a message could work out how to decrypt it. This was adequate for communication between a small number of trusted people sharing a secret encryption key. However, in a situation where large numbers of people want to communicate securely (like modern internet commerce) it is impossible for everyone to share a 'secret' key.

This problem was solved by the advent of **asymmetric** or **public key cryptography** (PKC). PKC involves pairs of keys: a 'public' key which can be made openly available, and a 'private' key. Once information has been encrypted with the public key, nobody but the holder of the private key can decrypt it. In reverse, if the private key is used for encryption, anyone with the public key can decrypt it. It is very hard to derive the private key from the public key. Because the private key does not need to be exchanged, PKC is much more secure than earlier techniques, so it can be used for applications such as internet commerce (POSTnote 114). Asymmetric encryption is slower than symmetric encryption, even on fast computers, so most modern encryption uses a combination of both methods.

Box 1. How does encryption work?

Encryption involves taking an original message or **plaintext** and converting it into **ciphertext** using an **encryption algorithm** and an **encryption key**. Historically, encryption acted on letters of the alphabet. The Caesar Cipher, one of the oldest techniques, gives a very simple example:

- Take the plaintext is *Parliament is in session*;
- Encrypt according to the encryption algorithm 'replace each letter with that *X* places to the right of it in the alphabet', where *X*, the encryption key, is 3;
- the ciphertext is *sduoldphqw lv lq vhvvlrq* and can be converted back to plaintext with a **decryption algorithm** and **decryption key,** in this case 'replace each letter with that three places to the left of it in the alphabet'.

Computers store electronic data in binary form, as sequences of 'bits' (1s and 0s). Modern algorithms are mathematical functions that act on these data with keys that are themselves sequences of 1s and 0s. Keys are generally stored in computer files that are themselves encrypted and can be accessed only with a passphrase (similar to a password but longer).

Practical applications of encryption

Confidentiality and access control

Encryption can be used to protect electronic information so that only an authorised party can access it. This has numerous applications (see Box 1 for examples).

Box 2. Applications of encryption

Private use - encryption software packages are readily available commercially and by free download from the Internet. One free e-mail encryption package is Pretty Good Privacy (PGP), available since 1991.[2] An alternative is S/MIME, supported by most e-mail vendors.

Securing networks - Secure Sockets Layer (SSL) is an encryption protocol that enables secure communications and user authentication over open, unsecured networks like the Internet. Its use is usually indicated in web browsers by a small padlock icon, seen for example when a user submits credit card details online. Besides protecting data, this system will also check that a given website is authentic and sometimes verifies the identity of the user. Similar protocols are used to secure private networks.

Wireless (or Wi-Fi) networks are also vulnerable to interception. An international security standard called Wi-Fi Protected Access (WPA2) can be applied to encrypt data sent over wireless networks.

Access control - Digital television providers control subscriber access by encrypting audio and video signals. Subscribers are equipped with a descrambling device comprising the decryption algorithm and decryption key, which together decrypt pictures and sound.

Integrity and non-repudiation

An important feature of public key cryptography is that if the holder of a private key encrypts a message, anyone with the corresponding public key can decrypt it. However if a message has been tampered with, decryption will not work. Digital signatures exploit this principle and allow parties to sign emails or electronic documents electronically. They can be used to verify **integrity** (to check who sent a document and to confirm that no-one else has modified it). They can also be used for **non-repudiation**: if a party digitally signs an electronic document, they cannot later deny this.

Large scale use: Public Key Infrastructure (PKI)

Public key cryptography enables communication without the necessity of sharing secret encryption keys. However there remains a significant problem: establishing whether the person publishing a public key is genuine. Certification and Registration Authorities (CAs and RAs) are an established centralised way of managing keys. CAs and RAs validate the identity of people (or companies and their websites) and issue them with certificates which they digitally sign (Box 3) to show their endorsement of that identification. The resulting digital certificates associate a given public key with an identity. When a browser connects to a website, the digital certificate can be checked. Provided that the CA is trusted (see page 4), the user can be assured that the website is genuine. VeriSign is an example of a large CA that provides a digital certificate service to the financial and retail sectors among others.

Box 3. How do digital signatures work?

The sender of a message uses a **cryptographic hash algorithm** to condense an entire message into a short, unique fingerprint. This fingerprint is encrypted with the sender's private key to produce the digital signature, which is attached to the original message and sent to the recipient. The recipient uses the sender's public key to decrypt the digital signature. He/she then uses the cryptographic hash algorithm to calculate the fingerprint of the message itself. If the two are identical, this shows the message not been tampered with and comes from the sender associated with that public key.

Reliability of encryption

The strength of an encryption technique describes how difficult it is to 'break' it (decrypt the information without knowing the decryption algorithm, decryption key or passphrase, see Box 1). Information security experts agree that there are already algorithms which are very strong and if used correctly are effectively unbreakable. Choosing appropriate encryption depends on:

- what kind of information needs to be secured;
- how long it needs to be protected;
- who the potential interceptors are;
- what resources they might have.

The security of encrypted data depends primarily on the choice of algorithm and key length (see next section). For example, personal details stored on a medical database would require protection by a strong algorithm and a long key that would be very difficult to break. Where data sensitivity is short-term, it would not necessarily require such robust protection. As computing power increases and cryptographers identify weaknesses in algorithms, new standards emerge. Some algorithms thought to be secure 20 years ago are now considered weak.

Breaking encryption

Algorithm strength is often described by the bit length of the encryption key: '56-bit', '64-bit', '128-bit' (see Box 1). The more bits in the key, the harder it is to decrypt data simply by trying all possible keys (an 'exhaustive key search'). Cracking a 56-bit algorithm with an exhaustive key search might take around a week on a very powerful computer, a 57-bit algorithm 2 weeks, a 58-bit algorithm 4 weeks and so on. Most modern algorithms operate using 128, or increasingly, 256 bits.

There are many ways an investigator might try to break encrypted data. If they have access to the encryption software, they could study how the algorithm worked, identify any weaknesses, and try to work out how to break it. Even if the algorithm is hard to break, the software may be poorly designed. Some software accidentally copies the unencrypted message onto the hard disk. Also, some algorithms have known weaknesses and tools are available to break them. In practice, most successful attempts result from human

factors, either deliberate or accidental. People might write their passphrases where they can be easily found or disgruntled employees might intentionally cause security breaches.

Legislation and policy

Safeguarding personal data

There is no explicit obligation under the Data Protection Act (DPA) to use encryption to safeguard personal data, although the 7th principle of the act stipulates that "appropriate technical measures" should be taken. This could be interpreted as referring to encryption.

Regulation of cryptography service providers

The Electronic Communications Act (2000) gives digital signatures a legal recognition comparable with written signatures and gave the government powers to establish a body to approve cryptography service providers (such as the CAs and RAs that issue digital certificates), (page 2), if self regulatory efforts proved unsatisfactory. However, industry established a self-regulatory body (tScheme) and after five years of successful operation the power granted in the act has lapsed. Thus, the government does not regulate CAs and RAs.

Issues

The benefits of encryption in helping to secure electronic commerce and safeguard privacy are clear. However, it also provides a way of concealing unlawful activity. The policy debate about encryption centres on how to strike a balance between its risks and benefits.

The government's role in uptake of encryption

Electronic information security at home, and within organisations, is a topical issue, as the volume, type and complexity of computer crime increases (see POSTnote 271 on computer crime). The Government's 'Get Safe Online' computer security education initiative was launched in 2005.[3] The scheme promotes computer security awareness and encourages the use of encryption to protect sensitive data and communications.

A survey of UK businesses carried out by the Department of Trade and Industry reported that, of the businesses surveyed, 30% of those who use online transactions, do not encrypt them.[4] The Information Commissioner's Office (ICO), which enforces the DPA, expects that an organisation's information security policy and practices should reflect the technology that is available. Thus, as encryption becomes cheaper and more accessible, the ICO would expect organisations to use it, especially for sensitive data. For example, medical records stored electronically as part of the national NHS IT programme 'Connecting for Health' will require long-term protection and secure transmission when shared over a network.

Drawbacks of encryption

Encryption and criminality

Criminals can use encryption to secure communications, or to store incriminating material on electronic devices. There are no official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data. However law enforcement agencies consider that the incidence of both is increasing, as discussed below.

Digital forensics

Police investigations increasingly involve seizure of computer equipment, which may require digital forensic analysis, including decryption. This often involves examining devices such as: hard disk drives; mobile phones; digital cameras; music players and portable storage devices (such as memory keys). The aim is to discover whether these devices contain evidence relating to illegal activities, or intelligence that can inform an investigation. Each police force has digital forensic officers. However, specialist support may be required, for example if the data have been protected by encryption and are inaccessible, or use software which is unfamiliar.

When the police encounter encrypted data they can take several steps to obtain the original information:

- try to break it with available decryption tools;
- try a 'brute force attack' using powerful computers to try all possible keys;
- use intelligence about an individual. For example, the suspects might have selected a poor passphrase based on a name familiar to them;
- make use of the expertise and computing resources of the National Technical Assistance Centre (NTAC). This is usually the last option if all the above fail.

The Serious Fraud Office estimates that almost all cases it investigates involve some encryption. Their inquiries are mainly in corporate environments. The encryption encountered is usually weak and easily broken.

The Government has consulted publicly on plans to bring into force controversial new powers contained in Part III of the Regulation of Investigatory Powers Act, 2000 (Box 4).[1] Where the Police lawfully obtain protected data, they would be able to demand that suspects decrypt the data or hand over the decryption key. If not, they might face a custodial sentence. Some aspects of Part III of RIPA have received opposition from groups such as Liberty and the Foundation for Information Policy Research.

Box 4. Regulation of Investigatory Powers Act (RIPA), 2000

The act was introduced to provide a basis in law for the conduct of covert surveillance. It also amended legislation for the interception of communications to take account of the growth of the Internet and modernised police powers to undertake intrusive surveillance. Part III of RIPA, to be brought into force following consultation and Parliamentary debate in early 2007, requires that a suspect must make the encrypted data under investigation intelligible. In some circumstances they must disclose the decryption key to the police. Failure to do so will carry a penalty of up to two years' imprisonment. Terrorist suspects already face up to a five year sentence under existing anti-terrorism legislation.

If the sentence is likely to be less than that which a suspect would face if the data were decrypted, there

would be little incentive to comply. Some argue that it would be very difficult to enforce, since suspects can claim to have forgotten the key - and it may be very difficult to prove otherwise. However, forensic computing techniques may be able to establish if the suspect was regularly accessing the encrypted files. Further problems include the use of hidden encrypted volumes. Suspects might provide a password which allowed access to innocuous data but another password, not provided, would be needed to access data that the suspect was really trying to hide. Some suggest that the new powers, and other aspects of RIPA, (see POSTnote 183) may discourage businesses from operating in the UK, and deter honest users from using encryption to secure their computers and private information.

Terrorism

In January 2006, the House of Commons Home Affairs Select Committee conducted an inquiry into the government's plans to extend pre-charge detention for terrorism suspects to 90 days.[5] Dealing with increasing volumes of encrypted data was one of the justifications for the required extension, put forward by the Association of Chief Police Officers. However, digital forensics experts giving evidence said that if encryption cannot be broken within a few days, it is unlikely to be broken over a longer period. They also said that police resources were insufficient to deal with the amount of computer hardware and digital forensic work that is now encountered in criminal investigations. The Committee recommended that Part III of RIPA should be implemented as soon as possible, but added that this "would not solve the problem of encrypted data".

Consumers and encryption

Access control and copy protection

Encryption almost always forms the basis of digital rights management systems, such as those which govern access to pay-per-view television services, or how consumers can use music purchased from the Internet. Some say this could create monopolies, leading to an overall reduction of consumer choice.

PKI, certification and trustworthiness

The use of digital certificates within the PKI, particularly in electronic commerce, raises a number of issues:

- Do the digital certificate and public key actually belong to the organisation specified?
- How did the Certifying Authority (CA) verify the identity of the organisation?

Criminals can establish their own CAs to verify false organisations, in order to carry out criminal activities on the Internet, such as directing consumers to fraudulent retail sites to harvest credit card details. In the UK, the industry's tScheme approves and monitors UK electronic cryptography services which depend on secure, reliable identity authentication.[6] Approved organisations can use the tScheme logo to indicate compliance with the scheme's standards. However due to the international nature of the Internet, consumers may deal with overseas organisations not covered by the tScheme.

Future developments

Commercially available encryption tools are becoming more sophisticated. Microsoft will launch its new computer operating system, Windows Vista, in late 2006.[7] Two versions will incorporate 'BitLocker Drive Encryption' which enables the entire contents of a hard drive to be encrypted. This makes data inaccessible to unauthorised users who do not have the decryption key. It can also help to identify whether a computer has been tampered with. The aim is to limit disclosure of sensitive data if computer devices are lost or stolen. However, some say that widespread availability of this and other encryption products will frustrate criminal investigations.

Quantum computing and cryptography

Quantum computers are in their infancy but some experts anticipate that they will be faster and more powerful than today's computers. This may mean that existing encryption techniques can be more easily 'broken' (page 2). However quantum physics also lends itself to new forms of cryptography that may be useful for long term safeguarding of information. There are already prototypes of new devices developed for research purposes, but with limited functionality. The NTAC say the engineering problems that need to be overcome to build a quantum computer are so large that it may be several generations before they are feasible.

Overview

- Encryption is one of a number of tools that can be used to safeguard electronic information and privacy.
- Encryption tools are widely available and are becoming more sophisticated; the government is encouraging their uptake both for private users and for businesses.
- Availability of encryption tools means that the government faces a challenge in encouraging its legal use whilst ensuring that it is not misused by criminals.
- Part III of RIPA will give public authorities new powers relating to handling encrypted data and will be the subject of Parliamentary debate in early 2007.
- There is a need for users to monitor advances in encryption technology continually to ensure electronic data is adequately protected.

Endnotes

1 www.security.homeoffice.gov.uk/surveillance/ripa-updates/
2 www.openpgp.org/
3 Get Safe Online, www.getsafeonline.org/
4 *Information Security Breaches Survey,* 2006, Department for Trade and Industry, www.pwc.com/extweb/pwcpublications.nsf/
5 The Home Affairs Committee, Fourth Report of Session 2005-06, *Terrorist Detention Powers* HC 910-II
6 tScheme, www.tscheme.org/
7 Microsoft Windows Vista, www.microsoft.com/Windowsvista/

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

For further information on this subject, please contact Dr Sarah Bunn at POST.

The Parliamentary Office of Science and Technology, 7 Millbank, London SW1P 3JA; Tel: 020 7219 2840; email: post@parliament.uk

www.parliament.uk/parliamentary_offices/post/pubs2006.cfm