Information and Privacy Commissioner of Ontario

Fact Sheet

Number 16
July 2010

Health-Care Requirement for Strong Encryption

The Office of the Information and Privacy Commissioner (IPC), in Order HO-004, and most recently in Order HO-007, required that health information be safeguarded at all times, specifically by ensuring that any personal health information stored on any mobile devices (e.g., laptops, memory sticks, PDAs) be strongly encrypted.[1] The Order did not otherwise define what constitutes "strong encryption" in the context of protecting the confidentiality, integrity, and availability of personal health information.

Accordingly, this paper provides a working definition of strong encryption and discusses the minimum functional and technical requirements of what may be considered to be strong encryption in a health-care environment. These, in turn, will provide procurement criteria that, if met, will ensure that personal health information stored on encrypted mobile devices or storage media will remain accessible to authorized users, but no one else.

Special thanks go to Dr. Robert Kyle, Durham Region Commissioner and Medical Officer of Health, for supporting the production of this paper.

Strong Encryption

Introduction

The term 'strong encryption' does not refer to a particular technical or design specification, or even to a specific encryption feature that could be inserted into a procurement or audit specification. No particular encryption technology — no matter how 'strong' it may be — can ever, by itself, ensure that information remains secure. Instead, a variety of circumstances and factors need to be taken into account to ensure that personal information is protected against access by unauthorized parties.

To begin with, a good encryption algorithm must be used — one that has been subjected to rigorous peer review. Next, the algorithm must be properly implemented. This may only be confirmed if the encryption system is tested by an independent security testing lab. Once the encryption system is deployed, the encryption keys must be protected and managed effectively. Users who are authorized to decrypt data must be securely authenticated by means of passwords, biometrics, or security tokens.

Systems must not leave unencrypted copies of data in web browser caches or on laptop disk drives where they may later be read by an unauthorized third party. Authorized users should be properly registered, trained and equipped. The encryption system's protections should be operational by default, without busy health-care users needing to take special steps to ensure that data remains encrypted. Finally, personal health information must remain available throughout its life cycle, regardless of forgotten passwords or misplaced security tokens.

The above considerations place several requirements on encryption systems that are used to protect the confidentiality of personal health information.

Technical and Functional Requirements

As explained in detail below, all of the following are technical requirements for strong encryption:

1. **Secure implementation:** The encryption system should have met a minimum standard for the protection of sensitive information. This, in turn, has two components: encryption systems must be designed to meet a minimum standard; and encryption products should be independently validated against standards to ensure that they are designed and implemented properly. As explained below, the most suitable and widely used standard for encryption systems for mobile devices is FIPS 140-2[2] and this standard specifies only a few acceptable algorithms. Strong encryption requires the use of devices or software programs that are FIPS 140-2 certified for use in the way that they are designed to be operated.
2. **Secure and managed encryption keys**: Encryption keys must:
   - 2.1 be of a sufficient length (sometimes also called key size and measured in bits) that they effectively resist attempt to break the encryption; and
   - 2.2 remain protected so that they cannot be stolen or disclosed to unauthorized individuals.
3. **Secure authentication of users**: Prior to decrypting, authorized users must be securely authenticated (e.g., by means of robust passwords) to ensure that only authorized users can decrypt and access data.
4. **No unintended creation of unencrypted data**: No file containing decrypted data should persist as a consequence of a user having accessed encrypted data and viewed or updated it in decrypted form. A copy of the decrypted data must not persist unless an authorized user has intentionally created one.

In addition, the following are functional requirements of encryption systems that protect client privacy while at the same time supporting health-care providers in their ongoing provision of quality health care:

5. **Identified, authorized and trained users**: Health information custodians should be able to determine at any given time which users have access to encrypted information on a given mobile device or on mobile media. This means that users who are authorized to access or update encrypted data need to be individually identified beforehand and given appropriate authentication tokens (e.g., robust passwords), as well as adequate

training in how to access and protect the encrypted information.

6. **Encryption by default**: Once an encryption system has been installed on a mobile device or to protect mobile media, users should be able to rely on the encryption being in place without having to explicitly activate it to protect data.

7. **Availability and information life cycle protection**: There must be a reasonable assurance that encrypted data will remain available (e.g., despite forgotten passwords, staff who are unavailable due to illness or death, etc.). This, in turn, requires centralized management of passwords and other authentication tokens. It also requires that encrypted files or media be capable of being backed up along with other (unencrypted) files during routine backup operations.

All of the above considerations apply when encryption is used to secure the data stored on mobile devices and media such as laptops, cell phones, portable hard drives and memory sticks. They also apply to encryption used as an integral part of secure communications such as virtual private networks, secure email systems, and secure web access. But there is a final functional consideration when entire IT infrastructures are being designed and built:

8. **Threat and Risk Assessment**: IT infrastructures that use security technologies such as encryption should be subjected to a Threat and Risk Assessment prior to live operations (and preferably prior to implementation) to ensure that they work as expected.

Each of the above requirements is explained in more detail below.

1. Secure Implementation

Encryption technology has evolved rapidly over the last decade, and formerly acceptable encryption algorithms such as the Data Encryption Standard (DES) and Wired Equivalent Privacy (WEP) are now considered much too weak to be relied upon. There are also many examples of proprietary algorithms from vendors that later proved to be flawed. Fortunately, well-respected encryption standards exist that clearly specify which algorithms are acceptable and which vendor products have properly implemented those algorithms.

The most widely used standard for cryptograph models is the (U.S.) Federal Information Processing Standard FIPS 140-2, published by the (U.S.) National Institute for Standards in Technology (NIST). The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products that have been validated as conforming to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). Vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. The CSE accredits such laboratories in Canada.

In addition to accreditation, FIPS 140-2 specifies an essential component of any encryption system: suitable encryption algorithms. FIPS

140-2 Annex A lists the approved encryption algorithms that can be used. Of the three that are currently approved, only two are in widespread use in mobile device encryption: the Advanced Encryption Standard (AES), and the Triple-DES encryption algorithm.[3] Either one is acceptable for use in FIPS 140-2 validated encryption solutions.

2. Secure Encryption Keys

AES supports key lengths of 128 bits, 192 bits, and 256 bits, and all are currently considered secure for routine use. As a practical matter, key lengths (sometimes also referred to as key sizes) for AES of 128 bits may not be sufficiently secure for the long-term storage of sensitive information, especially if the encrypted information is being archived for many years. Triple-DES supports a key length of 112 and 168 bits. Triple-DES keys of 112 bits are also no longer typically used for storage of sensitive information.

Encryption keys are best kept secured inside a hardware device with dedicated cryptographic support, such as a USB stick, smart card, or laptop with a crypto-module installed. In the absence of hardware protection, the keys must be protected by software modules that store the keys in encrypted format and only provide access to an authorized crypto-program that in turn can only be activated by users who are successfully authenticated.

3. Secure Authentication of Users

A variety of means is provided by commercially available encryption systems for remote media and devices. These include strong passwords (a mixture of alphabetic characters, special characters, and digits of at least eight characters in length), biometric fingerprint readers (in the case of mobile devices and USB memory sticks), and USB fobs (in the case of mobile devices such as laptops). Whatever authentication method is chosen, it must be able to securely defeat attempts by unauthorized users to impersonate authorized users.

4. No Unintended Creation of Unencrypted Data

A copy of the decrypted data must not exist unless an authorized user has intentionally created one. Poorly designed encryption systems may leave temporary file copies of encrypted data in unencrypted form on the disks of mobile devices such as laptops. This can happen, for example, where the encryption product vendor has failed to take account of events, such as a power interruption, to a laptop. Poor design can also plague web-based systems that allow browsers to cache unencrypted copies of data that were otherwise securely delivered to the user via SSL (Secure Sockets Layer). See the discussion below on Threat and Risk Assessment.

5. Identified, Authorized and Trained Users

It is not usually sufficient in health care to merely authenticate users; e.g., by giving all users the same password. Otherwise, the dismissal of a single staff member would require that dozens, perhaps hundreds, of other users would need new passwords. Moreover, if users shared passwords it would not generally be possible for health information custodians to be able to say with any assurance which users had accessed a given file or database. Users who are authorized to access or update encrypted data

need to be individually identified beforehand and given unique user names and appropriate authentication tokens (e.g., robust passwords). Whatever access control system is used to track users and equip them with user IDs, the system must work seamlessly with the chosen encryption system.

Finally, only users who are adequately trained can be relied upon to gain access to encrypted data when it is needed and to protect its confidentiality throughout its use.

6. Encryption by Default

Busy health-care providers cannot be expected to check an encrypted data file every time they view the data or update it to ensure that the encryption system is still working, and that the data remains encrypted. Once set up, the encryption system must reliably continue to protect encrypted data without ongoing configuration and testing by users who use the system to view or update the data.

7. Availability and Life Cycle Protection

Personal health information used in the provision of health-care must be accessible round-the-clock and hence encryption systems must be able to make data available whenever it is needed. If an encryption system renders data permanently unreadable when a user becomes unavailable (e.g., through death, illness, or other calamity), or when a user merely forgets his/her password, then that encryption system is unsuitable for deployment in a health-care environment. Fortunately, a variety of products exist from well-known vendors that provide centralized management features that allow master passwords, remote password resets, and other features to facilitate the deployment and management of a large number of mobile devices or media without fearing loss of data.

In a similar vein, encryption systems must either facilitate the backup of encrypted data files, or at least not impede backup systems already in place, so as to ensure that copies of encrypted data files are securely backed up on a regularly scheduled basis.

8. Threat and Risk Assessment

Encryption must be commensurate with, and responsive to, known threats and risks: loss or theft of a portable device, staff carelessness or lack of training, malice, hackers, and many others. If organizations building IT infrastructures cannot articulate and weigh the threats and risks to their data holdings in a methodical, objective and credible manner, then they will never know whether they have deployed encryption properly. The best method for ensuring that an encryption technology is properly deployed within a larger IT infrastructure is to carry out a Threat and Risk Assessment (TRA). Fortunately, there is a widely used and well-respected methodology for performing TRAs that was jointly created by the Canadian Communications Security Establishment (CSE) and the RCMP and is available at www.cse-cst.gc.ca/its-sti/publications/tra-emr/index-eng.html.

In Ontario, health information network providers are required to perform a Threat and Risk Assessment by provisions of the *Personal Health Information Protection Act,* (*PHIPA*) and its regulations.[4]

Additional IPC Guidance

PHIPA Order HO-008 (June 2010)

PHIPA Order HO-007: Encrypt Your Mobile Devices: Do It *Now* (January 2010)

PHIPA Order HO-004 (March 2007)

Fact Sheet #12: Encrypting Personal Health Information on Mobile Devices (May 2007)

Fact Sheet #14: Wireless Communication Technologies: Safeguarding Privacy & Security (August 2007)

Further Reading

FIPS standards:
http://csrc.nist.gov/publications/PubsFIPS.html

List of FIPS 140 certified encryption products:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

ISO/IEC 19790:2006 – *Security requirements for cryptographic modules*

ISO 27799: *Health informatics – Information security management in health using ISO/IEC 27002*

The following Government of Ontario guidance document is intended for provincial government Ministries, but contains useful material on how encryption/passwords should be properly addressed. See in particular Appendix A: Approved Algorithms and Protocols:

Government of Ontario IT Standard (GO-ITS) 25.12: *Security Requirements for the Use of Cryptography* Version #: 1.1 (2008) at: www.mgs.gov.on.ca/en/IAndIT/258071.html

NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

About Ross Fraser

Ross Fraser is an acknowledged expert in health-care privacy and security. He has lectured on confidentiality, authentication, cryptography, and digital signatures across Canada, the U.S., and the U.K. and has written security policies and implemented security systems for private sector corporations, Canadian governments and ministries of health, the National Health Service in Great Britain, and health-care organizations in the not-for-profit sector. Ross also served for six years as convenor of the health informatics security working group at ISO, the International Standards Organization (ISO), and was senior editor of four international standards on security in health care.

1 See www.ipc.on.ca/images/Findings/ho-007.pdf

2 See http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

3 Triple DES is defined in ISO/IEC 18033-3:2005 Information technology —Security techniques—Encryption algorithms—Part 3: Block ciphers

4 *PHIPA* O. Reg. 329/04 states (s.6(3)[5]) "The [health information network] provider shall perform, and provide to each applicable health information custodian a written copy of the results of an assessment of the services provided to the health information custodians, with respect to: i) threats, vulnerabilities and risks to the security and integrity of the personal health information…" See www.canlii.org/en/on/laws/regu/o-reg-329-04/latest/o-reg-329-04.html

Fact Sheet

is published by the **Office of the Information and Privacy Commissioner of Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA
M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée « Feuille-info », est également disponible en français.

30% recycled paper