Integrating Cryptography into Trusted Systems: A Criteria Approach

William Brierley
Information Security Specialist
Communications Security Establishment
Ottawa, Canada, K1G 3Z4

Abstract

In this paper, we present the rationale behind the requirements for cryptographic implementations which have been integrated into version 3.0 of the Canadian Trusted Computer Products Evaluation Criteria. We believe that an integrated set requirements for cryptography is an essential step toward bridging the gulf between communications and computer security.

1 Introduction

The traditional separation of communications security (COMSEC) and computer security (COMPUSEC) has become blurred with the advent of distributed computing. However, until very recently these disciplines have been treated as distinct by standards organisations. Some initial attempts have been made to draw COMSEC and COMPUSEC together. The Trusted Network Interpretation [11] published by the National Computer Security Center in the US detailed how traditional COMPUSEC notions may be mapped onto computer networks and detailed the additional considerations related to communications aspects of networks. From the other direction the NIST has provided requirements for cryptographic implementations in [9][FIPS 140-1] which begin to address the need for these implementations to be integrated into secure computing environments. The ISO has also provided valuable step forward in the OSI security architecture [3]. To date however, there is no one document which provides a unified approach to information security (INFOSEC). In this paper we present another contribution toward a truly INFOSEC criteria by providing requirements for cryptographic implementations which are integrated into the Canadian Trusted Computer Products Evaluation Criteria.

The Communications Security Establishment (CSE) recognised the need to integrate cryptography into the Canadian Trusted Computer Products Evaluation Criteria (CTCPEC). This need was driven by the requirements of CSE's customers in the Government of Canada to process designated (sensitive but unclassified) information efficiently and inexpensively and by vendors anxious to satisfy this market. This meant that COMSEC had to be integrated with COMPUSEC into both desktop and portable personal computers; the traditional COMSEC box was no longer a viable option. Consequently, CSE, included an adapted version of [9] into version 2.0 of the CTCPEC [1]. However, these requirements were poorly integrated with the body of the criteria, thus it became apparent that an truly integrated set of security requirements for cryptographic implementations were required for version 3.0 of the CTCPEC. [2]

The approach taken to develop the security requirements for cryptographic modules took three things into consideration. First, we were to target cryptography for designated information only. Second, the requirements must be specified using the CTCPEC. This was necessary to achieve a truly integrated set of requirements. Finally, the requirements must be drafted as a composable specification. Cryptography must be integrated into trusted computer products to be useful, so it is necessary to specify the security requirements for cryptography as requirements on a trusted component.

The goals for this project were to reduce vendor cost for producing INFOSEC products; speed the evaluation process; and move toward an INFOSEC criteria. With requirements for commercial COMSEC in one program and criteria for COMPUSEC in another, it was time consuming and costly for vendors to attain endorsement for products which integrated COMSEC and COMPUSEC. From the evaluation side, it was found that the division of COMSEC and COMPUSEC led to products which were designed to meet the requirements of only one of the programs and often required redesign to meet the requirements of the other. By moving toward an INFOSEC criteria, we have not eliminated the need for two programs, but it is our hope that the bureaucratic overhead to vendors will be reduced and that better INFOSEC products will be produced.

The constraints on the development of security requirements for cryptographic modules were the need for these requirements to be compatible with existing standards and programs and to provide requirements which could be implemented with current technology at a reasonable cost. The requirements had to be compatible with the Canadian Cryptographic Endorsement and Assessment Program (CEAP). To do this we set the goal of providing a scalable set of requirements which would be sufficiently general to meet the needs of both COMSEC and COMPUSEC and for which the delta to the CEAP was minimal. In order to
address the North American market the requirements also had to be compatible with the NIST’s FIPS 140-1 [9]. Our customer base in the Government of Canada requires inexpensive technology now to protect designated information thus the requirements for cryptographic modules must be requirements for today’s as well as tomorrow’s technology.

This paper is divided into seven sections. The first section is this introduction. The second section provides a brief overview of the CTCPEC with particular emphasis on those features of the CTCPEC which facilitated the development of security requirements for cryptographic modules. The third section discusses the scope of the security requirements for cryptographic modules. The fourth section discusses the structure of the security requirements document. Section five addresses the requirements on the implementation of a cryptographic module. Section six describes the requirements on the integration of cryptographic modules into INFOSEC products. Finally section seven provides a summary of the project and its perceived success.

2 Overview of the CTCPEC

Version 3.0 of the CTCPEC is designed to be a flexible criteria against which information security products may be rated. A rating against the CTCPEC does not provide an endorsement of a product for use in a given environment, rather it provides a basis upon which to compare information security products and upon which to assess the suitability of a rated product for use in given environment. In order to achieve the desired flexibility, the CTCPEC has separated assurance from functionality and has assumed a policy independent view of functionality.

An information system is trusted if it is known that this system does what it is specified to do and nothing else. Thus assurance criteria should address what it means to know that a system does what it is specified to do. In this sense assurance is independent from functionality.

If the environment is known, one can construct a specification which assures the proper functioning of a system in that environment. In this context assurance is intimately linked with functionality since it is the functionality of the information system which provides protection against the environment. The United States Trusted Computer Security Evaluation Criteria [10] (Orange Book) approaches assurance from this point of view. The Orange Book was written to address the security concerns of a particular environment. Consequently assurance and functionality are inexorably linked in that document. The European ITSEC [5] presents assurance criteria as the quality of the evidence that a system is faithful to its specification, however it requires each specification to address a specific environment. While correct in theory this approach appears burdensome on the evaluation process and on the market place. To reduce this burden, the ITSEC provides a number of broad functional classes which are targeted at certain environments.

The approach taken in the CTCPEC is to view assurance as the quality of evidence that a system is faithful to its specification and to provide a set of largely independent generic security services from which a functional security specification can be built. The generic security services presented in the CTCPEC are grouped according to the broad security objectives targeted by the service and are largely independent of security policy. Within each class, the services are graded according to the inherent strength of the service, the granularity of application, and the functionality. By choosing to implement one of these generic services one provides security against a class of environmental threats. Thus a product rating against the CTCPEC provides a compact characterisation of the threats countered by the security services provided by the product.

When designing the functional security criteria of the CTCPEC, there were three guiding principles. First, the service must be largely independent of policy: the CTCPEC is intended to address all manner of information security concerns, consequently it must not be bound to any one security policy. Second, there must be a quantifiable difference between levels of a given service: unless there is an increase in the strength of the service, or a finer granularity of application, or an increase in functionality between levels, it would be impossible to provide consistent or meaningful ratings. Finally, the functional classes chosen must be useful to our customers and the levels within these classes must address potential threats from the environment. It is this last principle which enforces order on the criteria and is the point at which expert knowledge enters the criteria. For example, when defining the mandatory confidentiality class, four levels were identified: at the lowest level, information in a given form is either provided to all users or to no users; at the second level, for a defined subset of subjects and objects, information contained in an object is disclosed to some subjects but not others; at the third level, access by any subject to the information within any object is mediated; finally at the fourth level access by any subject to the information contained within an object is further constrained to the method of access. The transitions from level one to two and from level three to four result in an increase in the functionality, whereas the transition from level two to three result in a stronger service with finer granularity of application.

A benefit of isolating generic security services is that it permits composable security specifications. Since a rating for a given service entails protection against a given class of potential threats, the residual vulnerabilities of a rated module can be assessed. These residual vulnerabilities can then be addressed by placing requirements on the modules which interact with the rated module. For example, one could build a pure audit module to meet the WA-3 criteria; specify its interfaces and place requirements on the host to ensure the proper integration of the module. This is the approach that was taken when designing the security requirements for cryptographic modules.

3 Scope

The CTCPEC requirements for cryptography address the proper implementation of encryption, digi-
tal signatures, and key management from the perspective of a cryptographic server. The requirements for cryptographic modules, in themselves, do not place constraints on the use of cryptography only on its implementation and integration. The use of cryptography is constrained by the functional security criteria for the security service which uses cryptography in its implementation. It is recognised that cryptography may not be suitable in all circumstances so it is recommended that cryptography be used to implement or support only the following functional classes from the CTCPEC: discretionary and mandatory access control (CD-1 to CD-3, ID-1 to ID-3, CM-1 to CM-2, and IM-1 to IM-2), object reuse (CR-1), identification and authentication (WI-1 to WI-3), trusted path (WT-1 to WT-2), separation of duties (IS-1 to IS-3), and something which we have called confidential export.

Confidential export is a security service for the secure transport data across an un-mediated environment. Confidential export addresses data confidentiality for both communications and data storage. For example, data written to a floppy drive rated for confidential export from a computer processing sensitive data places a constraint on the disk. If one were to require to take precautions to protect the disk, one may wish to have a notebook computer with a hard disk rated for confidential export, so that the notebook computer may be left unattended when not in use.

Unfortunately, confidential export could not be addressed using the functional classes in the CTCPEC. This is a short coming of that document. In fact, the process of writing the requirements for cryptographic modules has shown that within version 3.0 of the criteria there is no direct means to address requirements on the channel when considering distributed systems. At present the security services in the CTCPEC address security mediation at the point of interaction between objects and suppress the security concerns generated by the process of interaction. We hope to address this short coming in a supplement on the application of the CTCPEC to distributed environments.

4 Structure of the requirements

The security requirements for cryptographic modules are divided into three parts. The first part addresses the security policy governing cryptography. The third part addresses what is required of a host system for the proper integration of a cryptographic module. Since the CTCPEC functional classes do not impose a specific policy, it is necessary to state the particular security policy to which a set of security requirements is designed to meet. For cryptographic modules this security policy may be summarised in the following principles:

- to maintain the integrity of the information under its control;
- to allow access only to authorised users.

A cryptographic module is treated as an independent trusted component. The requirements for implementation apply to this component without regard to end systems into which the cryptographic module may be integrated. These requirements specify the interfaces to the cryptographic module and the internal security mechanisms which must be present. Since these requirements are independent of the end system, the mechanisms used to implement the security requirements of the cryptographic module may have nothing to do with those in the end system. This causes some confusion when a cryptographic module is implemented as a combination of hardware and software on a host system since it may make use of security mechanisms in the host to satisfy its requirements and conversely, it may implement its own security mechanisms which are not available outside the cryptographic module. Since the cryptographic module is a trusted component, it becomes part of the trusted computer base when integrated into the end system.

The integration requirements address the security features which must be present in the end system to ensure the proper integration of the cryptographic module. These requirements do not address requirements specific to the security mechanisms which the cryptographic functions support, since these are contained in the body of the criteria. Confidential export is the exception to this rule. Since confidential export is not addressed in the body of the criteria it was necessary to address the specific requirements needed to support this mechanism.

In the absence of confidential export, we identify two configurations of a cryptographic module within a host system: stand alone off-line and embedded off-line. Stand-alone cryptographic modules interact directly with the user for all security critical interaction such as identification and authentication and key variable entry. For embedded cryptographic modules, all interaction between a user and the module is mediated by a host system.

Confidential export requires a separation be maintained between the sensitive information on the host system and the device rated for confidential export. Therefore, four configurations must be identified. The stand alone and embedded distinction is still relevant. The other distinction which is relevant is whether the cryptographic module is in-line or off-line. An in-line module maintains a physical separation between the device rated for confidential export and the sensitive data on the host. Off-line modules rely on the host to maintain this separation. Thus requirements are provided for stand-alone in-line, stand-alone off-line, embedded in-line and embedded off-line cryptographic modules.

32
5 Implementation Requirements

5.1 Confidentiality

Confidentiality is a prime security concern of a cryptographic module. Since all forms of cryptography rely on some secret information it is essential that this information not leave the cryptographic module. Equally important is the ability of the cryptographic module to protect sensitive information from being leaked to the cipher text interface; encryption does not provide much of a service if the information is available at the cipher text interface in un-encrypted form. Thus, a cryptographic module must be subject to a confidentiality policy.

The confidentiality requirements of a cryptographic module are specified by requiring the cryptographic module implement a policy consistent with red/black separation. Red refers to sensitive (plain text) data and black to non-sensitive data. Key data is also recognised. Briefly red data may be converted to black only by the application of an encryption function and black data becomes red on the application of a decryption function. Key data must not leave the cryptographic module in plain text form. Such a policy is consistent with the CM-1 criteria of the CTCPEC which requires a mandatory decision as to which information and in which form it may be disclosed for a defined subset of object. Also red/black separation does not easily apply to digital signatures, so greater flexibility is achieved by requiring mandatory confidentiality to be applied to a defined subset of subjects and objects rather than all subjects and objects, a second property of the CM-1 criteria.

Every cryptographic module requires at least basic key management. Since secret keys should not leave the cryptographic module, the cryptographic module must provide some form of key database for key storage and retrieval. A cryptographic module may however be used as a dominant component in a fully integrated electronic key management and distribution scheme. Thus requirements on key data are provided. These requirements address key variable generation, key storage, key entry, key distribution, and key destruction.

5.2 Assurance

The CTCPEC assurance criteria provide a measure of the quality of evidence to support the assertion that the product under consideration is faithful to its security specification. The CTCPEC recognises that evidence may be provided in numerous ways and thus presents its assurance criteria in six sections: architecture, development evidence, security testing, security manuals, life cycle process, trusted distribution and generation. In the following paragraphs, we discuss the application of the CTCPEC assurance criteria to the implementation of cryptographic modules.

Cryptographic modules are required to meet the CTCPEC T-3 assurance criteria. The T-3 assurance criteria is comparable to "B2-type" assurance in the Orange Book [10] or E-4 assurance of the ITSEC [5]. However the T-3 assurance criteria has been weakened slightly to accommodate both cost and hardware constraints of embedded systems.

The T-3 requirements on the hardware architecture require the trusted computing base (TCB) to maintain a domain for its own execution; use available hardware to separate protection critical and non protection critical elements; to enforce the principle of least privilege; and to have completely specified interfaces. In specialising these requirements to cryptographic modules, we have expanded on the requirement to use available hardware to separate protection critical and non protection critical elements by requiring that the design prevent against single hardware failures. For example, addresses for red data should differ from addresses for black data by at least two bits. The required interfaces to the cryptographic module are also specified at this point as is the requirement that only approved cryptographic algorithms be used.

The CTCPEC requires development evidence to be presented in three stages: at the functional specification stage, at the software architecture or preliminary design stage, and at the detailed design stage.

At the functional specification stage, the interface to the cryptographic module must be specified and the functionality of the module defined. In addition, a semi-formal security policy model must be presented and informally shown to implement the security policy. The security policy model for a cryptographic module must at least model the red/black separation by defining the objects subject to mediation and the rules governing mediation in some form of restricted syntax. For example, if the design of a cryptographic module uses a finite state machine model then the inputs and outputs to the state machine and the states themselves might constitute the mediated objects. Rules governing the mediation might take the form of red input is allowed only in red states. Such a policy model would correspond to the requirement in [5] that all input/output, plaintext/ciphertext data paths be defined.

At the software architecture stage a high level structural design of the product is given and is traced to the security policy model. This stage provides both risk reduction in the design process and improved development evidence by forcing the designers to isolate the high level concepts used in their design and relate them to the security model. The security policy model may be thought of as the security relevant denotational semantics for the product, whereas the design documentation may be thought of as the operational semantics. A cryptographic module must present its operational semantics using some form of restricted syntax such as data flow diagrams.

The detailed design is the final specification of the product. From this point it should be relatively straight forward to implement the product. The security policy model must be traced to the detailed design to demonstrate that the detailed design is faithful to the security policy model. Finally, the detailed design must be faithfully mapped to the implementation.

The T-3 requirements on security testing require the vendor to provide detailed security testing procedures for approval and to execute those procedures. The evaluation authority will then spot check the func-
tional testing done by the vendor and perform additional tests of their own. The test performed by the evaluation authority are penetration tests, however, their number is limited in order to reduce evaluation time and hence the cost of the product.

The T-3 assurance life-cycle process require the vendor to describe and apply coding standards in the development process. The vendor is also required to place the product development under configuration management. The configuration management system need not be automated at this level provided that the system gives reasonable assurance that the design documentation corresponds with the implementation of the product. The requirement on configuration management has a benefit to the vendor in that it facilitates rating maintenance which may include a port of the product to a new platform.

5.3 Integrity
Cryptographic modules are particularly sensitive to hardware failure. The nature of cryptographic algorithms is such that an apparently minor malfunction in a hardware component may cause a catastrophic security breach. For example, a flaw in a random source could significantly degrade the key variable generator. Or a minor flaw in the memory address logic could cause red data to be output via the cipher text interface. Thus cryptographic modules are required to meet the IT-3 criteria for self tests. The IT-3 criteria require self test to be performed at start up, on demand, and at least once per fixed period of time. The security requirements for cryptographic modules specify the specific tests which must be performed under the IT-3 criteria and require that some of these tests be done once in each twenty four hour period.

Cryptographic modules are a potential target for hardware tampering. Substitution of a fake encryption chip may greatly compromise the security of a cryptographic module and be un-noticiable to a user. To counter this threat, cryptographic modules are required to implement minimal tamper detection as specified in the IP-1 criteria of the CTCPEC.

To support the integrity of critical security parameters, a cryptographic module is required to implement user and crypto-officer roles. This role separation prevents the average user from changing the critical security parameters. Cryptographic modules require at least two roles: one for a crypto-officer to perform tasks such as key entry, and another for the user.

5.4 Availability
Should a failure occur which would compromise security, a cryptographic module should at a minimum be able to shut down gracefully and be restarted without compromising security. This requirement is addressed by the recovery criteria AY-1 of the CTCPEC.

5.5 Accountability
To support a separation of roles, cryptographic module requires some form of identification and authentication (I&A); consequently cryptographic modules must meet the WI-1 criteria. At one extreme a user may be required to log into a cryptographic module in order to use its services. At the other extreme, a cryptographic module may share an identification and authentication mechanism with the host machine. In the latter case, the identification and authentication mechanism falls within the cryptographic boundary and is subject to the assurance requirements for cryptographic modules.

Concern might be raised that requiring a cryptographic module to maintain individual identification and authentication is too burdensome on an an embedded system. However, this requirement is necessary to address the wide variety of implementations. Certainly, if one were to implement a cryptographic module as a trusted software module within the TCB of the host system, a judicious design decision would have the TCB implement I&A and role separation and have the cryptographic module call these services. In this case, the I&A mechanism and the role separation mechanism fall within the cryptographic boundary and are subject to the T-3 assurance criteria. However, another design might be intended as subsystem for a multi-user product which does not recognise a cryptographic module’s role separation. In this circumstance, a crypto-officer could be required to log into the crypto module and a trusted path be established while crypto maintenance is being performed.

Cryptographic modules are required to have a robust audit mechanism. This mechanism must be capable of detecting imminent violations of the security policy and trigger alarms. For particularly severe violations, the audit mechanism must be able to initiate a graceful shut down. However, since cryptographic modules are embedded systems, audit analysis tools are not required. While not required, audit data should be available in a format that would permit the use of such tools off-line.

6 Integration Requirements
Cryptographic modules are viewed as cryptographic service providers in the CTCPEC. As such, the implementation requirements discussed in the previous section provide a security specification for the provision of the cryptographic services only and do not address the secure use of these services. The secure use of a cryptographic module entails certain assumptions on the environment in which the module operates. These assumptions are made explicit in the requirements for integrating cryptographic modules.

6.1 Basic Requirements
If a cryptographic module is used to support COMPUTE security, then there is a single assumption on the module’s environment which drives the integration requirements: for critical functions, the interaction between the user and the module is trusted. Critical functions include key variable entry, identification and authentication of the user, and examination of the audit data.

This assumption entails two configurations for cryptographic modules. At the one extreme are stand-alone cryptographic modules in which the user interacts directly with the module for critical functions. At the other extreme are embedded modules for which all interaction with the cryptographic module is mediated by a host system. If a module is implemented
as stand-alone, then a host system automatically satisfies the assumptions about the environment. Consequently there are no general integration requirements on the host. The host system, however, is required to meet the specific requirements for the COMPUSERC mechanisms which use the cryptographic services.

Since a host system mediates the interaction between the user and embedded cryptographic modules, the host must be trusted to faithfully process this interaction. In the requirements for integrating embedded cryptographic modules, the functions requiring trusted mediation are key variable entry, identification and authentication, and the processing of audit information. To provide trusted interaction between the user and the cryptographic module the host is required to implement a trusted path mechanism, and an audit mechanism. The trusted path mechanism provides a trusted mediation between the host and the cryptographic module for identification and authentication and for key variable entry. The audit mechanism ensures that all audit data emanating from the cryptographic module is adequately protected from deletion or modification. It is not necessary for the audit mechanism on the host to implement detection of imminent violation since the audit mechanism inside the cryptographic module has this capacity and will prevent the provision of cryptographic services in such an event.

In addition to the requirement to implement a trusted path and an audit mechanism, a host is required to implement an identification and authentication mechanism, self tests and to meet the T-1 assurance criteria if it is to support an embedded cryptographic module. It is assumed that the host system will be used by trusted users, consequently only basic assurance is required. (T-1 assurance is roughly equivalent to the assurance criteria for C2 systems.) Requiring the host to implement an identification and authentication mechanism is a means of ensuring that only authorized users have access to the system. Self tests are required at start up and on demand in order to ensure the integrity of the interface with the cryptographic module against hardware failures.

6.2 Requirements for Confidential Export

A confidential export function provides confidentiality on the exchange of information across an unmediated domain. Such a function might provide for disk encryption when a disk must be removed from a secure environment. It might also provide confidentiality over a communications channel. Consequently, a confidential export function must provide a separation of the unprotected data being processed and the un-mediated domain; only protected data should be permitted to access the un-mediated domain. The integration requirements for confidential export are driven by the following assumptions on the environment provided by the host:

- for critical functions, communications between the user and the cryptographic module are trusted; and
- the plain text and cipher text ports lie in separate domains called red and black respectively; communication between these domains must be mediated by the cryptographic module.

The first assumption is the same as the assumption that drives the basic requirements. Thus the distinction between stand-alone and embedded cryptographic modules is still relevant as are the requirements for these configurations.

The second assumption entails two additional configurations on the integration of cryptographic modules: in-line and off-line. In-line cryptographic modules provide a physical separation of the red and black domains. The external media communicates exclusively with the cipher text interface and the host with the plain text interface. A cryptographic module which implements its own disk controllers, is an example of an in-line module: the host can communicate with the storage media through the cryptographic module only. For in-line modules the host is not required to implement any further security functionality.

Off-line modules communicate with the host through both the plain text and cipher text interfaces. Consequently the host is required to maintain the red/black separation. Thus we require the host to implement a mandatory protection mechanism over a relevant subset of objects to maintain red/black separation. This must be supported by object reuse and T-3 assurance. The assurance requirement is necessary to ensure that the steps taken within the cryptographic module to separate red and black data are not undone by the host.

In summary, there are four sets of requirements for integrating cryptographic modules when confidential export is being provided. There are no security requirements on the host entailed by a stand-alone in-line module. For stand-alone off-line modules, the host must implement red/black separation with T-3 assurance. An embedded in-line module requires the host to satisfy the basic requirements for embedded modules only; in particular, the host need only have T-1 assurance. Embedded off-line modules must both meet the basic requirements for embedded module and implement red/black separation; in particular, the host must meet the T-3 assurance criteria.

7 Summary

Data exchange is a fundamental part of information security. Traditional system security assumes the channel to either be trusted or subject to mediation. When a system is distributed, one cannot assume the channel is protected. Cryptography is a mechanism for providing security for the information on the channel when the channel itself cannot be protected. The CTCPEC requirements on cryptography address the proper implementation of this mechanism. With the exception of the requirements for confidential export, they do not address the how to properly apply cryptography. These requirements are thus the Canadian equivalent of [9].

By being integrated into the CTCPEC, the requirements on cryptography are more than just requirements on the implementation of the mechanism. They
are supported by criteria for its correct application. The CTCPEC does not provide functional classes for data exchange, however. Thus at the present time, the correct application of cryptography to communications may still require support from standards such as [3]. Once secure data exchange has been integrated into the CTCPEC, the goal of a unified INFOSEC criteria will have been achieved.

Acknowledgements
I would like to take this opportunity to thank all the members of the Criteria working group at Communications Security Establishment for their stimulating discussions during the design of these requirements; however, I am particularly greatful to Rick Doucette and Paul Cormier for their comments. I would also like to acknowledge the Gary Maxwell, and Ken Donaldson for their contribution in drafting the security requirements for cryptographic modules; their long experience in the field was invaluable.

References