DEPARTMENT OF DEFENSE

MILITARILY CRITICAL TECHNOLOGIES LIST

SECTION 17: INFORMATION-SECURITY TECHNOLOGY

May 2007

Under Secretary of Defense, Acquisition, Technology and Logistics
Pentagon, VA

PREFACE

A. THE MILITARILY CRITICAL TECHNOLOGIES PROGRAM (MCTP)

The MCTP supports the development and promulgation of the congressionally mandated Militarily Critical Technologies List (MCTL) and the Developing Science and Technologies List (DSTL).

Congress assigns the Secretary of Defense the responsibility of providing a list of militarily critical technologies (the MCTL) and of updating this list on an ongoing basis. The MCTL identifies technologies crucial to weapons development and has been a key element in evaluating U.S. and worldwide technological capabilities. The MCTP has provided the support for a wide range of assessments and judgments, along with technical justifications for devising U.S. and multilateral controls on exports. The DSTL, another MCTP product, identifies technologies that may enhance future military capabilities and provides an assessment of worldwide science and technology (S&T) capabilities.

The MCTP process is a continuous analytical and information-gathering process that refines information and updates existing documents to provide thorough and complete technical information. It covers the worldwide technology spectrum and provides a systematic, ongoing assessment and analysis of technologies and assigns values and parameters to these technologies.

Technology Working Groups (TWGs), which are part of this process, provide a reservoir of technical experts who can assist in time-sensitive and quick-response tasks. TWG chairpersons continuously screen technologies and nominate items to be added or removed from the list of militarily critical technologies. In general, TWG members are drawn from about 1,000 subject matter experts (SMEs) from the military Services, DoD and other federal agencies, industry, and academia. A balance is maintained between public officials and private-sector representatives. TWGs collect a core of intellectual knowledge and reference information on an array of technologies, and these data are used as a resource for projects and other assignments. Working within an informal structure, TWG members strive to produce precise and objective analyses across dissimilar and often disparate areas. Currently, the TWGs are organized to address 20 technology areas:

Aeronautics	Information Systems
Armament and Energetic Materials	Lasers, Optics, and Imaging
Biological	Processing and Manufacturing
Biomedical	Marine Systems
Chemical	Materials and Processes
Directed Energy Systems	Nuclear Systems
Electronics	Positioning, Navigation, and Time
Energy Systems	Signature Control
Ground Systems	Space Systems
Information Security	Weapons Systems

B. THE MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL)

The expanded MCTL provides a coordinated description of existing goods and technologies that DoD assesses would permit significant advances in the development, production, and use of military capabilities by potential adversaries. It includes goods and technologies that enable the development, production, and employment of weapons of mass destruction (WMD) and their means of delivery. It includes discrete parameters for systems; equipment; subassemblies; components; and critical materials; unique test, inspection, and production equipment; unique software, development, production, and use know-how; and worldwide technology capability assessments.

C. LEGAL BASIS FOR THE LIST OF MILITARILY CRITICAL TECHNOLOGIES

The Export Administration Act (EAA) of 1979 assigned responsibilities for export controls to protect technologies and weapons systems. It established the requirement for DoD to compile a list of militarily critical technologies. The EAA and its provisions, as amended, were extended by Executive Orders and Presidential directives.

D. USES AND APPLICATIONS

The MCTL is not an export control list. Items in the MCTL may not appear on an export control list, and items on an export control list may not appear in the MCTL. The document is to be used as a reference for evaluating potential technology transfers and for reviewing technical reports and scientific papers for public release. Technical judgment must be used when applying the information. It should be used to determine if the proposed transaction would result in a transfer that would give potential adversaries access to technologies whose specific performance levels are at or above the characteristics identified as militarily critical. It should be used with other information to determine whether a transfer should be approved.

This document, MCTL Section 17: Information-Security Technology supersedes MCTL Section 17 dated May 2003.

INTRODUCTION

A. ORGANIZATION OF THE MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL)

The MCTL is a documented snapshot in time of the ongoing MCTP militarily critical technology process. It includes text and graphic displays of technical data on individual technology data sheets.

Each section contains subsections devoted to specific technology areas. The section front matter contains the following:

- *Scope* identifies the technology groups covered in the section. Each group is covered in a separate subsection.
- *Highlights* identify the key facts in the section.
- *Overview* discusses the technology groups identified under "Scope."
- *Background* provides additional information.

Each technology group identified under Scope has a subsection that contains the following:

- *Highlights* identify the key facts found in the subsection.
- *Overview* identifies and discusses technologies listed in data sheets that follow.
- *Background* provides additional information.
- *Data Sheets*, which are the heart of the MCTL, present data on individual militarily critical technologies. The principal data element is the Critical Technology Parameter, which is the technology parameter that defines where the technology would permit significant advances in the development, production and use of military capabilities of potential adversaries.

B. TECHNOLOGY DATA SHEETS

The technology data sheets are of primary interest to all users. They contain the detailed parametric information that managers, R&D personnel, program managers (PMs), and operators need to execute their responsibilities.

- *Critical Technology Parameter(s)* includes the parameter, data argument, value, or level of the technology which would permit significant advances in the development, production and use of military capabilities of potential adversaries.
- *Critical Materials* are those materials that are unique or enable the capability or function of the technology.
- *Unique Test, Production and Inspection Equipment* includes that type of equipment that is critical or unique.
- *Unique Software* is software needed to produce, operate, or maintain this technology that is unique.
- *Major Commercial Applications* addresses commercial uses of this technology.
- *Affordability Issues* are those factors that make this technology an affordability issue.
- *Export Control References* indicate international and U.S. control lists where this technology is controlled.

  Note: Export control references are:

WA ML 2	(Wassenaar Arrangement Munitions List Item)
WA Cat 1C	(Wassenaar Dual Use List Subcategory)
MTCR 17	(Missile Technology Control Regime Item)

NTL B3	(Nuclear Trigger List Subitem – Nuclear Suppliers Group)
NDUL 1	(Nuclear Dual Use List Item – Nuclear Suppliers Group)
AG List	(Australia Group List)
BWC	(Biological Weapons Convention)
CWC	(Chemical Weapons Convention)
USML XII	(United States Munitions List Category – ITAR)
CCL Cat 2B	(Commerce Control List Subcategory – EAR)
NRC A	(Nuclear Regulatory Commission Item)

- *Background* provides a description of the technology.

SECTION 17—INFORMATION-SECURITY TECHNOLOGY

Scope

Highlights

- Strong personnel, facilities, equipment, standardization, training, and test and evaluation security programs as well as defensive *Information Operations* and *Operation Security* (OPSEC) are key components of secure militarily critical information and infrastructure assurance systems.
- Many commercial information security technologies, techniques, and products, which can be customized by adversaries, rogue states, sub-national groups, terrorists, criminals and international crime syndicates are widely available in world markets with capabilities that are adequate for the protection of some militarily critical information systems.
- Significant progress is being made toward the development of open, market-based information security products. These products include commercial public key infrastructures (PKI); cryptographic; steganographic; biometric, and software security systems, many of which are now covered by national and international standards, and national security export controls.
- There are few computers that are not connected to the Internet or some form of network. Internet connection commands and operating systems can be hacked, *malware* introduced, and operations disrupted by denial of service (DOS) attacks, all of which make *network firewalls* between computers and the Internet a necessity. Examples of malware appear in Appendix A.
- Open worldwide information security scientific investigation, research and development (R&D) is producing technologies, which have undergone international open scientific peer review, that are enabling the development of sound militarily critical information and national security information assurance security products.
- Both commercial and government information security technologies and products are becoming more affordable and armed forces are transitioning to network centric warfare (NCW).
- The potential adversaries of the United States have the same access to the global commercial industrial base and installed communications base, including some of the same information security technologies and products as do the U.S. military forces.
- Secure networks and reliable software are more important than ever before in cyberspace. New vulnerabilities will continue to be found. Network security must therefore emphasize detection, quarantine, recovery, and inoculations against re-attack.

OVERVIEW

The *Wassenaar Arrangement* countries define “information security” as:

> *“All the means and functions ensuring the accessibility, confidentiality, or integrity of information or communications, excluding the means and functions intended to safeguard against*

malfunctions. This includes cryptography, cryptanalysis, protection against compromising emanations, and computer security."[1]

This is consistent with the definition found in JP 1-02 – "The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users."

Information Security Technologies are essential for the protection of the critical national infrastructure and cyber attack risk management.

"Terrorists may seek to cause widespread disruption and damage, including casualties, by attacking our electronic and computer networks, which are linked to other critical infrastructures such as our energy, financial and security networks. Terrorist groups are already exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber attacks will become an increasingly significant threat."[2]

It is recognized that there is far more to information security than those technologies and products identified in this section.[3] However, in information security and related fields, no other information security technologies have been identified that are considered to be militarily critical. There are many other information security-related computer software and hardware, facility and equipment technologies, all of which are important to the security of militarily critical information systems and the national infrastructure. However, most of these are well known and widely available. These technologies repeatedly appear in public domain technical literature and trade journals. They are also advertised as widely available in the international market place.

Most (on the order of 85 percent) of the security breaches are due to operator error. For example, more than 8 out of every 10 computer attacks against businesses could be stopped if enterprises checked the identity of not only the user, but also the machine logging onto its network.[4]

Many of these important security-related technologies appear in the Common Criteria (CC).[5] Many are covered by National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS).[6] There also many covered in the American National Standards Institute (ANSI) and International Standards Organization (ISO) standards. These relatively 'low-tech' technologies have long been in the public domain and are not controllable through national and international export controls. This does not mean that they are/would not be of significant value to the security of U.S. militarily critical information systems and those of our adversaries.

A Common Criteria Evaluation Assurance Level (EAL) is specified in the first row of the data table in several of the data sheets in this section. See Appendix B for the relationship between the CC EAL levels and the level designations given in prior evaluation regimes. It is recognized that there may not be COTS products in the market today that meet or exceed these requirements.

The U.S. Security Objectives of Confidentiality, Integrity and Availability of data and adjective impact levels are defined in Federal Information Processing Standards (see Appendix C).

Responsibility and *accountability* are core principles that characterize security accreditation. Security accreditation is the result of the official management decision made by a senior agency official to authorize

---

1 http://www.wassenaar.org/controllists/16%20-%20WA-LIST%20(06)%201%-%20DEF.doc

2 *National Strategy for Homeland Security*, Office of Homeland Security, July 2002, p. 9.

3 Certain commercial entities, equipment, or materials are identified in this Section in order to describe a technique, policy practices or concept adequately. Such identification is not intended to imply recommendation or endorsement nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

4 Most Damaging Attacks Rely On Stolen Log-ins ***TechWeb*** (08/28/2006).

5 Information on the Common Criteria can be found at http://niap.bahialab.com/cc-scheme/

6 See http://csrc.nist.gov/publications/fips/index.html

operation of an information system and to explicitly accept the risk to agency operations and assets or individuals based on the implementation of an agreed-upon set of management policy security controls.

BACKGROUND

> *"War is a product of its age. The tools and tactics men fight with have always evolved along with technology.* Warfare in the Information Age (IA) *will inevitably embody the characteristics of the Information Age."*[7]

The computer and high-speed communications that have brought the United States and much of the world to adopt networks for electronic commerce and personal use have brought Network Centric Warfare (NCW). NCW is the term developed to describe the way U.S. forces will organize and fight using information. NCW is a force multiplier and the "shock and awe" that resulted from the swiftness of the "Thunder Run" to Baghdad and the initial American military victory in Operation Iraqi Freedom was due, in part, to NCW. It increases combat power, which is derived from the most efficient linking or networking of knowledge entities that are geographically and hierarchically dispersed. NCW gets the right information, in the right format, at the right time, to the right warfighter.

The E-Government Act of 2002 (Public Law 107-347), passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with responsibilities for standards and guidelines, including the development of, among other things, standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

To facilitate common understanding, this section uses The Department of Defense Dictionary of Military and Associated Terms [Joint Publication (JP) 1-02] and where JP 1-02 is silent or where additional informative technical detail is necessary Federal Information Processing Standards (FIPS) and American National Standards Institute (ANSI) standards. Section 17 identifies information security technologies that respond to the DODD S-3600.1 requirement that:

> *DoD activities shall be organized, trained, equipped, and supported to secure peacetime National Security objectives, deter conflict,* ***protect DoD information and information systems*** *and to shape the information environment. If deterrence fails, Information Operations shall seek to achieve US superiority in times of crisis or conflict.*

[7] David W. Alberts et al., Network Centric Warfare, sun Microsystems Federal, Inc., February 2000.

APPENDIX A

Malware includes the following major categories of malicious code and programs:

1. *Viruses,*[8] which are self-replicating code that insert copies of the virus into host programs or data files. Viruses often result from user interactions, such as opening a file or running a program and include:

    - *Compiled viruses* that are executed by an operating system. These include infector viruses, which attach themselves to executable programs; *boot sector viruses*, which infect the master boot records of hard drives or the boot sectors of removable media' and multipartite viruses which combine the characteristics of the file infector and boot sector viruses.

    - *Interpreted viruses* that are executed by an application. These include macro viruses that take advantage of the capabilities of macro programming language to infect application documents and document templates; and scripting viruses that infect scripts and are understood by scripting languages processed by services son the operation system.

2. Worms are self-contained and self-replicating programs that usually perform without user intervention. Worms create fully functional copies of them selves, and they do not require a host program to infect a system. Attackers often insert worms because they can potentially infect many more systems in a short period of time that a virus can. Worms include:

    - *Network service worms* that take advantage of vulnerabilities in network services to propagate and infect other systems.

    - *Mass mailing worms* that are similar to email-borne viruses but are self-contained, rather than infecting existing file.

3. Malicious mobile code is software with malicious intent that is transmitted from a remote system to a local system. The inserted programs executed on the local system, usually without the user's explicit instruction. Programs delivered in this way can be used by many different operating systems and applications, such as web browsers and email clients. Although the mobile code may be benign, attackers us it to transmit viruses, worms and Trojan horses to the user's workstation. Malicious mobile code does not infect files or attempt to propagate itself, but exploits vulnerabilities by taking advantage of the default privileges granted to mobile code. Languages for malicious mobile code include Java, ActiveX, Java Script, and VBScript.

4. Blended attacks use multiple methods of infection or transmission. A blended attack could combine the propagation methods of viruses and worms.

5. Tracking Cookies are persistent cookies that are accessed by many websites, allowing a third party to create a profile of a user's behavior. Tracking cookies are often used in conjunction with web bugs, which are tiny graphics on websites and which are referenced with the HTML content of a web page or email. The purpose of the graphic is to collect information about the user viewing the content.

6. Attacker tools might be delivered to a system as part of a malware infection or other systems compromises. These tools allow attackers to have unauthorized access to or use of infected systems and their data, or to launch additional attacks. Popular types of attacker tools include:

    - *Backdoors* are malicious programs that listen for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a system such as acquiring passwords or executing arbitrary commands. Backdoors include zombies (also known as bots), which

[8] Consumers paid as much as $7.8 billion over two years to repair or replace computers that got infected with viruses and spyware, a Consumer Reports survey found. Kim Hart, Viruses, Spyware Cost Users $7.8 Billion, *The Washington Post*, 8 August 2006, p. D5.

are installed on a system to cause it to attack other systems, and remote administration tools, which are installed on a system to enable a remote attacker to gain access to the systems functions and data.

- *Keystroke loggers* monitor and record keyboard use. Some require the attacker to retrieve the data from the system, while other loggers actively transfer the data to another system through email file transfer, or other means.
- *Rootkits* are collections of files that are installed on a system to alter its standard functionality in a malicious and stealthy way. A rootkit can make many changes to a system to hide the rootkit's existence, making it very difficult for the user to determine that the rootkit is present and to identify what changes have made.
- *Web browser plug-ins* provide a way for certain types of content to be displayed or executed through a web browser. Attackers often create malicious web browser plug-ins that act as spyware and monitor the use of the browser.
- *Email generators* are programs that can be used to create and send large quantities of email, such as malware, spyware and spam to other systems without the user's permission or knowledge.
- *Attacker toolkits* include several different types of utilities and scripts that can be used to probe and attack systems, such as packet sniffers, port scanners, vulnerability scanners, password crackers, remote login programs and attack programs and scripts.

Common non-malware threats associated with malware include *phishing*, which uses computer-based means to trick users into revealing financial information and other sensitive data. Phishing attacks frequently place malware or attacker tools on systems. Virus hoaxes, which are false warning of new malware attacks, are another common threat.

APPENDIX B

Table 17.0-1. Information Security Criteria Comparison

CC[a]	TSEC[b]	ITSEC[c]
EAL 0[d]	D: Minimal Protection	E0
EAL 1		
EAL 2	C1: Discretionary Security	E1
EAL 3	C2: Controlled Security	E2
EAL 4	B1: Labeled Security	E3
EAL 5	B2: Structured Security	E4
EAL 6	B3: Security Domains	E5
EAL 7	A1: Verified Design	E6

[a] CC is the abbreviation for *Common Criteria*, which is the short title for the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408.

[b] TSEC is derived from Telecommunications Security for identifying certain items of Communications Security (COMSEC) material.

[c] ITSEC is the acronym for Information Technology Security Evaluation Criteria.

[d] EAL is the acronym for Evaluation Assurance Level.

APPENDIX C

Table 17.0-2. Information Security Criteria Comparison

Security Objective	Low Impact	Moderate Impact	High Impact
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (U.S.C. Sec. 3542)	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (U.S.C. Sec. 3542)	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information. (U.S.C. Sec. 3542)	The disruption of access to or use of information or an information system could be expected to have **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations organizational assets, or individuals.

Source: Taken from FIPS 199, Standards for Security Categorization of Federal Information Processing Systems, February 2004, p. 6.

SECTION 17.1—CRYPTOLOGIC TECHNOLOGY

Highlights

- Cryptologic technologies and products provide security to information systems for Network Centric Warfare (NCW) and the required secure, reliable wide band communications links and information management nodes, which extend through the chain of command and channels of communications from the President to the warfighter and provide information dominance to U.S. armed forces.
- The worldwide proliferation of encryption has coincided with the explosive growth of the Internet. The civilian sector is now advancing the development, production and use of civilian commercial cryptologic technology and products.
- The legacy U.S. symmetric cryptography algorithm [the Data Encryption Standard (DES)] has been replaced by the Advanced Encryption Standard (AES), an algorithm of foreign (Belgian) origin.[9]
- There are opportunities for the U.S. cryptologic community to influence the future through cooperation with, and participation in the deliberations of, national and international standards bodies.

OVERVIEW

The National Institute for Standards and Technology (NIST) is responsible for the development of cryptographic standards and guidelines for the protection of the sensitive, but unclassified (SBU) information of U.S. federal government departments and agencies. The NIST cryptographic standards and associated guidance is also widely used by defense industry and many other nongovernmental activities, businesses and the financial service industry. Many of the definitions and much of the cryptologic information in this section is drawn from NIST publications.

The cryptologic technologies in this section are closely related to most of the information technologies for information systems specially designed or modified for military use. Cryptographic modules, components and systems must be tailored or integrated in or an integral component or module of, the basic information processing system hardware and software architecture during system development and throughout the life cycle of the secure information systems and associated weapons systems.

Some telecommunications technologies in MCTL Section 10, Information Systems are closely related, such as the spread spectrum and frequency-hopping technologies commonly used in both civilian and military cellular voice systems, which now normally incorporate cryptographic modules to protect the dialing and billing codes, and the nominal privacy of conversations over the radio frequency (RF) segments. (See Data Sheet 17.1-5, Secure Wireless Technology.) The networks and switching technology data sheets in the links and nodes of information communications systems are also closely related to the cryptography items. For example, link encryption is used to protect most of the commercial backbone links in the installed base, which is usually some from of stream encryption. It has been estimated that 85 percent of global military communications ride on the commercial backbone.

Cryptologic technologies are also closely related to satellite tracking, telemetry and commanding (TT&C) encryption and decryption technologies in MCTL Section 16, Positioning, Navigation and Time Technology. The commanding uplinks and mission data downlinks for both civilian and military satellites, such as the Global

[9] AES, FIPS PUB 197, 26 November 2001, is based on ***Rijndael***, developed by Joan Daemen and Vincent Rijmen of Belgium.

Positioning System (GPS), are increasingly protected by encryption to maintain positive control of the satellites and prevent mission data interception, intrusion and spoofing.

The ideal cryptographic algorithm functions and systems:

1. Encrypt bulk data quickly;
2. Fit on small CPUs with very little random access memory (RAM);
3. Efficient in hardware;
4. Efficiently encrypt small amounts of text with each key;
5. Permit frequent key changes;
6. Work on digital signal processors;
7. Perform encryption; and
8. Hash functions.

Cryptographic primitives and therefore cryptography has a natural taxonomy via the key(s) of a primitive. Therefore, there are three kinds:

1. No-key cryptography—Hash Functions;
2. Symmetric-key cryptography—Secret Key cryptography; and
3. Asymmetric-key cryptography—Public Key cryptography.

The militarily critical Information Security technologies and products in this Section require unique empirically validated systems engineering and integration (SE&I) experience, related techniques and software for the development, production and the operational life cycle of the information security technology products. The information technology (IT) life cycle is typically described in five phases:

1. Initiation (requirements generation);
2. Development/acquisition;
3. Implementation;
4. Operations/maintenance; and
5. Disposal.

To provide the highest level of security for any information system, encryption algorithms (no matter how strong) must be integrated in information system implementations that also have secure operating systems, sound protocols, authentication, and secure links to secure nodes and storage devices..

Computer operating systems and some applications now incorporate features that require high-performance processors and metaprocessing (parallel processing using the Internet) techniques that are shortening the cryptanalytic time required for an exhaustive key search, thus making most of the cryptology technologies and information processing and high performance computing technologies closely related.

The time required for cryptanalyses used to be primarily a function of both knowledge in the field of mathematics and the state of the art in high performance computing in the early days of cryptography with digital deterministic computers. Cryptanalytic procedures and techniques were dependent on the state of the art in high performance computing because processing power determined the length of time required to perform an exhaustive key search for a given key length and thus governed key life cycles (cryptoperiods), which were then primarily a function of key lengths. However, given the knowledge of mathematics today, it is generally computationally infeasible to exhaust any crypto key in serious use today that complies with applicable ISO, ANSI and NIST standards, even using the highest performance Central Processing Units (CPUs) and metaprocessing.[10] Now, key life cycles are primarily governed by fiduciary prudence and comparmentation in key management because the

[10] Metaprocessing is a form of parallel processing implemented by using the Internet to task a large number of processors.

longer a key is used and the more data that it protects, the more vulnerable it becomes to attack and the easier it is to attack the key, “in theory.”

BACKGROUND

The cryptologic technologies covered in this section are in the public domain, some of which meet or exceed the minimum threshold requirements for military criticality. U.S. Government (USG) Type 1 cryptologic technology, which falls within the purview of the National Security Agency (NSA), is generally classified and therefore not covered.

The history of cryptology is one of strife between cryptographers who developed codes and ciphers and cryptanalysts who tried to break them. Cryptographic algorithms are always at risk of disproof by the next cryptanalytic attack. The strength of encryption algorithms is based on assumptions, inferences and beliefs about the hardness of their underlying mathematics problem, therefore encryption can never be proven to be unbreakable or unconditionally secure as long as the assumptions and inferences about the hardness of their underlying mathematics problems are believed.

However, an algorithm can be proven insecure by successfully attacking the ciphertext and recovering the clear text, which happens from time to time. Until broken, most encryption algorithms are provisionally accepted as “strong” because they have undergone extensive international peer review in the public domain. The longer they are under peer review in the public domain, the greater the confidence will be in their strength and the assumptions and inferences about the hardness of their underlying mathematics problems.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.1. CRYPTOLOGIC TECHNOLOGY

The Secure Hash Function Technology data sheet was added because NIST and standards organizations are preparing for an international competition like the one conducted for AES to develop a new hash function in which there is reduced, or ideally, no probability of a collision.[11]

[11] A *collision* occurs when pairs of inputs have identical outputs. Collision is a problem with hash functions, which produce many-to-one outputs. Source: Alfred J. Menezes, et al., *Handbook of Applied Cryptography*, CRC Press, New York, 1997.

MCTL DATA SHEET 17.1-1. SYMMETRIC KEY CRYPTOGRAPHIC TECHNOLOGY

Symmetric key (secret key) cryptography is a classical form of cryptography in which the key required for encrypting is the same as the key required for decrypting. Secret-key systems use a single key that is held by two (or more) parties; the sender and recipient(s).

Critical Technology Parameter(s)	1) Undergone extensive open peer review and no attacks found that allow faster plaintext recovery than an exhaustive key search; 2) At least a 128-bit key space.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	High performance computers, operating systems and application software specially designed to perform Randomness, Correlation, Weak Key and Symmetry Under Complementation tests to evaluate the strength of new symmetric encryption algorithms during development, test and evaluation.
Unique Software	Operating systems and application software implementing cryptographic functionality specially designed and integrated so that the information systems match and maintain the Common Criteria Evaluation Assurance Level (EAL) protection profile requirements for the systems during their operational lifecycles.
Major Commercial Applications	Commercial cryptographic applications for the financial service industry, and Internet electronic commerce and business network applications have been the principal open source drivers for commercial cryptographic technologies in recent years.
Affordability Issues	Military criticality, not affordability, is the principal military acquisition issue for this technology.
Export Control References	WA ML 11; WA Cat 5A2; USML XI and XIII;[12] CCL 5A002.a.1.a.

BACKGROUND

Cryptographic primitives and therefore cryptographic systems have a natural taxonomy resulting from the key(s) of the fundamental primitive. Under this taxonomy concept, there are three basic classes of cryptography: 1) one-key or *secret key* (also called symmetric systems; 2) two-key or *public key* (also called asymmetric[13] systems); and, 3) no-key cryptographic hash functions—irreversible algorithms, which are widely used forms of cryptography for modification detection (MDC). Specific applications include virus protection and software distribution. Secret-key cryptography is faster than public-key cryptography. Hybrid (or mixed) systems use both one-key and two-key types of cryptographic keys[14] and exploit the strengths of each.

Most modern cryptographic solutions for business are hybrid systems because hybrid systems simplify key agreement and get the performance of secret key cryptography for longer messages, often with cryptographic hash functions for an integrity check.

Cryptography is a combination of two basic components: an algorithm (or cryptographic methodology) and a *key*. Algorithms are complex mathematical formulae, and, in the digital age, keys are strings of bits. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption and decryption. Generally, two related algorithms are required: one for encryption and the other for decryption. Keys may be any of a large number of binary values. The set of possible values of the key is called the keyspace.

---

[12] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

[13] Asymmetric Cryptographic Technology is discussed in MCTL Data Sheet 17.1-2.

[14] A cryptographic key is a parameter used in the block cipher algorithm that determines the *forward cipher function*, one of the two functions of the block cipher algorithm that is determined by the choice of a cryptographic key.

For secret-key cryptography, only one key is used in the nodes on both ends. The same key is used to encrypt plaintext and decrypt ciphertext. While secret-key cryptography is generally not as mathematically elegant as public-key methods, it should certainly do the required job for most systems—as it has for years. The power of symmetric-keyed cryptography is that for each added bit the key space is twice as large, so a brute force attack takes twice as long. In addition, secret-key cryptography is far more efficient than public key. The primary drawback to secret-key cryptography is the necessity to agree on a key. Another drawback is that secret-key cryptography does not provide for digital signatures.

MAC algorithms involve the use of a secret key to generate a small block of data known as a "message authentication code." This technique assumes that the two communicating parties share a key, which they have kept secret. The sender calculates the MAC, which is a function of the message and the shared secret key. The message and MAC are transmitted to the intended recipient. The recipient performs the same calculation on the message when it is received, using the shared secret key to generate a MAC.

The received MAC is compared to the calculated MAC. If the two MACs are identical, assuming only the sender and receiver know the secret key, then the receiver is assured that the message has not been altered and that the message originated the assumed sender. Further, if the message includes a sequence number, then the receiver can be assured that the sequence of the message is valid. An attacker could not successfully alter the sequence number enroute without also altering the MAC calculated by the recipient, resulting in a MAC that will not match the MAC sent in the message.

Non-repudiation is not provided by secret-key "signatures;" however, without hardware support to control key usage. The successful verification of a MAC does not guarantee that the associated message is authentic: there is a small chance that an unauthorized party can guess a valid MAC of an arbitrary (i.e., inauthentic) message. Moreover, if many message forgeries are presented for verification, the probability increases that eventually verification will succeed for one of them. This limitation is inherent in any MAC algorithm.[15]

[15] Morris Dworkin, NIST Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode, Methods and Techniques*, 18 May 2004.

MCTL DATA SHEET 17.1-2. ASYMMETRIC CRYPTOGRAPHIC TECHNOLOGY

Asymmetric (or public key) cryptography uses two related keys: a public key and a private key. The two keys have the property that, given the public key, it is considered computationally infeasible to derive the private key.

Critical Technology Parameter(s)	1) Undergone extensive, open peer review and no short-cut attacks discovered; 2) At least 3072-bit key spaces[16] for Digital Signature Algorithm—Diffie-Hellman (DSA/DH) and Rivest, Shamir, Adelman (RSA) systems; 3) At least 256-bit key spaces for Elliptic Curve Cryptographic (ECC) systems; 4) A hash value of at least 256 bits for digital signature functions, features or applications (ds); and 5) Time stamp features or applications that are ANSI X9.95 compliant using the NIST time[17] signal.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Test software specially designed to support: 1) Randomness; 2) Multiple Polynomial Quadratic Sieve (MPQS); 3) Double Large Prime Variation of the MPQS; 4) Number Field Sieve (NFS) factoring; and discrete log (e.g., index-calculus) algorithms for use in asymmetric system development, testing, quality control and evaluation. And, software specially designed to support: 1) Pollard's parallel collision; and 2) Koblitz tests for the security of elliptic curve cryptographic (ECC) systems.
Major Commercial Applications	The comparatively recent requirements for strong cryptographic applications established for the financial service industries, Internet, electronic commerce and business network operators have been the principal open source drivers of this technology.
Affordability Issues	The cost of security indoctrination and additional staff to manage and maintain secure cryptographic functionality for large complex systems is a significant affordability issue, even though most of these secure cryptographic processes can be automated But even after automation, there is still a potentially expensive requirement to recruit and retain technically qualified personnel worthy of cryptographic system high trust and great responsibility; and, to operate, manage and support the required end-user training, standardization, test and evaluation programs required for optimum protocol security and the maintenance of system security. Also, the manpower requirements to man and operate a public key infrastructure (PKI), especially the certificate authority (CA) and registration authority (RA) personnel requirements, will affect affordability. This, of course, depends on the CA's policies and the Certificate Policy Statement (CPS).
Export Control References	WA ML 11; WA Cat 5A2; USML XI and XIII; CCL Cat 5A002.a.1.b.

BACKGROUND

Asymmetric key cryptography uses pairs of keys: a public key that is widely available, and a corresponding private key known only to the person, application or service that owns the keys. These key pairs are related mathematically in such a way that what is encrypted with the private key can only be decrypted with the public key, and vice versa. Some asymmetric algorithms can also be used for authentication [digital signature (ds)] and to establish non-repudiation.

---

[16] In determining equivalent asymmetric key lengths that match the 3072-bit asymmetric key threshold specified, the measure used was TIME. TIME is a computer complexity theory concept, which is the (estimated) number of computer operations required to solve one instance of the general problem.

[17] See http//www.time.gov

For authentication, the message is signed with the private key, and the signature is verified using the public key. Authentication can also be performed with a hash function, which hashes and compresses a plaintext message of arbitrary length into a fixed-size digest, or hash value. It is currently considered computationally infeasible to alter a plaintext message without altering the hash value.

The security of public key systems is based on assumptions about the hardness of certain mathematical problems that have not yet been proven to be false.

There are three families of asymmetric algorithms:

1. Elliptic Curve Cryptography (ECC);
2. Finite Field Cryptography (FFC); and
3. Integer Factorization Cryptography (IFC).

The hardness of the integer factorization problem is the assumption supporting the cryptographic security of Rivest, Shamir, Adleman (RSA). The hardness of solving the finite field discrete logarithm (DL) problem[18] is the assumption supporting the cryptographic security of the Digital Signature Algorithm (DSA) and Diffie—Hellman (DH) systems (DH is usually made secure by incorporation of digital signatures). The assumption about the hardness of solving the elliptic curve discrete log problem is the basis for the security of elliptic curve cryptography (ECC) systems.

In public-key cryptographic systems the private key is not revealed. The public key may be known to the world. The public key of a pair of keys used for encryption requires the private key of the same pair for decryption. For a public-key system to be secure, the private key must be kept confidential, known only to its owner. The public key must also be known to belong to the owner as well as being arithmetically valid.

A digital signature (ds) is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key, which corresponds to but is not the same as, the private key. Each user possesses a private and public key pair. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only with the user's private key.[19] An adaptation of digital signature techniques can be used to originate and verify time stamps.

A time stamp is a time variant parameter that denotes a point in time with respect to a common time reference. As the military forces, business and industry increasingly conduct more business electronically, it is correspondingly becoming more important to ensure that there is a secure, standardize methodology to prove what and when digital data was created, transmitted, received, modified or stored. The duality of proving the "what" and the "when" necessitates that the methodology provide the ability to verify the integrity of the digital data and the time of the digital event. Such a time stamp must therefore be issued by a trustworthy authority, whose time originates from a trustworthy source, and whose time stamp is irrefutably verifiable.

Most public-key algorithms operate on fixed-size blocks, usually 1,024 bits or larger for RSA™ and the Digital Signature Algorithm (DSA).[20] For applications requiring the authentication of data integrity and the identity of the signer, the Digital Signature Standard (DSS)[21] is used in conjunction with the Secure Hash Algorithm (SHA-1) (see Data Sheet 17.1-7). When using these algorithms to create digital signatures, messages are typically run through a cryptographic hash function, and the output of this function is what is actually signed. This output is called the message digest.

---

[18] The DL problem can be stated as follows: Given two group elements *g* and *h*, find integer *n*, such that $h = ng$ whenever such an integer exists.

[19] FIPS 186-2, 27 January 2000, p. 1.

[20] The DSA is specified in FIPS 186, *Digital Signature Standard* (DSS).

[21] FIPS PUB 186-2, *Secure Has Standard* (SHS).

Part 1 of the NIST *Key Management Guideline*[22] encourages using compatible strengths for the algorithms when used together (e.g., for 80 bits of security, SHA-1 should be used with a 1024-bit Digital Signature Algorithm (DSA) or Rivest, Shamir, Adleman (RSA) key, or with an Elliptic Curve DSA (ECDSA) key between 160 and 223 bits in length). For digital signatures, SHA-224 will be used with a 2048-bit DSA or RSA key, or with an Elliptic Curve Digital Signature Algorithm (ECDSA) between 224 and 255 bits in length. The larger key sizes might be appropriate today for high security applications, which produce data that must have a long (70 years or more) secure life.

One rationale for the existence of larger AES key sizes beyond 128 bits is the possibility of quantum computers becoming a reality. A large quantum computer could threaten the security of existing key sizes with a square-root attack, the largest today is about 5 bits. Attacking a 128-bit key would take a 128-bit quantum computer about 2^{64} operations, which is much less than the 2^{128} operations on a von Neumann deterministic machine. Hence, the AES has 256-bit keys. Using the *TIME* metric, AES 256-bit key is about equivalent in security to an Elliptic Curve Cryptography (ECC) key of 512 bits and RSA/Digital Signature Algorithm (DSA) key at 15,360 bits.[23]

---

[22] See http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html

[23] For reputable analyses supporting these conjectures, see http://www.certicom.com, RSA Laboratories Bulletin Number 13, April 2000 at http://www.rsalabs.com/bulletins and http://cryptosavvy.com

MCTL DATA SHEET 17.1-3. CRYPTANALYTIC TECHNOLOGY

Cryptanalysis is defined by the Department of Defense as: "The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption."[24]

Critical Technology Parameter(s)	Technologies and techniques that enable the recovery of plaintext from strong adversarial ciphertext in time to provide: 1) months to days of strategic warning; and, 2) hours to minutes or seconds of tactical warning.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	High speed computers, operating systems and applications designed to test the ability of cryptanalytic systems to perform key searches, statistical, linear and differential cryptanalyses; and, factor 220 decimal digit, or larger, numbers.
Unique Software	Software applications specially designed to perform: randomness; correlation; weak key and symmetry under complementation tests to facilitate analyses of ciphertext. Software specially designed to perform: randomness; multiple polynomial quadratic sieve (MPQS); double large prime variation of the MPQS; number field sieve (NFS) factoring for large composites (110 decimal digit or larger); solving large matrices *mod 2*[25] and discrete log, e.g., index-calculus, analyses to facilitate the analyses of ciphertext protected by asymmetric ciphers. And, software specially designed to support a square-root attacks, based on the Pollard rho algorithm, and Koblitz attacks on elliptic curve cryptography (ECC) systems.
Major Commercial Applications	The primary commercial applications of cryptanalytic technologies and techniques are for: 1) continuing peer review of existing cryptographic systems; 2) testing to evaluate the strength of new encryption algorithms during their development, testing and evaluation phases; and, 3) cryptanalyses.
Affordability Issues	Cryptanalytic technologies may be the least affordable of the technologies in the cryptology component. Cryptanalytic computers and software both tend to be expensive. But, perhaps more importantly, the cryptographers capable of performing cryptanalyses can be even more expensive and there is a shortage of them. Expert cryptanalysts are rare, attract significant compensation for their services, and there is fierce competition among industry and from governments for reputable cryptanalysts in the labor market.
Export Control References	WA ML 11; WA Cat 5A2 and 5E2; USML XI and XIII; CCL Cat 5A002 and 5E002.

BACKGROUND

> "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."
>
> Edgar Allan Poe

In essence, cryptanalysis is the science and art of recovering the plaintext of an encrypted message without access to the key. The art of encryption is about devising ways to hide text behind walls of random binary numbers. The art of code-breaking is all about using mathematics to find patterns in that binary number randomness—to discover order in a universe that is intended to present none.

---

[24] Joint Publication (JP) 1-02 http://www.dtic.mil/doctrine/jel/new_pubs/jp1-02.pdf

[25] Mod is the abbreviation for modulus, which is the number of different numbers used in a system of modular arithmetic. The 2 indicates binary: relating to, being, or belonging to a system of numbers having 2 as its base (the digits 0 and 1). Mod 2 is the abbreviation for Modulo 2 arithmetic.

Decoding computer-generated messages is becoming increasingly more difficult. In time, multiple encryption techniques [i.e., Triple DES (Data Encryption Standard)] and the use of public-key encryption for transmitting a new session key for each message or packet) are expected to eventually overwhelm the best special-purpose cryptanalytic computers.

Almost all cryptography is theoretically breakable. Future breakthroughs in mathematics and the ever-increasing processing power of computers may give the cryptanalysts' temporary advantages. However, better encryption algorithms may be discovered, keys can be lengthened, and superencipherment (multiple encryption)—although time consuming—may be used with different algorithms and key lengths for each successive layer of encryption. Some writers believe that future cryptanalytic attacks will take so much time and cost so much that cryptanalyses may have little practical utility, even with more processor power and better cryptanalytic techniques.

Cheap encryption, coupled with signal-hiding techniques (i.e., spread-spectrum and frequency-hopping) could seal the code-breaker's fate.[26]

An attempted cryptanalysis is called an attack. The four general types of cryptanalytic attacks are:

1. Ciphertext-only;
2. Known plaintext;
3. Chosen plaintext; and
4. Chosen ciphertext.

A cryptanalytic team chooses the type of attack based on the availability of plaintext and ciphertext, the best guess at the algorithm used for encryption, and other indicators of its origin and nature that may be obvious or available. The number, skill and ability of the cryptanalysts and the computer resources available for the attack determine the size of cryptanalytic operation and the length of time it takes—sometimes called the "work factor"—for a successful attack. Of course, the work factor drops dramatically if the key can be acquired clandestinely or simply stolen.

[26] Martin C. Libicki, *What is Information Warfare?* Center for Advanced Concepts and Technology Institute for National Strategic Studies, National Defense University, August 1995, p. 32.

MCTL DATA SHEET 17.1-4. EMBEDDABLE PROGRAMMABLE CRYPTOGRAPHIC PROCESSOR TECHNOLOGY

An embeddable programmable cryptographic processor is a remotely programmable processor chip that can be embedded in information system hardware to allow information (data) to be encrypted/decrypted wherever it is generated or transformed.

Critical Technology Parameter(s)	All of the following: 1) On-board secure operating system (SOS); 2) The capability to support multiple individual security levels simultaneously; 3) Capable of handling 1,024 or more channels simultaneously; 4) Encrypt and/or decrypt multiple different algorithms simultaneously; 5) Can be initially loaded with one set of cryptographic algorithms and updated with software to include others; 6) Common Criteria for Information Technology Security Evaluation, Evaluation Assurance Level (EAL) protection profile equivalent to data protected; and 7) The unique, empirically validated system engineering and integration (SE&I), user system interface, algorithms and key generators have zero defects.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Software specially designed to perform tests of general purpose and application specific versions of cryptographic functionality and assess the results of these tests. Formal methods for hardware and/or software verification may be required.
Unique Software	Operating systems and application software implementing cryptographic functionality must be specially designed and integrated so that the information systems match and maintain the required assurance level protection profile of the cryptosystem during the operational lifecycles of the systems. The software programs for installing and uninstalling cryptographic algorithms, the secure operating system (SOS) and input/output (I/O) Interfaces built into the very large scale integrated (VLSI) chip that maintains the security of the cryptographic modules, are unique. Unique software cryptographic module security system engineering must comply with the provisions of *Security of Cryptographic Modules*, Federal Information Processing Standard (FIPS) Publication (PUB) 140-2, the requirements of the National Security Agency and maintain consistency with American National Standards Institute (ANSI) standards for symmetric key cryptography.
Major Commercial Applications	This is a dual use item suitable for use in commercial products such as satellite communications, computing, networking and automotive products.
Affordability Issues	Affordability is not an issue. This an easily customized product that has a lower overall cost than a "custom" VSLI chip due to the economies of scale since it can be used in many military and civilian applications. In addition, the life of information system equipment can be extended since premature equipment changes due to algorithm upgrades and keying material changes are not necessary.
Export Control References	WA ML 11; WA Cat 5A2 and 5E2; USML XI and XIII; CCLCat 5A002 and 5E002.

BACKGROUND

Motorola announced the initial operation of its programmable cryptographic engine in a system application on 28 October 1998. The Advanced INFOSEC Machine (AIM™) is a Very Large Scale Integrated Circuit (VLSI) programmable cryptographic processor, which has successfully communicated simultaneously with two Class A USG link encryptors on independent channels. The flexibility and security that the Embedded Cryptographic Processors offer to the communications, networking, banking, government and military sectors has not previously been available before in a single product component.

Before the development of this product, different devices running different algorithms were needed to address the different levels of sensitive information and classified data being encrypted. The AIM processor and similar products are configured in a standard package so that they can be embedded in the actual hardware information system product itself, rather than being contained in an additional "black box" with its own power and space needs. These VLSIs consist of over 9 million transistors, with active power management and can use as little as 35 milliwatts in a handheld radio application.

A Secure Operating System (SOS) is integrated into the Embedded Cryptographic Processors so even the most highly classified algorithms can be loaded with software alone. These VLSIs are capable of handling up to 1,024 channels simultaneously and can encrypt and/or decrypt data using multiple different algorithms. Both general-purpose and application-specific versions are available, which are smaller in size but contain the same SOS in-out (I/O) interfaces and programmability as the original chip for the hand held radio market.

Harris Corporation introduced the *Sierra*™ cryptographic solution on 6 June 2000, which combines the advantages of USG high-grade security with the cost efficiency of a reprogrammable, commercially produced encryption module. Sierra received its NSA Class A certification in June 2002. Sierra can be used to embed up to CC Level 5 [Common Criteria Evaluation Assurance Level (EAL) protection profile] security commercial and military encryption products. Available as a module or a chipset, Sierra can be easily embedded in two-way radios, modems and network cards.

Sierra provides a common security solution to users that have multiple encryption requirements. It can be programmed with a variety of encryption algorithms, including Class A for USG classified traffic, DES and Triple DES for financial and law enforcement users and other commercial algorithms for a wide variety of users. As a software upgradable module, Sierra provides a low cost migration path for future communications upgrades without the logistics and cost burden associated with hardware changes.

The Department of Commerce (DOC) has given a favorable commodity classification for the export of embedded programmable cryptographic processors. The Commodity Control List (CCL 5A992) allows the export of products that incorporate the un-programmed cryptographic platforms without having to invoke strong export controls and can be exported as easily as a cellular phone.

MCTL DATA SHEET 17.1-5. SECURE WIRELESS TECHNOLOGY

Secure wireless technology is the collective term for secure radio frequency communication systems.

Critical Technology Parameter(s)	If this technology is used in a military system, the following arrays of know-how are critical and should be protected: 1) Designed or modified to use cryptographic techniques to generate the spreading code for spread spectrum;[27] 2) the hopping code for frequency agility[28] systems; 3) at least 3072-bit key spaces for Finite Field (Diffie-Hellman (DH) and Digital Signature Algorithm (DSA)) and Rivest, Shamir, Adelman (RSA) systems; 4) at least 256-bit key spaces for Elliptic Curve Cryptographic (ECC) systems; 5) digital signatures (ds) hash value of at least 256 bits; 6) 128-bit AES link encryption using Bluetooth™, IEEE 802.11i data link level encryption and authentication protocols or Multiple Input–Multiple Output (MIMO) 802.11n and 802.16 point-to-multipoint architectures;[29] 7) SHA-256 hash value authentication with a 128-bit symmetric key and a 128-bit message authentication code (MAC);[30] 8) FIPS 140-2 compliant; 9) a fully implemented Public Key Infrastructure (PKI) that is X9.79[31] compliant; 10) The required system and subsystem Common Criteria (CC) Protection Profile (PP) appropriate for the classification level of the facilities, equipment, data and information supported; 11) A secure adapted or tailored wireless subsection with components integrated in militarily weapons systems or operations; and 12) Unique empirically validated systems engineering and integration (SE&I), related techniques and software for the development, production and operational life cycle so that the information systems match and maintain the required Common Criteria Evaluation Assurance Level (EAL) protection profile.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Mobile telephone devices, Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN), Cellular Digital Packet Data (CDPD), Global System for Mobile Communications, (GSM), Mobitex and Ground Positioning Systems (GPS) transceivers, Wireless-G Broadband Routers.

---

[27] Spread spectrum is the name of the technique for spreading energy in a relatively narrow-band over a much wider energy spectrum.

[28] Frequency hopping is the name of a form of "spread spectrum" in which the transmission frequency of a single communication channel is made to change by discrete steps.

[29] Commonly referred to as *WiMAX* or less commonly as *WirelessMAN*™ or the *Air Interface Standard*, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

[30] FIPS PUB 186-2, *Digital Signature Standard*, 27 January 2000 compliant.

[31] ANSI X9.79 *PKI Practices and Policy Framework*, September 2000.

Affordability Issues	Secure wireless products should be affordable, except for the customizing or tailoring that may be necessary weapons systems integration. This technology should become more affordable in future years because future generations of mobile telephone devices and wireless networks will evolve in the demanding, competitive international market place to provide the next (3rd) generation of designs or components for military GPS and mobile and portable tactical command radio communications equipment. There is a potentially expensive requirement to recruit and retain technically qualified personnel worthy of secure wireless system and Class A cryptographic trust and responsibility; and, to operate, manage and support the required end-user training, standardization, test, exercise and evaluation programs required for optimum protocol and system security.
Export Control References	WA ML 11; WA Cat 5A002 and 5E2; USML XI and XIII;[32] CCL Cat 5A002, 5D002 and 5E002.

BACKGROUND

Feature-rich portable and mobile wireless technologies have become increasingly popular and essential for military, business, professional and personal use. They are described as 'wireless' in the news and advertising literature as well as the trade journals and technical literature. NIST uses 'wireless' in the title for the Wireless Network Security.[33]

Wireless technologies use radio transmissions as the means for transmitting data. 'Wireless' in this data sheet includes all: cordless telephones; cell phones; Wireless Wide Area Nets (WWAN); IEEE 802.11b Wireless Local Area Networks (WLAN) or "Wi-Fi" (for wireless fidelity) networks; radio frequency identification (RFID), Cellular Digital Packet Data (CDPD); Global System for Mobile Communications, (GSM); and Mobitex.

This technology data sheet covers commercial, modified commercial and wireless systems developed explicitly or adapted for military use incorporating low probability of detection (LPD) and resistance to jamming as well as localized jamming and denial service attack resistance required of strictly commercial systems.

The major competing wireless technologies for network computing are 802.11b, 802.11g, and Blue Tooth™. All three systems operate in the 2.4 GHz band.[34] These systems are intended for short-range computing and telecommunication applications among low powered devices up to 100 meters apart. The 100 meters is optimistic. The actual effective range is about ¼ of that in most indoor environments. The 802.11b is the most widely distributed and delivers 11 Mbps.

The 802.11g products, which deliver up to 54 Mbps, are gaining market share rapidly. They are significantly faster than the 720 Kbps with current implementations of Bluetooth. The higher rate for the 802.11g comes at the expense of a somewhat shorter range. 802.11a technology operates in the 5 GHz band with 24 channels. The base transfer rate for that is 54 Mbps, but can be increased dramatically by splitting a data stream across two or more channels. The Wi-Fi Alliance plans to begin certifying next-generation Wi-Fi products starting in 2007 before the 802.11n standard is fully complete.

The higher frequency and transfer rates however conspire to make the normal effective indoor range for 802.11a something less than 10 or 15 meters. These technologies can be made secure from an encryption viewpoint, depending on the mobile computing power. However, the communication itself is somewhat vulnerable to disruption by the ubiquitous cordless telephones in urban environments.

---

[32] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

[33] Tom Karygiannis, and Les Owens, *Special Publication 800-48 Wireless Network Security, 802.11, Bluetooth™ and Handheld Devices*, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, November 2002.

[34] Actual frequency/channel allocation varies by country. See http://www.hp.com/rnd/pdfs/country_approvals_matrix520wl.pdf

From a networking perspective, available 802.11b and 802.11g devices generally require a wireless network access point (AP), which is essentially a receiver/transmitter leading back to a wireless local area network (WLAN) server. The server or an intervening router assigns addresses to the wirelessly connected devices, and the server manages the information packet addressing and dispatching for them.

Bluetooth is a more complex standard, with some of the features specified in the Infrared Data Adapter (IrDA) standard[35] that allows unique identification of active devices in the immediate environment. That device identification capability is the basis of ad hoc networking, where each device manages its own information packet traffic. The ad hoc network is defined for a set of devices essentially by configuring them to ignore activity that originates from those not on a list.

The 802.11b and 802.11g can be adapted to ad hoc networking by providing for device identification and the information packet traffic management with additional software layers, though it is not commonly provided in commercial applications. In June 2004, the IEEE ratified the 802.11i security standard calling for the 128-bit encryption AES (Advanced Encryption Standard) technology.

The 802.11x and Bluetooth are competing technologies. Which will ultimately prevail is difficult to predict. The Bluetooth standard offers a richer intrinsic feature set for more complex network applications, but is often not as straightforward in tailored implementations. The 802.11x standards are simpler, but are being enhanced by additional layers of software that can be assembled *a la carte* to meet the same challenges. Both design and development approaches have merit. IEEE 802.11b ad hoc networks may be more immediately useful for multi-hop routing that may be required in some field tactical military networks. Research is currently underway on "*Scatternets*" in Bluetooth, which creates a multi-hop network. The 802.112b work for these applications is currently further along than that with Bluetooth.

Multiple-input multiple-output, or MIMO (pronounced MY-moh), is an abstract mathematical model for some communications systems. In radio communications if multiple antennas are employed, the MIMO model naturally arises. MIMO exploits phenomena such as multipath propagation to increase throughput, or reduce bit error rates, rather than attempting to eliminate effects of multipath. MIMO can also be used in conjunction with OFDM, and it will be part of the IEEE 802.11n High-Throughput standard.

Encryption controls in the Export Administration Regulations (EAR) were expanded several years ago beyond Bluetooth and Home RF to "Wi-Fi" (IEEE 802.11b) consumer products.[36] No review or reporting on products controlled under Category 5 Part II (*Information Security*) is required for encryption products that incorporate short-range wireless encryption functions.

Some interesting radio frequency identification (RFID) uses have proliferated in the past several years:

1. Electronic key-size purchase tags in Arizona that replace conventional credit cards;
2. ID tags for Texas school children that allow local law enforcement officers to monitor their movements; and
3. Medicine containers electronically fitted nationwide to alert authorities to fraud, counterfeiting and even mistakes by hospital staff.

HP is now producing an RFID chip[37] that could be adapted for information security functions like circulation control and identity management. RFID is also covered in MCTL Section 16, Positioning, Navigation and Time Technology.

There is a U.S. exportability issue if radio telephones and laptops contain strong cryptography, although there has been some relaxation in rules concerning portable computers provided that they remain in the personal

---

[35] An Infra Red Data Adapter (IrDA) [specification 1.1] plugged into a desktop PC USB [specification 1.1] enables wireless data transfer between the Desktop PC and IrDA enabled peripheral devices such as a portable computer, PDA, Digital Camera, Handy Scanner and Printer, and for File Sharing, Photo Transfer, Printing, data exchange, and synchronization.

[36] Operating range exceeding 100 meters.

[37] http://biz.yahoo.com/bw/060717/20060716005035.html?.v=1

possession of a U.S. traveler and are returned to the United States with the traveler. The Wassenaar Arrangement[38] (WA) contains special provisions that similarly relax the export restrictions on Ground System Mobile (GSM) portable telephones. The GSM relaxation was a commercial necessity in Europe, where distances and travel times can be short.

[38] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

MCTL DATA SHEET 17.1-6. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a form of cryptography that exploits quantum theory, in particular the uncertainty principle—which states that it is impossible to measure all aspects of an object with absolute certainty.[39]

Critical Technology Parameter(s)	Any of the following: 1) Protocols, operating systems and application software implementing the quantum cryptographic functionality that have undergone extensive open peer review and no feasible attacks been found; 2) real-time quantum encryption key generation and distribution over optical fiber links > 80 Km or through the earth's atmosphere to space vehicles in 90 min orbit and beyond; 3) reliably transmit information through a noisy quantum channel; 4) exploit the high repetition rates of homodyne detection to overcome the limitation in detection rate that is typical for single-photon counting at standard telecom wavelengths; 5) robustly transmits an arbitrary two-level quantum state in a type of decoherence-free subspace;[40] 6) Quantum keys with a sifted key rate of less than 50 kbit/s and a quantum bit error rate between 3% and 5% when unattended;[41] or 7) the required nonorthogonal states are generated in a single nonlinear crystal.[42]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Operating systems and application software implementing quantum cryptographic functionality that is the product of unique empirically validated systems engineering and integration (SE&I), related techniques and software for the development, production and operational life cycle so that the information systems match and maintain the required Common Criteria Evaluation Assurance Level (EAL) protection profile of the cryptosystem during the operational lifecycles of the information systems the cryptosystem protects. The unique, empirically validated SE&I, protocols, user system interfaces, algorithms and key generators that have 'zero defects.' Cryptographic module security that complies with the provisions of Security of Cryptographic Modules, Federal Information Processing Standard (FIPS) Publication (PUB) 140-2, the requirements of the National Security Agency and is consistent with American National Standards Institute (ANSI) standards for cryptography.
Major Commercial Applications	Key management for financial service system transactions, however in the near term drivers that will be most important are the USG funded satellite control and communications system applications.

[39] Simon Singh, *The Code Book*, Doubleday, New York, 1999, p. 384.

[40] Experimental fault-tolerant quantum cryptography in a decoherence-free subspace, Qiang Zhang,1,2 Juan Yin,1 Teng-Yun Chen,1 Shan Lu,1 Jun Zhang,1 Xiao-Qiang Li,1 Tao Yang,1 Xiang-Bin Wang,3 and Jian-Wei Pan1,2, *PHYSICAL REVIEW*, A 73, 020301 R, 2006.

[41] Henning Weier1,2, Tobias Schmitt-Manderbach1,2, Nadja Regner1, Christian Kurtsiefer3,and HaraldWeinfurter1,2, 1 Ludwig-Maximilians-Universit¨at, 80799 München, Germany, 2 Max-Planck-Insititut fur Quantenoptik, 85748 Garching, Germany, 3 National University of Singapore, Singapore, Published online 4 August 2006.

[42] Practical Implementation of Multilevel Quantum Cryptography, S. P. Kulik a*, G. A. Maslennikov, b , and E. V. Moreva c, a Moscow State University, Moscow, 119992 Russia, b National University of Singapore, Singapore, 119077, c Moscow Engineering Physics Institute (State University), Moscow, 115409 Russia, *e-mail: skulik@qopt.phys.msu.su, Atoms, Molecules, Optics, Received 14 October 2005, PACS numbers: 03.67.Hk, 42.25.Ja, 42.50.Dv, DOI: 10.1134/S1063776106050037.

Affordability Issues	Customized quantum cryptography applications and features and the extensive unique empirically validated SE&I experience, related techniques and software for the development, production and operational life cycle of quantum products.
Export Control References	WA ML 11; WA Cat 5A2 and 5E2; USML XI and XIII;[43] CCL 5A002.a.9 and 5E002.

BACKGROUND

The only commercial quantum QC applications offered at the present time are key distribution systems, for which a comparatively short, unbroken line of sight or an unbroken fiber is a basic prerequisite.

Charles H. Bennett, a fellow at IBM's Thomas J. Watson Research Center, and Gilles Brassard, a researcher at the University of Montreal in Canada, first devised quantum cryptography in 1984 as a part of their study of the relationship between physics and information. They were not searching for a new cryptographic method, but simply applying some of the basic principles of quantum mechanics to real-world uses. What they found was that quantum mechanics are ideally suited for cryptographic key management because of the 'one-way-ness' of photons.[44] Their approach, BB84 (for **B**ennett, **B**rassard, **1984**), is the oldest quantum-encryption scheme and has exhibited some weaknesses attributable to the limitations of the existing technology in 1984.

The technology has advanced since 1984 and key distribution quantum cryptography has now reached the point that it is clearly beginning to cross over into the technology phase with companies in at least four countries producing commercial quantum key distribution cryptographic products that are, or soon will be, on the market.

The first significant communications application proposed using the quantum effect was quantum key distribution (QKD), which solves the problem of communicating a shared cryptographic key between two parties with complete security. Quantum key distribution can, in theory, make it impossible for the adversary to intercept the key communication without revealing her/his presence. The security of QKD relies on the physical effects that occur when photons are measured, and the security of the users' protocols, software and hardware. Properly implemented, QKD provides keys that can be used either as a one-time pad, or as a key for conventional cryptographic algorithms.

Most of the current quantum cryptography systems are relatively simple. The sender randomly polarizes a stream of photons and transmits them to the recipient, who has special receiving equipment that can count and determine the polarization of individual photons on arrival. Once the recipient has enough photons and has determined their polarization, s/he can then tell the sender out of band which photons s/he received. With that information, the sender can encrypt a message and send it over conventional media. In addition to polarization-based schemes, other quantum cryptographic systems have been devised to exploit different physical properties, but most of these have not moved beyond the laboratory stage.

[43] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

[44] Edmund X. DeJesus, Quantum Leap, *Information Security,* August 2001, p. 72.

MCTL DATA SHEET 17.1-7. SECURE HASH FUNCTION TECHNOLOGY

A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values.[45]

Critical Technology Parameter(s)	All of the following: 1) Undergone extensive open peer review and no attacks found that allow faster plaintext recovery than an exhaustive key search; 2) at least a 160-bit digest size; and 3) fully compliant with FIPS 180-2 and ANSI X9.30.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	High performance computers, operating systems and application software specially designed to perform Randomness, Correlation, Weak Key and Symmetry Under Complementation tests to evaluate the strength of new symmetric encryption hash algorithms during development, test and evaluation.
Unique Software	Operating systems and application software implementing cryptographic hash functionality specially designed and integrated so that the information systems match and maintain the Common Criteria Evaluation Assurance Level (EAL) protection profile requirements for the systems during their operational lifecycles. Cryptographic module security complies with the provisions of Security of Cryptographic Modules, Federal Information Processing Standard (FIPS) Publication (PUB) 140-2, the requirements of the National Security Agency and consistent with American National Standards Institute (ANSI) standards for symmetric key cryptography.
Major Commercial Applications	Commercial cryptographic applications for the financial service industry, and Internet electronic commerce and business network applications have been the principal open source drivers for commercial cryptographic technologies in recent years.
Affordability Issues	Military criticality, not affordability, is the principal military acquisition issue for secure hash technology.
Export Control References	WA ML 11; WA Cat 5E2; USML XI and XIII;[46] CCL 5E002.

BACKGROUND

Cryptographic primitives, and therefore cryptographic systems, have a natural taxonomy resulting from the key(s) used by the fundamental primitive(s). Under this taxonomy concept, there are three basic classes of cryptography:

- *One-key* or secret key (also called symmetric-key cryptography);
- *Two-key* or public key (also called asymmetric-key cryptography); and
- *No-key* cryptography, the most visible of which are cryptographic hash functions.

Secret-key cryptography is much faster than public-key cryptography. Hybrid (or mixed) systems use both types of cryptographic keys. Hybrid systems exploit the strengths of each. No-key cryptographic hash functions, which are irreversible algorithms, are widely used forms of cryptography for modification detection [modification detection code (MDC)]. Specific applications include virus protection and software distribution as well as data integrity.

Cryptography is a combination of two basic components: an algorithm (or cryptographic methodology) and a key. Algorithms are complex mathematical formulae, and, in the digital age, keys are strings of bits. A

[45] A. J. Menezes, P. C. van Oorschot, S. A.Vanstone, *Handbook of Applied Cryptography*, CRC Press, NY, 1997, p. 33.

[46] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

cryptographic algorithm, also called a cipher, is a mathematical function used for encryption and decryption. Generally, two related algorithms are required: one for encryption and the other for decryption. Keys may be any of a large number of binary values. The set of possible values of the key is called the keyspace.

For secret-key cryptography, only one key is used in the nodes on both ends. The same key is used to encrypt plaintext and decrypt ciphertext. While secret-key cryptography is generally not as mathematically elegant as public-key methods, it should certainly do the required job for most systems—as it has for years. The power of symmetric-keyed cryptography is that for each added bit the key space is twice as large, so a brute force attack takes twice as long. In addition, secret-key cryptography is far more efficient than public key. The primary drawback to secret-key cryptography is the necessity to agree on a key. Another drawback is that secret-key cryptography does not provide for digital signatures.

No-key cryptographic hash functions are widely used forms of cryptography used in combination with both symmetric and asymmetric cryptography to provide proof of data integrity. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

Each hash algorithm can be described in two stages: 1) preprocessing, and 2) hash computation. Preprocessing involves padding[47] the message, parsing the padded message into m-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a message schedule from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final value generated by the hash computation is used to determine the message digest.

The five algorithms specified in FIPS 180-2 differ most significantly in the number of bits of security that are provided for the data being hashed—this is directly related to the message digest length. When a secure hash algorithm is used in conjunction with another algorithm, there may be requirements specified elsewhere that require the use of a secure hash algorithm with a certain number of bits of security. For example, if a message is being signed with a digital signature algorithm that provides 128 bits of security, then that signature algorithm may require the use of a secure hash algorithm that also provides 128 bits of security (e.g., SHA-256).

Additionally, all five algorithms differ in terms of the size of the blocks and words of data that are used during hashing. Table 17.1-2 presents the basic properties of all five secure hash algorithms.

Table 17.1-2. Secure Hash Algorithm Properties
[Source: 180-2 (+ Change Notice to include SHA-224), 2002 August]

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)	Security Level (bits)	NIST Expiry
SHA-1	$< 2^{64}$	512	32	160	80*	2010*
SHA-224	$< 2^{64}$	512	32	224	112	2030
SHA-256	$< 2^{64}$	512	32	256	128	2031+
SHA-384	$< 2^{128}$	1024	64	348	192	2031+
SHA-512	$< 2^{128}$	1024	64	512	156	2031+

* Note: At Crypto 2005, a paper was presented which showed an attack which took less than 2^{80} calculations to find a collision by the user calling the hash function. Further results were presented at the NIST Hash Workshop in November. This result is still being assessed as to its impact.

[47] A bit or string of bits appended to a message in order to cause the message to contain an even multiple of the number of bits required by the cryptographic algorithm or for filtering.

SECTION 17.2—IDENTITY MANAGEMENT TECHNOLOGY

Highlights

- The universal requirement to control access to: sensitive facilities; information processing equipment and data require the establishment of identity.
- The reason for using identity management security technology is to provide enhanced security and to reduce espionage, fraud and identity theft.
- Smart card applications are increasingly used to replace passwords for logical access to sensitive facilities, equipment, and data; in identification and circulation control systems; and for digital signatures.
- Proper use of emerging secure biometric identity management automatic (computer-assisted) identification system technology with accurate enrollment can significantly improve identity management and reduce the national security and business risks associated with fraud and identity theft.
- National Strategy for Homeland Security describes biometrics as one of the eleven major security initiatives: "Apply biometric technology to identification devices."[48]
- On-board biometric identity management smart card processor and storage size limits the functions that can be performed by a secure biometric identity management system and can be a system performance limiting factor for those systems in which all functionality must be on the card.
- There are no complete set of established national and international standards specifying scales for the objective numeric measurement of biometrics, with which to make objective comparisons between biometric technologies, products or systems.
- Biometric technologies and techniques are not perfect and in some cases can occasionally be spoofed, defeated or circumvented.
- Biometric identity system errors can and sometimes do occur. Probable False Reject Rates (FRRs) and probable False Accept Rates (FAR) in biometric systems are never zero.
- Performance, cost, error rates and ease of use are usually the main driving factors in the choice of a biometric system.
- The biggest security risks to secure biometric identity management systems are the integrity of the enrollment process and system management.
- Accurate costs for secure biometric identity management systems are difficult to derive.

OVERVIEW

This section concentrates on selected militarily critical technologies required for the development, production and use of secure identity management systems: biometrics, smart cards, and system engineering and integration considerations.

Identity Management has developed several interpretations in the IT industry and is now associated as the management of a user's credentials and how they might log onto an online system. However, this view is quite narrow. The focus on identity management goes back to the development of directories such as X.500 where a namespace is used to hold named objects that represent real life "identified" entities such as countries, organizations, applications, subscribers and devices. X.509 defined certificates that carried identity attributes as two directory names, the certificate subject and the certificate issuer. X.509 certificates and PKI systems were used to prove one's

[48] *National Strategy for Homeland Security*, Office of Homeland Security, Washington, DC, July 2002, p. xi.

online “identity.” Therefore, identity management is more generally considered as the management of information (as held in a directory), which represents real life identified items (users, devices, services, etc.). Engineering such systems means that explicit information and identity engineering tasks become necessary.

The identity management technologies are relevant to essentially all the technologies in the Information Security Section, in that the more sensitive aspects of these items require at least some protection during their development and in the production and use of information security systems and articles of intrinsic military utility. The identity management technologies are also relevant to all of the Information Systems technologies (MCTL Section 10) that incorporate mandatory access controls. Finally, in a sense, identity management technologies are related to all of the militarily critical technologies because, there has always been a basic military information security requirement for identity management of friend and foe.

The heart of a secure biometric identity management system is the biometric data, which is derived from a human being and must be processed by a trusted biometric identity management system to verify claimed identity (authentication) or discover true- identity (identification).

A biometric is a scale of suitable length and granularity for measuring and objectively specifying the parameters of a human physiological characteristic or personal behavioral trait that can be used to securely identify, or verify, the claimed identity of an enrollee accredited in a secure biometric identity management system.

Foreign cooperation, and even collaboration, is becoming increasingly important in the timely development and maintenance of national and international standards. The open scientific method of peer review in the development of standards brings any technology to maturity more quickly and the United States befits from international comments and criticisms in the standards development process. Perhaps the best opportunity for the United States to benefit from international cooperation is through participation in the development of biometric standards, many of which are still in the earliest stages of development.

BACKGROUND

Many parts of the anatomy, personal characteristics and imaging methods have been suggested for biometrics. A few personal characteristics have been used successfully with various techniques and have legacies of many years. Some, such as facial recognition and fingerprints are ancient.

The more recent idea of using iris patterns for personal identification was originally proposed in 1936 by an ophthalmologist, Frank Burch. However, no important development work was done on this technology until 1994. Dr. John Daugman of the University of Cambridge, who was a student at MIT when he developed the IrisCode algorithms for encoding and recognizing iris patterns, first described them in (Daugman 1993–1994). The *Daugman* algorithms have since been used in the executable software in all commercial iris recognition systems. Both personal identification concepts and advanced computer science were required for biometric identity management systems to emerge. Biometric technologies such as the automatic fingerprint identification systems (AFIS) have been developed since the advent of the computer. Many biometric systems are still in the experimental phase.

Pioneering biometric methodologies have also included hand geometry, among others. In the late 1960s the Miller brothers of New Jersey executed the original hand reader concept in the form of a mechanical device. It featured a platen with finger groves upon which the user placed his hand while rods were moved in the groves to meet the fingertips. The other end of the rods corresponded with a predetermined pattern on a card, which either matched or did not match. Refinements of this idea were produced in a more advanced electronic version utilizing scanned photocells and magnetic cards, which were produced and marketed as a commercial product in the early 1970s by the Identimation Company. After financial difficulty, the rights to the product were passed to Identimat, Inc., which developed the product further for applications in the nuclear industry and academia. Identimat was absorbed by a larger group, which continued to develop and market variations on the original design until production finally ceased in 1987.

In May 1985 David Sidlauskas formed Recognition Systems, Inc., to further develop these ideas and the ID3D-S® hand geometry reader was born. The ID3D was tested and approved by Sandia National Laboratories in late 1985. The Sandia approval lead to sales in the government sector, leading to further development and marketing in the ID3D-U series of readers. These early devices relied on contemporary closed circuit TV (CCTV) optics, which kept costs relatively high. Texas Instruments refined and simplified the design resulting in the ID3D HandKey®

introduced in early 1991 and became a significant milestone in the fledgling biometric identity management industry. The ID3D system was very successful and continues to be marketed today.

Secure biometric identity management system technologies are moving very rapidly, driven primarily by:

1. The requirements of the electronic banking and other commercial Internet interests in the reduction of financial fraud;
2. Nation states' interest in the reduction of identity fraud; and
3. A third, and perhaps less demanding driver because of the usual funding difficulties, are the requirements of government and military sectors for a capability to control access to sensitive facilities, equipment, information and data.

The rate of change in identity management technologies is far outpacing the development of the national and international standards required for interoperability.

International Civil Aviation Organization (ICAO) specifies the form and contents of machine-readable travel documents (MRTD). Historically, ICAO has not made recommendations on the specific security features to be incorporated in travel documents. Each issuing nation State incorporates the safeguards it deems appropriate to protect its national documents against counterfeiting, forgery, and other forms of attack, with the proviso that nothing is to be included which would adversely affect their optical character reader (OCR) machine-readability.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.2. IDENTITY MANAGEMENT TECHNOLOGY

MCTL DATA SHEET 17.2-1. BIOMETRIC TECHNOLOGY

Biometric Technology is a human physiological characteristic or personal behavioral trait, which can be measured with a scale of suitable length and granularity, to objectively specify the parameters required to identify, or verify the claimed identity of, an enrollee accredited in a biometric identity management system.

Critical Technology Parameter(s)	Any of the following: 1) Two of any fingerprint scans in compliance with the FBI standard Wavelet Scalar Quantization (WSQ); 2) fingerprint readers that can provide "proof-of-life;" 3) Iris pattern digital camera subsystems; 4) transmission (or signal processing) system segments in compliance with the BioAPI[49] open-systems standard, the CBEFF;[50] XCBF[51] and ANSI X9.84, including Normative X9.82 References; 5) meets biometric system and subsystem Common Criteria (CC) Protection Profile (PP) requirements appropriate for the classification level of the facility, equipment, data and information for which the secure biometric system controls access in accordance with DoD and Federal Biometric System Protection Profile for Medium Robustness Environments.[52]
Critical Materials	None identified.
Unique Software	It is all proprietary.
Unique Test, Production, Inspection Equipment	1. UK Biometrics Working Group, Best Practices in Testing and Reporting Performance, 2000 http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf 2. FVC2002, and FVC2000, International Fingerprint Verification Algorithms Competition, http://www.bias.csr.unibo.it/fvc2002/, 2002. 3. FVRT2000, NIST Facial Recognition Vendor Test, http://www.frvt.org/FRVT2002/documents.htm, 2000. 4. IBG, Comparative Biometric Testing http://www.biometricgroup.com/index. htm, 2004.
Major Commercial Applications	Financial service industries and governments have been the driver. Other users include: transportation; manufacturing and distribution; education; health care, and preferred traveler's cards.
Affordability Issues	Affordability of secure biometric identity management system technologies and products should be an increasingly smaller issue over time, since rapid adoption in the civilian market place has created a competitive environment with improving products, which are becoming widely available at lower and prices.
Export Control References	None identified.

BACKGROUND

Although there are many definitions, currently the biometric community considers biometric technology to be the measurement of biological features that distinguish one person from all other persons; that is, "recognize" the

---

[49] American National Standards Institute (ANSI), InterNational Committee for Information Technology Standards (INCITS), ANSI INCITS 358-2002, *The BioAPI Specification*, Version 1.1, 22 March 2002.

[50] Common Biometric Exchange File Format, NISTIR 6529-A.

[51] XCBF is the XML Common Biometric Format. XML is a metalanguage, written in SGML, used for the interchange of documents on the World Wide Web. SGML is a standardized markup language for describing the logical structure of a computer document.

[52] Version 0.02, 2 March 2002.

person. Usually either physiological or behavioral characteristics can be used and, multiple characteristics can be used.

There were six leading biometrics judged best suited to military applications. The six are shown in Table 17.2-1.

1. Fingerprint Analysis;
2. Facial Features;
3. Hand Geometry;
4. Iris Recognition;
5. Speaker Recognition; and
6. Signature Recognition.

The science and technologies on which these six biometric systems are based are maturing rapidly. These six systems are already in wide commercial use and have a significant international market share. Biometric technologies are one of the enablers for secure biometric identity systems, not the end products.

Many parts of the anatomy, personal characteristics and imaging methods have been suggested. Some have been used successfully with techniques and technologies that have legacies of many years. An exhaustive biometric candidate list should include, among others: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits, odors, deoxyribonucleic acid (DNA) and head resonance.

However, the selection of candidates suitable for military application becomes easier when evaluated in terms of the criteria developed by the National Biometric Test Center (NBTC)[53] which used five criteria in the selection of biometrics suitable for identity management:

1. Robustness;
2. Distinctiveness;
3. Accessibility;
4. Acceptability; and
5. Availability.

Robust means repeatable and not subject to large changes. A biometric is *distinctive* if wide differences exist in the pattern(s) among the population. By *accessible*, they mean easily presented to an imaging sensor. *Acceptable* refers to the acceptability of the measurement technique to the users: usually those sensors perceived as non-intrusive are the most acceptable. *Availability* refers to the number of independent measures that can be presented by each user; that is, two iris patterns, or ten fingerprints.

Eight biometric systems were excluded from consideration in this data sheet since they are either still under scientific investigation or not in wide commercial use due to various factors that affect the identification accuracy, which are difficult to control. The eight excluded potential candidates are:

1. Keystroke dynamics;
2. Vein pattern;
3. Retinal pattern;
4. Facial thermograms;
5. DNA;
6. Gait;
7. Ear biometric techniques; and

[53] http://www.ece.unh.edu/biometric/biomet/_public_docs/nbtccw_TEST.pdf

8. Body odor.

These eight seem to be poorly suited to general use in military systems. In most cases the technologies are still; experimental; considered too intrusive; have large inherent error rates; or, like the biometrics used for a polygraph, are too complex, require elaborate data-capture facilities and equipment and highly-skilled, specially trained operators.

Five biometric characteristics and one behavioral characteristic (voice) were selected for this data sheet:

1. Fingerprint;
2. Facial Features;
3. Hand Geometry;
4. Iris Recognition;
5. Voice Recognition; and
6. Signature Recognition.

According to NBTC[54] in 2000, these six biometric traits were selected because they have been in use for many years and enjoy the top six positions in biometric systems commercial market share. The National Biometric Test Center closed its doors to enable Department of Defense (DoD) to consolidate the resources and funding.

An outline of the characteristics of these six selected biometrics and their 2006 international market share are shown in Table 17.2-1, *Biometric System Comparative Description.*

There are no suitable scales for the objective, numeric measurement of biometric characteristics, with which objective comparisons between biometrics can be made.

Note that only fingerprint systems and iris recognition systems are considered *very strong*. Very strong means comparatively *low* error rates and *limited* consequences from probable damage or compromise of data. Most biometric systems can be used for facility and equipment access control. Speaker recognition and signature recognition are not generally considered suitable for one-to-many identification systems with large populations.

[54] The National Biometric Test Center previously located at San Jose State University's Biometric Identification Research Institute is no longer an active test center.

Table 17.2-1. Biometrics Characteristic Comparative Description

	BIOMETRIC SYSTEM					
CHARACTERISTIC	**Fingerprint Systems**	**Facial Features**	**Hand Geometry**	**Iris Recognition**	**Voice Recognition**	**Signature Recognition**
Description	**Fingerprint analysis is the comparison of an enrolled template of the fingerprint pattern on an individual's fingertips, which have been entered by an enrolled individual for authentication and identification functions. May have up to 40 variables. Highly distinctive but not very robust since the fingerprints can be easily damaged.**	**Translates the characteristics of a face into a unique set of numbers for each individual. An eigenface algorithm maps the characteristics of a person's face into a multi-dimensional face space. This is the only biometric system that can be used passively. 3-D facial recognition differs in acuity, accuracy, speed, cost and versatility from 2-D facial recognition**	**Hand geometry systems take a physical hand biometric input by measuring various shape features of the hand and analyzing them. Less distinctive than fingerprints but more robust.**	**Iris authentication and identification systems analyze the iris features that surround the pupil. Requires no contact, only user cooperation. May have up to 250 variables. Robust and quite distinctive.**	**The two components are an Acoustic Channel and a Speaker Recognizer. The Speaker Recognizer consists of the acoustic processor and a speaker decoder. Not intrusive, but not very robust.**	**Signature verification systems analyze a written signature or other signed symbols for comparison with the authentic signature G10 template of an enrolled individual. Not very distinctive or robust**
2006 Market Share[55]	**44%**	**19%**	**9%**	**7%**	**4%**	**2%**
Strengths	**Very strong identification capabilities. Uniqueness of every fingerprint. No two alike have ever been found.**	**Strong identification capabilities. Non-invasive. Can be used surreptitiously.**	**Not as strong as fingerprint analysis systems. People's hands are more similar to others than their fingerprints.**	**Very strong identification capabilities. Can be more accurate than fingerprints. Uniqueness of every iris, which does not change with age.**	**Not suitable for identificatio n usage.**	**Not suitable for identification usage.**
Applications	**Facility and equipment access control in sensitive facilities and law enforcement applications.**	**Facility and equipment access control, circulation control in sensitive facilities, passenger and terrorist recognition at public places and events, casino surveillance.**	**Facility access and circulation control in sensitive facilities.**	**Facility and equipment access control in sensitive facilities, customer verification at ATMs and fraud reduction in the financial service industry.**	**Facility and equipment access control in sensitive facilities: still not secure enough to rely upon as a stand-alone biometric**	**Authenticating financial service transactions and fraud reduction in the financial service industry and legal transactions.**

Fingerprint Systems

Fingerprint images are acquired from live-scan fingerprint readers that scan the fingerprint directly from the subject's fingers. The scanned images are then processed to extract specific types of features that can be compared against a master file containing features extracted from previous images.

In Automated Fingerprint Identification Systems (AFIS), when the scanned fingerprint matches a master file image, a positive identification is reported. The Federal Bureau of Investigation (FBI) and the National Institute of

[55] Biometric Market Report 2000–2007, Biometric Group, http://www.biometricgroup.com/reports/public/market_report.html September 2003.

Standards and Technology (NIST) have established standards for fingerprint scanner image quality.[56] There may not be a perfect match, in which case an adjustable logic declares a match if the scanned fingerprint matches within the preset acceptable tolerance.

The fingerprints of every individual are unique. No two have ever been found that were identical. Even identical twins have distinct fingerprints. Fingerprint systems are the oldest biometric and considered the most effective identification biometric by most writers, however the emerging iris technology seems to be more accurate. The privacy risks associated with this biometric are rated "High" by the International Biometric Group (IBG).[57]

Facial Recognition

Sources used for the electronic capture of a subject's facial image (mug shot) include still and video cameras and other types of video recorders that capture images and produce digital image files directly from the subject's head and body. Scanners are used to digitize images from photographs, pictures, or sketches. The digital representations of these images consist of grayscale or color pixels depending on the application and equipment. These digital images may be stored, in a compressed or uncompressed from in an image storage and retrieval (ISR) system.

Textual descriptive data, and other information, is stored with each image. When required, specific images stored on a master file can be retrieved from the ISR and be incorporated as part of an electronic facial 'mug shot' book, or an electronic line-up. The privacy risks associated with this biometric are rated "High" by the IBG.

Hand Geometry

In hand geometry-based authentication systems, three-dimensional profiles of the hand are sensed. Finger lengths are relatively invariant and peculiar, although not unique, to each individual. The image acquisition system requires cooperation of the subject and captures frontal and side view images of the palm flatly placed on a panel with outstretched fingers.

The representational requirements of the hand are comparatively small (9 bytes), which is an attractive feature for bandwidth and memory limited systems. Since the hand geometry is not unique, these systems cannot be scaled up to provide identification of an individual in a large population of identities. In spite of this limitation, hand geometry has become a very popular access control biometric system for small domains and has captured almost half of the physical access control market.

Finger Geometry

Finger geometry is a variant of hand geometry and is a relatively new technology which relies on the geometrical invariants of the index and middle fingers. It is claimed to be more accurate than hand geometry, although it is not as mature as that of hand geometry. The privacy risk associated with both the hand and the finger biometric have been rated "Low."[58] Basic functionality of these technologies ensures that there are few, if any, privacy issues.

Iris Recognition

Iris recognition is now generally considered the most accurate, scalable and cost-effective authentication solution. It is also a robust biometric. Britain's National Physical Laboratory published a study that shows iris recognition technology decisively outperformed six other biometrics systems (facial recognition, fingerprint, hand geometry, vein and voice recognition) on accuracy and throughput (or processing) speed of the matching algorithms.[59] The evaluation measured each biometric technology's ability to positively identify users. The privacy risks associated with this biometric are rated "High" by the IBG.

---

[56] *Minimum Image Quality Requirements for Live Scan, Electronically Produced Fingerprint Cards*, FBI/NIST Appendix F/G, IAFIS-IC-0010(V2), December 1995.

[57] International Biometric Group, *BioPrivacy Initiative*, http://www.bioprivacy.org/index.htm, 2003.

[58] International Biometric Group, *BioPrivacy Initiative*, http://www.bioprivacy.org/index.htm, 2003.

[59] Tony Mansfield, and Marek Rejman-Green, *Feasibility Study on the Use of Biometrics in Entitlement Schemes*, National Physical Laboratory, February 2003.

Voice Recognition

Voice capture is unobtrusive and voiceprint is an acceptable biometric in almost all societies. Some applications entail authentication of identity over the telephone. The privacy risks associated with this biometric are rated “Medium” by the IBG. The basic functionality of the technology ensures that there are few, if any, privacy issues.

Signature Recognition

Dynamic signature verification can be the least expensive of the six biometrics considered in this item, but Voice verification can be even less expensive, depending on the implementation. The accuracy of this biometric is generally considered inferior to that of fingerprint scan and iris scan biometrics. The IBG rates privacy risks associated with signature biometrics “Low.”

MCTL DATA SHEET 17.2-2. SMART CARD TECHNOLOGY

A smart card, chip card, or integrated circuit(s) card (ICC), is defined as any pocket-sized card with embedded integrated circuits.

Critical Technology Parameter(s)	All of the following: 1) A secure multi-function card: 2) with an imbedded 16-bit on-board processor; 3) 128 kilobytes of imbedded data storage; 4) On-board template and scan match processing algorithms; 5) An on-board crypto module supporting 128-bit AES symmetric key and either 1024-bit RSA or DSA/DH asymmetric keys, or 161-bit elliptic curve ECDSA/ECDH keys, and an ANSI approved cryptographic hash function or SHA-2 hash; 6) USG Smart Card Interoperability Specification[60] compliant; and 7) Tamper resistant cards and associated secure card fabrication and initialization equipment that are ISO 7810 and 7816 or 14443 compliant.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Application software for COTS secure biometric identity management systems is proprietary. The operating systems are either proprietary commercial operating systems, such as IBM's S390/MVS, Mondex's Multos, Sun Mircosystem's Java Card™, the Mac O/S, or quasi-open systems such as Compaq Open VMS and Linux, which are used to provide cross-platform multi-vendor database synchronization.
Major Commercial Applications	Widespread commercial use, especially in Europe by various financial, telephone and cellular service industries has been the driver. The current commercial base for smart cards is in government and regulated commercial industries such as: transportation; banking and financial service; manufacturing and distribution; education; and health care.
Affordability Issues	Smart cards are comparatively inexpensive components of information security systems. The affordability issues result from comparison with the other system component and utilization costs and convenience factors.
Export Control References	There are no export controls on smart cards. If smart cards are loaded with cryptography, then they will fall under the normal cryptographic export controls: WA ML 11; WA Cat 5E; USML XI and XIII;[61] CCL Cat 5E.

BACKGROUND

In most technical references, the collective term integrated circuit card or (ICC) card covers:

1. *Smart cards*, featuring embedded complementary metal oxide semi-conductor (CMOS) micro-controllers and memory chips;
2. *Memory* or *dumb cards*, featuring embedded electronically erasable programmable read-only memory [considered software] (EEPROM) chips; and
3. Both *contact* and *contactless* (or *proximity* cards). Contact smart cards must conform to ISO 7816. Contact cards are easily identified by their standard metallic contact pads. Contactless smart cards, which must be in conformance with ISO 14443 (Type A or B), do not have power cells but have imbedded loop antennas, usually on the back. Contactless cards communicate with this imbedded loop antenna by radio frequency

[60] Government Smart Card Interoperability Specification (GSC-IS), Vol. 2.1, NIST, http://smartcard.nist.gov, 16 July 2003.

[61] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

(RF) modulation. Contactless cards are energized by insertion into the electromagnetic field produced by the transceivers.

Any of many existing bar codes, magnetic-stripes and proximity-card access features that may be required can be integrated within the same multifunction smart card.

The card format is preferred for military service over tags and other tokens because it provides a convenient and versatile platform that can house an RF antenna, and because chip cards are the highest-volume semiconductor card products manufactured worldwide.

The second type of card is called the "smart card" in which a microprocessor (typically 8, 16 or 32 bits) is embedded in the card as well as a magnetic memory of up to 128,000 bytes. There are also optical memory cards that can store up to four megabytes of data. These are the types used in most secure biometric identity management systems. True smart cards have the ability to make decisions about the data stored on the card and are not dependent on the unit to which they are submitted to make the applications work. The true smart card can also be a multifunction card.

There are two versions of the ICC card: 1) the contact version; and, 2) a contactless version. As the name suggests, the contactless card system passes the data between the card and the reader without any physical contact. The advantages of the contactless systems are their performance, reliability, and memory, security and, of course, there are no contacts to wear out, but the card and readers are more sophisticated and therefore more expensive.

The contacts on contact cards can be expected to last through the limited lifetime of the credential in most systems. For optimum operational security and accuracy, a biometric card must be updated every three to five years anyway because the templates must be updated to maintain template fidelity otherwise the normal human physiological changes will reduce the accuracy and efficiency of the system.

The goal of the DoD Common Access Card (CAC) program is to ultimately procure approximately 4.3 million cards and have them in the hands of U.S. military personnel, civilian DoD employees and on-site contractors. The CAC is used for strong physical and logical access control, to be used for everything from shared workstations to commissary access. By the end of April 2004, DoD had the largest U.S. deployment of open, multiapplication smart cards to date. These cards are part of a public key infrastructure (PKI) and are to be used for identification, electronic transactions, secure messages and digital signatures.

The GSA CAC procurement[62] calls out ISO 7816 and ISO 14443 as well as compliance with Federal Information Processing Standards. The chips on the CAC smart cards each have 32 kilobytes of memory and use the Java open-card standard, Java Card®, operating system under the federal government's interoperability specification. This specification allows multiple vendors to provide the cards, readers and middleware for about $10 less per user than for the previously used PKI-only cards, which ran about $50 each. The CAC smart cards will cost the government about $8 each.[63] The CAC incorporates bar codes and a magnetic stripe. More than 900 sites worldwide will issue the cards.[64]

The U.S. *Government Smart Card Interoperability Specificatio*n (GSC-IS) provides solutions to a number of the interoperability problems associated with smart card technology, laying the foundation for the development and deployment of large-scale interoperable smart card technology identity management systems across federal agencies.[65] Smart card operating system programs are usually hard coded into the logic of the smart card integrated circuits during the manufacturing process and cannot be changed after fabrication. ISO 7816-4 defines a hierarchical file system structure for smart cards. Cards that are ISO-7816-4 compliant are known as "file system" cards.

ISO 7816-4 also specifies a standard smart card communications protocol for the Application Protocol Data Units (APDUs) that are exchanged between smart cards and host computers. This APDU-based interface is referred

---

62 U.S. General Services Administration, Smart Card Handbook, http://www.estrategy.gov/information/smartcardhandbook.pdf 2004.

63 Associated Press, "Troops Add 'Smart Cards' to Arsenal," *The Washington Times*, 30 October 2001, p. A4.

64 Eugene A. DeMaitre, "Military Pioneers the Use of Multifunction Smart ID Cards," *COMPUTERWORLD*, 3 June 2002, p. 29.

65 *Government Smart Card Interoperability Specification*, Version 2.1, NIST, 16 July 2003.

to as the "*card edge*." In recent years, developers have incorporated chips in which the executable programs on smart cards can be loaded after the cards have been manufactured such as JavaCard™ Virtual Machine (VM).

Due to the widespread adoption of the JavaCard™ VM specification, the term "*virtual machine smart card*" is often used to generically refer to any smart card whose card operating system can be extended by loading executable programs onto a virtual machine card. GSC-IS compliant smart cards provide for the implementation of services across a standard Virtual Card Edge Interface (VCEI). Based on "card edge" definitions for VM cards, function modules such as those developed by the cryptographic service and public key infrastructure (PKI) cryptographic service providers can be developed for the various functional calls required for encryption, authentication and digital signatures.[66]

The Department of State has purchased $4.8 "Laser Visa" cards from Drexler Technology Corporation of Florida. The LaserCard®[67] Triple-Image identification cards are to be used by frequent visitors from Mexico crossing the border into Texas, Arizona and California for visits, shopping and other activities.[68] The Triple-Image ID card contains the owner's color digital photo on one side of the card, and a laser-engraved image of the same digital photo on the opposite side, which can be compared for visual confirmation of identity. It is difficult to alter the color facial photo, but it is virtually impossible to alter the matching laser-engraved facial image. The same image of the owner is also stored in the card in digital form and can be viewed with a standard PC and the Drexler card read/write drive.[69] The cards contain a biometric template of the owner's fingerprint. The LaserCard will hold over 4 megabytes of data and can store multiple biometric identifiers such as iris, retina and hand templates.

U.S. Department of Homeland Security ordered $2.6 million of LaserCard Optical Memory Cards for use as the enhanced "Green Card." The enhanced Green Card design will add new security technology, including the incorporation of LaserCard Systems Corporation's high security *optically variable device* (OVD) diffraction pattern into the card's optical media. This newly developed OVD feature provides unique visual and optical characteristics that allow immediate authentication of the card media. These upgrades, in addition to the 1,000 optical card read/write drives/Biometric Verification Systems that were purchased for installation at various U.S. points of entry, add significant value to the U.S. Government's investment in secure optical memory card biometric verification systems.[70]

The acceptance of smart cards is growing rapidly worldwide as well. The largest producers of smart cards are SchlumbergerSema, Gemplus and Oberthur. Smart cards are used around the world in GMS cellular telephones, which are ubiquitous in Europe and are now available in the United States. Smart chards are a part of the European culture and business system. The Judicial Organization of the Netherlands Ministry of Justice is storing biometric data on chip cards. The Ministry uses biometric-powered smart cards from Oberthur and Ultimaco allowing users to employ digital signatures and perform data encryption within applications such as Microsoft Outlook.[71]

In spite of European successes, there will have to be a large shift in U.S. culture and business dynamics[72] before smart cards are widely accepted in the United States. But, when the readers are in place and the users comfortable with the technology their use in the United States is expected to increase rapidly. Fredrick Spagnon, chief Operating Officer of Gemplus™ predicts that within 18 months, all keyboards will come with smart card readers.[73] The use of American Express' *Blue*, a combination smart/credit card, is growing rapidly in the United States. Visa, MasterCard and Target Corporation are close behind. Partnered with Glempus, Target is providing its customers with visa-sponsored smart cards and smart card readers. RSA Security's *Smart Card Solutions*™

---

66 *Government Smart Card Interoperability Specification*, Version 2.1, NIST, 16 July 2003. p. 25

67 The LaserCard is manufactured in Mountain View, California under ISO/IEC 11693 and 11594, Parts 1–4.

68 State Department Purchases "Laser Visa" Cards, FEDtechnology.com, 25 September 2001 Issue.

69 The LaserCard uses WORM (Write Once Read Many) optical recording technology. This allows data to be added or updated, but never deleted or erased to provide a permanent record of all additions, changes and attempted deletions.

70 U.S. Homeland Security Adopts LaserCard Biometric Verification Technology and LaserCard Visa for US-VISIT, LaserCard News Release, 19 December 2003.

71 Andy Briney, "A Smart Card for Everyone?" *Information Security*, March 2002, p. 40.

72 Ibid., p. 36.

73 Ibid., p. 40.

technology is beginning to make forays into the American market place. Smart Card Solutions has already been sought out in other regions, like Europe and Asia Pacific. The USG has successfully deployments in nine Departments and Agencies, with the Services leading the way. Military use of smart cards in the United States is expected on grow rapidly.

GlobalPlatform™ provides a proprietary architecture for fast and easy development of globally interoperable smart (microprocessor) card systems, which has not yet become popular with developers. The system architecture is comprised of three system segments—card, terminal and systems—each of which may include specifications, software and/or chip card technology. The GlobalPlatform website[74] carries the following technical data and specifications for download:

1. GlobalPlatform Card Specification v2.1.1—published March 2003.
2. Java Card Export file for the GlobalPlatform Card Specification v2.1 API—published March 2002.
3. Errata and Precisions List v1.1 for the GlobalPlatform Card specification v2.1.1—published October 2003.
4. FAQ List for the GlobalPlatform Card Specifications v2.1 and v2.1.1—published October 2003.
5. GlobalPlatform Card Security Requirements Specification v1.0—published May 2003.

The introduction of Java Card®[75] may significantly reduce the time required to develop and deploy application software resident in microprocessor cards. Java Card is proprietary and still undergoing some research. Card acceptance devices should be programmed and tested with the cards and other components of the application support infrastructure. Microprocessor card-based applications are most effectively implemented when the card and terminal application programs are developed in parallel from the same application specification.

Even though prices have fallen over the past few years, smart card systems are still more expensive to create than the magnetic stripe card and bar code systems. However, stripe and bar code cards have limited memory capacities and are comparatively unreliable, insecure read only systems. Smart cards have the advantage over the magnetic stripe in the data that can be stored and the processing feature in smart cards, although some bar code fields can hold a surprising amount of data. The security, ease of use and operational flexibility of a multi-function secure IC contact chip card makes it a user-friendly system segment option for secure identity management in military systems. Of course, pictures, magnetic and bar code stripes can all be located on the outside of an IC card, making it a highly flexible multifunction card.

Another contactless method for storing information is *Radio Frequency Identification* (RFID). RFID has been available for several years and is used in the control of railroad rolling stock, but is still only available in proprietary forms from a variety of vendors. RFID systems provide information from a RF tag from a distance of a few millimeters to several meters. The tags vary in size and form and fit from the tiny injectable glass transponders for tracing animals to brick size containers on the side of trains.

The frequencies vary from 125 kHz to 5.8 GHz. The *IC Vicinity Card* operates at 13.56 MHz, which is specified by ISO/IEC 15693. The biggest obstacle to RFID growth is the global availability of frequencies.[76]

Optical memory card technology is a technology similar to that used for music CDs and CD ROMs. A panel of the “gold colored” laser sensitive material is laminated in the card and is used to store information. A laser burns a 2.25-micron diameter hole in the material during the storage or recording cycle that can then be sensed by a low power laser during the read cycle. The presence or absence of a hole represents a binary symbol, either a “one” or a “zero.” Because the media is actually burned during the write cycle this is a write-once-read-many times (WORM) media. The data is non-volatile (not lost when power is removed) and these cards currently can store 4 to 6.6 megabytes of data. The State Department’s border crossing ID card used by frequent travelers at entry points along the U.S. border with Mexico are this type of card.

---

[74] GlobalPlatform: The Standard for Smart Card Infrastructure**:** Specifications, http://www.globalplatform.org/showpage.asp?code=cardspec**,** 2004.

[75] A registered trademark of Sun Microsystems, Inc.

[76] U.S. General Services Administration, Smart Card Handbook, http://www.estrategy.gov/information/smartcardhandbook.pdf, 2004.

MCTL DATA SHEET 17.2-3. SECURE IDENTITY MANAGEMENT SYSTEM TECHNOLOGY

Biometric data is derived from a human being and must be processed by a secure biometric identity management system to verify claimed identity (authentication) or discover the individual's identity.[77]

Critical Technology Parameter(s)	System compliance with all of the following: 1) the BioAPI[78] open-systems standard, the CBEFF,[79] XCBF,[80] and ANSI X9.84,[81] including Normative References;[82] and 2) a system and subsystem *Common Criteria* (CC)[83] Protection Profile (PP) appropriate for the classification level of the facility, equipment, data and information for which the secure biometric system controls access, except for systems that include databases, in accordance with *Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments*;[84] 3) for those systems that incorporate databases, the PP shall be appropriate for information classified CONFIDENTIAL and will in no case be less than a CC level of Evaluation Assurance Level (EAL 5)[85] in order to provide prudent protection for the privacy of the enrollees.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Application software for COTS secure biometric identity management systems is proprietary at this time.
Major Commercial Applications	The major commercial market for secure identity management system technology is for access to physical and virtual places, from secure doors to office computers, and for systems that must verify that people are who they claim to be.
Affordability Issues	Secure Biometric Identity Management Systems offer the potential for: 1) Increasing the operational security, privacy, efficiency and convenience of identity management systems while 2) Decreasing operational losses and identity fraud. A cost/benefit trade analysis of these two factors will prove or disprove the affordability business case.
Export Control References	WA ML 11; WA Cat 5D2 and 5E2; USML XI and XIII;[86] CCL 5D002 and 5E002. (These technologies are controlled due to the biometric system segments as well as the cryptographic modules.)

[77] *Frequently Ask Question, Definitions*, International Biometric Group, see http://bioprivacy.org/faq_main.htm and Michelle C. Frye, *The Body as a Password: Considerations, Uses and Concerns of Biometric Technologies*, A Thesis Submitted to the Faculty of the Graduate School of Arts and Sciences in Georgetown University, Washington, DC, 27 April 2001.

[78] American National Standards Institute (ANSI), InterNational Committee for Information Technology Standards (INCITS), ANSI INCITS 358-2002, *The BioAPI Specification*, Version 1.1, 22 March 2002.

[79] Common Biometric Exchange File Format, NISTIR 6529.

[80] XCBF is the XML Common Biometric Format. XML (Extensible Markup Language) is a metalanguage, written in SGML, used for the interchange of documents on the World Wide Web. SGML is a standardized markup language for describing the logical structure of a computer document.

[81] ANSI X9.84, *Biometric Information Management and Security*, 27 March 2003.

[82] Ibid., p. 2.

[83] The *Common Criteria* is also ISO 15408.

[84] Version 0.02, 3 March 2002.

[85] Based on Version 2.1 of the "Common Criteria," International Standard 15408. The Common Criteria can be found at http://csrc.nist.gov/cc

[86] Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

BACKGROUND

Secure Biometric Identity Management System Description

The information security community generally accepts three ways through which a *person can be *positively identified*; i.e., prove you are who you say you are; and, prove you are not who you say you are not, or not among a group of people already know to the system. The three ways a person can be positively identified are by:

1. *Something you have* (a credit card or driver's license);
2. *Something you know* [a password or personal identification number (PIN)]; and
3. *Something you are* (authenticated by biometric characteristics).

Biometrics technology is based on digital matching between a stored template and a submitted biometric sample. Relatively forge-proof unique identifiers of a human body, which can be objectively measured with biometrics, is a way of specifying *something you are* that can be used for authentication and identification purposes; and, have particular value for use among countermeasures against information system identity fraud security exposures. *Something you are* can be determined by objectively measuring human anatomical or physiological traits or characteristics that are unique to an individual such as a fingerprints or iris patterns.[87] For very small highly sensitive operations, personal recognition using trusted third party introductions is still the best and most secure system for identification, access control and circulation security.[88]

The American National Standard X9.49-1999 *Secure Remote Access to Financial Services* classifies these authentication factors as something you have (possession factor), something you know (knowledge factor) and something you are (biometrics factors). The standard provides a risk assessment methodology to determine an application's security requirements (confidentiality, integrity, authentication, and non-repudiation) for online financial services (e.g., home banking) where remote access is required.

The six biometrics selected for coverage in this technology item are a family of fairly mature technologies that are being widely used for applications such as access control systems in major airports and in other areas requiring restricted access. See Appendix to this data sheet.

Six leading biometrics judged best suited to military applications were selected for coverage in this technology item. The six are shown in the columns of the Comparative Biometric Systems table:

1. Fingerprint Analysis;
2. Facial Features;
3. Hand Geometry;
4. Iris Recognition;
5. Speaker Recognition; and
6. Signature Recognition.

The technologies on which these six biometric systems are based are maturing rapidly, already are in wide commercial use and have a significant international market share. Biometric technologies are enablers for secure biometric identity systems.

---

[87] Valene Skerpac, "Got Biometrics?" *Information Security Bulletin 41*, April 2000, p. 41.

[88] Samir Navavati, Michael Thieme, and Raj Nanavati, *Biometrics: Identity Verification in a Networked World*, John Wiley & Sons, Inc., 2002.

APPENDIX TO DATA SHEET 17.2-3—SECURE IDENTITY MANAGEMENT SYSTEM TECHNOLOGY

Table 17.2-2. Biometric System Comparative Description (Page 1 of 2)

	BIOMETRIC SYSTEM					
CHARACTERISTICS	**Fingerprint Systems**	**Facial Features**	**Hand Geometry**	**Iris Recognition**	**Speaker Recognition**	**Signature Recognition**
Median System Processing Time for a Single Transaction	8 seconds for systems with optical sensor readers. 15 seconds for chip-based sensor reader systems.	14 seconds	2 seconds for authentication. ~8 seconds, depending of size of data base	10 seconds	11 seconds	~15 seconds plus the highly variable time required for completion of the sample signature or other signed symbols.
System Requirements	Fingerprint imaging techniques encode finger print information as a series of "minutiae" for templates ranging from 220[89] to 2000 bytes and a system should require at least two fingerprints.	Requires large direct access storage for large populations. Templates require 350 bytes.[90]	Requires the least amount of storage. Storage requirements for hand and finger templates are 800 to 900 bytes.	Iris recognition systems require 512 kilobytes[91] for each template, and only one template is required per person.	Speaker Recognition Systems require 3 kilobytes[92] to 1 megabyte of voice data per 6 seconds.	Requires large direct access storage for large populations. Templates require as little as I kilobyte.[93]
One-to-One Authentication systems	Compares a sample to a person's enrolled authentic template on a card or in a trusted database in order to authenticate a claimed identity.	Authenticates by comparing a sample to a person's enrolled authentic template on a card or in a trusted database in order to authenticate a claimed identity.	Authenticates by comparing a sample to a person's enrolled authentic template on a card or in a trusted database in order to authenticate a claimed identity.	Authenticates by comparing a sample to a person's enrolled authentic template on a card or in a trusted database in order to authenticate a claimed identity.	Authenticates by comparing the voice of a speaker to a sample of an enrolled person's authentic voice pattern template on a card or in a trusted database in order to authenticate a claimed identity.	Authenticates by comparing a sample to a person's enrolled authentic template on a card or in a trusted database in order to authenticate a claimed identity.

89 "IdentAlink estimate, Computer Security Issues," *Biometric Technology Today*, June 2001, p. 10. Source: Elmar Hilgers, ehilgers@biometrics.ws.

90 John Chirillo, Implementing Biometric Security, *John Wiley Publishing*, 2003.

91 Ibid.

92 Buytel estimate, "Computer Security Issues," *Biometric Technology Today*, Ken Pilkington, mailto:ken@buytel.com, June 2001.

93 WonderNet estimate, an Israeli company, *Computer Security Issues*, Source: Alex Herman, alex@wondernet.co.il

Table 17.2-2. Biometric System Comparative Description (Page 2 of 2)

	BIOMETRIC SYSTEM					
CHARACTERISTICS	**Fingerprint Systems**	**Facial Features**	**Hand Geometry**	**Iris Recognition**	**Speaker Recognition**	**Signature Recognition**
One-to-Many Identification Systems	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.
False Accept (FAR) and False Reject (FRR) Error Rates	Recent study single-finger comparison false accept rates 0.1–5%. False reject rates 0.0–35%[94] (FNMR) 0.2–36% (FMR) 0–8%[95]	May be one of the higher error rate metrics. (FNMR) 3.3–70% (FMR) 0.3–5%[96]	Not as accurate as fingerprints. Hands are not as unique as fingerprints. (FMR)0–0-5% (FNMR) 2.1%[97]	Not as accurate as fingerprints. Hands are not as unique as fingerprints. (FMR) 0–0-5% (FNMR) 2.1%[98]	Performs verification and identification with a FAR of 0.0.[99] (FNMR) 0.2% (FMR) 0%[100]	May have high error rates due to normal variations in signature metrics and the physical condition of the claimant.
Ease of Use	May require significant cooperation from claimant.	Deserves a 10 on a scale of 1 to 10. Can be used surreptitiously.	Easiest to use.	Easiest to use.	Rated 9 on a scale of 1 to 10 in tests.	Most natural and some consider it easy.
Relative Cost[101]	**$$$$**	**$$$$**	**$$$$$**	**$$$$$$**	**$**	**$$**

[94] The Government Accounting Office, *Biometrics for Border Security*, GAO-03-174, 2003.

[95] IBG's Comparative Biometric Testing Round Five, International Biometric Group, Press Release, 7 January 2004.

[96] The Government Accounting Office, *Biometrics for Border Security*, GAO-03-174, 2003.

[97] Ibid., p. 69.

[98] Ibid.

[99] Gerald O. Williams, *Iridian Technologies*, Iridian Technologies, Inc., 2001, p. 7.

[100] The Government Accounting Office, *Biometrics for Border Security*, GAO-03-174, 2003.

[101] Relative costs taken from the *Zephyr™ Analysis*, see http://www.biometricgroup.com/e/zephyr_charts.htm

SECTION 17.3—NETWORK TECHNOLOGY

Highlights

- Network security hardware/software tools (appliances, "solutions") cannot replace user security training and discipline.
- All of these technologies and products exist in COTS versions. The critical technology parameter is a requirement for a certified[102] Common Criteria (CC) EAL 5[103] certification. No products currently available meet the EAL 5 criteria.
- *Firewall* functionality combinations now appearing in hybrid firewalls offer a variety of features and most can be tailored to meet unique business, and military, information system security requirements. Firewalls cannot defend against a data-driven attack in which something is mailed or copied to an internal host where it is then executed.
- *Application Proxy Servers* are software or software-and-hardware processors that operate between external and internal networks, which usually operate in concert with other types of firewalls.
- *Intrusion Detection (ID)* is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability or to bypass the security mechanisms of a computer or network.[104]
- *Peer-to-Peer Networking* technologies are used to share information (files/data) directly between users. Well known implementations such as Napster have been used to facilitate the improper sharing of copyrighted music and video files.
- *Virtual Private Networks (VPN)* provide for the secure connection of remote systems/clients to private networks via the public Internet.

OVERVIEW

This section covers the major types technologies used to protect sites from exploitation of the inherent vulnerabilities of the TCP/IP protocol suite and legacy single channel signaling, which is still in wide use and carries the bulk of Internet and other network traffic. The section also includes peer-to-peer, and virtual private networking technology.

The technologies in this section are closely related to some of those in MCTL Section 10, Information Systems Technology. Firewalls, and intrusion detection technologies are implemented as software, or hardware and software combination systems, interposed between assets to be protected, such as mainframes, servers, workstations, local area or enterprise and larger networks, and external, potentially hostile or uncontrolled networks and systems such as the Internet.

Internet applications are not addressed in this section. Such applications are mentioned only to provide a point of reference for the reader. The network applications themselves each add their own risks to the secure operation of a network. Each and every network application must be separately considered, in the context of the user's network security practice policy, after the base network has been properly configured and tested.

---

[102] Certified by a member of the National Voluntary Laboratory Accreditation Program (NVLAP).

[103] http://csrc.nist.gov/cc

[104] Special Publication 800-31, *Intrusion Detection Systems*, National Institute of Standards and Technology, U.S. Department of Commerce, p. 5.

BACKGROUND

In the Department of Defense, the concept of *Defense in Depth*[105] has been accepted for the security architecture of complex computer networks. With defense in depth, multiple countermeasures such as firewalls, intrusion detection systems, and virtual private network (VPN) tunnels are deployed to prevent, detect, and respond to potential network intrusions. The use of combinations of countermeasures provides a much higher probability of detection, and affords much greater protection to mission critical information. In good security architectures, firewalls are usually deployed as the first line perimeter defensive countermeasure, reflecting best commercial network security practices.

Firewalls operate at Layers 4, 3 and 2 of the Open Systems Interconnect (OSI)[106] model. Basic firewalls operate on a smaller number of layers. The more advanced firewalls will cover a larger number of layers. Generally, firewalls capable of examining a larger number of layers are more thorough and effective. The three firewall names selected for this section were taken from the names used in the recommendations of the National Institute of Standards and Technology (NIST) in their guidelines on firewalls and firewall policy:[107] 1) *packet filter* firewalls; 2) *stateful inspection* firewalls; and 3) *hybrid firewalls*.

Today a firewall is a mandatory element of any secure network architecture. Even home users with commercial dial-in connections and with cable or digital subscriber line (DSL) connections should routinely employ personal firewalls and firewall appliances.

Application Proxy Firewalls. Because application proxies examine packets at the application program level (OSI Level 7),[108] a very fine level of security and access control can be enforced and a high level of protection can be provided against "denial of service" (DOS) attacks. An application proxy firewall can be configured to reject all inbound packets that contain common executable file types such as .EXE or .COM files, which hackers, or "crackers" more precisely, often use to introduce dangerous virus and worm files into a network. Basically, a proxy software program or device makes software requests on behalf of another device on the network.

Intrusion Detection Systems can be implemented in two ways. Host-based intrusion detection systems (IDS) operate on a host to detect malicious activity on the host. Network-based IDS operate on the network data flows. A distinction can be made between intrusion and misuse detection. The term intrusion is used to describe attacks from the outside, where as misuse is used to describe an attack that originates from the internal network. These distinctions are not universally recognized or respected in the product marketing literature. The trend in the IDS market is toward full-blown intrusion management tools that bundle host protection and network-based scanning, vulnerability assessment and centralized data collection and analysis. The most common approaches to IDS are statistical anomaly detection and pattern-matching detection.

Peer-to-Peer networking is emerging as an alternative to client/server architectures. In the client/server environment data (files) are stored in a central location where authorized users can access them. User identification and authentication are managed at the central site/application. In peer-to-peer networks the data (files) are accessed at their "peer" location. The identification of the requesting user, and the authentication of the requested data can be problematic. Multiple "peers" can hold copies (versions) of each data set. There may, or may not, be centralized version management as part of the application. Peer-to-peer applications have some inherent advantages, but the security implications are challenging.

Virtual Private Networks (VPNs) provide an alternative to "traditional private networks consisting of leased lines connecting multiple sites together. An example would be two offices connected by a point-to-point T-1 line." In addition to the requirement to connect fixed facilities, organizations need to provide for the remote connection of off-site employees and trusted contractors.

---

[105] See http://www.ncs.gov/news/speech/speech01/speech_01_0517g.html

[106] The OSI model (ISO 7498, Open Systems Interconnect Reference Model) is an abstraction of network communications between computer systems and network devices.

[107] Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, January 2002.

[108] Descriptions of the 7 layer model can be found at http://en.wikipedia.org/wiki/OSI_model#Description_of_layers

A VPN provides an encrypted tunnel between two network endpoints. The VPN technology is used to protect private information while it transits a public network. In the TCP/IP environment a VPN is implemented with layer 2 tunnels.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.3. NETWORK TECHNOLOGY

MCTL DATA SHEET 17.3-1. PACKET FILTERING TECHNOLOGY

Packet filters protect network nodes/sites from undesirable external users.

Critical Technology Parameter(s)	Having all of the following: 1) Designed or modified to provide evaluated[109] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[110] of the Common Criteria (CC)[111] or equivalent (ISO/IEC 15408)[112] and 2) Pass data at connection rates equal to or greater than T1.[113]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Most commercial enterprises now consider the acquisition and maintenance of firewalls expected and essential.
Affordability Issues	Affordability is not an issue for COTS products because the highly competitive market place keeps margins small. However, the technology is moving so fast that there are often unusually high non-recurring-engineering costs, and a high probability of product obsolescence even before deployment, with all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support. Application proxies must be tailored for specific applications and protocols and must be changed when these applications and protocols are updated or further developed to incorporate additional features. The operation and maintenance of firewalls can be a significant cost.
Export Control References	WA ML 11; WA Cat 5E2; USML XI and XIII;[114] CCL Cat 5E002.

BACKGROUND

Packet filtering firewalls are software, or hardware and software combinations, which function at the interfaces between the assets to be protected and entities outside the firewall. Assets to be protected are workstations, local area and enterprise networks that must be defended from larger external potentially hostile or uncontrolled networks and open systems such as the Internet. Packet filters are the most basic and fundamental type of firewall. They include access control functionality for system addresses and communications sessions. Packet filters are normally located in routers to provide control and direction for Internet protocol (IP) addresses and designate the correct ports for connections. This simple functionality is a fundamental adjunct to more sophisticated protection applications. The packet filter access control functionality is governed by a set of directives collectively referred to as a ruleset. The operation of rulesets is described in the Appendix to this data sheet.

---

109 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

110 Ibid., p. 14.

111 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

112 (ISO/IEC 15408) source: http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

113 1.5 Megabits per second.

114 Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

A stateful packet inspection firewall is a packet filter that incorporates the added awareness of the Open System Interconnect (OSI) model layer 4 data. Layer 4 is the transport layer, the middle layer in the OSI 7-layer model. The stateful packet inspection function consists of monitoring and assessing all packets associated with each specific communication session. Communication sessions between two computers will often consist of several thousand packets, each of which is identified by a unique "source" and "destination" address and a "sequence" number, which makes it possible for all of the packets to be reassembled into the correct data file at the destination computer. The TCP specification requires that the client source port be some number greater than 1023 and less than 16384. Packet filters must allow inbound connection-oriented return packets to connect through high numbered ports from destination systems. Sometimes thousands of simultaneous sessions may be happening at the same time.

A stateful inspection firewall keeps track of these concurrent sessions and each packet of data is checked to ensure that it belongs to the proper session. Any stray packets that are not part of an established session are rejected. Each of the communication sessions is checked and validated by the source and destination addresses of the machines in the session to ensure that all packets belong to the proper session. Opening a large number of high-numbered ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful packet inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding client port number.

Hybrid firewalls, as their name implies is a name used to collectively identify a type of firewall, which recent computer science advances and inspired system engineering have made possible in response to the increasing variety of military information dominance requirements and business security requirements resulting from the growth in e-commerce on the Internet. Advances in network infrastructure system engineering, computer science and information security system engineering have resulted in a blurring of the original distinctions that differentiated the classic three once fairly pure first generation firewall types: packet filter, stateful packet inspection, and application proxy.

Many of the major products in COTS network firewalls are combinations of proxies and application level gateways.[115] Application level gateways are a powerful but complex and expensive form of network firewall, because packet inspection operations are performed on the data payload of the packet. This is the information that the application programs process, allowing for example:

- Virus scanning of incoming FTP files and email.
- Control over what FTP commands the user is permitted to execute.
- Control over which commands are to be allowed for the execution of any particular service.

[115] Raptor Eagle®, NAI/TIS' Gauntlet®, Harris' Nighthawk®, and SCC's Sidewinder®.

APPENDIX TO DATA SHEET 17.3-1—PACKET FILTERING TECHNOLOGY

PACKET FILTERING RULESETS

A ruleset is a software or firmware table of instructions that the firewall uses for determining how packets are to be routed across its interfaces. The ruleset is examined from top to bottom when making routing decisions. When a packet firewall accepts a packet, it determines the protocol in use and the packet's source and destination addresses and ports. Then the firewall runs down through the rules to determine the disposition of the packet. When a rule permits or denies the packet entry, the firewall takes one of three general actions:

- If the rule specifies "allow," the firewall *accepts* the packet and passes it through the firewall as requested, performing the logging functions incorporated in the firewall software.
- If the rule specifies "deny," the firewall *denies* the packet entry, dropping the packet and generating an error messaged to the source system, if required by the ruleset.
- If the rule specifies, "discard," the firewall *drops* the packet into the "bit bucket"[116] but does not generate an error message to the source system and may or may not generate a log entry, depending on the ruleset specification. The discard action implements the so-called "*black hole*" strategy of not revealing the presence of a firewall to an outsider.

The number of rules in a ruleset varies widely and a typical ruleset is much longer and more detailed than the illustration in Table 17.3-1 below. The packet filter software always reads the ruleset table from top to bottom.

Table 17.3-1. Packet Filter Firewall Rule Illustrations

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	137.123.2.0*	> 1023*	Allow	Rule to allow return TCP Connections to internal subnet.
2	Any	Any	137.123.2.0*	Any	Deny	Prevent external user from directly accessing the Firewall system
3	137.123.2.0*	Any	Any	Any	Deny	Prevents the firewall system from directly connecting to anything.
n	Any	Any	Any	Any	Deny	Everything not previously allowed is explicitly denied.
*Arbitrary notional number.						

The first rule is the "return connection" rule, which requires that responding packets from external systems be allowed to return to originating internal systems to complete the connection, assuming the connection is one that is authorized. If connection with the external system is allowed, the connection-oriented Transfer Control Protocol (TCP) rules require that responding packets from an external system must be allowed to complete the connection. Packet filter firewalls must allow inbound responding TCP network traffic packets that return from a selected destination system to enter, usually through any port with number higher[117] than 1023, as shown in the first rule in the ruleset illustration table above.

---

[116] Slang for delete.

[117] The convention is that any port less than 1024 is likely to be a low-numbered port at the destination on the remote host.

The second rule prevents any packet from any source outside the packet filter firewall from accessing the firewall directly.

Rule three prevents the firewall from directly connecting to any outside source. The other rules that are required to enforce the specified security policy follow.

The rule in the last row of the illustration table is very important and is always the last rule in a ruleset table. This rule (n) of the ruleset table simply blocks all other packets[118] from outside sources not specifically allowed by the rule set. If this last rule in the ruleset table were accidentally not included, all traffic originating from outside the firewall not covered by the ruleset would be allowed to enter.

With long, detailed rulesets it is only human to make disastrous mistakes in developing and maintaining the ruleset. The ruleset should be reviewed very carefully and thoroughly tested before implementation. In addition, the ruleset should be reviewed at regular intervals after installation to ensure that the specified ruleset protocols still meet the organization's ever changing requirements and to minimize the possibility of logical errors when new rules are added and old rules are changed or deleted. Basic packet filters are not aware of state.

For performance or other reasons, ordinary packet filters do not attempt to remember previous states of packets, connections and patterns to make access and security decisions.[119] Basic, non-stateful, firewalls are no longer widely used. Firewall "appliances" for applications, from the SOHO (small office/home office) to the largest enterprises, now commonly include "stateful" packet filtering. These products are available for as little as $150.[120] "Stateful" packet filtering is also included in the Internet Connection Firewall (ICF) that is a part of the current Windows XP® operating system.[121] See MCTL Data Sheet 17.3.2 for "stateful packet inspection firewall" technology.

---

[118] "Packet" was used for the first time in 1965 by Donald Davies, a British researcher at the National Physical Laboratory to describe a way of breaking up messages for transmission across new kinds of networks. ARPA sponsored the first study of cooperatively networked computers involving connection of two computers; one in CA and one in MA across a dedicated 2,000 bit per second telephone link.

[119] Ascend has adopted "Stateful Packet Inspection" (a descriptor also used by Checkpoint) that it calls Dynamic Firewall Technology, (also called "Secure Access" and "Perimeter Firewall") and shipped in a router product. Stateful packet inspection is a far more powerful control, but does not attempt processor-intensive functions such as email virus scanning.

[120] Home/Small business firewall: see http://www.netgear.com/products/details/FVS318.php?view=. For pricing, use http://www.pricewatch.com/default.htm and search for "FVS318."

[121] "ICF is considered a "stateful" firewall." Quote from the Windows XP® "Network Connections" help file.

MCTL DATA SHEET 17.3-2. APPLICATION PROXY TECHNOLOGY

Application Proxy Servers are software or software-and-hardware processors that operate between external and internal networks, which usually operate in concert with other types of firewalls.

Critical Technology Parameter(s)	Having all of the following: 1) Designed or modified to provide evaluated[122] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[123] of the Common Criteria[124] (CC) or equivalent (ISO/IEC 15408)[125] and 2) Pass data at connection rates equal to or greater than T1.[126]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential, untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Large commercial enterprises now consider the acquisition and maintenance of application proxy gateway firewalls essential and there are strong business cases supporting their use for the protection of high-value assets.
Affordability Issues	Affordability is usually not an issue for COTS. However, the technology is moving so fast that there are often unusually high non-recurring-engineering costs, and a high probability of product obsolescence even before deployment. Application proxies must be tailored for specific applications and protocols and must be changed when these applications and protocols are updated or further developed to incorporate additional features. The operation and maintenance of application proxy gateways can be a significant cost.
Export Control References	WA ML 11; WA Cat 5E2; USML XI and XIII; CCL Cat 5E002.

BACKGROUND

Internal systems may go on operating as if directly connected to external networks, while actually having their communications inspected and protected by the proxy. With correct tailoring, the proxy can be transparent, and should be of sufficient capacity to see all necessary control information (encryption can prevent such full inspection). Each conventional network service, such as Telnet and FTP, should be proxied. Proxies can perform additional useful functions such as network address translation.

Application proxy firewalls are advanced gateway firewalls that combine access control with application layer (7) functionality. Application proxies do not require a network layer (3) route between the inside and outside interfaces of the firewall because the firewall software performs the routing. If application proxy gateway software ceases to function, the firewall system is unable to pass network packets through the firewall system. All network packets that traverse the firewall must do so under application proxy software control. Each individual application proxy, also referred to as a "proxy agent," interfaces directly with the firewall access control ruleset to determine

[122] http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

[123] Ibid., p. 14.

[124] http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

[125] (ISO/IEC 15408) source: http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

[126] 1.5 Megabits per second.

whether a packet should be permitted to transit the firewall. In addition to the ruleset reference, each proxy agent has the ability to require authentication of each individual network user. This user authentication can be:

- User ID and password authentication.
- Hardware or software token authentication.
- Secure address authentication.
- Biometric authentication.

An application proxy firewall can be set up to take one class C[127] address and map it to another class C address. Various products can use this feature to map one address from the internet service provider (ISP) into multiple unregistered *packet* addresses on the internal network.

[127] A tutorial on IP address classes can be found at http://www.unix.org.ua/orelly/networking/firewall/appc_09.htm

MCTL DATA SHEET 17.3-3. INTRUSION DETECTION TECHNOLOGY

Intrusion detection hardware/software collects and processes information about attempts to penetrate information systems that are attached to public networks.

Critical Technology Parameter(s)	Having both of the following: 1) designed or modified to provide evaluated[128] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[129] of the Common Criteria (CC)[130] or equivalent (ISO/IEC 15408)[131] and 2) pass data at connection rates equal to or greater than T1.[132]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specifically developed or tailored software and a highly skilled software maintenance staff are required to operate and maintain intrusion detection throughout the intrusion detection system life cycle.
Major Commercial Applications	Widespread commercial use of IDS started in the mid-1990s for high value electronic commerce transactions and was predicted to continue growing for the foreseeable future.
Affordability Issues	1) The cost of the highly skilled system administrators, technical software and hardware operations and maintenance staff required for the acquisition of the IDS and the operation and maintenance of the IDS throughout its life cycle; 2) current lack of standards for the exchange of control and reporting of intrusion events between the various available IDS: standardization is being addressed with a proposal to create an RFC.[133]
Export Control References	WA ML 11; WA Cat 5D2 and 5E2; USML XI and XIII; CCL Cat 5D002 and 5E002.

BACKGROUND

Intrusion detection (ID) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability or to bypass the security mechanisms of a computer or network. Intrusion detection technologies and products are the key components of secure information systems. An intrusion detection system (IDS) sits, physically or logically, between the network firewall and the internal network. The IDS is critical to information assurance operations as it collects evidence on intrusion (attempts) that have penetrated the organizations network boundaries. A distinction can be made between *misuse* and *intrusion* detection. The term intrusion is used to describe attacks from the outside, whereas misuse is used to describe an attack, or an accidental action, that originates from the internal network. However, these distinctions are not widely recognized or respected in the product marketing literature. These ID systems should not be confused with physical perimeter intrusion detection systems used to protect borders, airports, nuclear power plants and other key facilities from terrorist threats.

---

128 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

129 Ibid., p. 14.

130 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

131 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

132 1.5 Megabits per second.

133 See http://www.ietf.org/html.charters/idwg-charter.html for the current status of the RFC development.

IDS are classified as being either *host-based* or *network-based*. Host-based IDS operate on a host to detect malicious activity on that host. Network-based IDS operate on the network data flows. Either of these types can be implemented as behavior-based, or as knowledge-based technologies. Behavior based IDS operate according to administrator specified behavior rules. Knowledge (signature) based IDS operate with a database of known attack mechanisms.[134] The trend in the IDS market is toward full sets of intrusion management tools that bundle host protection, network-based scanning, behavior based analysis, vulnerability assessment, centralized data collection and analysis. The most common approaches to ID are statistical anomaly detection and pattern-matching detection.

When most automatic data processing took place on mainframe systems, most IDS ran on the systems they protected. Intrusion detection systems were designed to notify, and in some cases prevent, unauthorized access to a networked host. Now, IDS should be designed to interact with firewalls automatically. The firewalls can be designed to respond to remote threats perceived by IDS automatically without waiting for a human command. If an attack is detected, the reaction from the firewall must be almost instantaneous to prevent a denial-of-service attack.

Most of the enterprise level intrusion detection systems are *networked-based*. These IDS detect attacks by capturing and analyzing network packets. One network-based IDS listening on a small network segment or on a switch can monitor the traffic, analyzing it for signs of security problems and protect several hosts. In larger networks, network-based IDS usually consist of a set of single-purpose sensors or hosts placed at various points in the network running in "stealth" mode in order to make it more difficult for an attacker to determine their presence and location, making them very secure against attack. Each of the single-purpose sensors in such a set performs local analysis of the traffic and report attacks to a central management console. A few well-placed network-based IDSes can monitor a large network, without interfering with normal operations and have little impact on the performance of the network.

Host-based IDS operate on the information within an individual computer system. There are even application-based IDS that are a subset of host-based IDS. Host-based IDS can analyze activities with precision, determining exactly which processes and users are involved in a particular attack on the operating system. Host-based IDS can directly access and monitor the data files and system processes targeted by attack that reveal the results of an attempted attack, using the host's operating system audit trails and system logs. The operating system audit trails are generated at the innermost (kernel) level of the operating system and are better protected than system logs. Operating system audit trails are smaller than system logs and harder to understand. Today, most host-based IDS are found in recent versions of desktop operating systems. These are designed for environments where more robust solutions are impractical or too expensive.

Behavior-based IDS protect the operating system from malicious attacks by protecting the operating system kernel from behaviors the administrator considers "malicious." Behavior-based IDS operate on an individual computer system according to allowed behavior rules specified by either the system administrator or the IDS provider. If an application tries to behave in a way not allowed, an alert is generated and the behavior is disallowed. This class of IDS is often categorized as *intrusion prevention* technology, because they do not use specific attack signatures or patterns for protection.

Knowledge-based (signature-based)—The IDS uses a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is detected. These types of systems are currently the most common but vendors are starting to blur the line between knowledge-based and behavior-based systems as a way to differentiate themselves and their competitors.

[134] See "Intrusion Detection: Cisco IDS Overview" at http://www.informit.com/articles/article.asp?p=24696&rl=1

MCTL DATA SHEET 17.3-4. PEER-TO-PEER NETWORK TECHNOLOGY

Peer-to-peer (P2P) technologies provide flexible file (data) sharing capabilities as compared to traditional client/server architectures.

Critical Technology Parameter(s)	All of the following: 1) Undergone extensive open peer review and no attacks found that allow faster plaintext recovery than an exhaustive key search; 2) At least a 128-bit security for cryptographic functions; 3) time stamp applications or features using the NIST time[135] signal and be ANSI X9.95[136] compliant; and 4) meet the Protection Profile (PP) requirements for the P2P network system components appropriate for highest classification of the information processed through the network, but in no case less than a certified Common Criteria (CC) level of Evaluation Assurance Level (EAL) 5.[137]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Major Commercial Applications	There is wide spread commercial use of P2P and instant messaging (IM) to form overlay network applications that sit on top of TCP/IP networks for communications between users. These applications can be used for: searching, downloading and exchanging information, file-sharing, instant messaging and distributed processing. P2P is a way for users to share files without the expense involved in maintaining a centralized server and as a way for businesses to exchange information with each other directly.
Affordability Issues	1) The high acquisition cost of the custom development or tailoring required and continuing update and development during the life cycle required for a P2P network that continues to meet militarily critical threshold requirements; and, 2) the cost of the highly skilled system administrators, technical software and hardware operations and maintenance staff required for the acquisition of the P2P network and the operation and maintenance of the P2P network throughout its life cycle.
Export Control References	WA ML 11; WA Cat 5D2 and 5E2; USML XI and XIII;[138] CCL Cat 5D002 and 5E002.

BACKGROUND

P2P technologies, policies and procedures are not new in the field of computing science. The USG sponsored predecessor of the Internet, and the first to take advantage of TCP/IP and packet switching, was the *Arpanet*. The Arpanet was composed of computer nodes that were behaving as equals or peers to each other. Every computer had equal rights in sending and receiving packets. Experienced users for research cooperation and collaboration originally used the Arpanet. Therefore, there was not much need for security precautions and the Arpanet generally worked smoothly. Even the client/server applications like ftp and telnet were used in a P2P mode. Every computer could ftp or telnet any other.

Another well-known and essential system for the Internet and P2P systems of today is the domain name system (DNS). The DNS is a hierarchy of information ownership. The DNS was born as a solution to the sharing of a text file called hosts.txt, which mapped IP addresses to human-friendly names. The DNS was copied throughout the

---

135 See www.time.gov

136 American National Standards Institute, X9.95, *Time Stamps*.

137 http://csrc.nist.gov/cc. It is recognized that there are currently no COTS products that meet this threshold at this time.

138 Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

Internet on a regular basis. As the Internet grew exponentially, this single text file was inadequate. DNS is a P2P system in the way that the name servers operate. When a client requests an Internet address using an Internet name, it sends a URL to its nearest name server. If the name server already knows the name, it replies with the corresponding IP address; if not, it propagates the query to the authority for that particular namespace. This authority (another name server) may forward the query to an even higher authority until the query is answered and the result is propagated back and cached along the way. In other words, the name servers are working in a P2P fashion since they are servers and clients at the same time. These systems prepared the way for the well-known *Napster*®. P2P computing was front-page headline news on technical Web sites in early 2000, largely due to Napster and cryptanalytic meta-processing successes.

Napster is often called P2P, but is really not P2P in the strictest sense because it uses a centralized server to store pointers and resolve addresses. However, P2P is having a significant impact on the design and development of system architectures and commercial applications. It is having a profound impact on the Internet and the Web as we build the next generation of network-centric applications. Although Napster is not a true P2P system, it was the first one that raised important issues for the P2P community. The most important of those issues was that the concepts of ownership and distribution of information were differentiated. Using Napster, many people would distribute multi-media files in a free and pseudo-anonymous manner.[139] Beyond Napster, other true P2P systems and ways to distribute computation were added to the Internet. The most important of those was a system similar to Napster, only a true P2P system, called *Gnutella*®.[140]

[139] The users owned this data in the sense that it existed as personal files on their local workstation. The copyright implications are a separate matter.

[140] http://www.gnutella.com/

MCTL DATA SHEET 17.3-5. VIRTUAL PRIVATE NETWORK TECHNOLOGY

Virtual Private Network (VPN) technologies provide for secure, encrypted, end-to-end connections to and between private users and servers communicating via public networks.

Critical Technology Parameter(s)	Having both of the following: 1) at least a 128-bit security for cryptographic functions; and 2) designed or modified to provide evaluated[141] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[142] of the Common Criteria (CC)[143] or equivalent (ISO/IEC 15408).[144]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Most commercial enterprises now consider the acquisition and maintenance of VPN's expected and essential. Due to the difficulty in configuring and testing VPNs without interfering with legitimate network traffic, VPN's are often not effective; i.e., they are permissively configured and easily exploited or bypassed by attackers. VPN client software is included in mass-market operating systems.
Affordability Issues	Affordability is not an issue for COTS products because the highly competitive market place keeps margins small. However, the technology is moving so fast that there are often unusually high non-recurring-engineering costs, and a high probability of product obsolescence even before deployment, with all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support.
Export Control References	WA ML 11; WA Cat 5A2 and 5E2; USML XI and XIII;[145] CCL Cat 5A002 and 5E002.

BACKGROUND

Virtual Private Networks (VPNs) provide an alternative to "traditional" private networks consisting of leased lines connecting (multiple) sites. An example would be two offices connected by a point-to-point T-1 line." In addition to the requirement to connect fixed facilities, organizations need to provide for the remote connection of off-site employees and trusted contractors. The traditional method (1980s) for providing those connections was via the use of internal/private banks of dial-in modems. A few years later internet service providers (ISPs) began setting up their own modem banks in multiple locations and offering Internet connectivity to the general public. Private organizations wanted to take advantage of the cost savings, and later the wide availability of broadband connectivity, and their own Internet connectivity, to replace their private facilities. VPNs provided the tools to make this transition practical, and secure.

---

141 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

142 Ibid., p. 14.

143 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

144 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

145 Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

A VPN provides an encrypted tunnel[146] between two network endpoints. The VPN technology is used to protect private information while it transits a public network. In the TCP/IP environment a VPN is implemented as a layer 2 tunnel. "VPN tunnels are created using a tunneling protocol such as L2TP[147] and secured using a protocol such as IPsec."[148]

VPN connections must transit network firewalls. See MCTL Data Sheet 17.3-1, Packet Filtering Technology, for additional information.

[146] http://en.wikipedia.org/wiki/VPN#Tunneling

[147] http://www.faqs.org/rfcs/rfc2661.html

[148] http://www.faqs.org/rfcs/rfc3193.html

SECTION 17.4—RELIABLE SOFTWARE TECHNOLOGY

Highlights

- Software is, and has traditionally been, unreliable and ridden with defects. Those defects make it impossible to create and maintain system security policy goals.
- The technologies addressed are those with the best chance of improving the current, state of the art for creation of truly reliable software in the near term.

OVERVIEW

This section is directly related to MCTL Section 10, Information Systems Technology. It includes: anti-tamper software; execution access; secure distribution; software inspection and test; digital rights management; active response; and secure micro-kernel operating systems technologies.

Many additional software reliability technologies are in various stages of debate and research. Some examples of those include: content tagging, data interoperability, and source fingerprinting.

BACKGROUND

There are many threats to reliable software. The following list is only to alert software developers to some of the threats that could be the cause of software failures in military weapons systems.

- 3rd party tools used by vendor could be compromised before being put under configuration management (CM) or could have built-in trap doors.
- A user could use a tool (e.g., prover) that is not under CM to get the results he wants and then try to put the fake results under CM.
- The user authentication mechanism could be compromised either by guessing, stealing or brute forcing a password or bypassing access0 control mechanism.
- Documents could be added without their appropriate upstream counterparts (e.g., proof of security model without the security model or with a dummy or rogue model).
- Documents could be added that do not correspond to existing ones.
- Person(s) responsible for managing the above process could make errors, either unintentional or malicious.
- CM could not, or did not, thoroughly check for inconsistencies.
- Input to CM model could not be checked by inspection by a second person (some changes to the CM model could really be “programming code” without being inspected).
- Non-atomic commits that could lead to partial configurations.
- Person(s) fail to follow manual parts of CM plan appropriately.
- Some data could be randomly corrupted creating availability and integrity failures.
- An attacker(s) could modify data in a desired way by going outside of the program.
- The system administrator can modify items that are supposed to be immutable such as committed items, configuration contents, or logs.
- An unauthorized user(s) could get access to a machine directly.
- An unauthorized user(s) could get access to machine remotely.
- A user(s) with access to the system is able to damage or replace a CM tool version.

- If files are not tightly linked together by a CM tool, a user(s) could substitute a file without detection.
- If user(s) were to change labels, they might mislead other users and prevent the target of evaluation (TOE) from being identified.
- If compare does not work correctly, it might not be possible to identify unauthorized changes that have been made.
- Names could be changed intentionally to confuse users, i.e., change 'Release_2.0_buggy' to 'Release_2.0_stable.'

Operating system (O/S), application, trusted computer base (TCB) must include:

- Secure application-centric development environments, creating a virtual "cocoon" in which an application can be created, developed, tested and prepared for distribution with very low risk of being compromised.
- Software application anti-piracy measures, such as node-locking features able to protect the code once it is in distribution.
- Application integrity measures, which ensure that users are running the code they intend to.

The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows XP reportedly contains about *40 million lines of code*, compared with about 16 million lines for Windows NT (V4.0). As reported by the National Institute of Standards and Technology (NIST), based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.

As soon as vulnerabilities are discovered, attackers concentrate on attempting to exploit them almost immediately. This prompt exploitation sometimes includes such things as setting up Web sites to take control of entire systems enabling the hacker to read, modify, or delete information on victim systems; disrupt operations with viruses and worms,[149] or launch any of many other forms of attack against systems. Attacks can be launched against distributed systems through viruses and worms. These are the basic reasons for installing patches promptly.

The reliable software technology section covers the following technologies:

Anti-tamper (Software) technologies addresses tamper-proofing/anti-tamper technologies as applied to software applications. These technologies are applied above and beyond the basic capabilities of most operating systems to control access to a specific application. Protecting algorithms, and their implementation, prevents competitors or attackers from building similar functionality at a fraction of the cost of designing it from scratch. Additionally, once an adversary steals software, it positions them with an ability to build countermeasures that will negate strategic advantages.

Execution Access technologies: Software protection technologies provide for the secure design, development, distribution, and execution of high value software. Software needs to be protected because of the value invested during development and the strategic advantages that adversaries could gain from exploits. In the commercial world these technologies are focused on measures (techniques, technologies) that have been designed to ensure license compliance and/or ensure that license fees are collected. Most commercial licensing mechanisms are best characterized as tools to help the honest customer maintain his contractual obligations.

Secure (software) Distribution technologies: Traditional software distribution has been anything but secure. Exceptions have been the occasional *ad hoc* methods employing software couriers for transferring the trusted software for sensitive projects from the trusted development organization to the users. The commercial market has not been concerned with who receives the software, but rather the concern has been the collection of licensing revenue.

[149] A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. In contrast, a worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

The scale of the distribution is also significantly different between the commercial software market and the military. In the commercial world the developer is planning to deliver thousands to millions of copies of an application. The product delivery cycle is spread out over several months, to a few years. Many defense programs are faced with the need to distribute dozens to thousands of copies of an application (or an application update) in a very short period of time.

Software Inspection and Test technologies: Software quality and security are related characteristics that must be considered in the specification, development and for the full life cycle of software for a military program. A correct product (software) security profile cannot be confirmed in a product of poor quality, i.e., software bugs can expose unintended security weaknesses. Products' specified security profiles might be confirmed with high confidence for software products with excellent error rates.

Digital Rights Management technologies: Digital Rights Management (DRM)[150] provides methods for controlling "use, dissemination, or access to" information after the information has been distributed. In this case digital content can include, but is not limited to, video, audio, text, images, applications, or anything else that can be instantiated in digital form. In the commercial world DRM is most closely associated with technologies used to control access to copyrighted music and video. In industry DRM is being used to protect corporate information and assets.

Active Response technologies: Active response technologies provide additional tools for the network Owner/Security Manager (SM). In a strongly secured, protected, network the SM is interested in learning, in significant detail about attempts to penetrate the security perimeter. The prudent SM will make use of, for example, attractive "*honeypots*"[151] within the secure perimeter in an attempt to quantify the strength of the perimeter. In this environment any activity at the honeypot represents either a failure at the perimeter, or it represents unauthorized internal activities. Either case is cause for the SM to formulate a response.

Secure Micro-Kernel Operating Systems technologies: Multiple Independent Levels of Security (MILS)[152] operating systems represent the current and near term state of the art. MILS systems are implemented with a small (mathematically provable) kernel with additional layers providing service to partitions dedicated to each specific security level. Complete "Cross Domain Solutions" (CDS),[153] where MILS kernels are a key component, provide secure methods of managing content of different classification on the same physical platforms. The CDS environments include the concept of "guards" to control the flow of information between security domains.[154]

---

150 http://www.csulb.edu/web/journals/jecr/issues/20033/paper3.pdf

151 http://en.wikipedia.org/wiki/Honeypot

152 http://www.ois.com/images/RT_MILS_CORBA-High_Assurance_Security_for_RT_DS.pdf

153 http://enterprise.spawar.navy.mil/getfile.cfm?contentId=536

154 http://en.wikipedia.org/wiki/Multilevel_security

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.4. RELIABLE SOFTWARE TECHNOLOGY

MCTL DATA SHEET 17.4-1. ANTI-TAMPER (SOFTWARE) TECHNOLOGIES

Anti-tamper (software) technologies are those that can be used to prevent the reverse engineering of important software.

Critical Technology Parameter(s)	Having the following: 1) at least a 128-bit security for cryptographic functions; and 2) designed or modified to provide evaluated[155] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[156] of the Common Criteria (CC)[157] or equivalent (ISO/IEC 15408).[158]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specifically developed or tailored anti-tamper software tools.
Major Commercial Applications	Commercial anti-tamper applications (tools) tend to be limited to providing partial/point solutions. For example, all commercial operating systems provide access control and password management capabilities. However, there are no generally recognized standards that address these technologies.
Affordability Issues	Highly skilled software maintenance staff is required to operate and maintain the reliable commercial and military software applications for the security of the information systems during the full life cycle of the systems.
Export Control References	WA Cat 5D;[159] CCL Cat 5D002.

BACKGROUND

Tamper-proofing, (and tamper-resistance, -detection, or -responding) are terms that are usually associated with hardware security modules[160] (HSMs) and safes. In the HSM context tamper-proofing describes a physical security regime. This data sheet addresses tamper-proofing/anti-tamper technologies as applied to software applications. These technologies are applied above and beyond the basic capabilities of most operating systems to control access to a specific application.[161] Protecting algorithms, and their implementation, prevents competitors or attackers from building similar functionality at a fraction of the cost of designing it from scratch. Additionally, once an adversary steals software, it positions them with an ability to build countermeasures that will negate strategic advantages.

A range of techniques is being developed/applied to improve the tamper-resistance of software applications. These methods include: the encryption of the applications' data, encryption of the applications' executable code along with methods to decrypt the application during execution, methods of detecting and preventing execution under the control of a debug process, obfuscation of the executable code, and loadable/encrypted instruction sets. Software anti-tamper technologies are applied, during development, to make the application resistant to reverse-engineering attempts.

---

155 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

156 Ibid., p. 14.

157 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

158 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

159 The Wassenaar Arrangement and the US CCL specifically exclude items providing access to, or execution of copy protected software.

160 http://www.utimaco.de/createframes.html?http://www.utimaco.de/content_products/cs2000_eng.html

161 Execution Access technologies are described in MCTL Data Sheet 17.4-2.

MCTL DATA SHEET 17.4-2. EXECUTION ACCESS TECHNOLOGIES

These technologies limit the use of software to those sites authorized by the software owner.

Critical Technology Parameter (s)	Having the following 1) at least a 128-bit security for cryptographic functions; and 2) designed or modified to provide evaluated[162] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[163] of the Common Criteria (CC)[164] or equivalent (ISO/IEC 15408).[165]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	COTS solutions are available to address the lower threat levels.
Affordability Issues	The cost of hardware and software COTS solutions vary significantly depending on the level of protection required, the complexity of the protection, maturity and language of the code being protected, and platform support requirements.
Export Control References	WA Cat 5A;[166] CCL Cat 5B, 5D and 5E.

BACKGROUND

In the commercial world execution access technologies are focused on measures (techniques, technologies) that have been designed to ensure license compliance and/or ensure that license fees are collected. Thirty-six percent of software installed worldwide in 2003 was pirated, costing commercial software providers over $29 billion.

Industry is addressing the issue of "execution protection" through a series of alliances and standards organizations. The lead effort is under the auspices of the Trusted Computing Group (TCG).[167] However, the TCG/NGSCB is a commercial endeavor, so it may not be reasonable to expect it to provide the required protection, particularly at the higher threat levels (e.g., nation state). These efforts, primarily aimed at the Windows desktop define methods of creating a trusted platform (HW and operating system environment) that can protect applications from each other. These compartmentalized applications are held in their own "sand box,"[168] and have only tightly controlled access to system resources.

While industry efforts focus on protecting revenue flow, the U.S. Government's objective is to prevent the unauthorized distribution and exploitation of national security application software by our adversaries. One recent, major, effort is the Software Protection Initiative (SPI). SPI focuses on the protection for the huge investment in High Performance Computing (HPC) applications that are critical to the work of the DoD laboratories. The SPI program recognizes a "threat model" that describes threats to critical applications in 5 Levels. These threat levels range, at the low end, from "Script Kiddies,"[169] to the threat imposed by nation states who desire access to the technology, or who look to deny access to authorized users. Countering, or attempting to counter each threat level

---

[162] http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

[163] Ibid., p. 14.

[164] http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

[165] http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

[166] Wassenaar and the US CCL, specifically exclude items provided access to, or execution of copy protected software. In the United States such items remain controlled, to a limited number of destinations, under the provisions of 5(A/D/E)992.

[167] https://www.trustedcomputinggroup.org/home

[168] "Sand box" is a slang term for various techniques used to quarantine untrusted applications. See http://atrey.karlin.mff.cuni.cz/~pavel/dipl/eng.html

[169] http://info.astrian.net/jargon/terms/s/script_kiddies.html

involves increasing prevention costs and value (judgements). This threat/prevention cost relationship is diagramed in Figure 17.4-1.

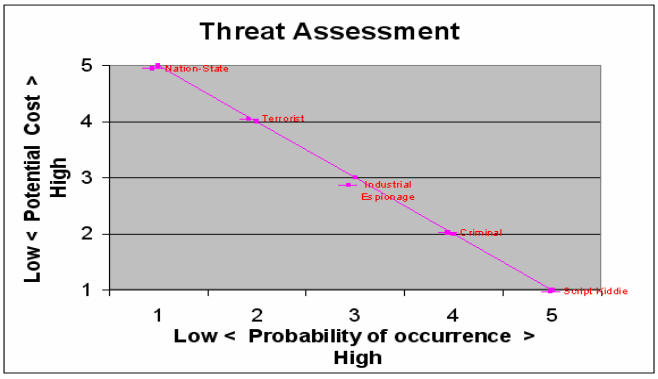

Figure 17.4-1. Network Threat Assessment
(Source: Tom Parker– Panel: Adversary Characterization and Scoring Systems, *Black Hat 2003*, Washington, DC)

Hardware-based execution access tools span the gamut from inexpensive mass-market solutions tolerating some exploitation to ultra-high security requirements that justify more burdensome costs. At one end of the spectrum, commercial suppliers provide anti-piracy "*Dongles*" that require the presence of a hardware license key to execute.[170] Protection is achieved through a series of encrypted queries to verify the Dongle is present on a USB, serial or parallel port. The Dongle returns to the calling program a numeric response used for validation. Dongles add an additional manufacturing expense of to each copy of the program and are incompatible with Internet based distribution of software.

Node locking is another hardware-based protection that commercial suppliers[171] use to restrict or lock software to a particular machine with a valid license key. Unlike Dongle-based licensing, node locking looks for a particular piece of hardware that's already built into the system[172] that will validate executing the software. A license key based on uniqueness within a particular hardware "node" is only valid on that computer and will not work anywhere else. Unique license keys are internally generated during software installation for each node based on physical properties of the CPU and motherboard, restricting operation of the software to a particular node, because each node has a distinctive key. This approach is more user friendly (as opposed to Dongles) because it does not require additional hardware, it facilitates Internet based distribution, and is unaffected by operating system upgrades and installs, disk replacements, and system utilities.

Stronger hardware-based protections use cryptographic processors[173] to off-load encryption and security functionality to a tamper-resistant dedicated processor. Specialized cryptographic electronics, along with a microprocessor, memory, and random number generator, are housed within a tamper-resistant environment to provide highly secure data processing.

---

[170] Examples of Dongle products:

Feitian Technologies Co. Ltd—Rockey: http://www.rockey.com.my/prod_dongle.htm

SafeNet—Rainbow Sentinel—SuperPro: http://www.safenet-inc.com/products/sentinel/superpro.asp

[171] Examples of node locking products:

MacroVision Inc.—FLEXlm—http://www.macrovision.com/
Agilis Software LLC—Easy Licenser: http://www.agilis-sw.com/ezlm/

[172] For example, the hard drive or Ethernet adapter serial number.

[173] Example: IBM—4758 PCI Cryptographic Coprocessor—http://www-3.ibm.com/security/cryptocards/

MCTL DATA SHEET 17.4-3. SECURE (SOFTWARE) DISTRIBUTION

Secure (software) distribution provides highly reliable distribution of software to the using organization.

Critical Technology Parameter(s)	Having the following: 1) at least a 128-bit security for cryptographic functions; and 2) designed or modified to provide evaluated[174] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[175] of the Common Criteria (CC)[176] or equivalent (ISO/IEC 15408).[177]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software for the secure distribution of software.
Major Commercial Applications	All medium to large businesses require tools to maintain their organizations servers, and desktop, configurations. These tools are unlikely to meet the security needs of DoD users involved in operational roles.
Affordability Issues	Not an issue.
Export Control References	WA Cat 5A2;[178] CCL Cat 5A2, 5B2, 5D2, and 5E2.

BACKGROUND

Traditional software distribution has been anything but secure. One possible exception has been the ability to courier software from the development organization to the users. The commercial market has not been concerned with who receives the software, but rather the concern has been the collection of licensing revenue.

The scale of the distribution is also significantly different between the commercial software market and the military. In the commercial world the developer is planning to deliver (sell licenses for the use of) thousands to millions of copies of an application product. The product delivery cycle is spread out over several months, to a few years. Many defense programs are faced with the need to distribute dozens to a few thousands of copies of an application (or an application update) in a very short period of time. For example there may be a need to have every fighter aircraft, and every AWACS in a theater receive a software update before allowing a next mission.

---

174 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

175 Ibid., p. 14.

176 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

177 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

178 Wassenaar and the U.S. CCL specifically exclude items provided access to, or execution of copy protected software. In the United States such items remain controlled, to a limited number of destinations, under the provisions of 5(A/D/E)992.

MCTL DATA SHEET 17.4-4. SOFTWARE INSPECTION AND TEST TECHNOLOGIES

Software Inspection and Test (SWIT) technologies are a key step in the development and maintenance of secure, reliable software (see Figure 17.4-2).

Critical Technology Parameter(s)	Having any of the following: 1) Software development environments and tools that are capable of producing applications programs that can be guaranteed to exactly conform to the products' specification; 2) Program proof and validation software using mathematical and analytical techniques and designed or modified for programs having more than 500,000 source code instructions; or, 3) software and/or technologies that facilitate the generation of programs exceeding 1 million source code instructions with a deployment time error rate of less than 0.05[179] errors per 1000 lines of code.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software for the development and testing of software.
Major Commercial Applications	Commercial applications are targeted to demonstrated requirements in the realm of real-time control systems such as those used in process control, power generation/distribution and automated airspace management.
Affordability Issues	Reliable software is widely considered to be expensive to develop and subject to slow operation. Significant additional research will be required to create tools to meet the critical parameter levels.
Export Control References	WA Cat 5B2, 5D2 and 5E2;[180] CCL Cat 5B002, 5D002 and 5E002.

BACKGROUND

Software quality and security are related characteristics that must be considered in the specification and development of a military program. A correct product (software) security profile cannot be confirmed in a product of poor quality, i.e., software bugs can expose unintended security weaknesses. Products' specified security profiles can be confirmed with high confidence for software products with excellent error rates.

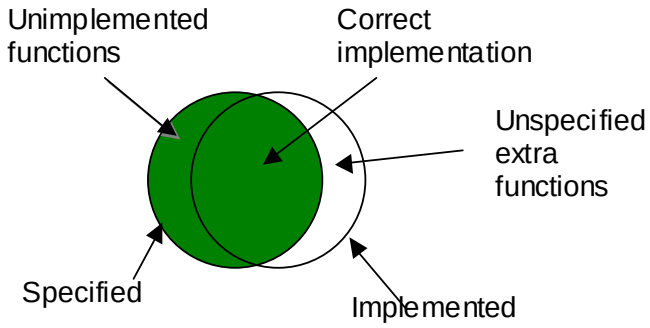

Figure 17.4-2. Inspection and Test Process

[179] The proposed critical technology level is two orders of magnitude better than today's norm. See, for example: http://panko.cba.hawaii.edu/HumanErr/ProgNorm.htm

[180] Wassenaar, and the US CCL, do not control software to test/inspect software. In the United States some such items remain controlled, to a limited number of destinations, under the provisions of 5(A/B/D/E)992.

Software defects are expensive. A recent NIST report[181] puts the cost of inadequate software testing at $59.1 billion annually.

Among the more significant software defects are software "bugs" and "malware:"

- A **software bug** (sometimes referred to as a "*glitch*") is an error, flaw, mistake, failure, or fault in a computer program that prevents it from working as intended, or produces an incorrect result. Bugs arise from mistakes and errors, made by people, in either a program's source code or its design.
- **Malware** is software designed to infiltrate or damage a computer system, without the owner's consent. The term describes the intent of the creator, rather than any particular features. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Malware should not be confused with defective software, that is, software that has a legitimate *purpose* but contains errors or bugs.

Software review-inspection technologies are intended to reduce or eliminate these errors. Quality aside there are three primary information security concerns that are rooted in programming errors. These are:

- Coding errors (bugs) in programs that are implemented according to the specification can cause a program to interfere with the protections provided by the operating systems.
- Programs can "*cache*" temporary information in "*working*" files, and/or in operating system registries. These temporary values, if not properly protected, for example by encryption, can leak information to other users of the system.
- Extra, unspecified, functions can include *Trojan code*. Trojan code is designed to surreptitiously extend the intended (specified) function of the program so as to subvert the systems' security.

[181] http://www.nist.gov/public_affairs/releases/n02-10.htm NIST report:http://www.nist.gov/director/prog-ofc/report02-3.pdf

MCTL DATA SHEET 17.4-5. DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (DRM) technologies provide mechanisms for the owner of an electronic item (document) to control permission to view/use the item.

Critical Technology Parameter(s)	DRM hardware/software having either of the following: 1) at least a 128-bit security for cryptographic functions; or 2) designed or modified to provide evaluated[182] information security, or user isolation, at a level equal to or exceeding class EAL 4 (Evaluation Assurance Level)[183] of the Common Criteria (CC)[184] or equivalent (ISO/IEC 15408).[185]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software for the secure storage, distribution, and authorization to use protected files.
Major Commercial Applications	Content Scrambling Systems (CSS),[186] Digital Library Systems (DLS).[187]
Affordability Issues	Early implements are likely to experience high startup costs because there are not yet any COTS DRM offerings at the required parameter level.
Export Control References	WA Cat 5-2;[188] CCL Cat 5(A/B/D/E)002.

BACKGROUND

Digital Rights Management (DRM) provides methods for controlling "use/dissemination/ or access to" information after the information has been distributed. In this case digital content can include, but is not limited to, video, audio, text, images, applications, or anything else that can be instantiated in digital form. In the commercial world DRM is most closely associated with technologies used to control access to copyrighted music and video. In industry DRM is being used to protect corporate information and assets.

The use of DRM for the control of entertainment media has resulted in huge debates. The content providers are searching for a way to enforce a revenue collection process on a set of consumers who may have been too casual about their use of unprotected, but copyrighted material. The technical side of the debate centers on the use of a non-public encryption algorithm called the Content Scrambling System (CSS), and the widely available tool (DeCSS)[189] that can be used to decrypt those (protected) DVDs. The debate, and the concerns, extend beyond CSS, and include similar problems with Adobe eBooks and other media. It is interesting that several big-name companies have failed miserably in the DRM marketplace. The following quote summarizes the current state of affairs.

---

182 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

183 Ibid., p. 14.

184 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

185 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

186 http://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

187 Example commercial product; http://www.contentreserve.com/

188 Wassenaar and the US CCL specifically exclude items provided access to, or execution of copy protected software. In the United States such items remain controlled, to a limited number of destinations, under the provisions of 5(A/B/D/E)992.

189 DeCSS (to decrypt CSS protected media; Anthology); http://www.cs.cmu.edu/~dst/DeCSS/Gallery/

> "*Unfortunately---or fortunately, depending on your perspective---the level of persistent protection provided by most DRM systems appears to lie somewhere between incredibly weak and really pathetic*."[190]

The technical problems with the CSS implementation of DRM in the DVD industry do not, in themselves, limit the potential usefulness of a different DRM solution. More secure, robust, DRM solutions are possible. Highly secure DRM implementations may require "anti-tamper" elements.[191] A fundamental problem in DRM is that the legitimate recipient is a potential attacker.

Digital assets management (DAM)[192] solutions/products, sometimes known as information rights management (IRM),[193] are focused on protection of information within the originating organization. These technologies are also known as "enterprise DRM."[194] As a result of their narrower scope and greater local control these solutions may be more effective. This is not really a technical issue. Instead, it is due to the fact that in an enterprise setting, the legal and enforcement side of the equation are more enforceable (a person could get fired, sued, etc.).

---

190 Dr. Mark Stamp in "ExtreamTech" at http://www.extremetech.com/article2/0,3973,1051610,00.asp

191 See MCTL Data Sheet 17.4-1.

192 Example product: http://www.authentica.com/products/securedocs.aspx

193 Example, in Microsoft Office: http://www.microsoft.com/office/editions/prodinfo/technologies/irm.mspx

194 http://www.drmwatch.com/special/article.php/3519841

MCTL DATA SHEET 17.4-6. ACTIVE RESPONSE TECHNOLOGIES

Active response technologies put the network owner and security team on the offense.

Critical Technology Parameter(s)	Active response hardware and software having both of the following: 1) at least a 128-bit security for cryptographic functions; and 2) designed or modified to provide evaluated[195] information security, or user isolation, at a level equal to or exceeding class EAL-5 (Evaluation Assurance Level)[196] of the Common Criteria (CC)[197] or equivalent (ISO/IEC 15408).[198]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software for the development and test of active response tools and technologies.
Major Commercial Applications	Commercial tool availability is limited at this time.
Affordability Issues	Early implements are likely to experience high startup costs because there are not yet any COTS offerings at the required parameter level.
Export Control References	WA Cat 5-2;[199] CCL Cat 5(A/B/D/E).

BACKGROUND

Researchers, network intelligence organizations, and organizations creating firewall/IDS filters, will create lightly defended networks populated with honeypots and "tar pits"[200] in order to gain insight into penetration methods and techniques. These organizations may also develop and deploy "worm followers" so as to learn the source of an attack and to generate counter-attacks. Network traffic analysis[201] is another tool that can be useful in understanding when/if an attack is underway.

Tools such as honeypots and tar pits present an attractive target and wait for a probe. An alternative strategy is to initiate your own probe, and actively seek out network sites that may be preparing to attack your assets. One example of this type of tool is the "HoneyMonkey"[202]which is used to probe for malformed and malicious code in web pages, but it could be customized to search for other types of data.

When the security manager recognizes that an attack is in process the next step (after blocking the attack) is to identify the attack source. The major problem that must be solved in the trace process is that the attacker will have taken steps to disguise their own network (source) address. Attacks may be coming from compromised "victim" intermediary systems.[203]

---

195 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

196 Ibid., p. 14.

197 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

198 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

199 Wassenaar and the US CCL specifically exclude items provided access to, or execution of copy protected software. In the U.S. such items remain controlled, to a limited number of destinations, under the provisions of 5(A/B/D/E)992.

200 http://en.wikipedia.org/wiki/Tarpit_%28computing%29

201 An example commercial traffic analysis tool is "StealthWatch." See http://www.lancope.com/products/

202 http://en.wikipedia.org/wiki/Honeymonkey

203 http://www.cisco.com/warp/public/707/22.html#tracing

Striking back, at an attacking system, can involve ethical questions. It is entirely legal and ethical to employ a honeypot in order to learn about a probe of your own network. The questions begin, at the 4th bullet, when the security manager employs an active defense against outsiders. For example,

- Blocking the IP address of an attacker at your gateway;
- Slowing an attack by the use of a tar pit that forces the attacking system to break each packet to a very short length, and then delaying acknowledgement of each packet until it must be retransmitted many times;
- Asking your ISP to block all packets originating at an attacking system;
- Reversing the attack so as to flood the attacking system with your own denial of service flood. The attacking system may itself be an unwitting contributor to the attack, having been previously compromised by the actual attacker;
- Force a shutdown of a remote system via network commands; and
- Tracking down, and physically visiting an attacker.

MCTL DATA SHEET 17.4-7. SECURE MICRO-KERNEL OPERATING SYSTEMS (MILS)

MILS operating systems are the major component of cross domain solutions (CDS), allowing the isolation of information, of more than one classification level, residing on a single computer.

Critical Technology Parameter(s)	Having either of the following: 1) at least a 128-bit security for cryptographic functions; or 2) designed or modified to provide evaluated[204] information security, or user isolation, at a level equal to or exceeding class EAL 5 (Evaluation Assurance Level)[205] of the Common Criteria (CC)[206] or equivalent (ISO/IEC 15408).[207] EAL 6 is required for CDS.[208]
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software for creating proofs of other software.
Major Commercial Applications	MILS is specified for the computers in the Boeing 787.[209]
Affordability Issues	MILS operating systems (kernels) are just becoming available from COTS sources.
Export Control References	WA ML 11; WA Cat 5E2; USML XI and XIII;[210] CCL Cat 5E002.

BACKGROUND

Military operations have a requirement for both protecting and sharing classified information. Most operations include information that is classified at various levels, and that information needs to be made available only to those users who have suitable clearances, and the "need to know." The management of the classification and distribution of classified information by traditional (paper based) methods is slow and complex.

> *"In the DoD, a system's security operations are characterized according to minimum user clearances and the maximum security levels of data either processed or transferred by the systems. According to these characteristics, the DoD defines the following four modes of operation:*
>
> - Dedicated;
> - System high;
> - Partitioned (or compartmented); and

---

204 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

205 Ibid., p. 14.

206 http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

207 http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip

208 http://enterprise.spawar.navy.mil/getfile.cfm?contentId=536 at slides 9 and 14.

209 Green Hills Software Inc., http://www.ghs.com/news/20050706_honeywell.html claims their INTEGRITY (Real-Time) operating system is the only commercial operating system that was designed from day one to meet the EAL 7 level. They claim this product has been selected for the Boeing 787 due to its security capabilities. This product is listed as being "under test" by the Common Criteria (CC) for certification at level EAL 6+.

210 Cryptography, cryptographic devices and technical data regarding them are subject to Federal export controls, unless exempt.

- Multilevel.

  Restrictions on the user clearance levels, formal authorization requirements (i.e., for access to special access programs, compartmented information, and other close-hold data), need-to-know requirements, and the range of sensitive information permitted on the system are inherent in each of these security modes"[211]

The first three of these methods (above) have been available for many years, with "partitioned" or "compartmented mode workstations" (CMW) available from COTS sources since the middle 1980s. "Trusted operating systems" with CC evaluations to level EAL 4 are available from a number of vendors.[212]

MILS[213] (Multiple Independent Levels of Security)[214] operating systems represent the current near term (less than five years) state of the art. MILS systems are implemented with a small (mathematically provable) kernel with additional layers providing service to partitions dedicated to each specific security level. Complete CDS,[215] where MILS kernels are a key component, provide secure methods of managing content of different classification on the same physical platforms. The CDS environments include the concept of "*guards*" to control the flow of information between security domains.[216]

---

[211] "Multilevel Security in the Department Of Defense: The Basics." See http://nsi.org/Library/Compsec/sec3.html at Section 3.1.

[212] List of CC evaluated operating systems: http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#operatingsystem

[213] MILS is sometimes referred to as MSL (Multiple Security Levels).

[214] An overview of a MILS implementation can be found at: http://www.ois.com/images/RT_MILS_CORBA-High_Assurance_Security_for_RT_DS.pdf. A technical paper on MILS can be found at: http://www.stsc.hill.af.mil/crosstalk/2005/08/0508Vanfleet_etal.pdf

[215] http://enterprise.spawar.navy.mil/getfile.cfm?contentId=536

[216] http://en.wikipedia.org/wiki/Multilevel_security