Tactical Military Encryption in a Multinational Environment

Background

Tactical forces always have been faced with the protecting of critical, sensitive, or classified information. In modern warfare, an increasing amount of information is digital. The tactical requirement for media protection through encryption differs from a non-tactical situation in two primary areas. First, the information stored in tactical equipment is often very perishable or time sensitive. That is, after a period of time, the utility of the information expires, and it no longer requires protection. Although this is not true for all tactical data, typically the media encryption needs to be only good enough to prevent the enemy from breaking the encryption within a short period (days to weeks). Also, tactical users often require extremely fast (near real time) media encryption. The media encryption process should be transparent to the tactical user, allowing the user to control the process in real -time, and quickly protect the information in a time of crisis.

Multinational operations in which U.S. tactical forces are involved have increased dramatically. Reusing encryption equipment that requires declassifying before it can be given to multinational forces takes considerable time to complete. With today's limited budgets, U.S. forces do not have the luxury of purchasing multiple sets of systems for each level of classification, as a specific system could apply to a specific international force. Security techniques such as tamper-proof cryptography, programmable cryptographic chips that can erase keys and algorithms, over-the-air key load, and zeroize functions have been used. The Electronic Key Management System (EKMS) delivers a black key from the Central Facility to a local key distribution device, but the transfer of keys to lower echelon levels is still performed by a soldier carrying a key fill device, full of red keys. (Reference: Information Assurance Technical Framework (IATF) - Framework release 3.1)

A New Security Technique

A new direction for implementing encryption within the tactical multinational environment can be added to the existing security techniques. By combining Department of Defense (DoD) Information Systems Security Organization (ISSO) and the Department of Commerce oversight of two existing programs, the concern over loss of encryption devices in a tactical situation can be addressed while maintaining a balance between security techniques and the exploitation of these techniques against the US. These two existing programs are concerned with Levels of Robustness and Export Approvals for security products and technologies.

New technologies in key management and access control can be extended into existing security techniques resulting in reaching a balance and in achieving a distribution process that can be

extended to the lower echelon levels. Also, the combination of the two agencies oversight would address the concern over what level of security assurance is mapped into tactical multinational environments. The suggested new direction combines the Department of Commerce Export Approval with a DoD Robustness Level for commercial encryption products.

Export Approval

Commercial encryption products that are to be sold and used outside of the United States must conform to the export regulations managed by the Department of Commerce. The National Security Agency (NSA) also has a role in the export licensing process. The process offers an opportunity for these agencies to determine if there is technology that should not be exported, but controlled within the US. The size of encryption key lengths within certain usages is an example of the extent of regulatory oversight. From this perspective, national security is viewed through what is established as specific technologies that would be detrimental to the national defense and need to be controlled through the export regulations. Encryption has always been regulated, not only by the US, but also by most all other nations that use encryption.

DoD Robustness Levels

A Robustness Level establishes a level of security assurance to address different levels of threats, different levels of vulnerabilities, and a countermeasure valuation scheme for an Information Systems Security (INFOSEC) solution. The strategy of robustness levels deals primarily with the levels within individual security services and mechanisms, based upon information on a given value in a particular threat environment. The intent of establishing Robustness Levels is to apply an enhanced level of assurance to commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and hybrid solutions.

A series of matrices have been developed through the Information Assurance Technical Framework (IATF) to establish a measure for Robustness. The degree of Robustness consists of different references such as the value of the information, the potential threat level, and the strength of the security mechanism, including an effective encryption key length and associated key management. The multinational tactical environment can be summed up in a Basic Robustness level. Of course, the tactical environment in itself also includes Secret and Below Interoperability (SABI) and Top Secret and Below Interoperability (TSABI). Since the tactical situation tends to be fluid, different Robustness levels may be in order for SABI and a more traditional high -grade encryption level such as Type 1 may be required for TSABI.

Encryption can be a further leveraging technology within Robustness levels itself. Establishing an effective key length for the symmetric key (used for encrypting the data) at 256 bits presents a high work factor to the enemy that would have to be applied to perishable tactical information. If the encryption paradigm were shifted to protecting the content as it is manifested in information, the changing mathematics of a random value that is integral to an encryption process would add another dimension to the work factor.

There are choices today to apply the encryption paradigm. Encryption can be included as a protection enhancement to a communications channel such as a Virtual Private Network (VPN) or a protection mechanism with an Internet protocol such as Secure Sockets Layer (SSL). Encryption may also be bound to the virtual object. Encryption can be a black box that is put on

Copyright 2014
All Rights Reserved

either end of a communications link, or encryption can be server controlled for multiple links, or encryption can be part of the users experience for instance, bound to a file. In addition to providing Confidentiality (normally associated with encryption), it can be also used for enhancing identity and access control techniques. The work factor associated with encryption can be further enhanced by a system integration of multiple encryption techniques.

Of course, encryption cannot be effective without key management. The secrecy of the key must be maintained in a management cycle that extends from its formation to its destruction, and during all of its intermediate usage steps.

Robustness Levels and Export Approvals are effective tools for measuring a role for encryption within a national security environment. Whether a commercial or government solution, there are other factors that must be considered. Standards, for instance, provide a peer acceptance within an industry or a group of industries that can be seen as establishing an assurance level from a different perspective of Robustness or Export, per se. The financial sector in the US has emerged with the largest portfolio of encryption standards. Their intent is to maintain the encryption tools that would be needed to protect the economic infrastructure of the US. The encryption algorithms, encryption frameworks, and key management designs defined in the financial sector are mere mirrors of the encryption techniques seen in defense.

A New Framework for Combining Robustness and Export

From the financial standards has emerged an encryption framework that includes a cross section of the mathematics of asymmetric algorithms, symmetric algorithms, and hash functions to create an Authorization capability enforced by encryption. The framework includes a key management administrative model that can be a complement to the Public Key Infrastructure (PKI) architecture while differentiating PKI for Authentication and this framework for Authorization.

The financial standard for this framework is found in ANSI x9.69 and ANSI x9.73 and is called Constructive Key Management® (CKM®). The Authorization encryption paradigm found in CKM draws on Persistent Tagging that is associated with information flow and control. (Ref: Persistent Tagging Enforced through Encryption, a white paper, June 16, 2010).

Authorization is effected through a binding of roles, rules, or other tagging methodologies with an asymmetric algorithm that further can separate access to information for read or write permissions. The combination of these permissions with other encryption algorithms can result in an encryption paradigm for Confidentiality of the communications channel or the virtual object. Also, the combination establishes an information sharing and collaboration capability that can take on virtual nesting properties (a virtual object can be encrypted within another virtual object and the nature of the encryption paradigm results in a demonstration of data entities being separated through encryption).

CKM® can be applied to the tactical environment through various communications or computing protocols. It can be manifested in various Robustness models including Basic Robustness and brought in line with current US export regulations. The selection of the combination of algorithms can be designed to address the other multinational operations issues.

Copyright 2014
All Rights Reserved