Chapter VI

Cryptography: Protecting Confidentiality, Integrity and Availability of Data

Henry B. Wolfe
University of Otago, New Zealand

The protection of information for business or private purposes can be achieved through the careful selection and use of cryptographic tools. Throughout recorded history the art and science of cryptography has been the exclusive domain of government in the form of military and diplomatic use. For the most part the many and varied techniques were used for protecting strategic communications. With the advent of the microcomputer the tools to incorporate some of the complex mathematical tools necessary to provide strong encryption became readily available to the public at large. That availability has contributed to the proliferation and use of cryptographic tools that are capable of providing strong encryption to anyone who would care to use them. This important security technique has become the main tool for protecting communications of all kinds and is used throughout the business community. The banking community, for example, is probably one of the largest users of data encryption for the protection of their clients’ financial transactions.
INTERNATIONAL ISSUES - IMPORT, EXPORT AND USAGE

The Rationale for Cryptographic Restrictions

The use of data encryption is controlled, regulated or outlawed in some nations. The reason for this approach to the use of cryptography is to prevent the citizens of these nations from having the ability to communicate privately and/or from having the ability to store private information in a way that cannot easily be inspected in real time and without the knowledge of the originator. Nations who take this approach tend to be dictatorial in nature, however, many of the so-called free world nations are beginning to be concerned with the use of data encryption by their citizens.

Much of the concern in the “free” world is centered around the notion that the “bad” guys will use this tool to help them accomplish bad things. Emotional issues like child pornography, terrorism, drug dealing, etc are used to justify the proposition that no one (except government) should be able to communicate in a totally secure way. Further that government, specifically law enforcement and/or intelligence, should be able not only to intercept any communications but also be able to decode any encrypted communications as well. The important part of this proposition is that they declare that they need to be able to do all this without notification or cooperation from the parties to the communication in order to “protect” or “defend” their citizens or for “national security”.

The one issue that those who would take the restrictive position on cryptography have consistently failed to address adequately is that of some sort of proven linkage between being a “bad” guy and being stupid. No matter what restrictions may be put in place to prevent the use of strong encryption, it is inevitable that the “bad” guys will not obey them. No thinking person should be hoodwinked into believing that the “bad” guys would be stupid enough not to use freely available strong encryption to protect their privacy. The realities are that they will and do use strong encryption.

The advent of the Internet has changed the way we look at national boundaries. In fact in cyberspace there are no enforceable national boundaries (other than being cut off from the Internet completely). This means that Internet users can transmit all sorts of
Related Content

A Host-Based Intrusion Detection System Using Architectural Features to Improve Sophisticated Denial-of-Service Attack Detections
Ran Tao, Li Yang, Lu Peng and Bin Li (2010). International Journal of Information Security and Privacy (pp. 18-31).
www.igi-global.com/article/host-based-intrusion-detection-system/43055?camid=4v1a

A Semi-fragile Image Watermarking using Wavelet Inter Coefficient Relations
www.igi-global.com/article/semi-fragile-image-watermarking-using/2467?camid=4v1a

Risk of Contract Growth and Opportunistic Behavior: A Comparison of Two Megaprojects
www.igi-global.com/article/risk-contract-growth-opportunistic-behavior/70233?camid=4v1a

www.igi-global.com/chapter/encryption-decryption/66333?camid=4v1a