CRYPTO 81, IEEE Workshop on Communications Security,
University of California, Santa Barbara, August 23-26, 1981.

ABSTRACT -

Current Market: Products, Costs, Trends

by
J. Michael Nye, President
Marketing Consultants International, Inc.
Hagerstown, Maryland
(301) 791-0290

In the short time available, I would like to make a few comments about the relative status of the current cryptography market from the vendors/users perspective. For the most part this conference has dealt with the technical aspects of cryptography in the development of algorithms and key management schemes. On the other hand, I will be concentrating on the current situation in the marketplace with respect to vendors/products, application trends and issues, and the promise of the future with respect to this rapidly expanding marketplace.

Most of my comments are based on the results of a recent book we published entitled "Who, What, & Where in Communications Security". The purpose of this publication was to take this complex subject and attempt to describe the important issues concerning it in a non-technical manner so that a typical user may more clearly understand the basic fundamentals of cryptography along with detailed information about the wide variety of currently available products.

We have identified more than 35 major domestic and foreign vendors offering in excess of 180 different products. These products provide communications protection in such diverse technologies as analog scramblers, narrowband digital voice encryption (normal telephone calls), wideband digital voice encryption (radio communications), data communications security, and facsimile security. In spite of such a wide product range, most domestic vendors of this equipment are struggling to maintain their presence in this industry. In fact, some have already

withdrawn good products from the market due to lack of sufficient sales activity.

From my point of view, there are several significant "road blocks" in the rapid expansion of this industry:

1. Almost all products are stand alone with prices ranging from several thousand dollars per "black box" to prices approaching $20,000 each. For a customer to adequately protect at least one data channel it could cost as much as $40,000.

2. Most domestic vendors have a limited product mix. This is due primarily because of the relative immaturity of the domestic market place. For example, most of the non-domestic vendors offer products in a variety of technological areas including scrambling to digital facsimile protection. Such diverse product mixes assist in offering interoperability for mixed application requirements for many users. Unfortunately, most domestic vendors offer only a single product type, whether it be a data encryption device or analog scrambler, but not a mix of products across a wide application range.

3. There is a significant lack of user awareness to the problems of electronic interception or the vulnerabilities of the existing communications network. It is reasonably simple to physically tap communication lines, intercept RF communications with low cost scanner technologies readily available and, the ability to intercept microwave communications has been demonstrated to be possible for only a few thousand dollars. Furthermore, the rapid expansion of mini/microcomputer technology has created an environment for passive or active electronic interception with particular vulnerability to dial-up networks.

There have been some "half-hearted" attempts to educate the user group through press coverage of major criminal activity or coverage in the technical press. However, it is difficult to convince users to acquire cryptographic equipment when the equipment itself may cost several times more than the equipment the

encryption device is to protect. For example, how do you convince a customer who spends $1,200 for an analog fax machine to add on a sophisticated scrambler which sells for at least $5,000.

In some sense, the scientific communities debate on the Data Encryption Standard (DES) has been counterproductive in the user groups. The unfortunate, extensive press coverage of the DES debate concerning its weaknesses to determined attack has given the reader the opinion that the DES is of no value, therefore, the customer does nothing.

In spite of the slow sales success of existing products, there are trends in the industry that are substantially increasing the need for user education into the vulnerability issues and the available technologies for protection. Specifically, there is a virtual explosion of new equipment in the automated office. Information previously "safely" stored in filing cabinets, binders, notepads, and desk drawers, are now being organized, recorded on electronic media, and processed in the modern office with such devices as word processors, text editors, distributed data processors, and so on. Other rapidly expanding technologies include information distributors (copy machines that communicate), a facsimile network approaching 500,000 units, teleconferencing, electronic mail, voice mail, store and forward, and who knows what new technologies will be available tommorrow. All of these technologies are equally vulnerable to interception when commuicating over the phone line. It seems unlikely that many of these new technologies, particulary teleconferencing and electronic mail, will obtain much success without first resolving the communication security issue.

Currently, about $30 billion is spent annually on voice and data communications services. Businessweek projects this figure to increase to $150 billion by 1990. It has been estimated that there are more than 1 million personal computers already installed in the domestic market with aggressive projections expected over the next few years. Some estimate that as much as $3 billion annually is lost through electronic thievery. The expanding finanical and technical resource capabilities of terrorist organizations, represent an increasing threat to the economic stability of the financial and business community.

There are a number of programs that should be instituted immediately that will be a step in the right direction in solving some of these vulnerability problems. In particular, a comprehensive education program should be instituted by the government, academic, and private sectors that will educate the user to the vulnerability issues. More importantly, we must educate the manufacturer of communications equipment by encouraging the inclusion of cryptographic options built into the primary product. The value added feature of cryptographic options to existing communications equipment can substantially reduce the cost of such options to the user without materially impacting the cost of the manufacture of the original product itself.

There needs to be a more clear definition of the type of information that should be protected in relation to the perceived threats. For example, the most common threat to industry and civil government is the casual or inadvertent release of information caused by such phenomenon as "cross talk" in voice conversations or pure transmission mistakes. Other threats include motivated students, revengeful employees, security consultants or market researchers (industrial espionage), and organized crime. Obviously there are other groups of vulnerability which have reasonable financial and technical resources along with the motivation for interception and counterfeiting of traffic. It is reasonable to assume that DES or DES-like crypto systems can adequately provide protection for these threats.

It is strongly recommended that the scientific community "cool it" on the debate on how secure is secure specifically with the DES. For example, secure from whom. The relative arguement against the level of protection offered by DES may be valid only if the perceived threat is the NSA, KGB, or the GRU. For that matter, any publicly available crytographic system is probably not strong enough to protect against the sophistication of these threats if these organizations are determined to intercept traffic. However, a DES system can make it quite expensive for them, suggesting that other less expensive methods of information gathering will be used which increases the possibility of detection.

DOMESTIC VENDORS
(MAR 81)

© Marketing Consultants International, Inc.

Vendor	Products	VS-A	VE-N	VE-W	DE	FAX-A	FAX-D
American Satellite Corp.	1				1		
Boeing Aerospace Company	1	1					
Burroughs	1				1		
Codex Corporation	2		1		1		
Collins Telecommunications	5	3	1		1		
Com/Tech	2				2		(2)*
Controlonics	16	16					
Datotek	13	4		1	7	1	(1)
Fairchild Electronics Co.	1				1		
GTE Sylvania	2		1	1			
Harris CCSD	1		1				
Harris RF	6			6			
IBM	2				2		
Lear Siegler	1	1					
Mieco	12	12					
Motorola, Inc.	7	1		6			
Motorola, Inc. (Government)	1				1		(1)
Ocean Technology	2	1		1			
Racal-Milgo	1				1		
Rapicom	3						3
Scientific Radio	1	1					
SPI Data Systems	2				2		
Technical Communications Corp.	10	5			3		2(2)
Summary: Products - 93 Vendors - 23		45	4	15	23	1	5(6)

NON-DOMESTIC VENDORS
(MAR 81)

© Marketing Consultants International, Inc.

Vendor	Products	VS-A	VE-N	VE-W	DE	FAX-A	FAX-D
AB Transvertex	6		1	2	3		
AEG Telefunken	5		1		4		(2)*
BBC Brown Boveri	10	7	1	1	1		(1)
Crypto AG	13	2	1	2	8		
Gretag	13	2	2		9		(1)
Marconi C&B	1	1					
Marconi S&D	8	1	2	1	3		1
Merck & Hollander	1				1		
Miller Comm. Ltd.	1	1					
Racal-Datacom	12	6		1	5		
Tadiran	3		1	1	1		
Telsy	6	6					
Summary: Products - 79 Vendors - 12		26	9	8	35	0	1(4)

*()Indicates that these products are listed in other product areas as their primary application but that they can also be used to protect FAX transmissions.