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

ABSTRACT -

THE IMPORT/EXPORT DILEMMA

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

In compiling information for our recently published book, "Who, What, & Where in Communications Security" we encountered some rather intriguing aspects of our government's policy (or the lack of policy) with respect to the import/exportation of cryptographic equipment. After talking to most of the major foreign suppliers of communications security equipment, it appears that these vendors enjoy higher sales volumes in the U.S. domestic market than do our own manufacturers. Even though domestic vendors are experiencing difficulty in achieving respectable sales levels in the domestic market, foreign vendors see the U. S. market as huge. Many have expressed interest in acquiring Data Encryption Standard (DES) chips to include this algorithm in their equipment for import into the United States. Unfortunately, due to restrictive government regulations, DES hardware is not approved for export without specifically obtaining a license which is not normally granted to offshore manufacturers of products. Licenses are normally granted for the specific use application and not for incorporation into other non-domestic products.

This situation severely hampers domestic manufacturer sales activities particularly in international business. Specifically, ITAR Restrictions as defined in Title 22 - Code of Federal Regulations, Parts 121 - 128 require that a license be granted for export of all cryptographic equipment including the DES. What is interesting about this is that the DES algorithm has been published for several years now in well documented publications provided by the U.S. Department of Commerce.

Another interesting aspect of the export business is that many foreign countries require that the cryptographic key be given to responsible government authority as a condition for the importation of cryptographic equipment. However, foreign cryptographic equipment can be easily imported into the United States often escaping any specific identification of it being cryptographic equipment. There is no organized program in the federal government to regularly track the types of cryptographic equipment imported into this country or its application uses.

The restrictive export requirements combined with very loose or non-existant import regulations regarding cryptographic equipment places U.S. manufacturers at an extreme disadvantage in the marketplace. In one sense, an agency of the U.S. government is encouraging the development and use of DES based systems as a cryptographic standard in the future for non-classified communications. Such a standard is sorely needed in order to ensure the orderly growth of communications security systems while maintaining interoperability. On the other hand, other government agencies are in the business to discourage the international use of DES based systems by restricting the export of DES chips to be incorporated into foreign manufactured communications security equipment.

Put yourself in the position of a telecommunications manager designing an international, multi-million dollar communications network. In order to provide communications security for this network there may be an unacceptable risk to include U.S. manufactured cryptographic equipment because of the possibility of not being able to obtain the appropriate license for export. Consequently, telecommunications managers are encouraged, for that matter almost pressured, into designing a communications system that excludes domestic cryptographic equipment.

I have trouble understanding why one agency of the federal government can publish specific operating details of a cryptographic algorithm while another agency withholds the exportation of implemented hardware of cryptographic devices that have widely published algorithms. Perhaps we have developed a unique approach to cryptographic hardware. After all, who's to say we can manufacture the best crypto equipment when for a long time now the Swiss, Germans, and English have had to cope with active terrorist activity and concentrated esponiage activity. It is reasonable to assume that these vendors have developed adequate technology to protect against the bulk of the perceived threats of

terrorist and limited resource industrial espionage. One of the biggest U.S. corporations, International Telephone & Telegraph, has been for years rountinely encrypting all data communication messages of any significance between all offices, divisions, and company organizations domestic and international. This encryption is provided by equipment manufactured in Sweden.

I believe there are a number of remedies that can be instituted to change this situation. In particular, we must have a national cryptographic policy with respect to the protection of non-classified communications. This policy should deal with both the import and exportation of crytographic equipment. Additional research should be encouraged in the public key area since it appears that public key offers the best alternative to resolving the troublesome key management problems of existing equipment. At the same time, there should be the development of other technologies or techniques for key management that would allow for true cryptographic communication standardization, while at the same time allowing interoperability.

We need a more realistic policy with respect to the exportation of DES hardware. For example, there has been considerable debate in the scientific community about the potential weaknesses of the DES algorithm. Obviously, publishing the algorithm while not allowing the general exportation of hardware appears suspicious to many users and adds fuel to the speculation that the hardware implementation of DES contains some unique trapdoor weakness. For the short range we need to keep track or require registration of all imported cryptographic equipment in order to measure how well non-domestic vendors are doing in the U.S. market. At best, we should be able to measure why foreign equipment is selected over domestic equipment and determine what impact government regulation has on these selection criterias. Finally, we need an intensified education program of specifically targeted multi-national organizations to acquaint them with the problems and vulnerabilities of transborder data flow.