Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard

United States Senate Select Committee on Intelligence

The appropriate committees of Congress should address the question of public cryptology by clarifying the role which the federal government should have in policies affecting public cryptology.

INTRODUCTION

The Senate Select Committee on Intelligence recently completed a classified study concerning allegations that the National Security Agency (NSA) was improperly involved in the development of a Data Encryption Standard (DES). The DES resulted from efforts of the National Bureau of Standards (NBS) to certify a single DES to be used for all government nonclassified data.

The interest of the Committee stems from its oversight responsibility for NSA and as a result of several allegations made about NSA harassment of scientists working in the field of public cryptology. The classified study, undertaken late in 1977, is based on interviews with both public and private scientists and engineers, including representatives of the following government agencies, private companies, and professional associations: NSA, NBS, the National Science Foundation (NSF), the Department of Defense (DOD), International Business Machines (IBM), and the Institute of Electrical and Electronics Engineers (IEEE). Over 200 pages of private and public papers and documents were also analyzed.

BACKGROUND

Two developments caused the NBS to begin a search for a process which they could propose as a federal standard to be used for all government nonclassified data stored and transmitted by computer. One was the Brooks Act of 1965 which gave NBS the responsibility to create standards which would govern the purchase and use of computers for the federal government. The second, a general movement which culminated in the Privacy Act of 1974, was an attempt to keep confidential and secure all data on U.S. citizens in the possession of the government.

In 1968, the head of the NBS Institute for Computer Science and Technology initiated several studies assessing the need for computer security within the government. As a result of the studies, the NBS decided to foster the development and establishment of a government-wide standard for encryption devices which would offer adequate security for unclassified government data. NBS also decided that the best encryption method would be the use of an encryption algorithm.[1]

Knowing of NSA's experience and expertise in the field of cryptology, NBS officials made contact with NSA and, among other things, asked for NSA's assistance in evaluating the quality of a DES algorithm.

NBS issued a federal solicitation through the *Federal Register* of May 1973 encouraging interested developers

The Senate Select Committee on Intelligence is chaired by Senator Birch Bayh (Indiana). U.S. Senate, Washington DC 20510.

This summary of the committee's investigation was released to Dr. N.D. Pundit, IEEE Director of Technical Activities, on April 13, 1978.

[1] An algorithm consists of rules of procedure which are used to solve complex mathematical problems, most commonly those with frequent repetitive operations. In cryptology an algorithm is used to transform plaintext data into encrypted data by using rules of procedure so complicated that decryption is unlikely without knowing the algorithm or rules of procedure through which the plaintext was encrypted. This process requires a key which governs encryption and decryption.

to submit possible algorithms for consideration as the DES. That solicitation evoked few responses and a second solicitation was issued in August 1974. IBM, having had some experience with encryption algorithms used in a secure cash transaction system they had marketed a few years earlier, responded with an algorithm to be considered for the DES.

NBS, in consultation with NSA, judged the IBM algorithm to be the best of those submitted and NBS decided that the IBM formula would become the government DES. Before this was announced, however, some private computer scientists and engineers who had been developing their own encryption systems, expressed concerns about the strength of that algorithm and the process through which the IBM algorithm had been chosen.

As a result of those concerns, NBS sponsored two workshops on DES at which many related issues were discussed. At the first workshop (August 1976) the practicality and economic feasibility of constructing a special-purpose computer to attack the DES through a brute force or exhaustion attack was discussed.[2] Several estimates of the time and cost involved in such an effort were discussed at the workshop. NBS officials said that with their existing machinery, a brute force attack would take 17 000 years. The participants disagreed over the cost, development time, and exhaustion time necessary to construct special-purpose computer equipment designed to attack the DES. The majority of those present suggested ranges of 2–10 years for construction of equipment which would exhaust the DES—over a 6 month to 10 year period of time at a construction cost of $10 to $12 million dollars. One scientist argued that, given rapidly changing technology, it would be possible by 1990 to construct a special-purpose, parallel chip machine for $72 million which could exhaust all possible alternatives within one day.

The second workshop (September 1977) dealt with the mathematical and statistical characteristics of the DES. The conclusion of the workshop was that the DES was a sound algorithm. Concerns were expressed, however, at this workshop that it was not possible to assess all of the characteristics of the DES since IBM had not been willing to share all of the design criteria used in the creation of the DES. IBM replied that in the testing of their algorithms by NSA, certain information was learned which was sensitive and that NSA requested that information not be discussed publicly.

Public attention was called to the DES and related cryptologic developments because of a simmering scientific argument being conducted through some scientific magazines and because of the publicity given a July 1977 letter from Mr. J. A. Meyer to Mr. E. K. Gannett, Secretary of the IEEE Publications Board. The Meyer letter pointed to the possibility that some of the discussions and publications of members of IEEE's Information Theory Group might be in violation of U.S. export regulations relating to cryptanalytic equipment and information. The letter was circulated to members of the Information Theory Group without comment by Mr. Gannett. Copies of the letter were obtained by the press and stories were written alleging Mr. Meyer was an employee of the NSA and that the letter should be interpreted as NSA pressure on the scientific community to deter cryptologic research activities.

These stories gave rise to additional allegations about NSA activities related to the DES and to cryptologic research in general. The stories also suggested that NSA had exerted pressure on the NSF to persuade them not to fund certain grant proposals for support of cryptologic research.

The following allegations were investigated by the Senate Select Committee on Intelligence: that the NSA exerted pressure on officials in the National Science Foundation (NSF) to withhold grant funds for scholarly research in the field of public cryptology and computer security; that the NSA directed an employee, who was also a member of the IEEE, to write a letter to the IEEE warning its members that certain actions related to an upcoming Information Theory Group Conference could be in violation of government regulations affecting the publication and export of cryptographic information; that U.S. government harassment brought about a chilling effect in universities doing research in cryptanalysis and even resulted in one university withdrawing already published material from its library shelves; that the NSA, under the guise of testing the mathematical formulas (algorithms) submitted to the NBS for consideration as a DES, "tampered" with the final algorithm in order to weaken it and create a "trapdoor" which only the NSA could tap; that the NSA forced the company (IBM) whose algorithm was chosen, to compromise the DES's security by reducing the key size[3] used in the encryption and decryption process; and that the DES failed to allow for future technological advancements which will permit successful brute force attacks within the next several years.

Based on its staff study, the Senate Select Committee on Intelligence concludes the following:

- The NSA has not put pressure on the NSF to prevent funding of grants for cryptological research. However, the very uncertainty and ambiguity surrounding cryptology has prompted some NSA officials to express concern to NSF about certain grants with cryptological ramifications and to suggest that NSA be involved in reviewing these proposals. The NSF has agreed to the latter request, since it views NSA as the only location of competent cryptological expertise in the government, but has not lessened its interest in, or willingness to fund, good research proposals in this field.
- The Committee has determined that Mr. Meyer's letter to Mr. Gannett of the IEEE was initiated solely by Mr. Meyer in his capacity as a member of the IEEE and was not prompted by any NSA official.
- There has been no direct or indirect government harassment of scientists working in the field of computer security. Nor has any university withdrawn library material as a result of NSA pressure. Nevertheless, the very newness of public cryptology and the vagueness and

[2]A brute force or exhaustion attack transforms encrypted text into every possible combination in an effort to discover the original plaintext.

[3]The key is the string of binary numbers which directs the encryption process. In a sense, the longer the key, the longer a brute force attack takes. Decryption is possible, otherwise, only if the encrypting key is known, or if the algorithm is weak, this permitting shortcut attacks.

ambiguity of federal regulations pertaining to cryptology create an uncertainty which in itself is not conducive to creative scholarly work.[4]

- In the development of the DES, NSA convinced IBM that a reduced key size was sufficient; indirectly assisted in the development of the S box structures[5]; and certified that the final DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weaknesses. NSA did not tamper with the design of the algorithm in any way. IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended.
- While the Intelligence Committee is in no position to settle scientific arguments regarding the exhaustion time necessary to break a DES encrypted message, it can report that the overwhelming majority of scientists consulted felt that the security afforded by the DES was more than adequate for at least a 5–10 yr time span for the unclassified data for which it will be used. The Committee notes that NSA has recommended that the Federal Reserve Board use the DES in their funds transfer system.

In order to reduce the potential capriciousness which is possible in ambiguous and uncertain situations, this Committee recommends:

- that the appropriate committees of Congress should address the question of public cryptology by clarifying the role which the federal government should have in policies affecting public cryptology.
- that the NSF should decide what authorities and obligations it has to consider the national security implications of grant proposals.
- that NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of research funds for public cryptology.
- that NSA and NSF should discuss the need for NSA to become part of NSF's peer review process for the review of grant proposals for research in cryptography or cryptanalysis.
- the NBS should continue to follow developments in computer and related technology in order to be aware of any developments which could lessen the security of the DES.

[4]There are a number of federal regulations of various types which are interpreted to have some effect on cryptology. Among them are: International Traffic in Arms Regulations (ITAR), 22 CFR 121-128; the Mutual Security Act of 1954, Section 414-22 USC 1934; 42 USC 2274-77; 18 USC 798; 18 USC 952; and Executive Order 12036.

[5]The S box structure is that part of the algorithm which performs the iterative process.

The NBS should continue to follow developments in computer and related technology in order to be aware of any developments which could lessen the security of the DES.