USA

Marc Rotenberg

The only locksmith in town

The NSA's efforts to control the dissemination of cryptography

In August 1989, the National Security Agency (NSA), a secret intelligence organisation in the United States, attempted to suppress the dissemination of an article written by Ralph C. Merkle, a computer scientist at Xerox's research center in California, in which he showed how to protect, cheaply and effectively, the privacy and security of computer communications. It was only the most recent incident in a long history of NSA efforts to limit public knowledge of innovations in cryptography.

The National Security Agency was created in 1952 by a presidential memorandum that is still classified. It has operated since that time under a series of presidential orders, outside the normal channels of government accountability. The NSA's secrecy is legendary: it has no legislative charter and its existence was not even acknowledged until 1962; no director of the agency appeared in an open hearing of Congress until 1975, and its budget, though in excess of several billion dollars, is secret and not known to many members of Congress.

The NSA is charged with safeguarding classified communications for the United States government around the world. But it is also engaged in collecting computer communications and telephone signals, cracking communications locks throughout the world, and gathering intelligence. It is of particular interest to computer scientists because of its extraordinary computational resources (several Cray supercomputers have been installed at Fort Meade outside Washington, DC) and because of its classified research in signal processing and data encryption.

President Reagan tried to expand the NSA's authority when he signed a National Security Decision Directive on 17 September 1984 which gave the NSA authority over computer and communications security for the entire government. (Previously, the National Bureau of Standards (NBS), a civilian agency, had been responsible for computer security for other civilian agencies in the federal government.) Congress responded by passing the Computer Security Act, a law meant to reestablish civilian control over computer security. But a memorandum of understanding signed recently by the NSA and the National Institute of Standards and Technology (successor to the NBS) calls into question whether the Act will be implemented as Congress intended.

Still, the NSA continues its efforts to control the flow of research on data encryption, and for good reason. As countries become increasingly dependent on computer communications, the need to ensure the privacy and security of messages that travel along computer networks grows, and computer scientists are particularly aware of the vulnerability of these communications. Data encryption is the most important technical safeguard for ensuring the privacy and security of these messages, but the NSA has repeatedly used funding restrictions and outright censorship to try to control the publication of cryptography research and to limit public access in this way.

In 1975, the NSA warned the National Science Foundation, the primary funding authority for scientific research in the US, against funding cryptography research, claiming that the NSA had sole authority to conduct such research. The agency continued to use strong-arm tactics in subsequent years to discourage unclassified research on data encryption.

When the NSA's efforts to control funding proved insufficient to restrict this research, a system of voluntary submission of materials by cryptography researchers was established, often with consent from the academic community. George Davida, a computer scientist at the University of Wisconsin and a member of the special committee of the American Council for Education that recommended submission of research to the NSA, opposed the plan.

In David Burnham's book, *The Rise of the Computer State*, Dr Davida describes how the rapid computerization of information has created electronic windows that make it possible to peer into the 'most intimate details of people's lives'. The databases become one-way mirrors, and encryption is often the only way to create a curtain to shield information from intruders. Dr Davida warns that 'the need for a civilian (or nongovernmental) effort in cryptography is a strong one'.

Despite these sorts of efforts, the NSA recently lost its battle to decertify DES, a widely-used encryption procedure that allows the parties involved in the communication to control the encryption scheme. The NSA had proposed a proprietary technology that would have required the use of cryptography keys developed by the NSA. But US businesses, particularly the Bankers' Association, successfully opposed this, fearing that it would grant the NSA the ability to examine computer communications, regardless of national security interest.

The NSA contends that it must retain the capacity to decrypt any communication in the world to protect national security. But at the heart of the debate over the agency's role in cryptography research is whether it should be the only locksmith in town. Fifteen years ago, when the US Select Committee on Intelligence conducted hearings on the activities of intelligence agencies, Senator Frank Church, the chairman of the committee, agreed that the NSA's intelligence-gathering capabilities were essential to the country's security, but warned that the eavesdropping devices and computers of the NSA created 'tremendous potential for abuse'.

A 1987 report prepared by Congress's Office of Technology Assessment (OTA) was similarly critical of giving the NSA sole control. Though OTA noted that the 'NSA sees its signal intelligence mission to be at risk if effective cryptography were available worldwide', the report also found that the United States can no longer base its cryptography policy on the interests of the national security community because of challenges in technology, 'continued pressure to improve business and government operations', and the 'emerging internalization' of encryption technology.

Computer Professionals for Social Responsibility, a non-partisan national membership organisation, has recommended that Congress conduct open hearings on cryptography research and explore the impact of the NSA's efforts to restrict public access to new developments in the field. With the growing dependence of computer users on digitized transmission, date encryption and the policies controlling it become all the more important. ■

Marc Rotenberg, *Testimony before the Subcommittee on Legislation and National Security, Committee on Government Operations, US House of Representatives on the Computer Security Act of 1987*, May 4, 1989.

***Marc Rotenberg** is the Director of the Washington Office of Computer Professionals for Social Responsibility and former Counsel to the Senate Judiciary Committee.*