Nervous System: How to Have a Secure Conversation with a Stranger

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System *is a monthly series that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

Encryption involves encoding information so that it cannot be directly understood. Put another way, the act of encrypting digital information entails replacing the binary data that constitutes that information with something else. Whereas data compression techniques rely on easily reversible methods of substitution, effective cryptography requires the substitution to be unpredictable, opaque, and difficult—if not impossible—to reverse without the use of a special key. Therein, however, lies one of the most vexing dilemmas in the history of modern cryptography. For two participants to engage in an encrypted conversation, each party needs access to the encryption key. Distributing the key to the participants *before* the secure conversation begins is the problem. If the key were to be exchanged over an unsecured, unencrypted channel, any eavesdropper would be able to pilfer the key for their own use.

During World War II, the elite cryptographers at Bletchley Park had armies of tailors sewing silk sheets containing encryption keys into the clothing of spies before they were sent into the field. But it is highly impractical to expect customers to visit the headquarters of their favorite online retailer to obtain a secret key to take back home and use when they want to send their credit card information securely over the internet to make a payment—and then make another personal roundtrip to obtain a new key for the next purchase. As a practical, logistical matter, the system needs to transmit the keys between users ahead of use, meaning one first must solve the problem of key distribution in order to manage key distribution. For years, the problem seemed like a catch-22.

A further complication arises in the fact that each set of senders and recipients needs a unique pair of encryption/decryption keys—otherwise, an authorized party in one communication could decrypt everyone else's as well. For two people to communicate, each needs a key. For three people to communicate, each needs *two* keys. This quickly escalates. The system as a whole needs keys for each possible pairing. To manage secure communications between a thousand people calls for the generation and distribution of almost half a million keys.

In 1967, Howard Rosenblum, deputy director for research and development at the National Security Agency (NSA), solved this riddle with a protocol he called the "session key." This invention has sat at the heart of encrypted telecommunications ever since.

The NSA had developed a secure telephone system developed for encrypted communications between secured locations. To manage any widespread implementation, though, the NSA needed to create, maintain, and distribute unique key pairs for every possible network connection. This was logistically unfeasible.

Rosenblum devised a clever trick to do this on an ad hoc basis, rather than ahead of time. Each individual phone had its own key, to be used only for secure communications with a central hub (the "key distribution center"). If station A wanted to secure a line to talk to station B, the operator at A would use the existing key to call into the hub and request a new one-time "session key" to communicate with B. The hub operator would create a temporary set of keys and distribute them directly to the operators at stations A and B, who could then use them immediately for their call. After that communication finished, the keys would be discarded.

Although the system involved human operators speaking over telephone connections, the underlying principle of key distribution could be automated and applied to the world of secure computer networks. That is, the concept *could* be applied—if it were known. As it happened, Rosenblum's session key idea was classified as "confidential," and therefore information about it was not public.

Either by clumsy accident or sly design, the NSA lifted the curtain itself on Rosenblum's technique and released the notion into the realm of civilian and commercial use. According to Jerome H. Saltzer's article "On the Origin of Kerberos" (published in 2021 in the *IEEE Annals of the History of Computing*), an otherwise obscure but unclassified 1973 paper by NSA staffer Dennis Branstad included a generic description of the idea. Branstad's paper itself was little noticed, an afterthought in an unheralded publication, but it caught the attention of researchers Roger Needham and Michael Schroeder at Xerox's Palo Alto Research Center, who developed a computerized implementation of the principles. In 1978, Xerox's scientists published their results and began creating a commercially available version of a technique that, unknown to them, had originated as a classified NSA protocol. The Needham-Schroeder protocol became the basis for Kerberos, a now widely used computer network authentication protocol. Meanwhile, Branstad helped develop the Data Encryption Standard (DES), the first publicly available cryptography algorithm, and for a time the most widely used cryptographic standard in the world.

Legaltech news

This article was originally published in Legaltech News on August 2, 2022.