Securing Networks: End-to-End Encryption vs. Link Encryption and Trusted Systems

Whitfield Diffie
Bell-Northern Research
Mountain View, California

Abstract

Today, two components are prominent in the technology of communication network security: cryptography and trusted systems. Reflection on the roles of these two components shows that both are essential, that some element of each must occur in any secure network. At the same time, there is an element of competition and some network designs treat encryption as primary, supported by only the minimum of trusted software, while others take the opposite course.

At one extreme, a network can employ end-to-end encryption as its primary security mechanism. In such a network, two users in secure contact rely on their exclusive possession of a common key to guarantee that their messages cannot be understood or imitated by others, regardless of whether intervening components of the network perform correctly or not. Here, trusted systems are limited to the role in which they cannot be avoided: decisions on how keys are to be distributed.

At the other extreme, a network can employ cryptography only to create the appearance of overall physical security. Link encryption is used to protect the exposed communication paths and for no other purpose. The problem is reduced to that of designing a multi-level secure operating system; the fact that it may span continents is concealed.

In arguing for the cryptographic approach, one could point out that trusted system technology is new and its products are prone to the performance and cost problems common with new technologies. They would say that cryptography, by comparison, is a well developed art. The trusted system people, on the other hand, would assert that cryptography is inflexible and cannot adequately support the complex security policies required.

Despite the value of many of these implementation arguments, the actual distinction lies more in the network builders notions of trust and authority. The user of a system that relies primarily on trusted system technology may be extremely well protected from opponents outside the network, but can have no true security from the network builders and administrators. This sense of security is perhaps best suited to users who are employees and act within a hierarchical authority structure. The user of an end-to-end encrypted network on the other hand can be very certain that his traffic is protected from everyone except the person he is conversing with. This situation is more closely aligned with our notions of a user who is part of a voluntary association.