Paper title and authors; where appeared.

Using Encryption for Authentication in Large Networks of Computers. Needham and Schroeder. CACM, Dec 1978

What is the main problem this paper attacks?

Authentication is the problem of knowing who you are communicating with. Needham and Schroeder consider how to use sequences of messages to ensure that conversations cannot be misdirected to the wrong partner.

What solution does the paper propose?

The paper proposes protocols that use cryptography to select a conversation key, and nonces to tie the messages together into sessions. The nonces and cryptography prevent an adversary from introducing the wrong key (for instance, an old conversation key) into a conversation.

What central idea did the authors use to solve it?

Using nonces to define sessions is new in this paper.

Also new is the authors' description of the threat model: The adversary can insert computers anywhere in the network to capture messages, replay them, or insert replacement messages of the adversary's choice.

What is a weakness or limitation of the paper?

The authors mention that it is hard to be sure whether subtle errors exist in this sort of protocol. In fact, the two main protocols that the authors present both have important errors.

Why is this paper important?

This paper initiated the idea of using nonce-based cryptographic protocols to set up authenticated sessions. This idea is used widely today in e.g. TLS, SSH, and many other protocols. The paper also identified the strong adversary model to measure authentication protocols against. It focused the community's attention on the likelihood that protocols would turn out to be wrong, and on the need to develop proof methods to ensure that a protocol is not wrong.