Paper title and authors; where appeared.
An attack on the Needham-Schroeder public key authentication protocol. Gavin Lowe. Elsevier Information Processing Letters, 1995.

What is the main problem this paper attacks?
This paper is an exposé on the authentication component of the original Needham-Schroeder public-key protocol, which contained a flaw that would allow an attacker to masquerade as a legitimate participant by engaging in multiple sessions. This attack had the potential to trick the legitimate participants into disclosing to the attacker what they believed to be a pair of shared secrets.

What solution does the paper propose?
Lowe provides a simple solution, adding the responder's name to his response before it is encrypted. The initiator then has an indication of which participant generated the responder's nonce (ostensibly his shared secret), and can match this identity with the participant with whom he believes he initiated the protocol.

What central idea did the author use to solve it?
The author refers to a paper entitled *Prudent engineering practice for cryptographic protocols* which provides a useful principle that happens to be directly applicable to this protocol's inadequacy:

> If the identity of a principal is essential to the meaning of a message, it is prudent to mention the principal's name explicitly in the message.

While not a particularly formal description, this approximately describes what was wrong with the protocol, and the corresponding solution; this indicates that a formal set of rules for protocol design might be beneficial.

What is a weakness or limitation of the paper?
Again this paper provides no exploration of proofs of correctness, nor does it attempt to formalize the notions cited in the Abadi & Needham paper. Without a formal proof of the properties of the protocol, it is still possible that a devious, unforseen attack (perhaps just a very slightly modified version of this one) could compromise the usefulness of the protocol in another way.

Why is this paper important?
Needham-Schroeder seems to have been a long-standing and well-loved example in the world of cryptographic protocols. By exposing a major flaw in a protocol which had been fairly rigorously studied and implemented for over 15 years, the author demonstrated the fragile nature of cryptographic protocols, emphasizing that even simple protocols such as this one may be vulnerable to subtle attacks which are difficult to detect with just a cursory glance. This would indicate

very strongly that an elegant formalism is desirable for future specification and verification.