In Defense Of Protocol Verification (Abstract)

Jonathan Millen
The MITRE Corporation
Bedford, MA

Cryptographic protocols, if designed improperly, may have flaws that make them vulnerable to message modification attacks or sometimes even eavesdropping attacks. Formal verification approaches have been suggested to detect protocol flaws. Protocol flaws depend on the logic of message exchange and content, and should be distinguished from weaknesses in cryptosystems and similar mechanisms whose strength is judged in the context of computational complexity.

One can take either an analysis or a synthesis approach to designing secure protocols. The analysis approach does not constrain the original proposed protocol design, but uses formal methods to analyze the design and either prove it correct or search for protocol flaws. The synthesis approach focusses on identifying design principles and techniques which, if followed, guarantee *a priori* the security of the resulting protocol.

Although current formal methods are subject to limitations inherent to the method or in its application, designs based on a synthesis approach are often unsatisfactory. There are at least four reasons for this, and examples can be given in support of them:

- Design constraints do not guarantee that protocols meet security goals that were not foreseen or addressed by the design approach;
- Design constraints may be inconsistent with security goals that are incompatible with the design approach;
- Design constraints are often not flexible enough to permit safe simplifications that improve the efficiency of the protocol;
- Design principles are sometimes insufficiently precise, so that a protocol may appear to obey a principle but in fact is flawed in a way that should have been prevented.

For these reasons, it is important to continue to develop and use verification approaches to gain assurance in protocol designs.