

Panel: What Is an Attack on a Cryptographic Protocol?

Organizer and Moderator:

Paul Syverson

Center for High Assurance Computer Systems

Naval Research Laboratory

Washington, DC 20375

Attacks on cryptographic protocols are often subtle and hard to find. This is certainly true in the context of protocol design. It is also true in the context of protocol analysis: researchers continue to announce new flaws discovered in protocols that have been repeatedly scrutinized using a variety of methods. Read another way, however, this means that attacks are all too easy to find; much harder to find is a protocol that is free of attack.

Still, once we have discovered an attack, it is clear that we've got one. If we figure a way for an attacker to follow the protocol specification yet still learn a secret key, then we have an attack. If we figure a way for an attacker to follow the protocol specification yet still convince Bob that Alice is present when she is not, then we have an attack. If we figure a way for an attacker to follow the protocol specification and convince Bob that Alice said one thing when she intended another, then we have an attack.

Or is it so clear? Just as protocols themselves depend on assumptions that are often implicit, attacks do as well. Put another way, all protocols have both secure and insecure implementations. And, what a protocol analyzer may term an attack the protocol designer may term a blatantly unrealistic insecure implementation.

Assumptions about goals are as important as assumptions about implementations. Attacks on protocols are often directed against goals that the protocols were never intended to fulfill. For example, in [BAN89] the Needham-Schroeder protocol is analyzed. A result of this analysis is that the protocol achieves entity authentication of Bob (the recipient) to Alice (the initiator). It is possible to attack this result. But, the result is not an intended goal of the protocol as originally published. Since protocols may be misapplied, in terms of either goals they are to achieve or environmental assumptions that are made, these may still be seen as important attacks; although it may be harder to say on what they are attacks. Is it a design flaw if a protocol is easy to implement in an insecure manner? What if the original protocol publication specifically recommends against such implementation?

It is sometimes unclear from its presentation whether or not a protocol was meant to achieve a goal or be applied in an implementation environment. Some protocols cannot be used with some cryptographic algorithms but are fine with others. Also, depending on the understanding of such widely used expressions as "authentication" or "no secrets leaked" something may be an attack or not. In fact, putative attacks are often used to refine our understanding of such expressions as well as our understanding of what we intend in our protocols. Once these are properly refined, an attack may no longer exist.

The goal of this panel is to discuss what we mean by 'attack' and to discuss what sorts of assumptions and definitions are necessary before we can give a clear answer to that question.

Invited Panelists:

Yvo Desmedt	University of Wisconsin-Milwaukee
Dieter Gollmann	University of London
Gavin Lowe	Oxford University
Catherine Meadows	Naval Research Laboratory

References

- [BAN89] Michael Burrows, Martín Abadi, and Roger Needham. A Logic of Authentication. Research Report 39, Digital Systems Research Center, February 1989.