PANEL:
Design Versus Verification:
is verification the wrong approach?

Contact person:
desmedt@cs.uwm.edu

A lot of work in the Computer Security community has concentrated on designing tools to *verify formally* the security of cryptographic protocols. On the other hand, in the Cryptographic community research has focused on *designing provably secure protocols*, *i.e.*, protocols that are as secure as the underling cryptographic primitive. With such protocols, if there is a weakness in the protocol, this can be exploited to break the underlying cryptographic scheme or assumption.

Both approaches have had their problems. Criticisms on formal verification include:

- key distribution protocols claimed secure under BAN logic, have been broken,
- BAN logic and its formal verification alternatives do not prove that a weakness in the protocol implies that the cryptoscheme, on which it is based, can be broken.

Criticisms on provably secure protocols range from:

- a lot of time has been waisted on designing useless protocols such as playing poker over the telephone,
- the methods used result in impractical protocols,
- many researchers find the methods used confusing.

Several researchers in the cryptographic community feel that in the near future, more effort will be spent on designing secure protocols and less on formal verifications. Their arguments are:

- there are two very powerful design tools which make it possible to achieve provable secure protocols, namely:
  1. Pseudo Random Functions, invented by Goldreich-Goldwasser-Micali.
  2. Zero-Knowledge, invented by Goldwasser-Micali-Rackoff.
- although these tools were first introduced in a theoretical context, (for example originally zero-knowledge was designed to prove Oblivious Transfer secure), they have now been used to design several practical protocols.

The method based on Pseudo Random Functions is controversial since it usually relies on the assumption that a block cipher such as DES behaves as a pseudo random function. This assumptions is often viewed as being rather dubious. On the other hand the zero-knowledge based approach is as strong as theoretically possible.

The goal of the panel is to debate whether formal verification methods or provable secure design methods are preferable and what the potential of these methods is.

PANEL MEMBERS:

Yvo Desmedt (Univ. of Wisconsin-Milwaukee: moderator),

Mike Burmester (RH, Univ. of London, UK: used zero-knowledge to design key distribution protocols),

Jonathan Millen (Mitre: to defend the verification approach),

Others to be announced.