Gaps in the standard

Felix Würsten

How do I know that the person I am communicating with on the internet is actually who he claims to be? And how do I know if the data he is conveying is actually what he wanted to send me? Such questions are inevitable when confidential information is to be transferred though the internet. And thus it goes without saying that sensitive transactions require a secure and reliable authentication of the partners involved.

Consequently, a whole series of protocols has been devised in recent years based on different approaches. Every bank, for instance, uses its own protocol. Nevertheless, many of these protocols have a common basis: they orient themselves by the ISO/IEC-9798 standard, which lays down the fundamental principles as to how such protocols should be composed.

On behalf of the Japanese government, David Basin, a professor at the Institute of Information Security, and his colleagues Cas Cremers and Simon Meier have now investigated just how reliable this standard really is, as the Japanese government would like to use it for its own e-government solutions.

If you want to check whether a protocol is secure, first you need to define what features it should have. Is it only supposed to prevent outsiders from receiving information through observation? Or should it offer protection from active attacks? The scientists from ETH Zurich discovered that many protocols described in the ISO standard do not actually have the features they are supposed to.

"Really, we thought the ISO standard would be a solid basis. It has already been used for a long time and refined constantly", reports Cremers. Admittedly, they only discovered subtle weaknesses. "But these can still be exploited by attackers." With his team, he has now put together a series of recommendations as to how the ISO standard can be improved. These have already been adopted by the ISO Committee in a new version of the standard.

The researchers conducted their study with the aid of tools that Basin's group had developed in recent years. "These tools provide mathematical proof that a particular protocol has got the features it should have", explains Basin. "Not only did we find the aforementioned weaknesses in the ISO standard; we were also able to demonstrate that our recommendations can actually remedy these shortcomings." ■

www.infsec.ethz.ch →