The Secret Prover: Proving Possession of Arbitrary Files While not Giving Them Away

Wouter Teepe

Artificial Intelligence, University of Groningen,
Grote Kruisstraat 2/1, 9712 TS Groningen, The Netherlands,
email: w.g.teepe@ai.rug.nl

Abstract

The Secret Prover is a Java application which allows a user (A) to prove to another user (B), that A possesses a file. If B also possesses this file B will get convinced, and if B does not possess this file B will gain no information on (the contents of) this file.

This is the first implementation of the protocols described in the paper "New Protocols for Proving Knowledge of Arbitrary Secrets While not Giving Them Away" [2], which is also discussed in this volume [3].

1 Introduction: Proving Secrets

In application domains where sensitive information plays an important role, such as police research, intelligence, finance and the medical domain, one may want to ask whether someone knows a specific fact. Because of the sensitivity of the information concerned, it is often undesirable for the specific fact itself to be told by way of posing the question. For example posing the question "Did you know that Geertje is pregnant?" will inform the asked person about a fact. If it is the aim to ask this very question without informing the asked person about the fact, we need a dedicated protocol for asking such questions. [2] Introduces six protocols which offer a solution to this problem.

The trust needed between the participants of the protocol is minimal: essentially, only the prover must truly want to prove knowledge of a fact to others who also know.

In this demonstration, we introduce the Secret Prover, a Java application implementing these protocols.

The kind of secrets that the Secret Prover can handle is secrets in the form of a file. A file can be considered as a sequence of bits, and knowledge of this sequence can be proven using the Secret Prover. No limitation exists on what kind of files can be used.[1]

[1] Note that in this scenario, the file name is irrelevant to the protocol.

2 The ANITA project

The research contributing to the protocols and this demonstation is the Administrative and Normative Information-Transaction Agents project, ANITA for short[1]. The ANITA project is funded by NWO/ToKeN2000. Its aim is to use multi-agent systems to provide methods for both complete and legitimate information exchange of sensitive information, such as in the Dutch police domain.

The Dutch police offers us a very interesting application area for our protocols. Police investigation teams typically want to keep their files secret, but *do* want to know whether other teams are investigating on the same persons or locations. If indeed multiple teams are investigating the same person, they would better co-operate, or at least make sure they do not hinder one another.

3 System requirments

The demonstation software is a Java application, which can be used on any computer with a currect Java installed. To run the protocol, two computers running this software are needed, and the computers need to be connected through the internet. One of the computers needs to allow "incoming connections", which means its firewall should not be set too paranoid. The protocol can also be run within just one single computer, but this may make understanding the protocol somewhat less easier. The demonstration will approximately take 25 minutes. The software can be found at `http://www.ai.rug.nl/~woutr/provingsecrets/`

4 Future application of the software

The protocols can be run in standalone applications such as this demonstation, but typically the protocols will be components of larger access control systems. In our forthcoming research, these protocols will be incorporated within the prototypes which will be developed in the ANITA project.

References

[1] The ANITA project,
`http://www.rint.rechten.rug.nl/onderzoek/anita/anita.html`.

[2] W. Teepe. New protocols for proving knowledge of arbitrary secrets while not giving them away. In Sieuwert van Otterloo, Peter McBurney, Wiebe van der Hoek, and Michael Wooldridge, editors, *Proceedings of the Knowlegde and Games Workshop*, Liverpool, July 2004. available at `http://www.ai.rug.nl/~woutr/provingsecrets/`.

[3] Wouter Teepe. New protocols for proving knowledge of arbitrary secrets while not giving them away. same volume.