ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Semester Thesis

A Cocoa GUI For The AVISPA Protocol Analyzer

Contact: paul.drielsma@inf.ethz.ch, paul.sevinc@inf.ethz.ch

Expected start date: October/November 2005

Introduction & Project Objectives

Cryptographic protocols – even simple ones – are notoriously difficult to design correctly. Indeed, certain protocols have been published, put into practice, and found to be flawed only *years* after their introduction! For this reason, formal analysis of security protocols is a very important field.

The Information Security Group at ETHZ co-develops the AVISPA Tool ([1]), a push-button tool for the formal analysis of such protocols. The AVISPA Tool is available either for download or via a web-based graphical interface. The downloadable package, however, incorporates only a command-line interface and an XEmacs mode.

The goal of this project will be to design and implement a graphical user interface for the AVISPA Tool. The interface will be implemented for Mac OS X using the Cocoa application frameworks (see `http://developer.apple.com/cocoa/` and [3]) and should adhere to the Apple Human Interface Guidelines [2].

Work Plan

The student should first develop a design for the look and functionality of the interface as well as an object-oriented design for its implementation. The design should be as modular as possible so that future extensions to the AVISPA Tool can be accommodated by the interface with minimal modification. An important aspect of the project is that the design decisions taken be documented and explained and that there be traceability back to the Human Interface Guidelines so that conformance is evident from the design documents.

Several challenging extensions to this project are possible, time permitting. In particular, it would be interesting to implement a message sequence chart generator that gives a graphical representation of protocol attacks returned by the AVISPA Tool. A port of the interface to the GNUStep frameworks (`http://www.gnustep.org/`) under Linux would also be of interest.

Prerequisites

Students must have a working knowledge of Java or Objective-C. Experience with programming against the Cocoa API [3] or with using the Interface Builder tool is not necessarily required but would be helpful.

Supervision

The project will be supervised by Paul Hankes Drielsma, Paul Sevinc, and Prof. D. Basin.

References

[1] AVISPA. The AVISPA Tool. Available at `http://www.avispa-project.org`, 2005.

[2] Apple Computer. Apple Human Interface Guidelines. Available at `http://developer.apple.com/documentation/UserExperience/Conceptual/OSXHIGuidelines/index.html`, 2005.

[3] Aaron Hillegass. *Cocoa Programming for Mac OS X (2nd Ed.)*. Addison-Wesley Professional, 2004.