



# A Cocoa GUI For The AVISPA Protocol Analyzer

Semesterarbeit WS05/06

Von: Natalie Trommer  
Betreuer: Paul E. Sevinç  
Paul Hankes Drielsma

# Übersicht

- Aufgabenstellung
- AVISPA
- Cocoa
- Design
- Implementation
- Demo
- Fazit & future work
- Fragen

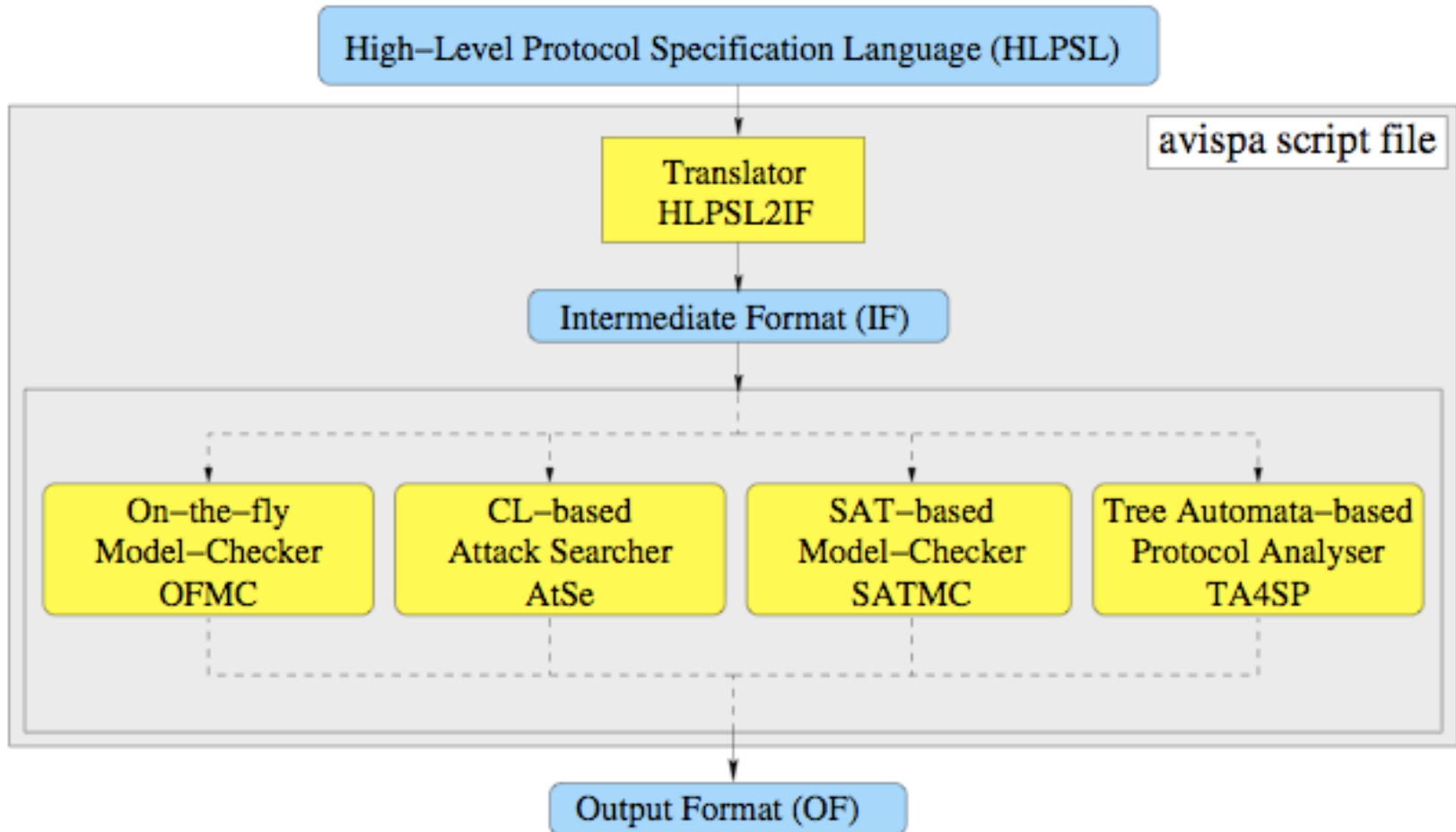
# Aufgabenstellung

- Design und Implementation eines graphischen user interface für das AVISPA Tool
- Implementation:
  - Mac OS X
  - Cocoa application frameworks
  - Apple Human Interface Guidelines

# AVISPA

- Automated Validation of Internet Security Protocols and Applications
- Tool um die Sicherheit von Internet-Protokollen und Anwendungen zu analysieren

# AVISPA

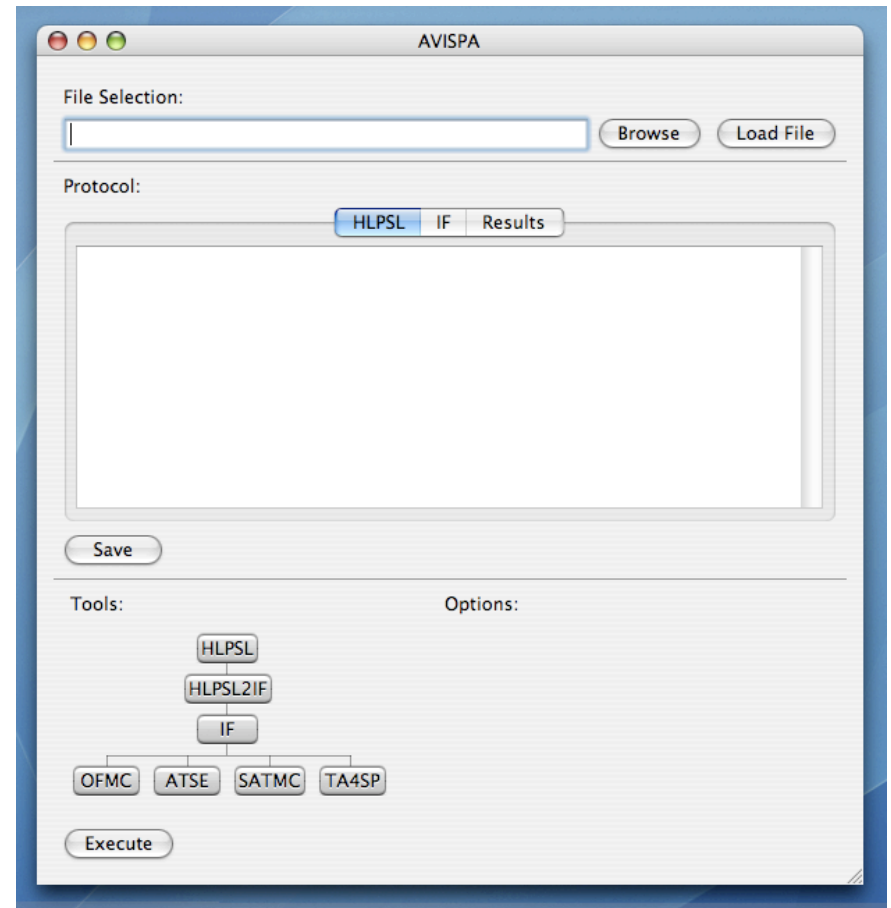
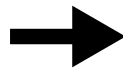


# Cocoa application frameworks

- Objekt-orientierte Entwicklungsumgebung für Mac OS X Applikationen
- Besteht aus mehreren objekt-orientierten Software Libraries und einer Runtime Engine
- Objective-C oder Java
- „Schnell & einfach“

# Design – Funktionalität & Aussehen

- hpsl Files öffnen, editieren & speichern
- Tools ausführen & Optionen auswählen
- Resultate editieren & speichern



# Design – Funktionalität & Aussehen

The screenshot shows the AVISPA GUI with the following elements:

- File Selection:** A text box containing `/Users/natalie/Testfiles/EKE.hpsl`, with `Browse` and `Load File` buttons.
- Protocol:** A tabbed interface with `HLPSSL`, `IF`, and `Results` tabs. The `HLPSSL` tab is active, displaying a list of protocol metadata:

```
%% PROTOCOL: EKE: Encrypted Key Exchange
%% VARIANT: basic
%% PURPOSE: Encrypted key exchange
%% REFERENCE:
%% url(http://citeseer.ist.psu.edu/bellovin92encrypted.html)
%% MODELER:
%% begin(itemize)
%%   item Haykal Tej, Siemens CT IC 3, 2003
%%   item Sebastian M{o}dersheim, ETH Z{u}rich, December 2003
%% end(itemize)
%%
%% ALICE_BOB:
%% begin(verbatim)
%%   ...
```
- Tools:** A tree view showing the selected tool `HLPSSL` and its sub-tools: `HLPSL2IF`, `IF`, `OFMC`, `ATSE`, `SATMC`, and `TA4SP`.
- Options:** A section for configuring analysis options.
- Buttons:** `Save` and `Execute` buttons are visible.

The screenshot shows the AVISPA GUI with the following elements:

- File Selection:** A text box containing `/Users/natalie/Testfiles/EKE.hpsl`, with `Browse` and `Load File` buttons.
- Protocol:** A tabbed interface with `HLPSSL`, `IF`, and `Results` tabs. The `IF` tab is active, displaying the specification of the `IF` interface:

```
%% IF specification of /Users/natalie/Testfiles/EKE.hpsl

section signature:

state_eke_Resp: agent * agent * symmetric_key * nat * text * text * text * public_key * set
(agent) * nat -> fact
state_eke_Init: agent * agent * symmetric_key * nat * public_key * text * text * text * set(agent) *
nat -> fact

section types:

sec_k2, nb, na, sec_k1: protocol_id
...
```
- Tools:** A tree view showing the selected tool `HLPSSL` and its sub-tools: `HLPSL2IF`, `IF`, `OFMC`, `ATSE`, `SATMC`, and `TA4SP`.
- Options:** A section for configuring analysis options, including:
  - Session Compilation
  - Depth:
  - Path:
- Buttons:** `Save` and `Execute` buttons are visible.

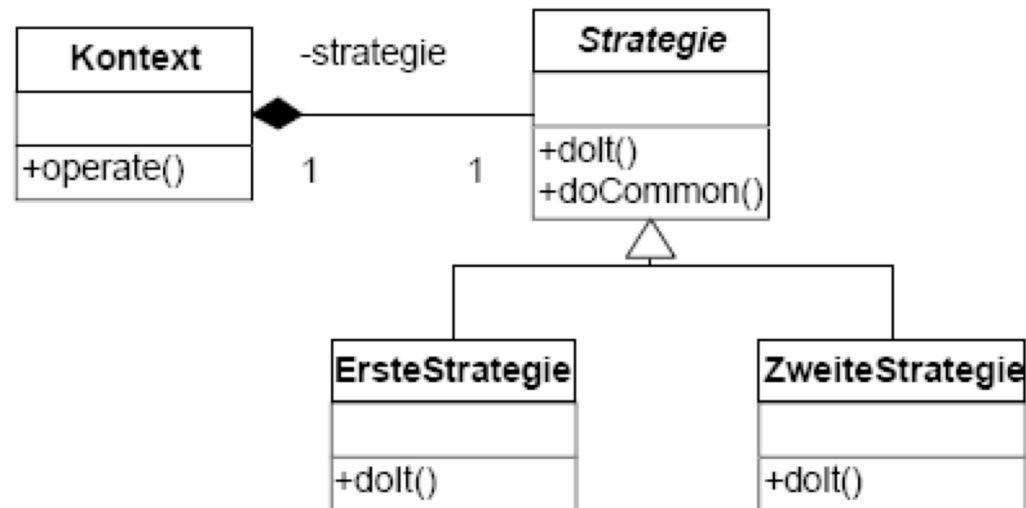


# Design – Implementation

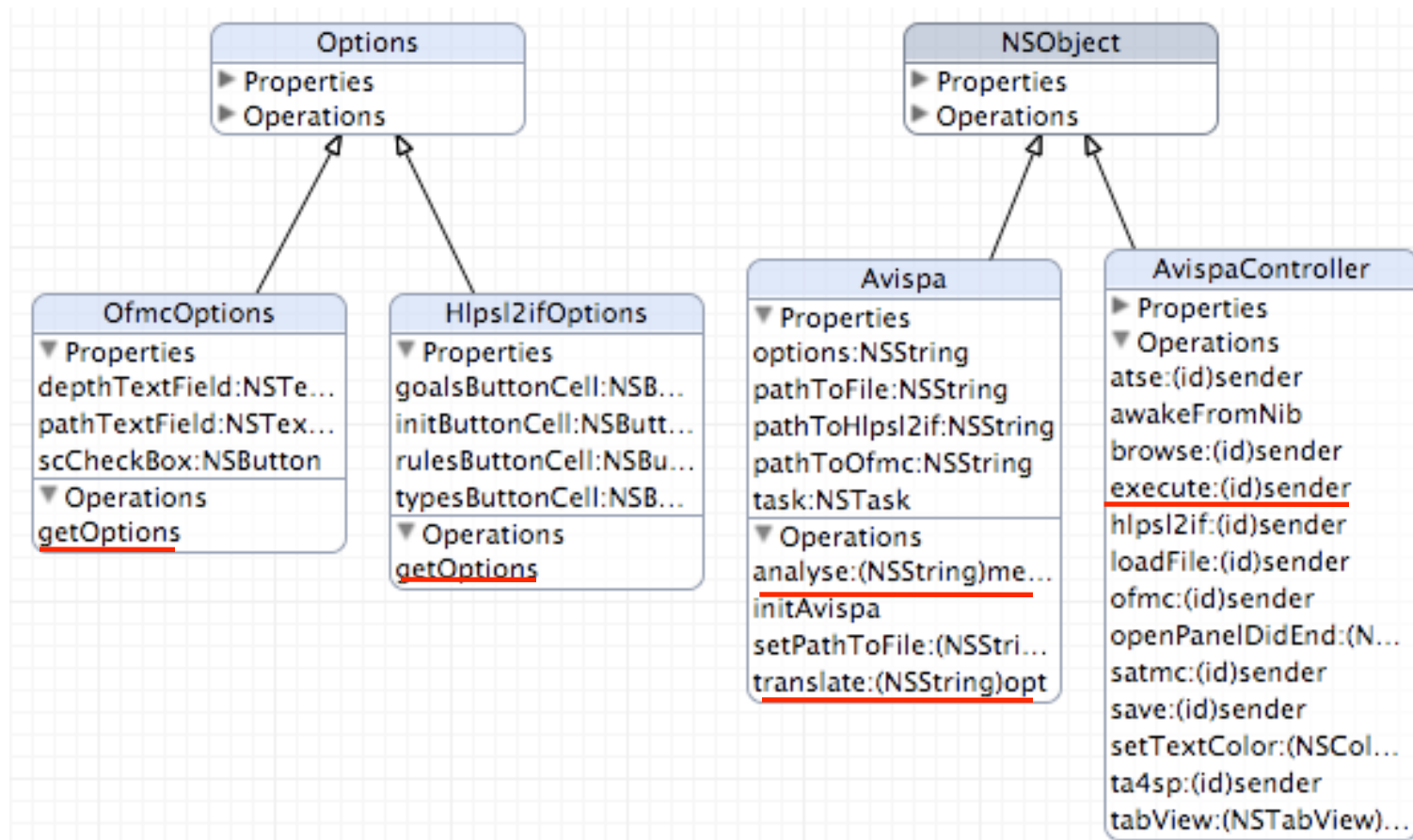
- Anforderung:  
So modular wie möglich, damit zukünftige Erweiterungen nur minimale Modifikationen benötigen
- Unterste Schicht AVISPA besteht aus vier Analysetools ...
- ... Lösung: Strategy-Pattern

# Implementation – Strategy Pattern

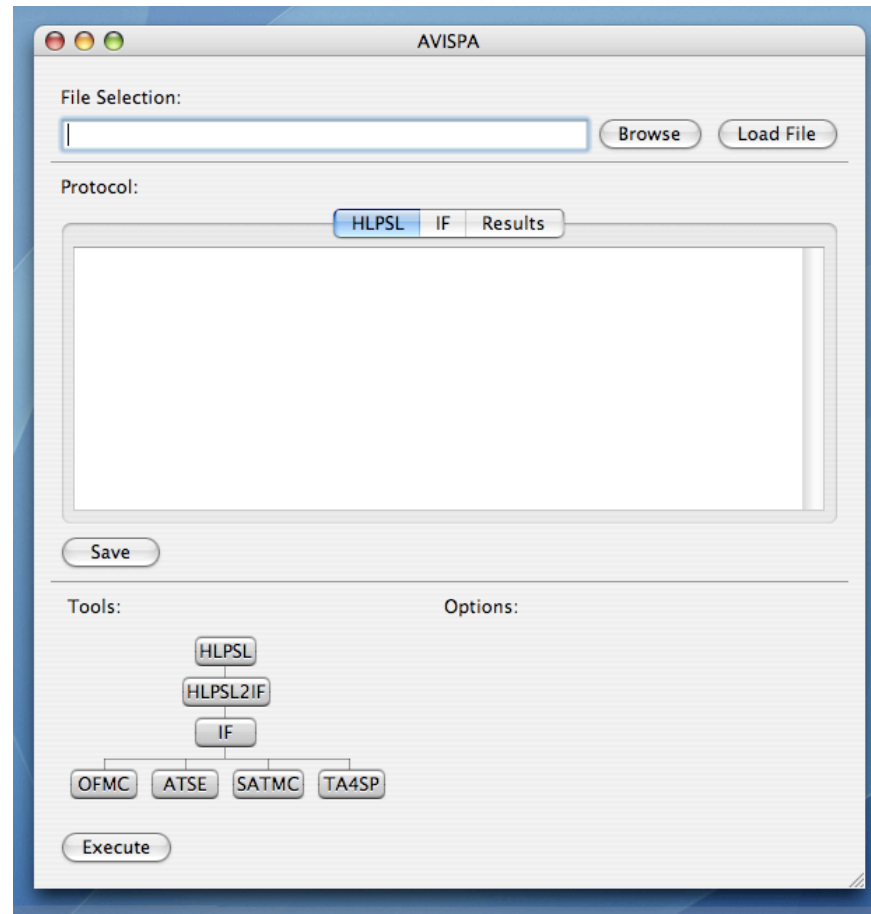
- Eine Kontext-Klasse kann auf verschiedene Versionen eines Algorithmus zugreifen



# Implementation – Klassendiagramm



# Demo



# Fazit & future work

- Spannende Arbeit
- 'unbekanntes' Mac OSX kennengelernt
  
- Resultate der Analyse:  
Text → Grafik: Message Sequence Chart
- Portieren der restlichen Analysetools



# Fragen

???