

# Automated Analysis of Permission-based Security using UMLsec

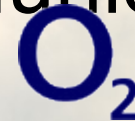
Jan Jürjens<sup>1</sup>, Jorg Schreck<sup>2</sup>, Yijun Yu<sup>1</sup>

<sup>1</sup>Computing Department  
The Open University, GB



<sup>2</sup>O<sub>2</sub>(Germany)

Munich



J.Jurjens@open.ac.uk

<http://www.jurjens.de/jan>

# Why Analysis of Security Permissions?

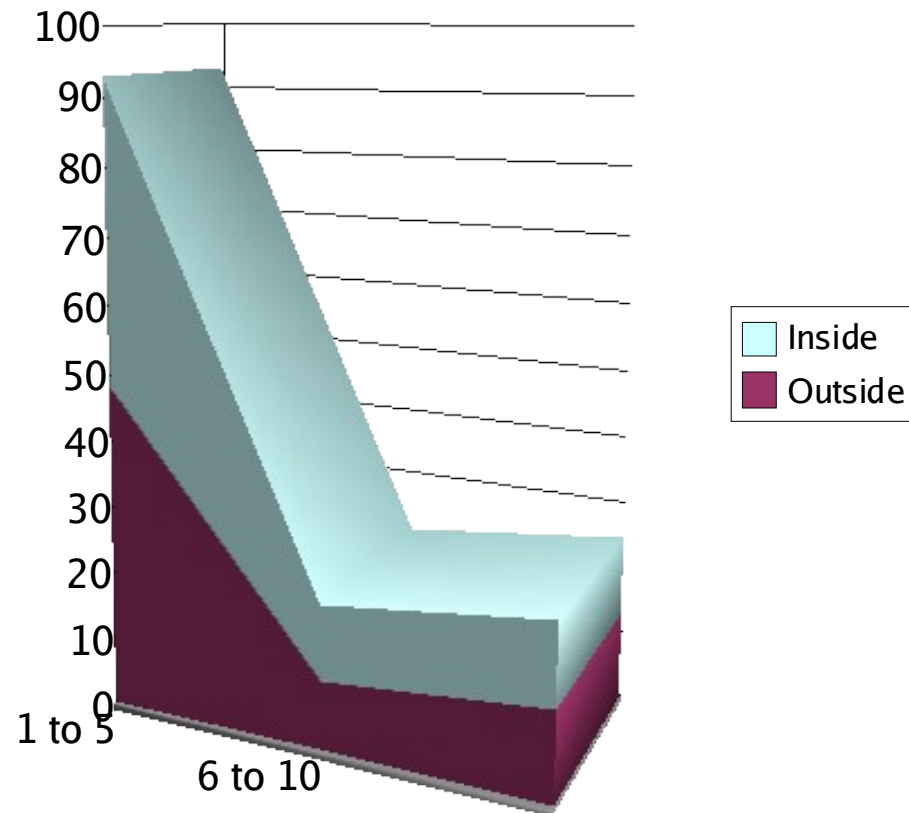
## Computer Crime:

- 99% detected breaches
- 223 firms loose \$ 455,848,000
- 50% inside attacks

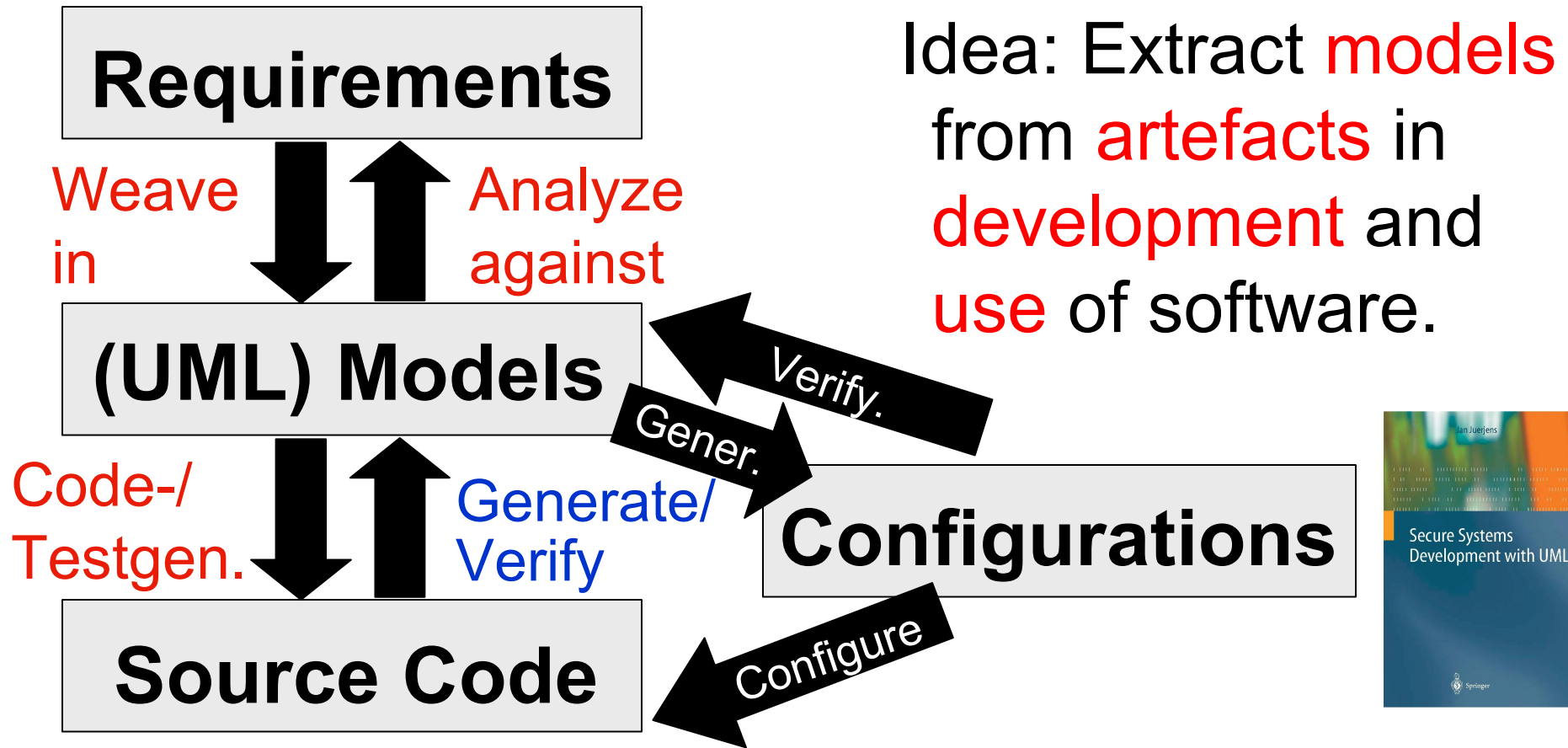
## Automated Analysis

- Manual review of permissions impossible
- Huge amount of data
- Attacks from reviewer ?

Where Attackers come from

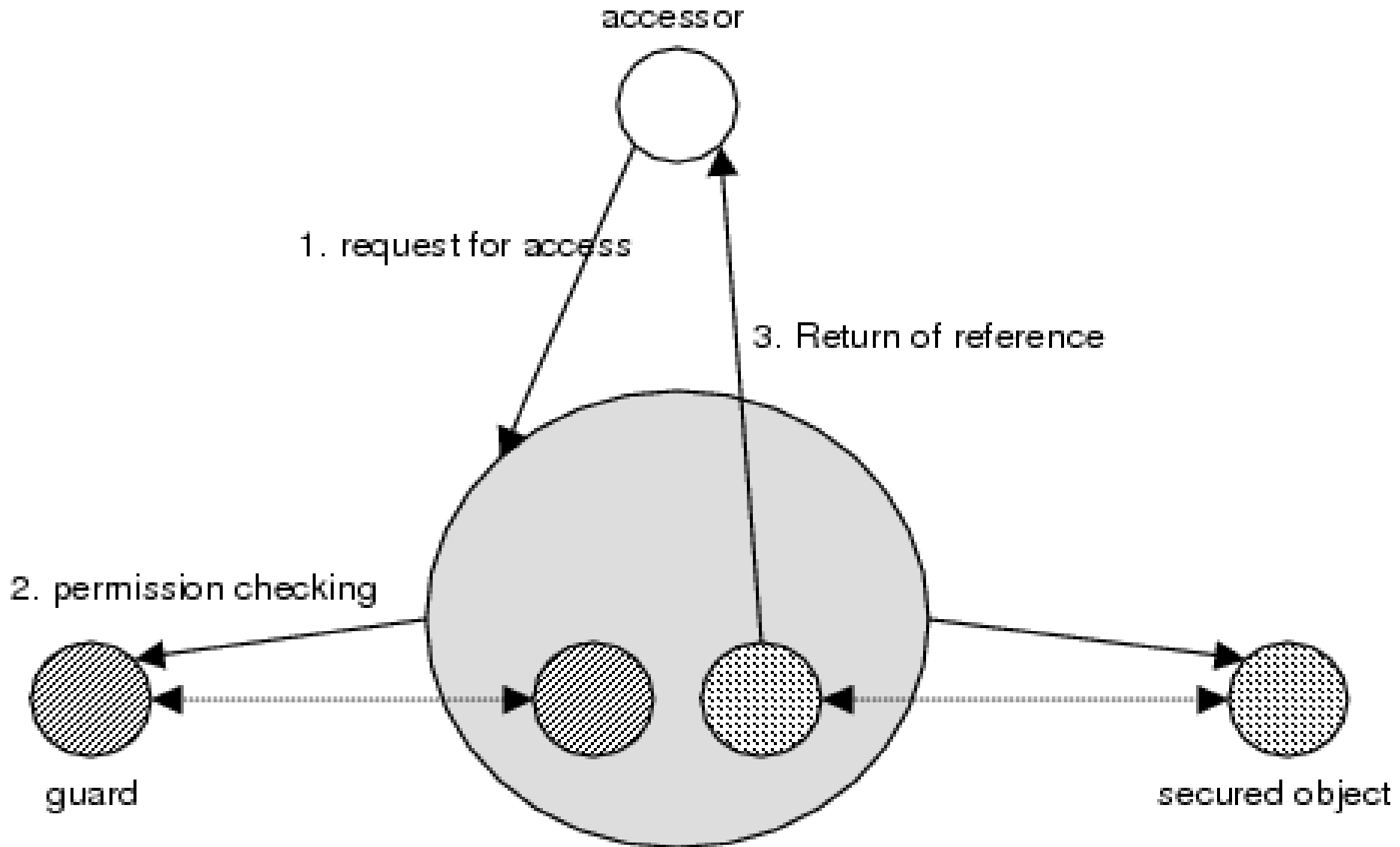


# Background: Model-based Security Engineering



→ Long-term goal: Tool-supported, theoretically sound, efficient automated security design & analysis.

# Java Security with Guarded Objects

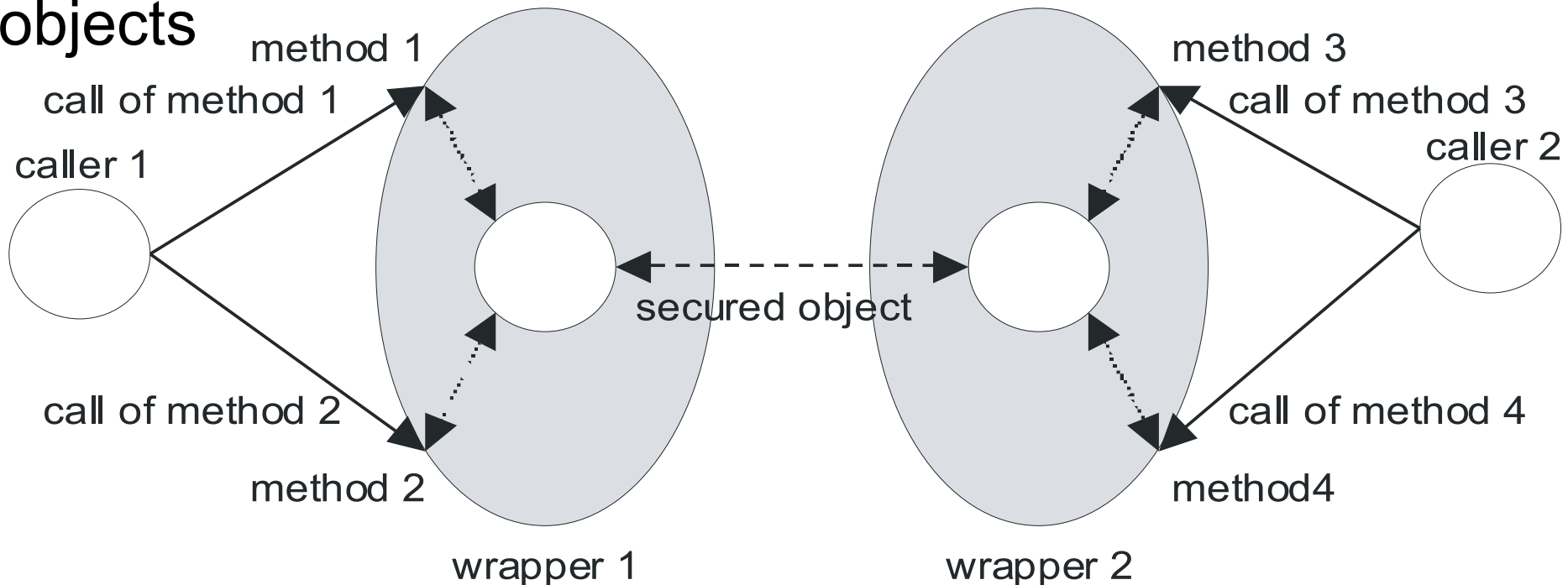


# Delegation using Certificates

GuardedObject manages certificates

- Passed as parameter to getObject() method
- Secured by asymmetric key

Per-method permission check by returning wrapper objects



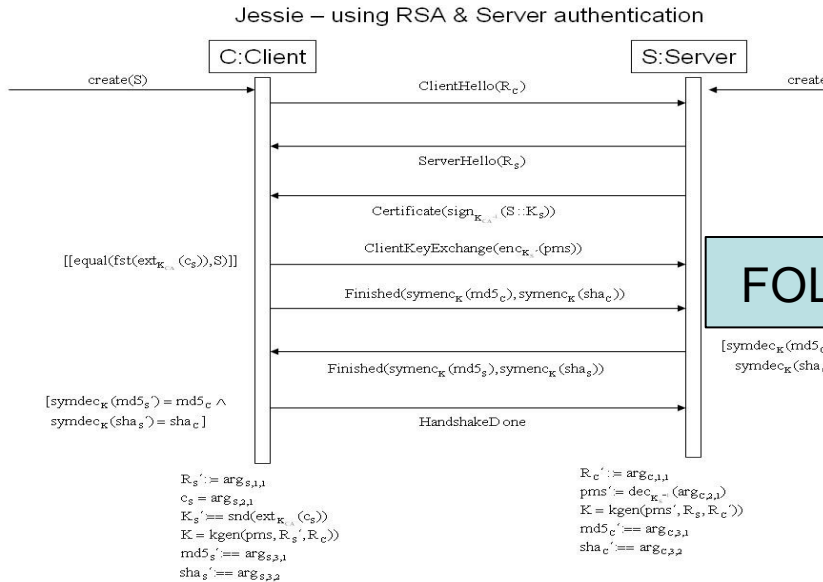
# Problem: Complexity

---

- Granting of permission depends on **execution context**.
- Access control decisions may rely on **multiple threads**.
- A thread may involve several **protection domains**.
- Have method **doPrivileged()** **overriding** execution context.
- Guarded objects defer access control to **run-time**.
- **Authentication** in presence of adversaries can be subtle.
- **Indirect** granting of access with capabilities (keys).
  - **Difficult** to see which objects are granted permission.
  - ⇒ use **UMLsec**



# Static Checking



FOL

```

...
((
  knows (ArgC_3)
  & (equal (fst (ArgC_3), type_serverkeyexchange))
  & (equal (snd (ext (snd (snd (ArgC_3))), k_ca), skey))
  & (equal (snd (ext (snd (ArgC_2), k_ca), fst (snd (ArgC_3))))))
))
=> (
  ((knows (ArgC_4_1)
    & equal (ArgC_4_1, type_serverhellodone))
  => (
    ( (true & equal (ClientKeyExchange, enc (premasterkey, skey))
      )
    )
  ))
...
%----- Conjecture -----
input_formula (attack, conjecture, (
  knows (mastersecret) )).
  
```

ATP

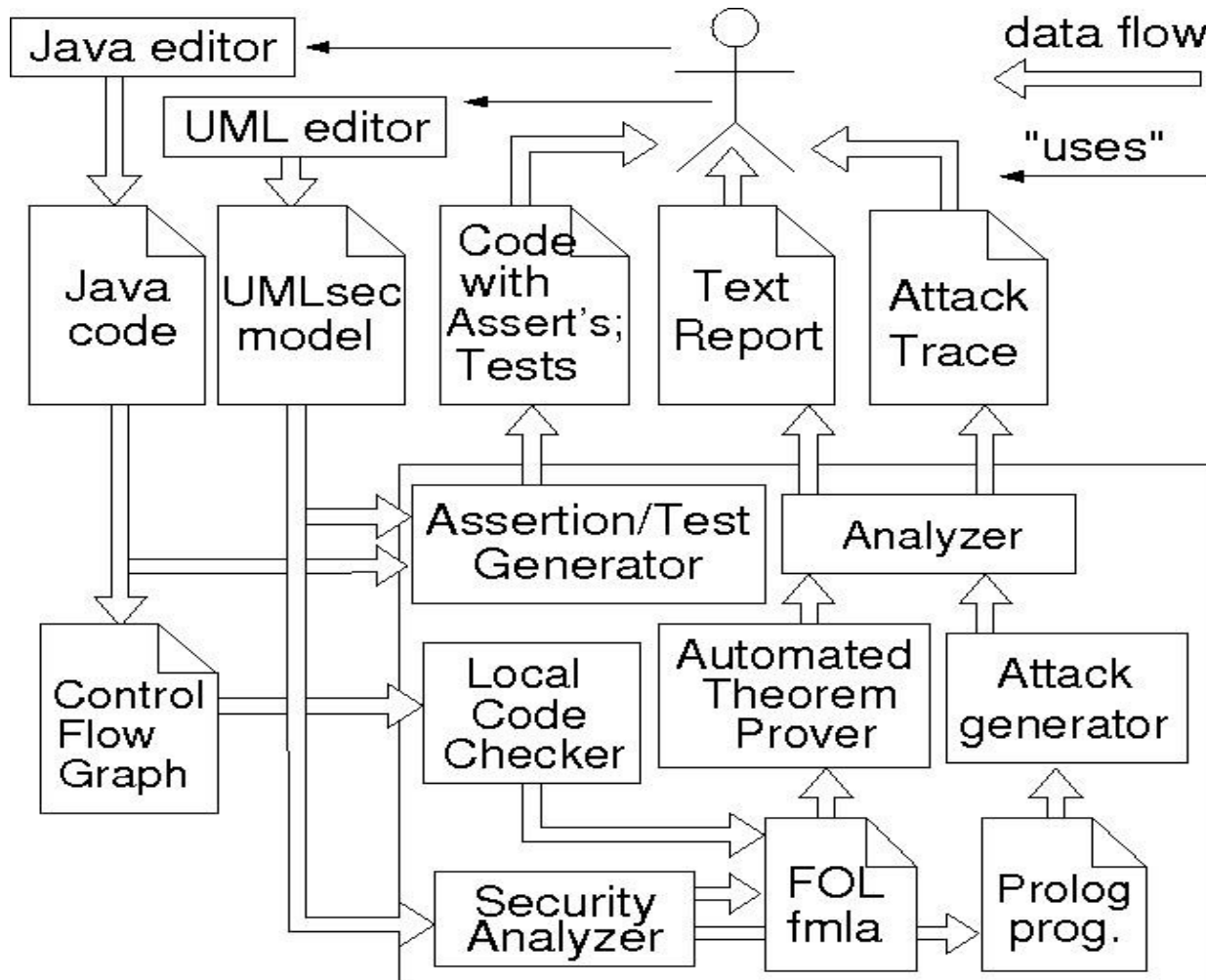
```

analyzing results ...
model found/total failure
time limit information: 19 total / 18 strategy
(leaving wrapper).
task myUML_PID1491 on atbroyl has status SUCCESS
(model found by strategy 300) consuming 1 seconds
deleting temporary files.
e-SETHEO done. exiting
  
```



# Tool Support

[FASE05, ICSE06, ASE07, STTT07, ICSE08]



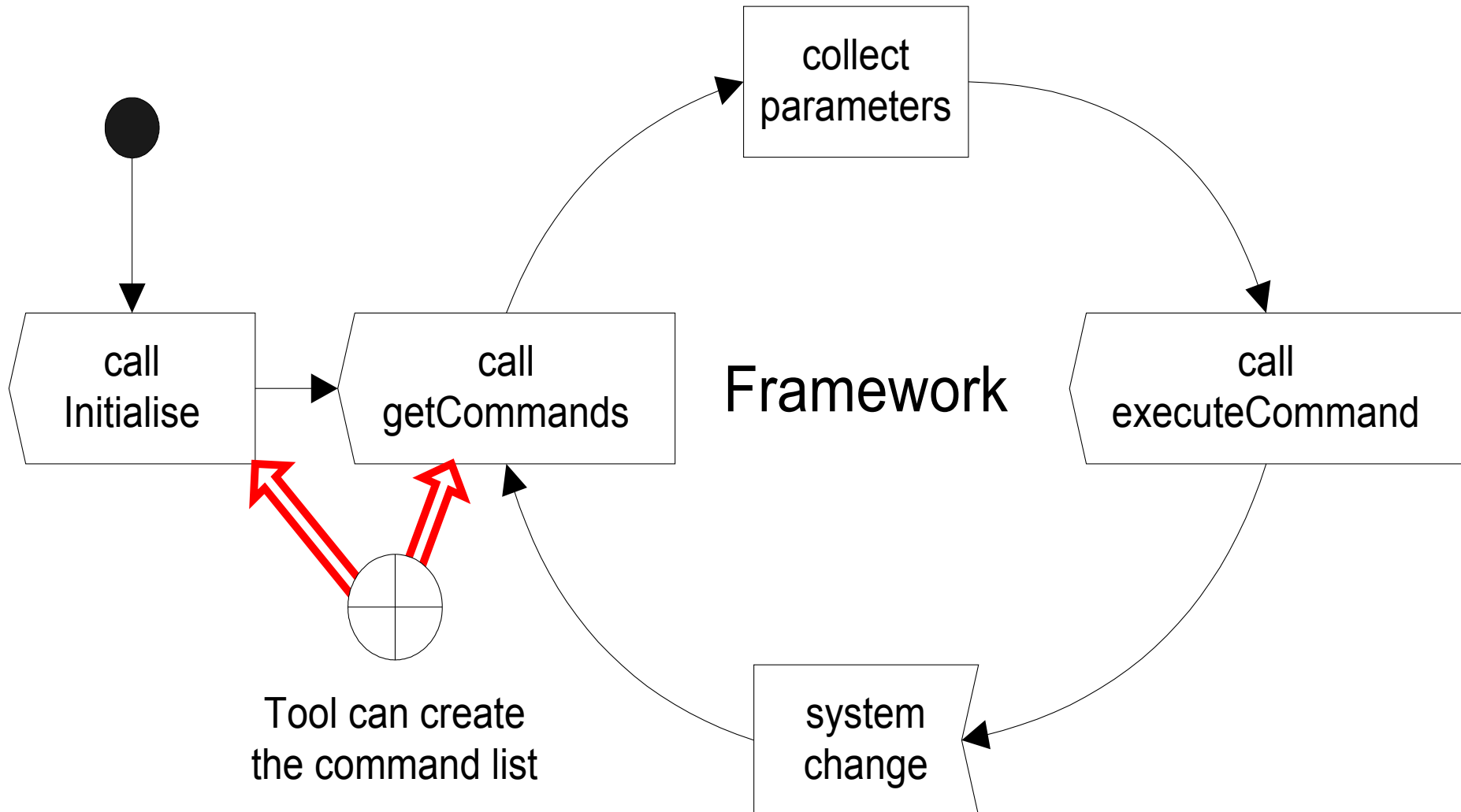
Configuration analysis:

- user permissions,
- firewall rules/policies

Open-source



# Exposing Commands



# Demo

**Viki UML(sec) verifier**

File Tool Window

**Project Tree:**

- v
  - {v}k
- java
- Protocol
  - Object: Bob
  - Object: Alice
  - Class: Responder
  - Class: Initiator
    - Operations
    - Attributes
    - AssociationEnds
    - StateMachine: Ini
- Intruder
  - type: Insider
  - capabilities: Read, W

**Code Editor:**

```
/* *****  
 * Class Initiator  
 ***** */  
#define SID_Initiator_Initial_State_1 0  
#define SID_Initiator_Final_State_1 1  
#define SID_Initiator_State_3 2  
#define SID_Initiator_State_2 3  
#define SID_Initiator_State_1 4  
  
proctype ClassInitiator(TYPE_DATAVAL rv_thisId; chan rv_channelIn; cl  
  
/* internal promela variables */  
TYPE_STATEID rv_currentStateId = SID_Initiator_Initial_State_1;  
TYPE_EVENT rv_currentEvent;
```

DynamicVerifier StaticCheck MdrViewer Activity Sequence Statechart Subsystem

Loading model from file: BasicSnoopSymmetric.zargo  
success  
Ready

# Some Applications

T-Systems

Analyzed designs / implementations / configurations e.g. for

- Biometry- or smart-card-based identification
- authentication (crypto protocols)
- authorization (user permissions, e.g. SAP systems)

Analyzed security policies, e.g. for privacy regulations.

Allianz 

Deutsche Bank 

HypoVereinsbank 

CEPS™

BMW Group

 Münchener Rück  
Munich Re Group

 Bundesministerium  
für Bildung  
und Forschung

 Bundesministerium  
für Wirtschaft  
und Technologie

O<sub>2</sub>

 infineon



# Related Projects

---

- PhD project on Verifying Implementations of Cryptoprotocols in C (MSR Cambridge / A. Gordon)
- RoySoc JIP with TU Munich on Formal Model-based Analysis of Cryptoprotocol Implementations
- RoySoc JIP with NII (Tokyo) on Security Requirements vs Design
- PhD project on IT security risk assessment with Munich Re
- PhD project on Adaptive Security for Ambient Technology
- PhD project on fuzzy reasoning for IT security risks
- PhD project on model-based development for avionics

# Questions ?

More information  
(papers, slides, tool  
etc.):

[J.Jurjens@open.ac.uk](mailto:J.Jurjens@open.ac.uk)