

Me and My Research

Mohammad Mousavi
`m.r.mousavi@tue.nl`

Department of Computer Science,
Eindhoven University of Technology

FSA Seminarium, 2011

Outline

Me

Security

Model-Based Testing

Outline

Me

Security

Model-Based Testing

Wondering How to Pigeonhole Me?

Status	Subject	Date
Born	Mohammad Mousavi	1978
B.Sc.	Automatic Website Generator	1999
M.Sc.	Nondeterminism in CZ	2001
Ph.D.	Structuring SOS	2005
Assist. Prof.	Electrical Engineering	2005-2006
Postdoc	Process Algebras	2006-2007
Assist. Prof.	Analysis and Design of Systems	Since 2005
Director of Program	Embedded Systems	Since 2010

Research Areas

1. Formal Semantics
2. Process Algebras
3. Software/Hardware Verification
4. Security
5. Model-Based Software Testing

Outline

Me

Security

Model-Based Testing

Dining Cryptographers



Dining Cryptographers

The Plot

1. n cryptographers sitting at a round table;
2. the NSA watching over them;
3. secretly either a cryptographer or the NSA pays the bill;
4. goal: discover whether the NSA has paid without compromising anonymity.



Dining Cryptographers

Protocol

1. a cryptographer or the NSA **pays** (the cashier is decent enough to refuse a second payment);
2. cryptographers **flip coins**;
3. each tells the **neighbors** the result of the coin flip;
4. each announces the **"xor"** of the results from the two neighbors if she has not paid or its negation, if she has;
5. if the number of announced heads is **odd** then a **cryptographer** has paid, if it is **even**, the **NSA** did.



Dining Cryptographers

Correctness Criteria

1. it will eventually be the **common knowledge** all whether a cryptographer or the NSA has paid;
2. if a cryptographer has paid **nobody else** will ever **know** this.



Challenges

1. **Belief** of Processes
2. **Applying** Epistemic Verification to **Voting** Protocols
3. **Efficient Model Checking** of Epistemic Formulae
4. Bridging the Gap Between **Tools**

Some Resources

Main Paper

F. Deschesne, M.R. Mousavi and S. Orzan, Operational and Epistemic Approaches to Protocol Analysis: Bridging the Gap. Proc. of LPAR'07.

Outline

Me

Security

Model-Based Testing

Model

What is it good for?

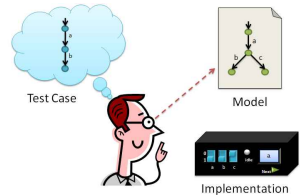
- ▶ specify the intended **behavior** of system and environment
- ▶ used to **derive test-cases** in a structured (mechanized) manner



Model-Based Testing

Approach

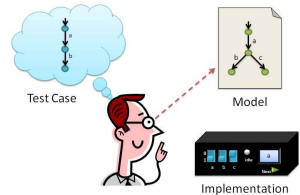
1. Construct a **model**:
 - 1.1 separate **concerns**,
 - 1.2 **abstract** from irrelevant concerns,
 - 1.3 specify the relevant **behavior** of the system and its **environment**



Model-Based Testing

Approach

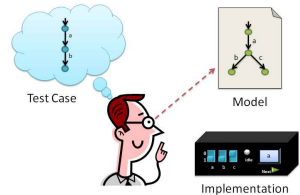
1. Construct a **model**:
 - 1.1 separate **concerns**,
 - 1.2 **abstract** from irrelevant concerns,
 - 1.3 specify the relevant **behavior** of the system and its **environment**
2. Define a test **selection** criteria based on test goals



Model-Based Testing

Approach

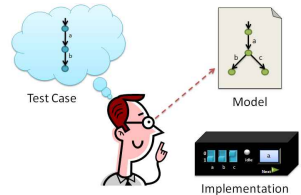
1. Construct a **model**:
 - 1.1 separate **concerns**,
 - 1.2 **abstract** from irrelevant concerns,
 - 1.3 specify the relevant **behavior** of the system and its **environment**
2. Define a test **selection** criteria based on test goals
3. Generate a **test suite**



Model-Based Testing

Approach

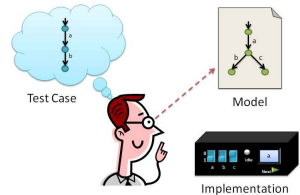
1. Construct a **model**:
 - 1.1 separate **concerns**,
 - 1.2 **abstract** from irrelevant concerns,
 - 1.3 specify the relevant **behavior** of the system and its **environment**
2. Define a test **selection** criteria based on test goals
3. Generate a **test suite**
4. Build the test **infrastructure** (adaptor, scripts, coverage tools)



Model-Based Testing

Approach

1. Construct a **model**:
 - 1.1 separate **concerns**,
 - 1.2 **abstract** from irrelevant concerns,
 - 1.3 specify the relevant **behavior** of the system and its **environment**
2. Define a test **selection** criteria based on test goals
3. Generate a **test suite**
4. Build the test **infrastructure** (adaptor, scripts, coverage tools)
5. **Run** the tests and **analyze** the results



Challenges

1. Data: how to **attach data** to behavior,
2. Strategies and coverage: how to **choose** the next step, when to **stop**, how to link **requirements** and **risks** with **models**
3. Product-line, variability, regression testing: upon **change** (in model or implementation) which test-cases should be **adapted** / **re-executed**

Some Resources

- ▶ H.R. Asaadi, R. Khosravi, M.R. Mousavi, and N. Noroozi. Towards Model-Based Testing of Electronic Funds Transfer Systems. Proc. of FSEN 2011.
- ▶ N. Noroozi, R. Khosravi, M.R. Mousavi, and T.A.C. Willemse. Synchronizing Asynchronous Conformance Testing. Proc. of SEFM 2011.