Security analysis of COM with Alloy

Presenter:
AliReza Namvar

Outline
- Motivation
- Problem
- Review of COM
- Security in COM
- Modeling with Alloy
- Preliminary Conclusions
- References

Motivation
- Security aspects in SD
  - Network security protocols
  - Secure applications
- Architectural infrastructures
  - Security in infrastructures
- Component-based SD
  - Secure component communications
Problem

- Formal analysis of existing component based architectural frameworks
- Case study:
  - modeling security in COM
  - Analysis Tool: Alloy Analyzer
- Evolution of Security model of COM
  - Extracting Invariant abstractions
  - Specifying the invariants in Alloy

Overview of COM

- What is COM?
- Interface negotiation
- Legal/outer vs. inner components

Security in COM

- Two categories of security
  - Activation
  - Call
- Utilizes OS security: permissions of a user to start a code, etc
- Based on DCE RPC security architecture
- Security in cross-process, cross-network server
Security in COM (cntd)
- "Service Control Manager"
  - CoRegisterClassObject, IRunningObjectTable::Register
  - IActivationSecurity Interface
- Call Security
  - DCE RPC mechanism
  - Automatic by COM infrastructure
- CSS: general APIs, server-side APIs, call-context interfaces

Alloy
- A first-order notation: Combines the best features of Z and UML
  - Schema structuring and a simple set-theoretic semantics
  - Various declaration shorthands

Why Alloy
- Specification in first order logic
  - Atomic representation for objects
  - Relational language
- Finite Search
- Deep semantic analysis
- Offers fully automatic analysis of object models
- Checks consistency of constraints
- Simulates execution of operations
**Analysis approach**

- Alloy Analyzer is a model refuter!

**Preliminary Conclusions**

- First model:
  - Declarative model of Security in COM
  - Extracting security patterns in COM

**References**

- Box, D., Essential COM, Addison-Wesley, 1998
- Jackson D., Alloy: Lightweight Modelling and Analysis with Alloy (Alloy Book)