Security Verification

Marieke Huisman
Jaco van de Pol

Fasten your seat-belts: co-chairing

- Key-message:
    - Better software design increases security
- Can we guarantee flaw-less protocols/designs and bug-free software/ code?
    - Probably not
    - But tools do help
- Protocol verification
    - Based on Process Algebra and Model Checking

With MACS1
(week 5-8)

- Software verification
    - Based on Program Logic and Formal Verification

With System Validation
(week 1-4)

Philosophy of this course

- Focus on verification technology; provided in the following basic courses:
    - System Validation
    - Models and Analysis of Computer Systems (1)
- Application to Security
    - Examples + Practical Excercises
    - Self-study: literature + presentation
- Somewhat related course in 2nd quartile: *Software Security*
    - Focus is on hardening software for security
    - Verification tools play a role, but only as a tool
- (these two new courses have been mixed up on blackboard at some point)

Part 1: System Validation

- Focus on software / code

- Annotations in the code specify "intended behaviour"

- Validated at design time
  - Based on Program Logic Technology
  - (Under the hood: automated reasoning)

- Can be used to:
  - Find vulnerabilities in code
  - Analyse information flow

Marieke Huisman

Zilverling 3039

M.Huisman@utwente.nl

Part 2: Modeling and Analysis of CS

Jaco van de Pol

Zilverling 3055

J.C.vandePol@utwente.nl

- Protocols are “programs for multiple parties”
  - Focus on interaction, input/output behaviour
  - Process algebra
- View a security protocol as:
  - N honest participants
  - 1 powerful intruder (Dolev-Yao model: describes “intruder capabilities”)
- Apply exhaustive verification
  - Generates all behaviour, including all possible attacks (in a limited setting)
  - Model checking

Important practicalities

- You will be added to the SV and MACS blackboard automatically
  - (to be sure we don't forget to update you)

- We will use a mailing list, also to broadcast the slides before the lecture:
  - sev@lists.utwente.nl

- Introduction meeting Security Verification:
  - Today, 13:45, room Carré CR 3D
  - Skype: sev2016-2017@outlook.com
  - Questions: over SkypeChat

- Please, do send us a mail ***right now*** if you are participating but not registered
  - M.Huisman@utwente.nl and J.C.vandePol@utwente.nl