Security Verification

Marieke Huisman

and all members of the
Formal Methods and Tools group

Why Security Verification?

- Better software design increases security
- Formal modelling and analysis can be used to improve security
  - Detect security vulnerabilities, information leakage, integrity violations…
  - Investigate if a security patch indeed solves the vulnerability
  - Investigate if a security patch does not have unwanted effects on functionality

- Can we guarantee flaw-less protocols/designs and bug-free software/ code?
  - Probably not
  - But tools do help
  - This course: try it yourself!

Practicalities

Marieke Huisman

Zilverling 3039

M.Huisman@utwe

- Basic understanding of various formal modelling and analysis techniques: follow System Validation (Q1, first lecture today, 5EC)

- Security Verification (any time of the year, 5EC)
  - Individual assignment
  - Coordinator: Marieke Huisman
  - Assignment supervisor: any FMT staff member
  - Goal of the assignment: use formal modelling and analysis on a concrete case study to detect or prevent security vulnerabilities

- Some ideas
  - Investigate if and how existing security vulnerabilities could have been detected
  - Analyse an existing application, and try to detect security vulnerabilities
- You are free to choose which properties to investigate, and which formal techniques to use