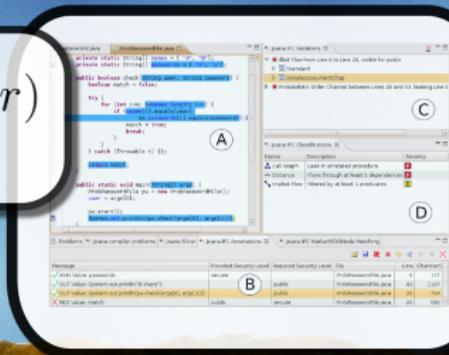


# Software-Sicherheitsanalyse

Seminar WS 14/15

Prof. Dr.-Ing. G. Snelting

$$\sum_{r \in \mathcal{I}} P_t(r) = \sum_{r \in \mathcal{U}} P_u(r)$$



- Veranstaltung unter dem Dach der MA-Module “Informatik-Seminar 1-3”
- Termin: Mo 16:00-17:00 (ab 8.12.), Raum 010
- Vortrag (ca 45min + Diskussion) + Ausarbeitung (ca 12-15 S.), 3 LP
- Allgemeine Einführung zum Thema *heute*
- Themenverteilung *heute*

- Veranstaltung unter dem Dach der MA-Module “Informatik-Seminar 1-3”
- Termin: Mo 16:00-17:00 (ab 8.12.), Raum 010
- Vortrag (ca 45min + Diskussion) + Ausarbeitung (ca 12-15 S.), 3 LP
- Allgemeine Einführung zum Thema *heute*
- Themenverteilung *heute*
- jeder Vortrag erarbeitet neuere Publikation(en) zum Thema
- wichtig: nachvollziehbare Präsentation
- wichtig: Erarbeitung *eigener* Beispiele
- wichtig: selbständige Recherche im Umfeld des Themas
- 1-2 Vorbesprechungen pro Vortrag
- Ausarbeitung *nach* dem Vortrag

- Veranstaltung unter dem Dach der MA-Module “Informatik-Seminar 1-3”
- Termin: Mo 16:00-17:00 (ab 8.12.), Raum 010
- Vortrag (ca 45min + Diskussion) + Ausarbeitung (ca 12-15 S.), 3 LP
- Allgemeine Einführung zum Thema *heute*
- Themenverteilung *heute*
- jeder Vortrag erarbeitet neuere Publikation(en) zum Thema
- wichtig: nachvollziehbare Präsentation
- wichtig: Erarbeitung *eigener* Beispiele
- wichtig: selbständige Recherche im Umfeld des Themas
- 1-2 Vorbesprechungen pro Vortrag
- Ausarbeitung *nach* dem Vortrag

Empfohlene Vorkenntnisse: ProgPar, sowie Compiler oder FOO  
Fragen?

- Veranstaltung unter dem Dach der MA-Module “Informatik-Seminar 1-3”
- Termin: Mo 16:00-17:00 (ab 8.12.), Raum 010
- Vortrag (ca 45min + Diskussion) + Ausarbeitung (ca 12-15 S.), 3 LP
- Allgemeine Einführung zum Thema *heute*
- Themenverteilung *heute*
- jeder Vortrag erarbeitet neuere Publikation(en) zum Thema
- wichtig: nachvollziehbare Präsentation
- wichtig: Erarbeitung *eigener* Beispiele
- wichtig: selbständige Recherche im Umfeld des Themas
- 1-2 Vorbesprechungen pro Vortrag
- Ausarbeitung *nach* dem Vortrag

Empfohlene Vorkenntnisse: ProgPar, sowie Compiler oder FOO  
Fragen? und nun: Einführungsvortrag

- A. Sabelfeld, A. Myers: Language-Based Information-Flow Security. IEEE J. Selected Areas in Communications, Vol 21 No 1, S. 5–19, 2003.
- G. Snelting et al.: Checking Probabilistic Noninterference Using JOANA. IT-IT, to appear, 2014. Preprint:  
`pp.info.uni-karlsruhe.de/publication.php?id=joana14it`
- G. Snelting: Understanding Probabilistic Software Leaks. Science of Computer Programming, 2013. Electronic edition:  
`pp.info.uni-karlsruhe.de/publication.php?id=snelting13scp`

1. Einführung: Sabelfeld 2003, Snelting 2013, ...  
gute Ausarbeitung besonders wichtig
2. Toolvergleich: TAJ/Andromeda, TaintDroid, FlowDroid, SX10, JOANA.  
systematischer Vergleich aller Implementierungen anhand Benchmark
3. Typsysteme: Smith JCS 1999, Smith JCS 2006, Nipkow JFR 2013.  
ProgPar/FOO/Formale Systeme hilfreich
4. IFC mit PDGs: Snelting ITIT 2014, Snelting 2009 IJIS , Giffhorn IJIS 2014,  
Sudbrock LOPSTR 2012.  
Compiler hilfreich
5. Quantitativer Informationsfluss: Ernst PLDI 2008, Smith FOSSACS 2009, Köpf  
SFM 2013, Tri PhD 2014.  
Kenntnisse in Informationstheorie hilfreich
6. Probabilistische Lecks: Volpano POPL 1998, Huisman 2996, Huisman FVOOS  
2011, Huisman ESSOS 2013.  
Kenntnisse in Semantik hilfreich
7. Verteilte Systeme: Mantel JCS 2003, Alpizar FAST 2009, Hennessy ENiTCS  
2014.  
Kenntnisse in Parallelprogrammierung hilfreich