

## 9. Übungsblatt

SS 2015  
Rechnersicherheit  
Ausgegeben am 11.06.2015  
Abgabe 18.06.2015

Marian Margraf  
Inst. für Informatik  
Freie Universität Berlin

### Aufgabe 1. (Bell-LaPadula)

Um die Umsetzung des Need-to-Know-Prinzip im Bell-LaPadula-Sicherheitsmodell zu vereinfachen, wurden in der Vorlesung Zuständigkeitsbereiche eingeführt und die Funktionen *cl* zu *sl* erweitert. Wie müssen die Zugriffskontrolleigenschaften (*ii*) und (*iii*) angepasst werden, damit die in der VL formulierten Ziele erfüllt werden?

### Aufgabe 2. (Biba-Integrity-Model)

Das in der Vorlesung kennengelernte Bell-LaPadula-Modell setzt das Schutzziel Vertraulichkeit (Informationsflusskontrolle) um. Beschreiben Sie das datenintegritätsorientierte Biba-Modell<sup>1</sup>. Vergleichen Sie die Modelle hinsichtlich der Zugriffskontrolleigenschaften.

### Aufgabe 3. (Flickercode)

Untersuchen Sie das „Flickercode“ Authentisierungsverfahren (auch: *chipTANcomfort*, *Sm@rtTANplus* oder *SmartTANoptic*) hinsichtlich ihrer Resistenz gegen Phishing, Key-Logging und Replay Attacks. Welche Schutzziele werden verfolgt und werden diese erreicht?

---

<sup>1</sup>Biba, K. J. „Integrity Considerations for Secure Computer Systems“, MTR-3153, Mitre Corporation, Juni 1975.  
(<http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf>)