technische universität dortmund

Prof. Dr. Jan Jürjens, Christian Wessel
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
Modellbasierte Softwaretechniken
für sichere Systeme – 26.06.2012

Modellbasierte Softwaretechniken für sichere Systeme - Übung 11

1 CEPS-Ladeprotokoll

1.1 Welcher Angriff wäre beim Aufladen der Karte möglich, wenn der in der Vorlesung genannte Transaktionszähler NT nicht existieren würde? (1 Punkt)

1.2 Modellieren Sie den Angriff auf das CEPS-System beim Aufladen der Karte als Sequenzdiagramm. (2 Punkte)

2 Sicherheitsrisiken in Cloud-Computing-Umgebungen

2.1 Beschreiben Sie die verschiedenen Arten von Cloudsystemen (IaaS, PaaS, SaaS), sowie die dazugehörigen Zugriffsmodelle (1 Punkt)

2.2 Erklären Sie die Sicherheitsrisiken, die sich durch die verschiedenen Zugriffsmethoden ergeben. (2 Punkte)

2.3 Cloud-Computing-Systeme sind aufgrund ihrer Architektur besonders gefährdet für bestimmte Angriffe. Nennen Sie mögliche Angriffsszenarien auf Cloud-Computing-Systeme. (2 Punkte)

Gehen Sie dabei auf die verschiedenen Zugriffsmodelle ein. Private Clouds sind beispisleweise anderen Angriffen ausgesetzt als Public Clouds.

3 Modellierung von Cloud-Computing-Systemen (2 Punkte)

Gegeben sei ein cloudbasiertes SaaS-Angebot in einer Public Cloud. Dabei handelt es sich um einen kostenpflichtigen Webmail-Dienst über den Kunden Mails schreiben, empfangen und lesen können. Die Benutzeroberfläche wird über Webserver zur Verfügung gestellt und die eigentlichen Mails werden zur besseren Handhabbarkeit in Datenbanken gespeichert. Das Abrechnungssystem des Dienstes befindet sich ebenfalls in der Cloud. Modellieren Sie den Dienst als UML-Diagramm und annotieren Sie das Diagramm mit den passenden UMLsec-Stereotypen, damit Sicherheitsrisiken möglichst minimiert werden.