Batchelorthesis

# Entwicklung und Implementierung eines Honeypots mit den Amazon Web Service

## Ausgangssituation

Angriffe auf Netzwerkdienste sind eine ständige Gefahr. Mit sogenannten Honeypots ist es möglich, Informationen über Angriffsmuster und das Angreiferverhalten zu erhalten, ohne Produktionssysteme einer Gefahr auszusetzen. Honeypots simulieren Produktionssysteme, sollen Angreifer beschäftigen und möglichst viele Informationen über das Verhalten der Angreifer speichern.

## Konkrete Aufgabenstellung

Ihre Aufgabe beinhaltet u.a. folgende Teilaufgaben:

- Evaluation, welche Netzwerkdienste für einen Honeypot interessant sind.
- Evaluation der Möglichkeiten, Informationen über das Angreiferverhalten zu erfassen und zu sichern (insbesondere Scans der Netzwerkports, fehlgeschlagene und erfolgreiche Anmeldeversuche, ausgeführte Kommandos in der Shell, usw.).
- Realisierung eines Honeypots mit den Amazon Web Services oder mit einem vergleichbaren Infrastrukturdienst (inklusive Erstellung einer detaillierten Installationsanleitung).
- Analyse der gewonnen Erkenntnisse aus erfolgten Angriffsversuchen auf den realisierten Honeypot.

Interessenten werden sich bitte an Prof. Dr. Christian Baun:
christianbaun@fb2.fh-frankfurt.de
http://www.christianbaun.de