PhD-Seminar des „Kompetenzzentrum für Netzwerke & verteilte Systeme“

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Wann: Mittwoch, 31. Januar 2018, 17:00 Uhr

Wo: BCN-Gebäude, Raum 533

Im Rahmen des Angebotes der CEDAR-Graduiertenschule der Frankfurt University laden wir Sie gerne zum ersten PhD-Seminar in 2018 für Promovierende und Professor/-innen des „Kompetenzzentrum Netzwerke und verteilte Systeme“ ein:

- **Begrüßung**
- **Damir Dobric:**
- *"Artificial intelligence, machine learning algorithms and models on top of scalable distributed system"*
- **Fragen & Diskussion**
- **Dr. Lorena Gutiérrez-Madroñal:**
  "Mutants and IoT as research lines"
- **Fragen & Diskussion**
- **Thekla Unthan**
  "Real Time Data Anomaly Detection as a tool to identify possible Probing Attacks for Network Forensics."
- **gemeinsamer Ausklang**

Zu den Referenten und ihren Themen:

1. Damir Dobric ist Microsoft Regional Director und Lead Software Architekt bei DAENET. Er ist Dozent für Software Engineering und Distributed Systems an der Frankfurt University of Applied Sciences mit Fokus an Internet of Things, Machine Learning und Cloud Technologie.

Seine in 2018 gerade gestartete Doktorarbeit hat das Ziel zu untersuchen, wie verteilte Systeme wie z.B. Actor Model und andere helfen können, die Machine Learning Algorithmen zu skalieren. Im besonderen Fokus dieser Arbeit steht die Erforschung und Implementierung von Modellen, die mit der Funktionseise von Neocortex inspiriert sind.
Solche Modelle sollen in der Lage sein das kontextuelle Lernen im verteilten System abzubilden.

Dieser Vortrag soll die grundlegende Idee darstellen, die auf Basis von neuesten Erkenntnissen aus Neurowissenschaften und verteilten Systemen darstellt.

2. Dr. Lorena Gutiérrez-Madroñal ist ein Mitglied der UCASE Software Engineering research group der University of Cádiz (Spanien).

Das Internet of Things (IoT) wird in vielen Bereichen immer wichtiger. Eines der Hauptprobleme von IoT Systemen ist die große Menge der Informationen, die diese Systeme bewältigen müssen. Damit die richtigen Entscheidungen getroffen werden können, muss die Information in Realzeit verarbeitet werden. Als Konsequenz müssen neue Wege (Werkzeuge, Geräte, Mechanismen) der Informationsbeschaffung, Verarbeitung und Übertragung beschritten werden. Die sogenannten "Event Processing Languages" (EPL) dabei erwähnenswert. Sie wurden entwickelt, um Vorfälle von Interesse in einer speziellen Domäne in Echtzeit zu entdecken. Eine große Menge an Daten wird von den ELPs verarbeitet und analysiert, daher kann jeder Programmierfehler, wegen eines schlechten Entscheidungsfindungssystems, ernste Folgen haben.
Bedenkt man, dass die Verarbeitung der Daten entscheidend ist, wird klar, dass die EPL Programme sorgfältig getestet und analysiert werden müssen. Um diese Programme zu testen, wird eine große Menge an Vorfällen mit spezifischen Werten und Strukturen benötigt. Da dies eine schwierige Aufgabe ist, die sehr fehleranfällig ist, wenn sie manuell durchgeführt wird, soll hier eine Methode vorgestellt werden, die die automatische Erstellung solcher Vorfälle anspricht. Diese Methode kann auf verschiedene Tests angewandt werden: Negative Testing, Stress, Unit, Mutation Testing… Das Mutation Testing, eine Technik, die im Fault Testing verwendet wird, wurde in einer Reihe von Studien, die verschiedene Programmiersprachen entwickelt haben, untersucht. Da diese Technik bisher nicht auf das IoT angewendet wurde, ist die EPL von EsperTech ausgewählt worden, um das zu ändern. Die Resultate von Experimenten und real-welt Tests zeigen, dass die entwickelte Methode den an sie gestellten Ansprüchen genügt.

3. Thekla Unthan ist eine wissenschaftliche Mitarbeiterin an der Frankfurt University of Applied Sciences und koordiniert unter anderem die Forschungskooperation zwischen dem Fachbereich 2: Informatik und Ingenieurwissenschaften der Frankfurt University of Applied Sciences (FRA-UAS) und der Plymouth University (PU).

Mit all den positiven Möglichkeiten des Internets wachsen leider auch die Möglichkeiten für Missbrauch zum Beispiel Phishing oder Angriffe mittels Schadsoftware.
Um diese Art Kriminalität aufzuklären, bedarf es besonderer Methoden. Die größte Herausforderung beim Aufklären von Internet Verbrechen besteht darin, dass die Spuren, die der Datenverkehr in Netzwerken hinterlässt, enorm flüchtig sind. Dem kann man nur proaktiv begegnen, indem die relevanten Daten rechtzeitig gesichert werden.
Zu entscheiden welche Daten relevant sind und welche nicht, wenn keine Informationen darüber vorliegen ob, wann und was für ein Angriff stattfindet, ist allerdings kein triviales Problem. Damit der zur Verfügung stehende Speicherplatz nicht durch Daten aus dem normalen Netzwerk Verkehr ausgeschöpft wird, soll mit Hilfe von Maschine Learning Methoden nach Anomalien gesucht werden. Dabei soll der Focus auf dem Probing liegen, das häufig dem eigentlichen Angriff vorausgeht. Beim Probing sucht der Angreifer mittels Port Scans oder Ping Sweeps nach Schwachstellen des potentiellen Opfers, die er dann für den eigentlichen Angriff ausnutzen kann.

Sie sind interessiert? Falls ja, senden Sie bitte eine kurze Nachricht an thekla@fb2.fra-uas.de. Sie kennen weitere interessierte Masterstudierende? Dann leiten Sie diese E-Mail bitte einfach weiter. Wir freuen uns auf Ihre aktive Teilnahme!

Mit freundlichen Grüßen
Thekla Unthan