Kategorie „Beste Dissertation"

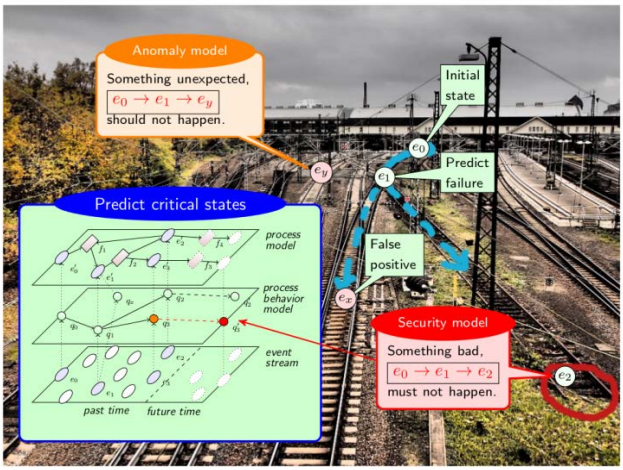
Security Analysis of System Behaviour - From 'Security by Design' to 'Security at Runtime'

Dr. Roland Rieke http://rieke.link
Fraunhofer SIT, Darmstadt
Philipps-Universität Marburg

Das Internet bietet heute das Umfeld für neuartige kooperierende Systeme, die sich weit über den im Voraus geplanten Zweck entwickeln können. Gleichzeitig wachsen die Sicherheitsbedürfnisse. Dies gilt insbesondere für neue kritische Infrastrukturen (z.B. Fahrzeug-ad-hoc-Netzwerke und vernetzte Flugsicherungsdienste) aber auch für mobile Geldtransferdienste und wichtige Geschäfts- und Fertigungsprozesse (Industrie 4.0). Modellbasierte Methoden haben sich etabliert, um die Komplexität beim Entwurf und der Implementierung sicherer Systeme besser zu bewältigen (Security-by-Design).

Dr. Roland Rieke
Beste Dissertation 2015

In dieser Dissertation wurden Methoden und Tools zur Verifikation von Sicherheitseigenschaften kooperierender Systeme und zur Optimierung der Konfiguration der Systeme entwickelt. Ein wichtiger theoretischer Beitrag sind *Konstruktionsprinzipien*, die gewährleisten, dass Sicherheitseigenschaften skalierbarer Systeme bei einer Erweiterung um gleichartige Komponenten erhalten bleiben.



Security@Runtime ergänzt Security-by-Design

Zur Sicherheitsüberwachung zur Laufzeit werden modellbasierte Methoden derzeit nicht genutzt. Die in dieser Dissertation erarbeitete *prädiktive Sicherheitsanalyse* erweitert daher die Methoden um die Anwendbarkeit zur Laufzeit. Die Kooperation in den hier betrachteten Systemen wird meist über Geschäftsprozesse und technische Abläufe gesteuert. Die Idee ist nun, das Wissen über das erwartete Verhalten der Prozesse und die Sicherheitsvorgaben zu nutzen, um die Sicherheit von vernetzten kooperierenden Systemen zur Laufzeit vorausschauend zu bewerten. Dies ermöglicht eine Warnung vor möglichen Gefahren und eine der Situation angepasste, proaktive Reaktion. Die prädiktive Sicherheitsanalyse bietet dazu (a) Prozesskonformitäts-Tracking, (b) Sicherheits-Compliance-Tracking und (c) die Prädiktion von sicherheitskritischen Zuständen.

Das *Prozesskonformitäts-Tracking* in Bezug auf Verhaltensanomalien (mögliche Angriffe) nutzt ein ausführbares Prozessmodell, um das damit vorgegebene (‚de-jure') Verhalten mit dem ‚de-facto' Verhalten des laufenden Prozesses zu vergleichen. Das ‚de-facto' Verhalten wird dabei über einen Ereignisstrom aus den überwachten kooperierenden Systemen gegeben. Ein neuartiges *Uncertainty Management* unterstützt eine semi-automatische Anpassung des Prozessmodells, falls auftretende Abweichungen durch die natürliche Evolution der Prozesse ausgelöst werden. Bei Fehlverhalten oder Störungen des Prozesses wird jedoch ein Alarm ausgegeben, der auch Entscheidungs- und Reaktionshilfe bietet. Je nach Situation können damit Trigger für automatische Gegenmaßnahmen ausgelöst werden.

Das *Sicherheits-Compliance-Tracking* nutzt Sicherheitsvorgaben, welche über Monitorautomaten operationalisiert werden, um explizite Verstöße gegen die Sicherheitsregeln zur Laufzeit festzustellen.

Die *Prädiktion von sicherheitskritischen Zuständen* in der nahen Zukunft nutzt darüber hinaus das ausführbare (‚de-jure') Prozessmodell zur Simulation des Prozessverhaltens in der nahen Zukunft. Damit können die Sicherheitsmonitore das Prozessverhalten auch auf bevorstehende sicherheitskritische Zustände untersuchen.

Die Machbarkeit wurde anhand von Prozessen aus mehreren Industrieszenarien in den Bereichen Logistik, mobiler Geldtransfer, kritische Infrastrukturen und dem IT-Management der Olympischen Spiele demonstriert.

Diese Arbeit wurde von Prof. Dr. Bernd Freisleben und Prof. Dr. Bernhard Seeger an der Philipps-Universität Marburg betreut. Download: http://archiv.ub.uni-marburg.de/diss/z2014/0499/