Fraunhofer
FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

RACOMAT

Kontakt
Johannes Viehmann
Geschäftsbereich SQC
Tel. +49 30 3463-7274
Fax +49 30 3463-99 7274
johannes.viehmann
@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de

RACOMAT
Risk Assessment COMbined with Automated Testing

Vernetzte Informations- und Kommunikationssysteme sind in unserem Alltag allgegenwärtig: In der industriellen Produktion oder in kritischen Infrastrukturen wie der Stromversorgung oder dem Bankensektor sind wir bereits heute hochgradig von ihnen abhängig. Mit neuen Technologien, wie z. B. autonomen Fahrzeugen, wird ihre Bedeutung weiter zunehmen. Das unmittelbare, existenzielle Wohl von Personen wird damit verstärkt Informations- und Kommunikationssystemen anvertraut. Entsprechend hoch sind die Anforderungen an deren Sicherheit und Zuverlässigkeit. RACOMAT ist ein Werkzeug für das Risiko-Management solcher Systeme, das Sicherheitstests mit einem komponentenbasiertem, kompositionalem Risiko Assessment verbindet. Dadurch wird eine Automatisierung von der Risikomodellierung bis hin zum Sicherheitstesten möglich.

Das RACOMAT Tool

Um ein Bild der Risikolage zu modellieren und zu visualisieren, verwendet das RACOMAT Tool intuitiv verständliche Risikographen. RACOMAT unterstützt das Identifizieren von potenziellen Schwachstellen und Gefährdungen mit vorhandenem Expertenwissen aus bestehenden Bibliotheken. Ausgehend von einem Gesamtbudget für das Risiko Assessment berechnet das RACOMAT Tool, wie viel Aufwand für das Security Testen sinnvoll ist, um die Qualität des Risikobildes durch Reduktion von Unsicherheiten zu verbessern. Mithilfe von Security Test Pattern und Tool-generierten Systemmodellen wird automatisches oder zumindest semi-automatisches Testen realisiert. Für ein weitergehendes Risiko Management, also für die Risikobewertung und Risikobehandlung, ist eine kompaktere Darstellung mit Fokussierung auf die wirtschaftlichen Aspekte sinnvoll. Das RACOMAT Tool bietet dem Management dazu ein Dashboard, in dem die Risiken als zu erwartende Kosten pro Zeiteinheit ausgedrückt werden und Funktionen, um die Risikobehandlung zu planen und zu kontrollieren.

MIT DEM RACOMAT-TOOL GELINGT EIN RISIKO-MANAGEMENT AUCH BEI KOMPLEXEN SYSTEMEN

Vorgehensweise beim Risiko-Assessment

RACOMAT erlaubt es, Business Szenarien zu modellieren und die Geschäftsprozess-Modelle mit der dahintersteckenden technischen Infrastruktur zu verknüpfen, sodass die Auswirkungen technischer Risiken auf das Kerngeschäft analysiert werden können. Mithilfe Domain-spezifischer Assistenten kann auch dies bis zu einem gewissen Grad automatisiert werden. Für den Finanz- und Bankenbereich wurde bereits ein solcher Assistent als Plug-In entwickelt.

Vorgehensweise beim Risiko-Assessment

Das RACOMAT Tool unterstützt ein zum Industriestandard ISO 31000 konformes Risiko-Management. Es legt eine iterative Vorgehensweise beim Risiko-Assessment nahe. Ein initiales, grobes Risikobild wird dabei in mehreren Runden schrittweise verbessert. Die Konzepte Risk-Based Security Testing (RBST, also die Optimierung des Sicherheits-testensmithilfe des Risiko Assessments) und Test-Based Risk Assessment (TBRA, also die Verbesserung des Risiko Assessments mithilfe von Sicherheitstests) werden dazu vereint, um die Stärken beider Ansätze zu verbinden.

Iteratives Risikomanagement

1. Initiales Risikomodell basierend auf Literatur, Erfahrungswerten und Experteneinschätzungen entwickeln
2. Ereignissimulationen nutzen, um die Konsequenzen und Gesamtrisiken von Bedrohungen zu berechnen
3. Bedrohungsszenarien mit den größten Unsicherheiten auswählen, welche mithilfe von Sicherheitstests genauer analysiert werden sollen
4. Erforderliche Testfälle generieren
5. Tests ausführen und mithilfe der Ergebnisse das Risikomodell verbessern
6. Mit verbessertem Risikomodell erneut Ereignissimulationen durchführen, um Gesamtrisiken genauer zu ermitteln

– Weiter mit Schritt 3 bis das Budget für die Risikoanalyse aufgebraucht ist

7. Finale Risikoevaluation und Maß-nahmen zur Reduktion unakzeptabel hoher Risiken

jda | 1307 (Fotos: iStock – oluolu3)