Modell-basiertes Testen von IT-Sicherheitsaspekten

Ina Schieferdecker

Über 90 Prozent aller Software-Sicherheitsstörfälle werden durch Angreifer verursacht, die bekannte Sicherheitslücken ausnutzen. Das Projekt DIAMONDS (Development and Industrial Application of Multi-Domain Security Testing Technologies) erarbeitet unter der Leitung von Fraunhofer FOKUS, Berlin effiziente und automatisierte Sicherheitstestmethoden für sicherheitskritische, vernetzte Systeme in verschiedenen industriellen Domänen wie Industrieanlagen, Banking oder Telekommunikation.

Die Vernetzung unterliegt derzeit drastischen Veränderungen: Die Zeiten eher statischer Kommunikation über streng kontrolliert gekoppelte Netze zu einem begrenzten Zweck sind vorüber – das Internet und andere Kommunikationstechnologien durchdringt immer mehr private, wirtschaftliche und soziale Bereiche mit neuen Ansätzen hinsichtlich dynamischer und offener vernetzter Umgebungen. Während die Verbindung von Systemen neue Funktionalitäten und Funktionen ermöglicht, ergeben sich daraus auch neue Dimensionen an Schwachstellen, welchen üblicherweise mittels der Absicherung eines Systems gegen Angriffe von direkten Systemanwendern begegnet wird. Sicherheitstechnik steht heute immer mehr vor den Herausforderungen der Offenheit, Dynamik und Verteilung vernetzter Systeme: Die meisten Nachweis- und Gültigkeitsprüftechniken wurden im Rahmen statischer oder bekannter Konfigurationen mit vollständiger oder genau definierter Kontrolle über jede einzelne Systemkomponente entwickelt. Wir müssen vernetzte Systeme ganzheitlich berücksichtigen, die mobilen oder festen Zugang über das Internet oder andere Kommunikationstechnologien ermöglichen.

Ina Schieferdecker

Dieser Trend betrifft eine Reihe von Bereichen, beispielhaft seien hier die Transportbranche (Zugkontrollsysteme), die Medizin (computergestützte Arbeitsablaufsystem für das Gesundheitswesen), die Automobilbranche (Fahrzeugnet-

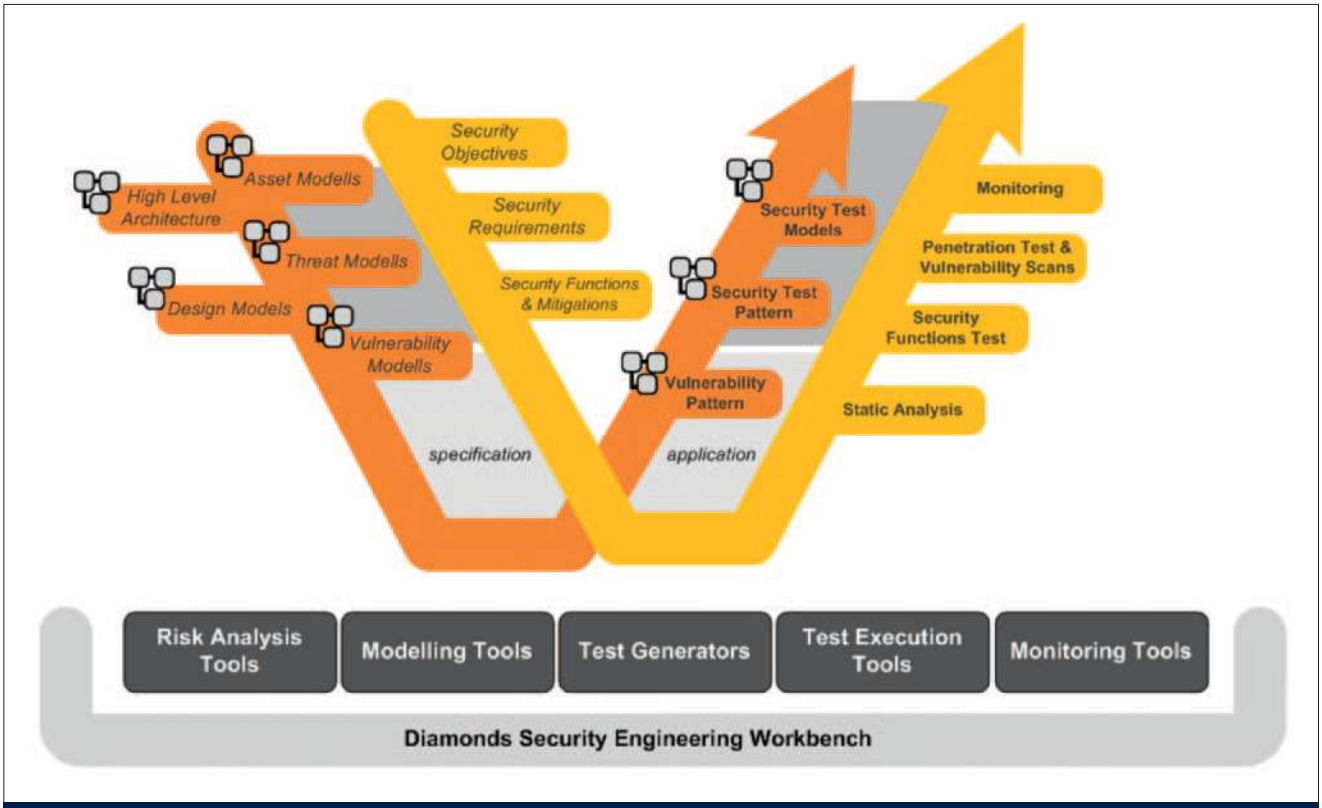

Abb. 1: Überblick der DIAMONDS-Sicherheitstestmethodik

ze, Car2X-Kommunikationssysteme) oder die Telekommunikation (mobile vernetzte Systeme, Web-X.0-Systeme und -Anwendungen) genannt. Viele dieser Systeme unterliegen kritischen Bedingungen: Ihr Ausfall kann menschliches Leben und die Umwelt gefährden, ernsthafte Schäden für die industrielle und soziale Infrastruktur bedeuten, Vertraulichkeit und Privatsphäre gefährden und die Überlebensfähigkeit ganzer Wirtschaftssektoren untergraben.

Während die Verbindung von Systemen neue Funktionalitäten und Funktionen ermöglicht, ergeben sich daraus auch neue Dimensionen an Schwachstellen. Sicherheitstechnik steht heute immer mehr vor den Herausforderungen der Offenheit, Dynamik und Verteilung vernetzter Systeme: Die meisten Nachweis- und Gültigkeitsprüftechniken wurden im Rahmen statischer oder bekannter Konfigurationen mit vollständiger oder genau definierter Kontrolle über jede einzelne Systemkomponente entwickelt.
DIAMONDS bezieht diese besonderen Sachverhalte der Sicherheitsprüfungen für vernetzte Systeme mit ein, um die Zuverlässigkeit vernetzter Systeme angesichts von Böswilligkeit, Angriffen, Fehlern oder Unglücken zu überprüfen. Wir konzentrieren uns auf bestimmte Sachverhalte, um das Vertrauen in solche Systeme aufzubauen, indem wir die Robustheit und Fehlertoleranz vernetzter Systeme gegenüber Angriffen aufzeigen. DIAMONDS untersucht Sicherheitslücken von vernetzten Systemen ganzer Branchen aus ausgewählten Bereichen (einschließlich Banken, Chipkarten, Mobilfunk und Industrieautomatisierung), um daraus gemeinsame Prinzipien und Methoden abzuleiten und damit effiziente Sicherheitsprüfmethoden von industrieller Bedeutung zu ermöglichen.

DIAMONDS ist ein europäisches ITEA (Information Technology for European Advancement) Projekt mit 22 Partnern aus Finnland, Frankreich, Luxemburg, Norwegen, Österreich und Deutschland. Das Projekt mit 120 PJ wurde im Oktober 2010 gestartet, wobei weitere Partner im Laufe dieses Jahres eingestiegen sind, und wird bis Mai 2013 laufen. DIAMONDS befasst sich mit dem steigenden Bedarf an systematischen Sicherheitsprüfmethoden, indem es Techniken und Methoden entwickelt, die effizient zur Absicherung von vernetzten Systemen und Anwendungen in verschiedenen Domänen eingesetzt werden können. Das Projekt arbeitet an (siehe auch Abb. 1): fortgeschrittenen aktiven modellbasierte Sicherheitstestmethoden, die Testmodelle und verschiedene Testgenerierungsstrategien zur Erhöhung der Sicherheit in den sicherheitsrelevanten Bereichen nutzen, der Entwicklung von passiven Testtechniken, die auf automatisierten Monitor-Techniken basieren

und die Robustheit dynamischer Systeme bewerten, der Erstellung eines Katalogs von Sicherheitstestmustern für die unterschiedlichen Anwendungsbereiche und an einer Open-Source-Plattform für die Integration von Sicherheits-Testwerkzeugen.

DIAMONDS widmet sich insbesondere der Applikation der Methoden und Techniken in der industriellen Anwendung. Daher liegt ein besonderer Schwerpunkt bei DIAMONDS auf den zahlreichen und sehr unterschiedlichen Fallstudien. Es soll nachgewiesen werden, dass die Methoden nicht industriezweigspezifisch, sondern allgemeingültig Anwendung finden können.

Das deutsche DIAMONDS Projekt, das vom Bundesministerium für Bildung und Forschung teilfinanziert wird, beschäftigt sich vor allem mit dynamischen, aktiven Tests von Sicherheitsaspekten vernetzter Systeme entsprechend der Vorgaben des ISO Common Criteria (CC) Katalogs und deren modell-basierter Generierung. Es werden zwei industrielle Fallstudien verfolgt: Zum einen die vernetzte Banknoten-Maschine von Giesecke & Devrient GmbH, die für zukünftige Szenarien auf IT-Sicherheit hin untersucht und getestet wird. Zum anderen in der Fallstudie von Dornier Consulting ein Automotive Infotainment System in Relation zu Fahrzeugnetzen. Der Technologiepartner Testing Technologies bringt seine Expertise in der Testautomatisierung und Entwicklung von Testwerkzeugen ein. Fraunhofer FOKUS ist der Forschungspartner im Projekt und wird basierend auf seinen Methoden, Technologien und Werkzeugen mit den anderen Partnern die DIAMONDS-Sicherheitstestmethodik entwickeln. Dabei liegen die Schwerpunkte auf der Anwendung und Erweiterung modell-basierten Testens für Sicherheitstests. Ausgangspunkt ist eine Risikomodellierung unter Nutzung von CORAS, die sicherheitsorientierte System- und Testmodellierung unter Nutzung von UML in Kombination mit dem risiko-orientierten Testansatz, der in ROTESS entwickelt wurde und derzeit mit TestBE ausgebaut wird. Ergänzend werden Testmethoden entwickelt, die auf Basis der UML eine effektive Generierung von Sicherheits- und Robustheitstestfällen erlauben (z.B. Fuzz-Test-Methoden für UML Sequenzdiagramme). Siehe weiterführende Informationen. Während sich Deutschland methodisch auf CC-kompatible, dynamische, aktive Tests konzentriert, betrachtet Norwegen im Wesentlichen Testprozesse und Optionen der Migration, Frankreich passive Tests, Finnland Fuzz-Test-Methoden und Österreich und Luxemburg die Bewertung der entwickelten Testmethoden. Im Wesentlichen folgen die Arbeiten in DIAMONDS den Anforderungen der Fallstudien, für die passende Methoden und Verfahren erarbeitet und in Werkzeugen umgesetzt werden. In Reflektion der Ergebnisse der Fallstudien wird die DIAMONDS-Sicherheitstestmethodik bewertet und optimiert. Die Ergebnisse werden Interessierten zur Verfügung gestellt – erste Ergebnisse sind auf der Projekt-Website veröffentlicht. Die Projektergebnisse werden zudem durch Beiträge in der Standardisierung bei ETSI und in Arbeiten mit dem BSI verfügbar gemacht. Es wurde eine Special Interest Group zum Thema Security Testing bei ETSI gebildet, die ein erstes öffentliches Treffen im Dezember 2011 bei Fraunhofer FOKUS, Berlin hat. Interessierte sind dazu herzlich eingeladen.

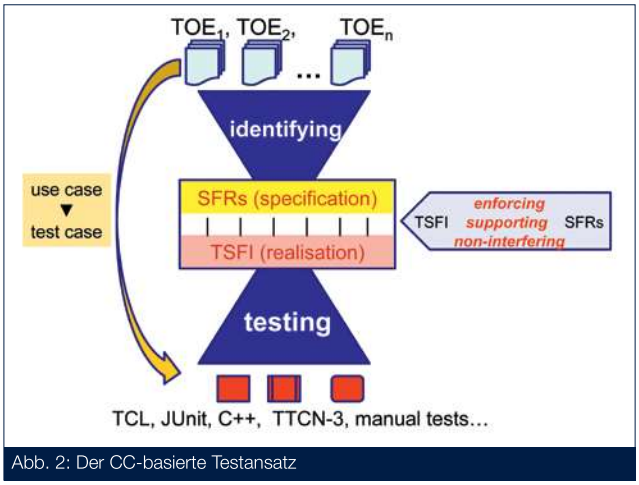

Abb. 2: Der CC-basierte Testansatz

Neben ersten Projektergebnissen konnte kürzlich ein Achtungserfolg erzielt werden: Das Projekt DIAMONDS überzeugte auf dem ITEA & ARTEMIS Co-Summit 2011 in Helsinki und gewann dort den ITEA Exhibition Award 2011 aus 42 ITEA-Projekten. Der Publikumspreis ehrt jährlich das Projektteam, das seine Ziele und Ergebnisse am anschaulichsten präsentiert.

WEITERFÜHRENDE INFORMATIONEN

DIAMONDS: Development and Industrial Application of Multi-Domain Security Testing Technologies, http://www.itea2-diamonds.org

CORAS: Model-based Method for Security Risk Analysis, http://coras.sourceforge.net/

UMLsec: Extending UML for Secure Systems Development, http://www-jj.cs.tu-dortmund.de/jj/umlsec/

ROT: Risk-Oriented Testing, http://www.fokus.fraunhofer.de/de/motion/projekte/laufende_projekte/ROTESS/index.html

TestBE: Testing based on Behavior Engineering Models, http://www.behaviorengineering.org/

Fuzz testing: Attack your programs before someone else does: http://www.ibm.com/developerworks/java/library/j-fuzztest/index.html

Die Autorin

Ina Schieferdecker arbeitet an der Freien Universität Berlin und bei Fraunhofer FOKUS an der Modell-getriebenen Entwicklung und Qualitätssicherung software-basierter Systeme und leitet das hier vorgestellte Projekt DIAMONDS. Sie erreichen sie über ina.schieferdecker@fokus.fraunhofer.de