complex solutions designed with little attention to real-world issues. Developers, frustrated by the difficulty of understanding the system operation underlying the language constructs, then resorted to C-like languages, ultimately arguing that higher-level abstractions were not feasible in real-world deployments due to resource scarcity.

With Torre Aquila, in contrast, we demonstrated that higher-level WSN programming abstractions are not only feasible in real-world deployments and do increase the programming productivity, but they are actually necessary to realize complex applications. Indeed, we designed and implemented the monitoring system in Torre Aquila atop our TeenyLIME middleware instead of the operating system. TeenyLIME abstracts away the fragmentation of memory space across neighbouring devices under a single memory space. Such design allowed us to push more functionality in the memory-scarce WSN nodes that we would have been able to do with the operating system alone. Our abstractions allowed many mechanisms across different functionality to be factored out, ultimately resulting in smaller overall memory occupancy.

Torre Aquila and the TeenyLIME middleware are not isolated examples. As much as we conceived further abstractions to tackle different programming challenges (eg the Logical Neighborhood abstraction and the Squirrel system), we also built real-world applications with them, notably including safety-critical ones like closed-loop control in operational road tunnels. The resulting systems performed effectively and efficiently, providing fine-grained environmental data or efficient control in a range of situations.

Of course, many challenges still lie ahead in this and closely related fields. The programming challenge itself is far from being solved. We will be in the position to claim so, for example, when domain experts will develop Internet of Things applications with little or no knowledge of embedded systems and distributed programming. We believe however, that one of the grand challenges on the horizon will be the testing and verification of Internet of Things applications, especially prior to deployment. Devising effective solutions in this field will increase confidence in Internet of Things technology and thus the opportunities to investigate novel applications, creating a virtuous circle that will ignite further developments, in the same way that it happened for the "standard" Internet.

Acknowledgements: The research described here is the result of joint efforts of the author with many talented researchers at Politecnico di Milano, University of Trento, Bruno Kessler Foundation, and SICS, the Swedish Institute of Computer Science. The author is deeply indebted to all of them.

Luca Mottola is a winner of the 2011 ERCIM Cor Baayen award.

Links:
http://www.sics.se/~luca
http://www.sics.se/nes

Please contact:
Luca Mottola, SICS, Sweden
E-mail: luca@sics.se

DIAMONDS do IT with MODELS: Innovative Security Testing Approaches

by Ina Schieferdecker, Axel Rennoch and Jürgen Großmann

Although security and model-based testing are not new areas of research, they are still under development and highly relevant. In particular, their combination is a challenge for academic work and industrial applications. Some examples of systematic and automated security testing include: security functional testing, model-based fuzzing, risk-oriented testing and the usage of security test pattern.

Multiple standardization committees provide significant efforts in the context of security testing. They cover fundamental frameworks but also detailed test specifications for concrete technologies. The range of activities is very large and includes classical concepts from security evaluation using Common Criteria (ISO/IEC 15408) for Information Technology Security Evaluation (CC) and innovative European activities from ETSI like TVRA (Threat Vulnerability Risk Analysis).

The CC is an international standard for the certification of IT-security products. The evaluation process is largely driven by developer documentation and focuses on product development, security testing and vulnerability assessment. In addition to creating trust in the product's quality, the evaluation results also allow the customer to compare the security functionality of similar products.

The TVRA method developed by ETSI benefits from the CC's work by using a well-established domain-independent generic catalogue of security functional requirements (SFRs), and is characterized by the following concepts and approaches: Threat types like interception, manipulation, denial-of-service, repudiation of messages; security objectives like confidentiality, integrity, availability, authenticity, accountability; UML to model relationships within systems; methods to analyze/evaluate threats, risks, vulnerabilities; calculation of attack potential; and the security requirements taxonomy for SFRs (from CC).

CC and TVRA both require further knowledge about how to derive security tests from the TOE description. The ITEA DIAMONDS project invests in the automatic generation of security tests from system models. The security tests needed in the quality assurance phase and/or evaluation procedures may be derived manually from the system description. Model-based approaches are currently used to contribute towards the generation of security tests. DIAMONDS work includes fuzzing, risk-based testing and security test pattern.

The aim of fuzzing is to find deviations of the real System under Test (SUT) to its specification that lead to vulnerabilities because invalid input is processed by the SUT instead of being rejected. Such deviations may lead to undefined states of the SUT which can be exploited by an attacker, for example by allowing a denial-of-service attack because the SUT is crashing or hanging.

Risk-based security testing can generally be introduced with two different goals in mind. On the one hand, risk based testing approaches can help to optimize the overall test process. The results of the risk analysis, ie the results of threat and vulnerability analysis, are used to guide the test identification and may complement requirements engineering results with systematic information concerning threats and vulnerabilities of a system. A comprehensive risk assessment additionally introduces the notion of risk values, that is the estimation of probabilities and consequences for certain threat scenarios.

The “Security Testing chocolate box” presented by DIAMONDS at the ITEA2/ARTEMIS co-summit event 2011 in Helsinki provides a catchy example and a basic model of most security relevant terms (using CORAS) in the context of model-based security testing. It uses a chocolate box as an analogy of a SUT / Target of Evaluation (TOE), different types of chocolate as the assets, and Fredi, an intelligent fox, as the threat that wants chocolate. A security analysis focuses on the box interfaces, vulnerabilities (cover plate and a slot in the cover plate) and threat scenarios (using some tools to get the assets out of the box), in order to avoid “unwanted incidents”, ie the chocolate leaving the box.

Details of fuzzing and risk-based testing can be found in the DIAMONDS deliverables. The project also looks at approaches for capturing security test patterns to create an initial repository thereof, based on the weaknesses and strengths of the systems involved. Like other types of pattern, security test patterns will be both procedural and structural, leading to various sorts of test artefacts, ranging from high-level test activities and methods, via more specific test requirements through to concrete elements of test design, eg test architecture, test behaviour and test data.

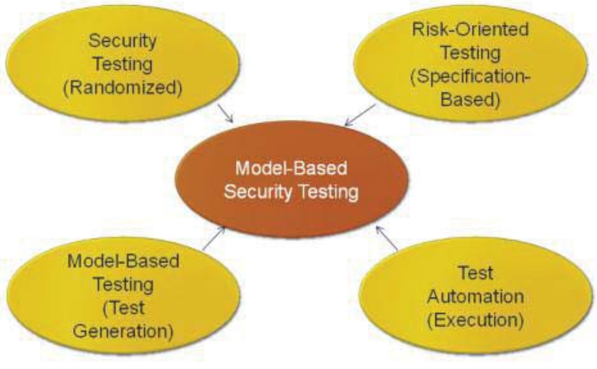
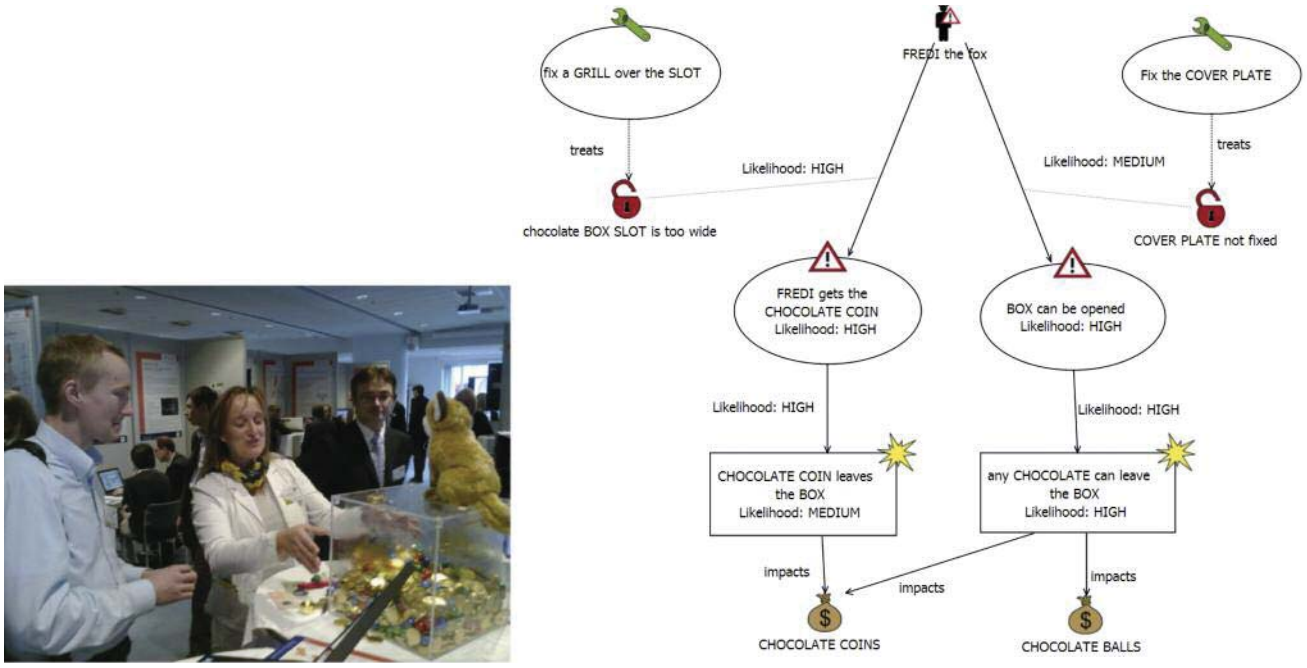

Security Testing (Randomized)
Risk-Oriented Testing (Specification-Based)
Model-Based Security Testing
Model-Based Testing (Test Generation)
Test Automation (Execution)

Figure 1: Security testing combined approaches

In the ITEA DIAMONDS project, 22 partners from six European countries are involved in case studies from the following domains: Banking, Smart Cards, Industrial Automation, Radio Protocols, Transport/Automotive, and critical infrastructures. Based on votes cast by participants at the ITEA2/ARTEMIS co-summit 2011 the DIAMONDS project won the prize for the best and most understandable ITEA2 project. We thank our colleagues from the project team at FOKUS and the international project consortium for their support.

Link:
http://www.itea2-diamonds.org

Please contact:
Ina Schieferdecker
Fraunhofer FOKUS, Germany
Tel: +49 30 3463 7241
E-mail: ina.schieferdecker@fokus.fraunhofer.de


fix a GRILL over the SLOT
treats
chocolate BOX SLOT is too wide
FREDI the fox
Likelihood: HIGH
Likelihood: MEDIUM
Fix the COVER PLATE
treats
COVER PLATE not fixed
FREDI gets the CHOCOLATE COIN Likelihood: HIGH
BOX can be opened Likelihood: HIGH
Likelihood: HIGH
Likelihood: HIGH
CHOCOLATE COIN leaves the BOX Likelihood: MEDIUM
any CHOCOLATE can leave the BOX Likelihood: HIGH
impacts
impacts
impacts
CHOCOLATE COINS
CHOCOLATE BALLS

(a) DIAMONDS chocolate box

(b) CORAS model

Figure 2: Security Models