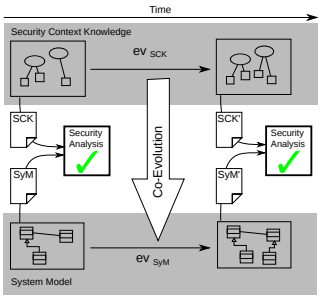
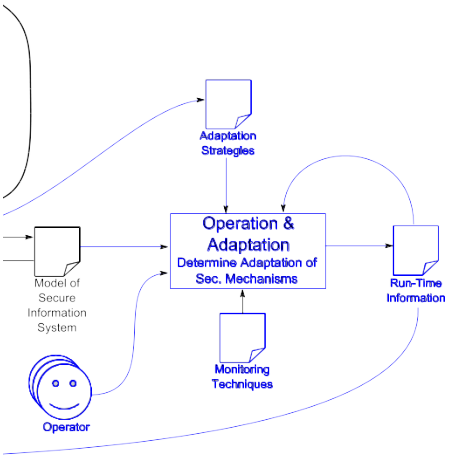
Master / Bachelor

Security Assessment using Monitoring / Securiy Assessment durch Monitoring

This thesis can also be supervised and written in English. For the English version of the announcement see below.



(a) Verhältnis von Evolution zu Co-Evolution



(b) Monitoring-Ansatz

Motivation

Modellgetriebene Softwareentwicklung eignet sich unter anderem dazu, die Einhaltung von Anforderungen an das System sicher zu stellen. Anforderungen (*requirements*) werden auf abstrakter Ebene im Entwicklungsprozess definiert oder sind bereits in Form von externen Quellen vorgegeben.

Software, die in kritischen Bereichen eingesetzt wird, wird oftmals über eine lange Laufzeit betrieben (*langlebiges System*). Langlebige Systeme sind insbesondere mit dem sich verändernden Wissen ihrer Umgebung konfrontiert, wie beispielsweise der Tatsache, dass bestimmte Verschlüsselungsalorithmen, die als sicher gelten, wenn ein System initial entwickelt wird, später unsicher werden können.

Das Projekt *SecVolution* beschäftigt sich damit, Wissen über ein Projekt und allgemeines Sicherheitswissen (Security Context Knowledge (SCK)) sowie generische Sicherheitsanforderungen (Essential Security Requirements (ESR)) zu sammeln und zu verwalten und als Annotationen an das Modell abzubilden, um die Einhaltung dieser Anforderungen bei der Modellierung / Implementierung sicherzustellen.

Ändert sich das Wissen (Evolution), muss überprüft werden ob das System-Modell die Sicherheitsanforderungen gegenüber dem veränderten Wissen noch erfüllt (s. Abb. 1a).

Zur Laufzeit muss überwacht werden, ob die in der Designphase gemachten Annahmen über Sicherheitseigenschaften zur Laufzeit eingehalten werden.

Aufgabenstellung/Ziele

Im Rahmen dieser Arbeit soll untersucht werden, inwiefern mithilfe von Monitoring-Techniken aus der Laufzeit eines Systems Rückschlüsse auf die Sicherheit des Systems gezogen werden können. Eine Skizze des Forschungsbereichs ist in Abb. 1b dargestellt. Die praktische Umsetzung soll anhand von Fallbeispielen und der Implementierung / Erweiterung vorhandener Werkzeuge / Ansätze erfolgen. Mögliche Teilziele sind:

- Nutzung von modelliertem Sicherheitswissen (ESRs) zur Ermittlung bestehender Sicherheitsanforderungen
- Bestimmung von Trace Links zwischen einem implementierten System und seiner Modellierung
- Evaluierung von existierenden Systemen/Ansätzen, die sich zum Monitoring eignen
- Beurteilen, wie gut ein System aufgrund der erhobenen Daten aktuell die Sicherheitsanforderungen erfüllt

Die Arbeit soll auf die bestehenden Vorarbeiten im Rahmen des Projekts SecVolution aufbauen.

Motivation

Modeldriven software engineering especially is used for compliance to requirements of software systems. Requirements are mostly rather abstract and can come from various sources (e.g. laws, domain-specific regulations, company policies).

Nowadays, many systems are used over a long timespan (i.e. long-living systems). Many of these are used to provide critical infrastructure, so that livelong compliance to security requirements is of vital significance.

The project *SecVolution* captures and manages knowledge of a specific project and general security knowledge (Security Context Knowledge (SCK)) as well as essential security requirements (ESR) and to make them part of a software model, thus supporting compliance to them during development and even run-time.

If the knowledge evolves, it needs to be checked if the system model still is compliant to the evolved knowledge (s. Abb. 1a).

During run-time, it is necessary to ensure that security assumptions made during design phase hold during the system execution.

Objectives

The goal of this thesis is to investigate, how monitoring approaches / tools can be used to assess a system's security during run-time.

Fig. 1b shows a prinicpal sketch. The practical realization of the approach to be developed shall be done extending existing approaches / tools. Conceivable subgoals are:

- Making use of modeled security knowledge (ESRs) to infer security requirements to be checked
- Establish trace links between a system model and its implementation
- Evaluation of existing systems that can be used for monitoring
- Design an approach on how to assess a system's security based on current run-time information

The thesis is in context of the SecVolution project and should be build by integrating with existing approaches and tools.

Organisatorisches

Kontakt:
Dipl.-Inf. Jens Bürger (buerger@uni-koblenz.de)