Abstract

The security of software and systems is becoming more and more important in the context of the rapid rise of distributed communication systems and their use into the private life of each individual. The development of new software is also accompanied by an immense time and cost pressure so that the aspect of IT security is often not taken into consideration within the software development process. Security gaps are now experiencing great media attention, especially when a large number of users are directly affected - most recently in an attack that led to a failure of a large number of Internet routers.

The aim of this work is to improve the integration of security engineering into software engineering. A model-based approach is used to determine values, security objectives, threats, and attacks in the requirement- and design phases, resulting in functional requirements for the software development process. The metamodel explains the relationships, a graphical and tabular analysis provides a method for integration into the requirements and design process.

Another key aspect is on the usability of model-based security engineering within the operating phase. An approach is presented that focuses on the dependencies of a secure software on the configuration, the execution environment, and external security policies. The need for such an approach is derived from the observation that a statement on IT security at the time of the development of a system or a software can only be a snapshot. The operation of secure applications is associated with the permanent risk of detecting a security vulnerability and appropriate responses. This question is all the more urgent because there is no direct control over these systems and vulnerabilities found are exploitable over a long period of time.

The practical use of the model-based approaches is exemplified on the development of a smart meter gateway. Smart meter gateways offer the communication interface between intelligent power meter and energy provider. In addition, these systems implement additional functions which are intended to pave the way for the modernization of the energy infrastructure. From an IT security perspective, smart meter gateways are devices that are deployed decentrally over a long period of time and are exposed to all threats that can be implemented through the Internet. Moreover these systems are exposed to physical manipulation attempts. For taking these aspects into account in an appropriate manner, the case study is a focal point of this work.

Zusammenfassung

Die Sicherheit von Software und Systemen rückt vor dem Hintergrund des rasanten Anstiegs verteilt kommunizierender Systeme und deren Nutzung bis hinein in das Privatleben eines jeden Einzelnen immer mehr in den Mittelpunkt. Die Entwicklung neuer Software geht zudem mit einem immensen Zeit- und Kostendruck einher, sodass der Aspekt der IT-Sicherheit innerhalb des Softwareentwicklungsprozesses oftmals nur unzureichend Berücksichtigung findet. Sicherheitslücken erfahren mittlerweile große mediale Aufmerksamkeit insbesondere dann, wenn eine Vielzahl von Anwendern in unmittelbarer Art und Weise betroffen sind – zuletzt bei einem Angriff, der zu einem Ausfall einer Vielzahl von Internet-Routern der Telekom führte.

Das Ziel der vorliegenden Arbeit ist die Verbesserung der Integration des Security-Engineerings in das Software-Engineering. Es wird anhand eines modellbasierten Ansatzes aufgezeigt, wie in der Anforderungs- und Designphase Informationen über zu schützende Werte, Sicherheitsziele, Bedrohungen und Angriffe gewonnen und im Ergebnis funktionale Anforderungen für den Softwareentwicklungsprozess abgeleitet werden. Das Metamodell erklärt die Beziehungen, eine grafische und tabellarische Analyse bieten ein Verfahren zur Integration in den Anforderungs- und Designprozess.

Ein weiterer Schwerpunkt ist die Nutzbarkeit des modellbasierten Security-Engineerings innerhalb der Betriebsphase. Es wird ein Ansatz vorgestellt, der die Abhängigkeiten einer sicheren Software von der Konfiguration, der Ausführungsumgebung und externen Sicherheitspolitiken in den Mittelpunkt stellt. Die Notwendigkeit eines solchen Ansatzes leitet sich aus der Feststellung her, dass eine zum Zeitpunkt der Entwicklung eines Systems oder einer Software getroffene Aussage zur IT-Sicherheit nur eine Momentaufnahme sein kann. Der Betrieb sicherer Anwendungen geht mit dem permanenten Risiko der Entdeckung einer Sicherheitslücke und angemessenen Reaktionen einher. Diese Frage ist bei der Vielzahl verteilter Systeme umso dringlicher, da über diese keine unmittelbare Kontrolle vorhanden ist und gefundene Sicherheitslücken über einen langen Zeitraum ausnutzbar bleiben.

Im Rahmen einer Fallstudie zur Entwicklung eines Smart Meter Gateways wird die praktische Nutzung der modellbasierten Ansätze gezeigt. Smart Meter Gateways bieten die Kommunikationsschnittstelle zwischen intelligentem Stromzähler und Erzeuger. Zudem realisieren diese Systeme zusätzliche Funktionen, welche den Weg zur Modernisierung der Energieinfrastruktur ebnen sollen. Aus der Perspektive der IT-Sicherheit sind Smart Meter Gateways Geräte, die über einen langen Zeitraum dezentral aufgestellt werden und sämtlichen mithilfe des Internets realisierbaren Bedrohungen ausgesetzt sind. Hinzu kommen physische Manipulationsversuche, denen die Systeme potentiell ausgesetzt sind. Der Fallstudie wird aus diesem Grund Raum gegeben, um diese Aspekte in angemessener Art und Weise zu berücksichtigen.