Security Engineering Methodology for Embedded Systems in Metering

Von der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen

zur Erlangung des akademischen Grades

Doktor der Ingenieurswissenschaften
(Dr.-Ing.)

genehmigte Dissertation

von

Dipl.-Inform. Donatus Weber

1. Gutachter: Univ.-Prof. Dr. rer. nat. Christoph Ruland
2. Gutachter: Prof. Dr.-Ing. habil. Roman Obermaisser
Vorsitzender: Univ.-Prof. Dr.-Ing. Horst Bessai

Tag der mündlichen Prüfung: 29.11.2013

UNIVERSITÄT SIEGEN

Institut für
Digitale Kommunikationssysteme

Forschungsberichte

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 29

Donatus Weber

Security Engineering Methodology for Embedded Systems in Metering

SHAKER VERLAG

Aachen 2014

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Siegen, Univ., Diss., 2013

Printed in Germany.

ISBN 978-3-8440-3078-5
ISSN 1614-0508

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

For Christina and Lysander

Abstract

Ongoing changes in the energy sector are leading to a need for decentralized energy supplies to enable use of green energy and reduce carbon dioxide emission. An efficient usage of these resources requires up-to-date information on the energy currently generated and consumed. The necessary infrastructure is provided by the smart grid, an intelligent network to control energy producers and consumers as well as storage.

Important components of the smart grid are intelligent metering systems with the capability of sensing measurements and communicating these to remote entities. Meters with these extended features, so called smart meters, are usually operated by embedded systems. Their communication units, referred to as gateways, provide connectivity to different networks. In operation, smart meters generate security and safety relevant as well as privacy sensitive data and transmit them over possibly insecure networks. A special protection of this data is therefore strongly required.

This circumstance was recognized by the German government in 2010 and induced the development of a Common Criteria Protection Profile for the gateway of a smart metering system by the German Federal Office for Information Security. This gateway Protection Profile is a first approach to establish security by design in the metering domain.

Newly developed gateway devices need to undergo a Common Criteria evaluation and certification before being deployed on the market. The metering domain, traditionally conservative, is now directly faced with software development processes and appropriate development documentation mandatory for a successful evaluation. Security engineering has become a key point in the metering system development. Beyond this, the complexity of metering systems is steadily increasing requiring modern development methods that allow reuse of security solutions to support cost efficiency and reduce development time.

The solution presented in this thesis encountering the mentioned problems is a security engineering methodology that combines key element concepts to provide security expert knowledge in different phases of the metering system development process.
Software patterns are a well-known technique to capture expert knowledge as solutions to commonly occurring problems. The security by design principle requires security to be taken into account even from the beginning of the development process. Combining security software patterns with Model Driven Engineering (MDE) techniques introduces the possibility to apply these patterns even in high level design phases of the system. Patterns are therefore stored in a model based repository offering a model transformation back-end to various domain specific development tool sets, which in turn are dedicated for use in different phases of the development process. With this precondition already established engineering processes and process tooling of companies do not need to undergo major changes with the result of widening the industry acceptance of the methodology. Furthermore security patterns may undergo a formal validation to verify the security properties provided by this solution.
Within this work a security engineering methodology applicable to embedded device development in the metering domain is developed by uniting the mentioned key concept elements. This comprises the definition of a development process with Common Criteria elements as well as the derivation and definition of security patterns dedicated for smart meter gateways.
The methodology is evaluated by applying the elements to a proof of concept gateway demonstrator. Furthermore a detailed insight into legal framework conditions as well as state of the art in market and regulatory environment of the metering domain is given.

Zusammenfassung

Der derzeitige Wandel im Bereich der Energiewirtschaft bedingt eine Umstrukturierung in Richtung dezentrale Energieversorgung, um erneuerbare Energien effizient nutzen zu können und den Kohlenstoffdioxidausstoß zu reduzieren. Für die erfolgreiche Einbindung dieser regenerativen Energieträger sind genaue Informationen über Verbrauch und Erzeugung unabdingbar. Die dafür notwendige Kommunikationsinfrastruktur wird vom Smart Grid, einem intelligenten Energieverteilnetz zur Verfügung gestellt. Dieses Netz bietet die notwendige Funktionalität, um Energieerzeugung, -verbrauch und -speicherung aufeinander abzustimmen.

Wichtige Komponenten dieses Smart Grid sind intelligente Zählersysteme, die in der Lage sind, gewonnene Messwerte mit Fernauslesestellen zu kommunizieren. Moderne Zählersysteme mit diesen Eigenschaften, im Volksmund als Smart Meter bezeichnet, sind immer leistungsfähigere eingebettete Systeme. Sie verfügen über Kommunikationseinheiten (Gateways) mit Anbindung an verschiedene Weitverkehrsnetze. Im stationären Betrieb kommunizieren diese Zähler Datensätze, die sowohl sicherheitskritisch einzustufen sind als auch datenschutzrechtlich als brisant gelten. Solch sensible Daten müssen in besondere Weise geschützt werden. Die deutsche Bundesregierung hat diese Umstände 2010 erkannt und daraufhin die Entwicklung eines Common Criteria Protection Profiles für Gateways von Zählersystemen durch das Bundesamt für Sicherheit in der Informationstechnik in Auftrag gegeben. Dies ist der erste Schritt für die Einführung des Security by Design Prinzips im Bereich des Messwesens.

Neu entwickelte Smart Meter Gateways müssen eine Evaluation nach Common Criteria durchlaufen, bevor sie zertifiziert auf den Markt gebracht werden dürfen. Das Messwesen, als traditionell konservativer Sektor mit Ausrichtung in den elektrotechnischen Bereich, ist nun direkt mit Entwicklungsprozessen für Software und der notwendigen Entwicklungsdokumentation im Rahmen der Common Cri-

teria Evaluation konfrontiert, die für eine erfolgreiche Zertifizierung unumgänglich ist. Security Engineering ist zuletzt damit zu einem wichtigen Bestandteil im Entwicklungsprozess für moderne Zählersysteme geworden. Darüber hinaus werden Systeme zunehmend komplexer, was wiederum moderne Entwicklungsmethoden erforderlich macht, welche die einfache Integration und die Wiederverwendbarkeit von Sicherheitslösungen erlaubt, um kosteneffizient zu arbeiten und Entwicklungsaufwand und -zeit gering zu halten.
Die in dieser Arbeit aufgezeigte Lösung zur beschriebenen Problematik basiert auf einer Security Engineering Methodik, die verschiedene Schlüsselelemente miteinander kombiniert, um in den verschiedenen Phasen des Entwicklungsprozesses eines Zählersystems IT-Security Fachwissen zur Verfügung zu stellen.
Software Pattern sind eine wohlbekannte Technik, um Expertenwissen in Form von generischen Lösungen für häufig auftretende Problemstellungen zu erfassen und Entwicklern zur Verfügung zu stellen. Dies lässt sich direkt auf Security Pattern übertragen. Das Security by Design Prinzip bedingt die Integration von Security Engineering Elementen in den gesamten Entwicklungsprozesses eines Produktes und dies von Beginn an. Kombiniert man Software Pattern mit Model Driven Engineering Techniken bietet dieser Ansatz die Möglichkeit, Pattern schon in frühen Designphasen anzuwenden, um die höheren Ebenen hierfür zu erschließen.
Hierfür sind die Security Pattern in einem modellbasierten Repository hinterlegt. Eine dazugehörige Anwendung bildet die Schnittstelle zwischen Repository und den in den verschiedenen Phasen des Entwicklungsprozesses eingesetzten Werkzeugen. Diese verfügt über ein Transformationsbackend, um die modellbasierte Artefakte direkt in die verschiedenen Entwicklungswerkzeuge einzubringen. Dies bietet die Möglichkeit, die Methodik auf bereits etablierte Entwicklungsprozesse und Abläufe in Firmen anzuwenden, ohne diese grundlegend ändern zu müssen.
Die in dieser Arbeit definierte Methodik vereint die genannten Schlüsselelemente und optimiert diese für die Anwendung im Bereich der eingebetteten Systeme im Messwesen. Dies umfasst neben der Definition eines detaillierten Entwicklungsprozesses mit Common Criteria Elementen auch die Implementation von typischen Security Pattern für einen Smart Meter Gateway. Ein Machbarkeitsnachweis evaluiert die Methodik abschließend am Beispiel eines Smart Meter Gateway Demonstrators.

Acknowledgment

This doctoral thesis contains results of research undertaken at the Chair for Data Communications Systems at the University of Siegen. Work on this thesis has been carried out during my employment as research assistant and has been supported by the research project Trusted Computing Engineering for Resource Constrained Embedded Systems Applications (TERESA) of the European Union.

I am most grateful to my supervisors, Univ.-Prof. Dr. rer. nat. Christoph Ruland and Prof. Dr.-Ing. habil. Roman Obermaisser. Special thanks to the chairman of my committee Univ.-Prof. Dr.-Ing. Horst Bessai and Prof. Dr.-Ing. Günter Schröder, who agreed to be my third thesis reviewer.

Furthermore I am thankful to my former colleagues Markus Dunte, Stephan Meyer, Hendrik Brandenburger, André Groll, Jan Holle, Christian Bodenstedt, Rainer Schick, Matthias Schneider, Andreas Schantin, Jinsuh Shin and Obaid Ur-Rehman for our many informal discussions.

Finally I would like to thank my family. The encouragement and support from my beloved wife Christina and our always positive and joyful son Lysander is a powerful source of inspiration and energy. These years have been a challenging trip, with both ups and downs. Fortunately, I was not alone on this road.

A special thought is devoted to my parents Jovita and Günter for a never-ending support throughout my life.

Contents