ENGINEERING SECURITY METHODOLOGIES FOR DISTRIBUTED SYSTEMS

by

Anton Victor Uzunov

May 2014

A THESIS SUBMITTED FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE SCHOOL OF COMPUTER SCIENCE
UNIVERSITY OF ADELAIDE

This page is intentionally left blank.

Table of Contents

Abstract

Over the last decade, researchers and practitioners have increasingly come to acknowledge that the introduction of security into software systems – especially complex, distributed systems – should proceed by means of a structured, systematic approach, combining principles from both software and security engineering. Such systematic approaches, particularly those implying some sort of process aligned with the development life-cycle, are termed *security methodologies*. While there are numerous methodologies in the literature, each with its own peculiar advantages and disadvantages, making it more or less suitable for a given set of project situations, none can lay claim to being universal, i.e. able to take into account all system-specific attributes, all technologies, all skill levels, and – in general – to be applicable to all project situations. In other words, the literature does not currently present developers with an "ideal" methodology (in an absolute sense); and, indeed, such a requirement would be infeasible, since "ideal" must necessarily be interpreted with respect to a given situation – encompassing system types, technologies, skillsets and whatever other qualities are seen as desirable. The problem facing the area is thus not so much the construction of "bigger and better" methodologies with novel or interesting features – i.e. (unattainably) ideal methodologies in an absolute sense – but the construction of (attainably) ideal methodologies for particular project situations.

This thesis proposes a comprehensive solution to the latter problem by developing a conceptual "toolkit" for engineering security methodologies, with an emphasis on security methodologies for distributed systems. The "toolkit" consists of a number of inter-related parts: a framework of process patterns, a domain-specific meta-model and a unifying meta-methodology for constructing and tailoring security methodologies (for any system type); a set of generic conceptual security artefacts – usable across different methodologies – for addressing various networked and distributed systems security features and for supporting threat modeling in a networked/distributed systems context; and a framework for assessing and improving security methodology quality, which, when combined with the meta-methodology, helps to ensure that all construction/tailoring efforts are sensible – i.e. of measurably good quality. Besides being part of an overall approach, each of these inter-related parts makes its own set of unique, self-contained contributions to the area of secure software engineering. Some of the parts are complete in themselves, while others require elaboration or specialization for different situations. In all cases the frameworks, artefacts and other "tools in the toolkit" can be customized and extended in various ways, providing developers, architects, methodology engineers and other team members with a high degree of freedom and flexibility. The latter point in particular, as well as the whole approach, is demonstrated incrementally throughout the thesis via the engineering of a specific pattern-based security methodology for distributed systems – a case study which in itself is another, final contribution. Of course, the case study methodology is also bigger and better (with respect to its predecessor) and contains novel features, but is only ideal with respect to its project situation. Through the presentation of the parts of the "toolkit" and the illustration of its use, the thesis accomplishes its task of both proposing and demonstrating the value of a comprehensive, holistic approach to engineering security methodologies, thereby offering a solution to the initial problem.

Declaration

I certify that this work contains no material which has been accepted for the award of any other degree or diploma in my name, in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. In addition, I certify that no part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint-award of this degree.

I give consent to this copy of my thesis when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

The author acknowledges that copyright of published works contained within this thesis resides with the copyright holder(s) of those works.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

_____

Anton Victor Uzunov
May 2014

Acknowledgements

First of all I would like to thank my two supervisors: Dr. Katrina Falkner and Prof. Eduardo B. Fernandez. I felt very fortunate throughout my degree to have two pairs of experienced eyes glance at my work and provide feedback from two different, complementary angles. I am particularly grateful to Katrina for promptly reading and always providing valuable feedback on all my manuscripts, even under excruciatingly tight deadlines; for encouraging me and supporting my work; for all the friendly discussions; for inspiring me towards excellence; and for allowing me to collaborate freely and trusting me to develop my ideas in the way I saw fit. I am particularly grateful to Eduardo for all his advice and his deeply insightful comments and suggestions; for always being “on-line”, even for late-evening Skype meetings spanning different continents, and being so generous with his time; for all the discussions on topics in software security and beyond; and in the end for helping me to realize what I myself had done (!). When I first spoke to Eduardo about external co-supervision a number of years ago, I was struck by his friendly unpretentiousness; in good time, I realized I had the privilege of meeting not only an immensely experienced and knowledgeable supervisor, but also a man with broad interests and a genuine friend. Collaborating with both my supervisors was always marked with mutual respect and understanding; in fact, I often felt as though I was working with peers or colleagues – something that I appreciated very much.

I would like to thank the University of Adelaide's School of Computer Science administrative staff – Sharyn Liersch and Julie Mayo – for taking care of my conference travel arrangements; as well as the postgraduate coordinators – Dr. Michael Sheng and Dr. Frank Neumann – for their readiness to help with filling out all the Graduate Centre forms. I would particularly like to thank Michael for helping me to settle in the School of CS at the beginning and also for his friendly encouragement.

Thanks goes to the local IT-admin guru (and fellow PhD student) Yuval Yarom, not only for setting up my University machine (which was used rarely, but to good purpose), user accounts etc., but also for the comradeship. Shalom Yuval!

I would also like to thank my colleagues, supervisors and line managers back at work – especially Richard Appleby, Bradley Hopkins, Chris North and Dr. Olivier De Vel – for supporting me in my decision to undertake PhD studies. My thesis topic is all my own, but it really is in security; after gaining many skills and much experience and expertise, I believe that (besides coming out alive – not a bad feat) I managed to become a bigger and better security expert and, above all, a bigger and better security researcher.

Finally, I would like to thank my family – close and distant – for all their love and support, which, although mentioned here last, was indispensable. To my grandad I would say: no, I didn’t worry too much at the end, and, yes, I mostly “hurried slowly” – *Eile mit Weile* (as the Germans say).

Anton V. Uzunov
October 2013