Chapter 1
Secure by Design:
Developing Secure Software Systems from the Ground Up

Haralambos Mouratidis
University of East London, UK

Miao Kang
Powerchex Ltd., UK

ABSTRACT

This paper describes results and reflects on the experience of engineering a secure web based system for the pre-employment screening domain. In particular, the paper presents results from a Knowledge Transfer Partnership (KTP) project between the School of Computing, IT and Engineering at the University of East London and the London-based award winning pre-employment company Powerchex Ltd. The Secure Tropos methodology, which is based on the principle of secure by design, has been applied to the project to guide the development of a web based system to support employment reference and background checking specifically for the financial services industry. Findings indicate the potential of the methodology for the development of secure web based systems, and support the argument of incorporating security considerations from the early stages of the software development process, i.e., the idea of secure by design. The developed system was tested by a third, independent to the project, party using a well known method of security testing, i.e., penetration testing, and the results provided did not indicate the presence of any major security problems. The experience and lessons learned by the application of the methodology to an industrial setting are also discussed in the paper.

1. INTRODUCTION

The application of ICT to the financial services industry can support the automation of a number of functions, which are crucial for the further development of the sector, such as the management of pre-employment screening, coordination of financial teams, compliance with relevant regulations and analysis of financial data. The credit crunch and the events of the last couple of years meant that the financial services industry is faced with large changes and as such the development

DOI: 10.4018/978-1-4666-2482-5.ch001

of software systems to support the financial services industry and peripheral sectors introduces a number of new challenges and difficulties.

Security is arguably one of the most crucial and necessary features of software systems that support the financial services industry and an acceptable financial software system may under no circumstances endanger the risk of monetary lose and the leakage of relevant sensitive (private or otherwise) data.

In software engineering practice the usual approach is to perform the analysis, design and implementation of a software system without considering security, and then add security as an afterthought (Devanbu & Stubblebine, 2000; Mouratidis et al., 2006). Nevertheless, recent research has shown that such approach introduces a number of problematic areas and it leads to security vulnerabilities that are usually identified after the implementation and deployment of the system. Since at this point it is quite expensive to redevelop the system to completely overcome such vulnerabilities, the usual approach is to "patch" some of these vulnerabilities as they are identified. However, this is not an acceptable standard for the development of high risk software systems software systems (Blobel & France, 2001; Mouratidis, 2004).

The last few years, it has been widely argued, especially within the requirements engineering (Haley et al., 2006; Basin et al., 2003; Hermann & Pernul, 1999) and information systems (Devanbu, 2000; McDermott & Fox, 1999; Mouratidis & Giorgini, 2006) research communities, that the number of security vulnerabilities could be reduced if security is considered from the early stages of the development process, i.e., a Secure by Design (SbD) approach is employed to support the development of secure software systems. Generally speaking, Secure by Design, within the context of software engineering, means that the software has been designed from the ground up to be secure. In academia, this practice is mostly known as secure software systems engineering or software engineering for secure systems amongst other terms. Our work is not the only effort at integrating security considerations into software engineering practices and methods. Security requirements frameworks have been proposed (Haley et al., 2006; Mead, 2006) for security requirements elicitation, specification and analysis. On another line of work, the behaviour of potential attackers is used to model security (Lamsweerde & Letier, 2000; Lin et al., 2003). Works have also been presented that extended use cases with respect to security analysis (Hermann & Pernul, 1999; Alexander, 2003). In addition, a large number of efforts are focused on extending existing methods and languages for software systems development (Basin et al., 2003; McDermott & Fox, 1999). Apart from the academic works, industry has also started to recognize the advantages of developing software systems following the Secure by Design principles. Microsoft has introduced the Security Development Process (http://www.microsoft.com/security/sdl/) while IBM has long supported the idea of introducing security as part of the development process (http://www-01.ibm.com/software/rational/announce/innovate/secure.html). McAfee and Citrix Systems have recently announced that they are focused on providing virtual desktops with products that are "secure by design" in order to protect large enterprises from the changing security landscape as employees are increasingly using mobile devices to access corporate resources (http://www.siliconrepublic.com/strategy/item/18252-citrix-and-mcafee-release/).

Nevertheless, empirical studies on the use of secure software systems engineering methodologies have so far been limited. In fact, as far as we are aware, an industrial case study on using a methodology that supports the idea of secure by design from the early requirements stages and throughout the development stages has not been published so far. This paper aims to contribute to this gap by presenting and discussing the application of a software engineering methodology, which supports the idea of secure by design by in-