Institution: University of East London

Unit of Assessment: 11

Title of case study: Using secure software systems engineering to improve business processes and information systems

1. Summary of the impact

Work conducted at UEL in the area of secure software systems engineering has had impacts on both the private and public sectors, in the UK and abroad. Through its application to financial pre-employment screening it has enabled an award-winning UK company to improve its security processes and become a world leader with respect to secure systems in their sector. This has, in turn, allowed the company to develop a competitive advantage in the market and attract more and larger multinational clients. In the public service sector our work has enabled a Greek governmental department – the National Gazette - to analyse the security implications of fully automating their processes and identify security mechanisms that enhance the security of their new systems. This has improved their service delivery, with significant impacts on Greek society.

2. Underpinning research

The security of software systems has been transformed in recent years from a mono-dimensional technical challenge to a multi-dimensional socio-technical challenge. Indeed technical challenges associated with the availability of appropriate technologies and their infrastructure must now be considered within a context that takes into consideration social challenges relating to social life and processes, as well as technological systems.

Rather than the traditional, technical-only treatment of security, we take a holistic approach to secure software systems engineering, considering security from the early stages of the development process, at multiple levels and from multiple viewpoints, and combining people, technology and processes in an integrated fashion. To this end, our work combines insights from and contributes to areas such as security requirements engineering, secure information/software systems engineering, security patterns, software engineering for regulation compliance, and trust requirements engineering. An important output of this multi-dimensional research, is the development of the Secure Tropos methodology (www.securetropos.org).

The methodology for Secure Tropos has been developed since 2003 at the University of East London by Dr. H. Mouratidis [1-6], with its origins in Mouratidis' PhD research. PhD students sponsored by the EPSRC (in collaboration with BT and ELC) and the Government of Luxemburg have also contributed to the project, along with members of the UEL Software Systems Engineering research group. Further funding from the London Development Agency and The National Institute of Informatics (Japan) has also supported the development of the methodology.

The main aim of this methodology is to support the effective integration by software engineers and information system developers of security analysis and development within the overall software systems development process. The theoretical framework underpinning Secure Tropos is the definition of security requirements as constraints on system functions [1] [5]. This allows a unified characterization and understanding of security requirements across the various stages of the development process. The aim for requirements engineers is therefore to elicit appropriate security-related constraints for the system.

To support such analysis, the UEL team developed a security-aware process and a modelling language and security aware process. The language is based on the Goal Oriented Requirements Engineering (GORE) paradigm - using concepts such as actor, goal, and plan - combined with concepts from security engineering such as threat, security mechanism, vulnerability and attack. The security-aware process supports the analysis of security requirements of stakeholders and the system, identification of potential threats and vulnerabilities and reasoning of security objectives and mechanisms that can be used to fulfil the security requirements.

Our work has also sought to develop techniques that support the consideration, analysis and

testing of security as part of the development process. To that end, the researchers have developed novel methods that assist developers in testing the developed system against potential security attacks (security attack scenarios) during the design process [4]. We have, moreover, developed security pattern languages that enable the representation of security patterns and guide developers through the process of designing a system [6], and pioneered work that identifies and analyses relevant legal regulations and aligns these with security requirements [2].

The methodology is supported by a suite of tools such as secTro (http://www.securetropos.org/), a platform independent analysis and modelling tool that supports the development and analysis of the methodology's models, and an advanced tool that is under development as part of the Open Models Initiative (OMI) (www.openmodels.at).

3. References to the research

Outputs [2], [3] and [5] best indicate the quality of the underpinning research.

[1] H. Mouratidis (2011), "Secure Software Systems Engineering: The Secure Tropos Approach", International Journal of Software, 6(3), pp. 331-339
doi: 10.4304/jsw.6.3.331-339

[2] S. Islam, H. Mouratidis, J. Jurjens (2011), "A Framework to Support Alignment of Secure Software Engineering with Legal Regulations", International Journal of Software and Systems Modelling (SoSyM), 10(3)
doi: 10.1007/s10270-010-0154-z

[3] H. Mouratidis, P. Giorgini (2007) "Security Attack Testing (SAT)-Testing the Security of Information Systems at Design Time" Information Systems 32(8) pp.1166-1183
doi: 10.1016/j.is.2007.03.002

[4] H. Mouratidis and P. Giorgini (2007) "Secure Tropos: A Security-Oriented Extension of the Tropos methodology" International Journal of Software Engineering and Knowledge Engineering (IJSEKE) 17(2) pp. 285-309
doi: 10.1142/S0218194007003240

[5] H. Mouratidis, P. Giorgini, and G. Manson (2005) "When Security meets Software Engineering: A case of modelling secure information systems" Information Systems 30(8) pp. 609-629
doi: 10.1016/j.is.2004.06.002

[6] H. Mouratidis, J. Jurjens, J. Fox (2006) "Towards a comprehensive framework for secure systems development" Proceedings 18th Conference on Advanced Information Systems Engineering (CAiSE) Springer Verlag, Lectures in Computer Science
doi: 10.1007/11767138_5

4. Details of the impact (indicative maximum 750 words)

Private sector impacts

The research outlined above has had impacts within the private sector through the application of the methodology to pre-employment screening. Security is essential to financial pre-employment screening due to the sensitivity of the information stored and analysed. Between 2009 and 2011 the research was applied to support this through an award-winning two year Knowledge Transfer Partnership (KTP) with Powerchex, a UK-based company specialising in the financial services sector of the City of London. The project's success was recognised by its "outstanding" grading [a] and nomination as one of eight nationwide finalists in the Technology Strategy Board's KTP Best of the Best 2012 awards [b].

The KTP originated from Powerchex's identification of security issues as a barrier to growth. To win major clients they had to be capable of handling more screening applications. Their own attempts to automate a screening process, however, proved labour-intensive, time consuming, prone to errors, and unable to guarantee the security of information. UEL's theoretical work on security engineering was applied to this complex business problem to improve the efficiency and speed of Powerchex's application process without compromising its security. In particular, the methodology enabled the elicitation of security requirements, in terms of security constraints; the analysis of such constraints and the identification of relevant threats and vulnerabilities; and the

development of a system comprised of security mechanisms and an architecture that supports the satisfaction of the identified security constraints. The new system has passed rigorous security checks performed by some of the biggest financial institutions. More specifically, our research was used to develop a secure Powerchex online application form with an electronic signature tool, incorporating electronic submission of applications, automated screening reports, customer bespoke data automation and form customisation, as well as automated criminal checks. Moreover, the newly developed system was linked with the UK criminal record check system, which gave Powerchex the fastest turnaround in the industry for UK criminal record checks, reducing the process time from 11-12 to 7-9 days.

The KTP led to a significant increase in systems, networking and IT security knowledge and experience at Powerchex, especially with respect to data security and privacy. According to the company's current Managing Director: "The project gave us [security] expertise and resources that, as a growing company, we would never otherwise have been able to access or afford" [d]. By enabling Powerchex to develop a software system with security in mind, our work allowed them to win large new contracts and attract high-profile new clients such as HSBC, whose stringent security requirements would previously have presented a barrier to them working with Powerchex. As the then-MD of Powerchex explained: "The security research expertise brought by Dr. Mouratidis helped us to develop a [software] system that passed rigorous security checks of potential clients and provided us with competitive advantage, in a sector where security is very important" [d].

Powerchex has publicly acknowledged the dramatic impact of the KTP on its capacity to compete successfully for large corporate business [d]. At the start of the KTP, Powerchex was a small business with 30 staff, providing pre-employment screening for small to medium-sized clients in the financial services sector. Turnover totalled £776k, yielding net profits of £120k. Despite a problematic recruitment market for the financial services industry, the company have announced that the KTP led to increases in turnover of £1.7m and annual pre-tax profits of £440k, whilst staff numbers grew to over 100. Increased process efficiencies – including in the time taken to complete criminal record checks - reduced costs by £40k [b, d].

The improvements accruing from the application of the research to Powerchex's security systems have also delivered significant benefits to the company's clients, who now include some of the largest financial organisations in the UK. Powerchex's capacity to deliver faster and more secure pre-employment screening improves efficiency within these organisations by reducing delays in their ability to appoint potential employees. In turn, those potential employees also benefit from employing organisation's capacity to notify them about their job applications in less time, but with a much-reduced risk of compromising the security of their personal details.

The new capabilities developed and embedded in Powerchex were a major factor in its acquisition in 2010 by HireRight, a leading global provider of on-demand employment background checks, drug testing, Form I-9 and employment education verifications. That acquisition has significantly extended the reach of the original research impacts on Powerchex through HireRight's adoption of the security-centric approached taken to the development of Powerchex software system. The company has integrated a number of the system functionalities within other systems amongst its EMEA branches.

Public Service Sector

The Greek National Gazette (GNG) is responsible for the issue and circulation of the Greek Government Gazette, publishing and communicating to the general public all governmental policies, laws and changes to the constitution; it is also used to meet the printing needs of the Greek Public Service. The Gazette's work currently involves manual input of thousands of local government documents to its systems, a process that is laborious, time-consuming, and prone to human error.

The application of insights and methods developed through the UEL research has enabled the Gazette to achieve an in-depth understanding of the various security, privacy and trust implications

of using the latest technologies to support the development of adaptable software systems to fully automate their processes. The project supporting this, which began in December 2011, was particularly developed through visits made by Dr Mouratidis to the National Gazette during sabbatical leave taken between February and July 2012. During those visits, the Secure Tropos methodology was applied to the Greek National Gazette to elicit security requirements and identify relevant security threats and vulnerabilities in the process of automating GNG operations. The development of an automated adaptable infrastructure to support the production and publication of information is expected to reduce the production time and increase production outputs of the National Gazette by 25%. However, it is important that such infrastructure, which has implications for all main Greek governmental departments, as well as local governments, does not endanger the security - and especially the integrity and authenticity - of the published information.

The application of our theoretical work to the Gazette elucidated and analysed security, trust and privacy issues related to the automation of the National Gazette's production systems, identified a number of potential vulnerabilities, and suggested ways to overcome these [c]. In particular, our analysis focused on the GNG's two main external services: "Receipt of the Documents" and "Publication of the Volume". Application of the secure Tropos methodology to a security analysis of these identified a number of security constraints related to integrity and availability, and privacy constraints related to unlikability and sender eligibility. A number of security mechanisms were implemented to address these. In the case of unlikability, for example, the application of our methodology facilitated onion routing, tor architecture and pseudonimisation to fulfil the relevant security and privacy requirements. Our analysis also focused on the trust and security issues of a potential migration of the National Gazette's systems to the cloud [e], enabling it to make an informed decision about which of its services could be moved without compromising their security. By analyzing and comparing two potential cloud computing deployment models, our work allowed the Gazette to identify the model that met their security and privacy requirements.

The National Gazette's public communication role makes public trust in its work essential. The project provided the Gazette with an analysis, not just of the technical security requirements related to its service delivery, but also of security and trust concerns arising from both providers and receivers of the published information, including local authorities and citizens [f], and thereby helped it meet its public trust requirements.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[a] For the KTP's "outstanding" grading: KTP Certificate of Excellence, Technology Strategy Board, Certificate Number KTP007046. Available on request.

[b] For nomination of the KTP as one of eight nationwide finalists in the TSB 2012 Best of the Best awards, and for a summary of key benefits delivered to Powerchex: (http://bit.ly/1bmefTA), page 7. Includes a quotation from Managing Director (2012-time of submission), Powerchex Ltd.

[c] The application of our theoretical work to the Gazette – and benefits accruing to date - are described in: H. Mouratidis, M. Kang (2011), "Secure By Design – Developing Secure Software Systems from the Group up", International Journal of Secure Software Systems Engineering, 2(3), pp.23-41. doi: 10.4018/jsse.2011070102

[d] The Founder and Managing Director of Powerchex, Powerchex Ltd (MD during KTP and until 2011) may be contacted for a full factual statement corroborating the impacts of the research on that organisation

[e] Our analysis of security issues involved in a potential migration of the National Gazette's systems to the cloud is described in: C. Kalloniatis, H. Mouratidis, S. Islam (2013), "Evaluating cloud deployment scenarios based on security and privacy requirements", Requirement Engineering Journal. doi: 10.1007/s00766-013-0166-7

[f] The Special Secretary to the Greek National Gazette may be contacted for a factual statement to corroborate the impacts described here within that organisation.