

Requirements Elicitation and Validation for Secure IT Enabling Supply Chain Networks

Elena Irina Neaga¹, Michael Henshaw¹

¹ Engineering System of Systems (EsoS) Group, Dept of Electrical and Electronic Engineering, Garendon Wing Bldg., Holywell Park, Loughborough University, LE11 3TU Loughborough, United Kingdom
{E.I.Neaga, M.j.d.Henshaw}@lboro.ac.uk

Abstract. This research fair proposal deals with business driven requirements engineering and management for the development of secure software systems that support effective supply chain collaboration. To enable effective implementation of security concepts for enterprises, including their supply chains, it is necessary for software developers to work alongside systems engineers who model the requirements in architecture at the “systems of systems” level. The target of this proposal is identification of case studies for practical approaches in order to capture the dynamic nature of software security requirements to support industrial supply chain networks. The proposal will also identify mechanisms through which software security requirements can be better elicited, expressed, and validated for effective system development as part of an integrated architectural enterprise approach to supply chain networks and solutions for changing requirements that arise as a result of the dynamic nature and behaviour of threats and vulnerabilities.

Keywords: requirements elicitation and validation, secure software systems, effective supply chain collaboration, vulnerabilities.

1 Introductory Aspects

IT enables supply chains to become more efficient and agile through enhanced collaborative working, but this appears to come at the expense of increased risks to information security vulnerabilities. Service oriented architectures have been the significant enablers, but the advent of cloud computing is now leading to even greater cost reductions and this field is expected to grow within the commercial world. This poses new, and complex, challenges for security protection and increases the difficulty for requirements management associated with software security. The rapid increase of the already large number of IT support systems being deployed as intranets and extranets in supply chain collaborations creates new possibilities for significant security vulnerabilities and threats. For instance, financial transactions can be interrupted or misdirected by the hackers or crackers; collaborative supply chain information may increase the risk of revealing sensitive information to competitors; logistics information can be illegally used to disrupt normal transportation operations, and attackers can break into an organization’s supply chain infrastructure to disrupt or totally collapse its operations and functions. Whilst these assumptions have not been completely validated by supply chain and security practitioners, it is noted that in a

recent UK Government Cabinet Report the annual cost of cyber crime to the UK economy was estimated for the first time to be £27Bn and that theft of intellectual property (IP) accounted for approximately £9Bn (<http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf>).

2 Industry driven Approach

Within an industry/Government-sponsored programme called Integrated Model for Governance, Risk and Compliance (iGRC) (<http://www.igrc.co.uk>), we have analysed supply chain vulnerabilities due to the use of IT-enabled collaboration and contingency planning. IT security of supply chains requires that the IT services and security software are viewed and developed within the context of the supply chain enterprise as a whole and the benefits of the systems engineering approach to integrating requirements modelling with (software) system analysis, design and development have been demonstrated. Baseline requirements for secure IT solutions to support supply chain collaboration have already been elicited.

2.1 Wanted from Industry

This approach driven by practical needs will advance the requirements engineering process applied to secure IT services through the active involvement of industrial practitioners with knowledge of supply chain management and experience in the specification of IT systems. We seek practitioners willing to help us develop case studies through interviews and/or discussions. We wish to consider the general issue of IT-enabled supply chain vulnerability, but will have a particular focus on organizations working in hi-tech areas in which loss of IP is an area of concern.

A framework for case study definition that focuses on requirements elicitation, verification and validation based on modelling approaches used within the iGRC research programme will be prepared in advance to assist effective information capture. Engagement with industry through the Empirical Research Fair will support validation of the iGRC research undertaken for:

- Approaches to the definition, expression and validation of software security requirements in the context of enterprise supply chain collaboration.
- Definition of real world solutions for changing requirements that arise because of the dynamic nature of threats and vulnerabilities that affect software systems.
- Development of an integrated modelling approach, validated by real world exemplars.
- Case studies of software systems implementations that draw out the challenges associated with management of system security requirements.