# Security Assurance Requirements Engineering (STARE) for Trustworthy Service Level Agreements

Yudhistira Nugraha
Centre for Doctoral Training in Cyber Security
Department of Computer Science—University of Oxford
Oxford OX1 3QD, U.K.
yudhistira.nugraha@cs.ox.ac.uk
http://www.cs.ox.ac.uk/people/yudhistira.nugraha/

***Abstract*—With the development of trustworthy services, security requirements are of paramount importance for any service *(X-as-a-Service)*. This work-in-progress paper motivates the need for a new approach to requirements engineering for trustworthy services, which helps organisations to systematically define a set of security requirements and describe these in a service level agreement (SLA). This proposed research aims to provide adequate assurances to users by introducing the concept of the *Trustworthy Service Level Agreement (TSLA)*. The proposed research design involves three stages: The first is to develop an initial method of *Security Assurance Requirements Engineering (STARE)* by refining the nine *Security Quality Requirements Engineering (SQUARE)* activities. The key activities of STARE include: eliciting security requirements, classification of security requirements, and developing the novel concept of the TSLA. In the second stage, the effectiveness of STARE is evaluated using two real-world case studies: state cyber defence and lawful interception as a service. Finally, the process of implementing the STARE activities will be evaluated using selected service providers that deliver such services to defence and law enforcement agencies. Given the current state of requirements engineering for services, it is anticipated that this research will have a significant impact in terms of guaranteeing secure and trustworthy services in various domains.**

***Index Terms*—Requirements engineering for services, requirements elicitation, levels of assurance, trustworthy service level agreement, empirical research.**

## I. Introduction

The term requirements engineering (RE) for services was first used in [10] to propose a new approach that differs from traditional RE. To have confidence in services, users require service monitoring, service negotiation, and Service Level Agreements (SLAs) [2]. From a requirements engineering perspective, the final product of RE for services is the specification of the service in the form of the SLA [11]. An SLA plays an equally important role in both requirements engineering for service users and for service providers [10]. Henning et al. [3] first introduced the concept of security service level agreements as a mechanism to specify security requirements for effective organisation, but did not provide assurance mechanisms. A lack of the security-relevant SLA statements can decrease the level of security provided. Thus, it is proposed that a new type of SLA, the *Trustworthy Service Level Agreement (TSLA)* should be developed to build users' confidence in services. The current Security Quality Requirements Engineering (SQUARE) [6], which is a well-recognized requirements engineering method, does not provide quantitative measures to evaluate security requirements. In addition, SQUARE only considers security as non-functional requirements for information technology systems and applications [6]. To overcome this limitation, this research proposes to develop a new method of *Security Assurance Requirements Engineering (STARE)*. This research presents three main contributions: The first is that it elicits security requirements specific to the scope of the problem [8] (e.g. in the contexts of state cyber defence [7] and lawful interception [1]). We concentrate on the establishing security requirements both as the functional and non-functional requirements, which have substantial novelty in these domains. The second is that we provide a set of categories for each security requirements. The third contribution is the development a novel concept of a TSLA. It is anticipated that the STARE method can be used to investigate the security requirements in various service domains and that the concept of the TSLA can be formalised and used to improve the trustworthiness of services.

## II. Proposed Approach

This research firstly develops an initial framework for *Security Assurance Requirements Engineering (STARE)* based on refining the nine SQUARE activities. A key advantage of STARE is that it includes the novel concept of the TSLA, which enables the user to evaluate the security capabilities of the service providers accurately and determine whether the services are trustworthy. STARE consists of ten activities, including additional notions of security, such as defining the scope, service model, threat modelling and the security goals. Each step identifies the inputs, suggested methods, and outputs. The practitioners must select appropriate methods at each step of the STARE process. Secondly, a case study research methodology taken in [9] will be used to evaluate the effectiveness of STARE in the contexts of state cyber defence and lawful interception as a service. The third element of this research will involve an experiment in industry [4], to work alongside the service provider to test the primary hypothesis that *the concept of the Trustworthy Service Level Agreement is an effective means for building users' confidence in various service domains*.

## III. Research Design

Three main research activities are proposed. Each contributes to the outcomes of the other activity.

### A. Eliciting Security Requirements

The first research activity involves eliciting security-relevant functional and non-functional requirements based on the user needs in the contexts of state cyber defence [7] and lawful interception [1]. Security requirements elicitation is of paramount importance in the process of developing trustworthy services. However, most security requirements engineering approaches tend to be very complex and costly to implement. This activity aims to address the question: *what security requirements arise from the user requirements in the given case studies?*

### B. Classification of Security Requirements

The second research activity is an investigation into the formulation and classification of security requirements. A set of assurance levels for each security requirement is essential for government agencies. When developing a new service, the service provider must take into consideration the users' needs and the type of information involved. To define the levels (Tier 1 to Tier n) of security requirements, we adopt approaches taken in [5]. This activity aims to address the question: *how should levels of assurance be defined to give users confidence that the security requirements can be measured and improved?*

### C. Trustworthy Service Level Agreement (TSLA)

The third research activity involves developing a novel concept of the TSLA, which aims to establish trust and build users' confidence in a particular service. The TSLA is expected to provide a guarantee of users' needs with respect to a provision of service providers. This activity aims to address the question: *what aspects should be defined in Trustworthy Service Level Agreements?*

## IV. Outcomes and Impact

The primary contribution of this research is that the development and evaluation of STARE and the TSLA that leads to three main outcomes. Firstly, this study will contribute towards enhancing the understanding of security requirements in cyber defence and lawful interception as a service. It is expected to produce novel and substantial security-related functional and non-functional requirements, which will be described in the TSLA. Secondly, this research will provide a set of assurance levels for each security requirement. Thirdly, this study will introduce the concept of the TSLA, which could be the basis for further work and potentially become a mechanism for influencing service selection. This research can have a significant impact on understanding security requirements in various service domains to increasing security RE usage in the enterprise and by government agencies, such as defence and law enforcement agencies. The main objective is to provide a means for determining which of those services are trustworthy.

## V. Conclusion and Future Work

This research proposes to include additional notions of security, levels of assurance and the novel concept of the TSLA into the STARE activities. One major part of this research will be to evaluate the effectiveness of STARE on two real-world cases (state cyber defence and lawful interception as a service).These given case studies will seek to address the research questions. Moreover, the evaluation of STARE will be performed using qualitative assessment criteria. Specific elicitation techniques, such as an adaptive wideband Delphi for state cyber defence requirements, will be used to collect user needs. A range methods, derived from a systematic literature review, eliciting security requirements from laws and expert interviews, will be used to study lawful interception capability requirements. Finally, the STARE method will be tested in two service providers, which provide services, such as cyber defence and intelligence for government agencies. It is expected to demonstrate how the required level of trustworthiness for services can be reached by adopting the concept of the Trustworthy Service Level Agreement.

## Acknowledgement

The author is a DPhil student with the Indonesia Endowment Fund for Education (LPDP) Scholarship, under the joint supervision of Prof Andrew Martin and Prof Ian Brown.

## References

[1] Ian Brown. Lawful interception capability requirements. *Computers and Law*, 24(3):14–16, 2013.

[2] G. Dobson, R. Lock, and I. Sommerville. QoSOnt: a QoS ontology for service-centric systems. In *Software Engineering and Advanced Applications, 2005.31st EUROMICRO Conference on*, pages 80–87, Aug 2005.

[3] Ronda R. Henning. Security service level agreements: Quantifiable security for the enterprise? In *Proceedings of the 1999 Workshop on New Security Paradigms*, NSPW '99, pages 54–60, New York, NY, USA, 2000. ACM.

[4] J. Leuser, N. Porta, A. Bolz, and A. Raschke. Empirical validation of a requirements engineering process guide. In *Proceedings of the 13th International Conference on Evaluation and Assessment in Software Engineering*, EASE'09, pages 21–30, Swinton, UK, 2009.

[5] Andrew Martin, Jim Davies, and Steve Harris. Towards a framework for security in e-Science. In *e-Science (e-Science), 2010 IEEE Sixth International Conference on*, pages 230–237. IEEE, 2010.

[6] Nancy R Mead and Ted Stehney. *Security quality requirements engineering (SQUARE) methodology*, volume 30. ACM, 2005.

[7] Y. Nugraha, I. Brown, and A.S. Sastrosubroto. An adaptive wideband delphi method to study state cyber-defence requirements. *Emerging Topics in Computing, IEEE Transactions on*, PP(99):1–1, 2015.

[8] Bashar Nuseibeh and Steve Easterbrook. Requirements engineering: A roadmap. In *Proceedings of the Conference on The Future of Software Engineering*, ICSE '00, pages 35–46, New York, NY, USA, 2000. ACM.

[9] Husam Suleiman and Davor Svetinovic. Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure. *Requirements Engineering*, 18(3):251–279, 2013.

[10] P. A. T. van Eck and R. J. Wieringa. Requirements engineering for service-oriented computing: A position paper. In J. Gordijn and M. Janssen, editors, *First International Workshop on e-Services at ICEC'03, Pittsburgh, Pennsylvania, USA*, pages 23–28, Delft, the Netherlands, September 2003. TU Delft.

[11] D. Zowghi and A. Bargi. Software versus IT service: A comparative study from requirements engineering perspective. In *Database and Expert Systems Applications (DEXA), 2011 22nd International Workshop on*, pages 31–35, Aug 2011.