Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

Unifying traditional risk assessment approaches with attack trees

Stéphane Paul [a,*], *Raphaël Vignon-Davillier* [b]

[a] *Thales Research and Technology, 1 avenue Augustin Fresnel, 91767 Palaiseau, France*
[b] *Bolloré Logistics, 31 Quai Dion Bouton, 92800, France*

ARTICLE INFO

Article history:
Available online 10 May 2014

Keywords:
Security
Risk assessment
Risk management
Cognitive scalability
Attack trees
Model driven engineering

ABSTRACT

As software-intensive systems become more and more complex, so does the assessment of the risks that these systems may have on people's businesses, privacy, livelihoods, and very lives. For very large long-lived industrial programmes, such as the Galileo programme of the European Space Agency (ESA), or the *French Pentagon* programme for the Ministry of Defence, traditional risk management approaches are now reaching their limit. This is true for tooling, but even more so for humans. This paper proposes novel techniques to deal with cognitive scalability issues in risk assessment studies, amongst which graphical extensions to traditional risk management approaches, such as *chain diagrams*, and the seamless integration of attack trees. Feedback and results were collected from security experts and other stakeholders, in a large industrial context (namely, the Galileo risk assessment programme) and through dedicated research and development demonstrations. The feedback and results show effective improvements with respect to standard practices, even though fine tuning is still needed to reach an adequate and financially acceptable equilibrium between: (i) dealing with a large number of small independent problems; and (ii) maintaining an overall understanding of the system's risks and risks treatment.

1. Introduction

There is something very reassuring when leading a safety risk assessment study: one gets as input a Target Level of Safety (TLS). For example, in the Air Traffic Management (ATM) domain, ESARR-4 defines the maximum overall tolerable probability of ATM directly contributing to an accident of a commercial air transport aircraft as 1.55×10^{-8} accidents per flight hour. This helps framing and dimensioning precisely the safety study. When leading an IT system's security risk assessment study, there is nothing similar.[1] This has two consequences. First, security risk assessments are usually qualitative (e.g. a threat scenario is qualified as *Likely*), based on probabilities that have little or no measurement to confirm them, whereas safety assessments are usually quantitative (e.g. 10^{-6} probability of equipment failure), based on statistical measurements. Second, it is very difficult to define what a secure system is, or deciding when a system under study is secured enough. In other words, it is impossible to guarantee a

* *Corresponding author.*
E-mail addresses: stephane.paul@thalesgroup.com (S. Paul), r.vignondavillier@bollore-logistics.com (R. Vignon-Davillier).

[1] With respect to this statement, equipment security risk assessment is excluded. For equipment, the assurance levels of the Common Criteria ISO/IEC 15408 come close to the TLS in safety.

http://dx.doi.org/10.1016/j.jisa.2014.03.006
2214-2126/

study's completeness; and there is no way to be certain, or even reasonably believe, that all attacks have been considered in the assessment process.

So, the *traditional way* to lead a security risk assessment study is to comply with norms in managing the risks, e.g. the ISO-27000 series (ISO/IEC 27001; ISO/IEC 27002; ISO/IEC 27005), ISO 31000, etc. If one considers those norms as too complex or too abstract, there are many methods and guidelines that ensure compliance to those norms, i.e. the NIST SP-800 series (Information Security, 2012), EBIOS (French National Agency, 2010), OCTAVE (Alberts and Dorofee, 2001), CRAMM, etc. Some articles state that there are more than 200 risk management methods/guidelines around the world. As a result, we have clearly defined processes and methods to follow, but still no answer to what a secure system is.

Most would no doubt agree that a secure system is a system that you can trust … probably because this is not saying much. Considering that each incident lowers the trust we have in a system, is a secure system a system that is resilient to all attacks, past, present and future? No such system exists. This fact of life is clearly acknowledged by the French National Agency for the Security of IT Systems (ANSSI) when it delivers a security certificate for a system; indeed, the security certificate is obsolete the minute it is signed!

Our understanding of a secure system is that of a system for which one[2] accepts all the residual risks. Acceptance of the residual risks requires a good understanding of the risks and the stakes at play, by which statement we mean that there is strong cognitive component to security risk management. Additionally, acceptance of the residual risks requires also high assurance that most (if not all) relevant threat scenarios and risks have been included in the study. Today's software and critical information systems have become so complex that a study's register typically contains 3000+ initial security requirements even before the beginning of the risk assessment study, 5000+ threat scenarios, 1000+ risks (mean figures extracted from the largest risk assessment programmes managed by Thales). Traditional risk management approaches are now reaching their limit, especially for long-lived systems, for which such large sets of data must be maintained over very long periods of time (e.g. 20+ years).

Beyond risk management tool scalability, human scalability has become a key factor in having stakeholders read, understand and assess the completeness of risk assessment reports. If this is essentially true for individuals, it also applies to teams, when the production work needs to be performed collaboratively by a group of security experts; issues of social scalability are however less pregnant than those of cognitive scalability because more and more tools are now offering multi-user capabilities. In the coming years, return on experience should provide information on how efficient these technical multi-user capacities are in ensuring social scalability.

Whilst solutions exist for efficient collaborative work, to our knowledge, individual cognitive scalability has not yet been explicitly addressed in the domain of risk assessment. Some standalone techniques that seem promising have been around for a long time, e.g. attack trees (Schneier, 1999), but their adoption is slow, failing to overcome the *Technology Trigger Phase* of Gartner's hype cycle (Wikipedia).

Table 1 – Graphical notations.

⚡	Feared event
➶	Impact
◎	Primary asset
ⓘ	Risk (unvalued – colour changes according to risk level)
✓	Security objective
✎	Security requirement
🔒	Security solution
💻	Supporting asset (equipment)
🌐	Supporting asset (generic)
👥	Supporting asset (people or procedures)
⌂	Supporting asset (premises)
💻	Threat (on equipment)
💣	Threat (generic)
👥	Threat (on people or procedures)
⌂	Threat (on premises)
☠	Threat scenario
✳	Threat source
▨	Vulnerability

To provide for the aforementioned two requirements, i.e. cognitive scalability and a higher completeness assurance, we have experimented along two paths: (i) performing traditional risk assessment through graphical modelling, and (ii) seamlessly integrating an attack tree approach with a traditional risk assessment approach. This paper first details the main

[2] In particular the customer, but it could also be a certification or accreditation authority.