Response to Emergency Situations in a Traffic Management System

Lotfi ben Othmane*, Thomas Cerqueus¶, Adrien Thiery†, Mazeiar Salehie‡, Nicolas Noel†, Anthony Labaere†, Rémi Domingues†, Arnaud Cordier†, Anthony Ventresque†, Liliana Pasquale‡, Philip Perry†, Bashar Nuseibeh‡§
* Secure Software Engineering Group
Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany
Email: lotfi.ben.othmane@sit.fraunhofer.de
¶ National Institute for Applied Sciences de Lyon
and Laboratoire d'InfoRmatique en Image et Systèmes d'information,
Université de Lyon, Lyon, France
Email: thomas.cerqueus@insa-lyon.fr
† Lero, University College Dublin, Ireland
Performance Engineering Lab, School of Computer Science and Informatics
Email: firstname.lastname@ucd.ie
‡ Lero, University of Limerick, Ireland
Email: firstname.lastname@lero.ie
§ Department of Computing and Communications
The Open University, Milton Keynes, United Kingdom
Email: B.Nuseibeh@open.ac.uk

***Abstract*—This paper describes CARDEMO, a Traffic Management System (TMS) designed to assist TMS operators. The CARDEMO prototype applies an emergency response model to the city of Dublin, Ireland, and suggests a set of security controls for protecting critical assets (e.g., hospitals, schools, banks) from unexpected and harmful events that may occur in the city. Given an emergency situation, the system collects information about the amenities and traffic lights in the area, and uses the response model to recommend a set of security controls to mitigate possible threats.**

I. INTRODUCTION

Effective response to emergency situations reduces the loss of life and damage to property due to natural and man-made disasters. Most countries have guidelines for emergency traffic control and scene management, see e.g., [1]. These guildlines rely on the scene assessment provided by first responders upon arriving to the incident scenes. Thus, there is a delay in the response to incidents.

There is a tangency towards connecting traffic lights to central command systems. For example, the city of Dublin, Ireland, has a system that communicates with the traffic lights of the city and it provides information about the traffic lights, the cameras that operate in the city, and the Points Of Interest (POIs) such as banks, schools and restaurants. This information could help to improve the response to emergency situations by helping to route the traffic and support evacuation activities [2].

We developed at Lero[1] CARDEMO [3]: a Traffic Management System (TMS) prototype that makes use of the data to provide services for several types of users: everyday users, public servants and TMS operators. The system offers among other services evaluating emergency response advices. This service aims to support TMS with having early decisions about response to incidents.

This paper demonstrates a cyber-physical system that uses a requirements-driven approach [4] to advice about the response to emergency situations. The paper is organized as follows. Section II provides an overview of goal-based adaptive security. Section III describes the emergency response model that we propose. Section IV describes the CARDEMO application and a demonstration scenario. Section V concludes the paper.

[1]The Irish Software Engineering Research Centre (www.lero.ie).

II. OVERVIEW OF GOAL-BASED ADAPTIVE SECURITY

Maintaining security goals requires applying effective security controls able to protect critical assets from harm. Salehie et al. [4] proposed a requirements-driven approach that uses a Fuzzy Causal Network (FCN) [5], [6] to analyse the consequences of assets and context changes on the security risk and the satisfaction of security requirements. This approach is based on the following steps.

Modelling the security concerns together with the system requirements. A KAOS *goal model* [7] is used to represent functional and non-functional requirements and a *threat model* (anti-model [8]) to represent threats and attacks. The goal model explicitly represents security goals and associated vulnerabilities. In particular, security goals can be associated with security controls, which can mitigate modeled vulnerabilities. An asset model represents assets to be protected and their

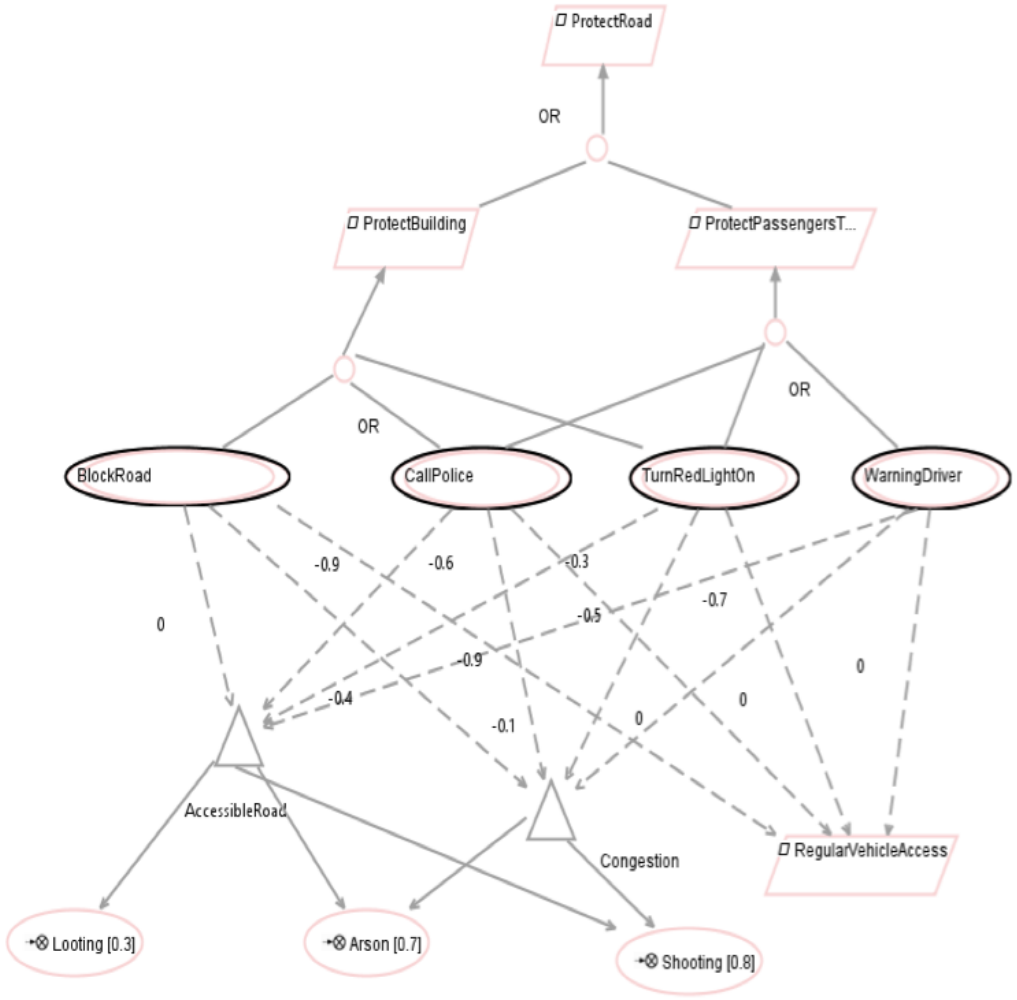

Fig. 1. Goal model of the emergency response system.

relationships. Assets are linked to the security goals and threats aimed to protect and harm them, respectively.

Configuring the FCN. The FCN is generated from the asset, threat, and goal models designed in the previous step. Each node of the FCN is associated with a security concern and has a specific semantics. For example, a node associated with an asset represents its value. The links of the network identify positive and negative causal relationships among security concerns. For example, a link between a security control and a vulnerability indicates how the security control reduces the likelihood of that vulnerability to be exploited. The FCN explicitly represents the impact that assets and other contextual factors can have on the system requirements and the security concerns. Therefore, it is used at runtime to estimate the security risk in specific situations (e.g., when assets or context change) and evaluate the utility of all possible configurations of security controls.

The rest of the section describes how the approach by Salehie et al. [4] has been adopted in this paper to support effective response to emergency situations.

III. Proposed Emergency Response Model

Response to emergency situations requires making decisions about the best actions to take to mitigate potential threats that may arise after undesired events, such as fire, shooting, explosion, looting, which may cause potential harm to the amenities (e.g., banks, hospitals, and schools) and persons placed in their vicinity. The approach proposed by Salehie et al. [4] allows us to relate assets (i.e. amenities) to potential threats and security goals. Threats can be discovered after emergency acquisitions; security goals are satisfied by applying security controls (i.e. emergency response). More precisely, the asset model is adopted to represent the amenities located in the area in which an undesired event took place. The goal model is used to represent the security requirements necessary to protect the amenities, and the vulnerabilities to be mitigated. The threat model represents the threats that can harm the amenities placed in the vicinity of the area where an undesired event took place. Threats are also decomposed into concrete attacks that can be performed by an offender to achieve them. The FCN generated from these models is used to

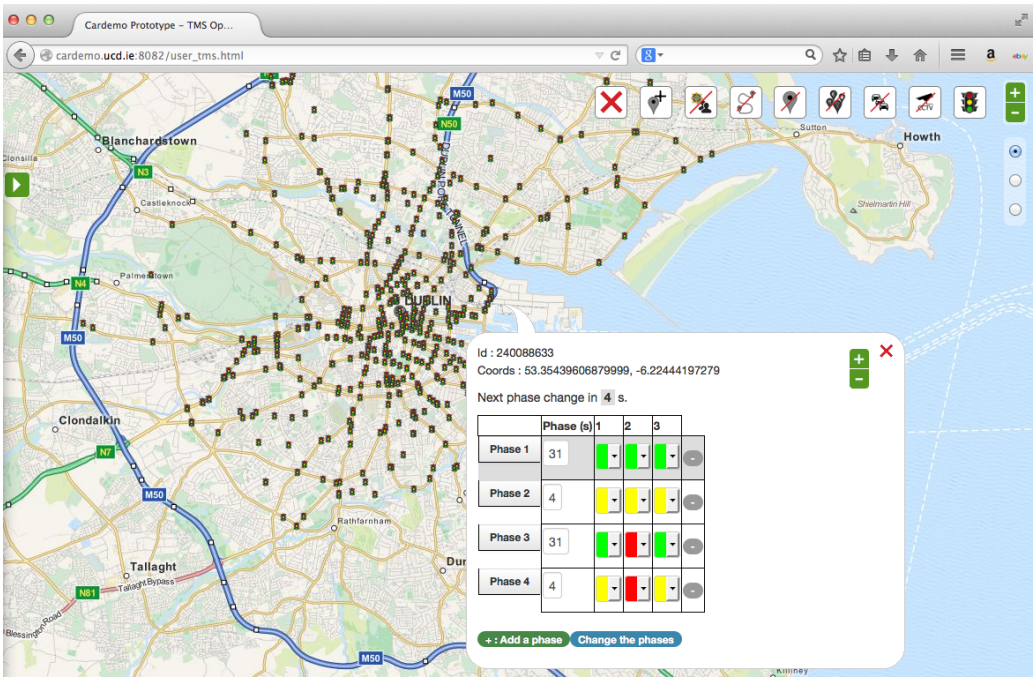

Fig. 2. Traffic lights in Dublin, Ireland.

estimate the security risk after an undesired event takes place and to identify the most adequate emergency response. This is expressed in terms of a configuration of security controls that minimise the security risk and maximise the satisfaction of the system requirements.

Figure 1 depicts the goal model of the scenario adopted in this paper.[2] The TMS must guarantee regular vehicle access and–at the same time–must ensure the security of each road segment (goal *ProtectRoad*). To protect a road segment it is necessary to protect the buildings placed in it and the car passengers who are traversing the road (goals *ProtectBuilding* and *ProtectPassengersT*). The buildings can be protected by blocking the road, calling the police or changing the phases of the traffic lights regulating access to the road segment (security controls *BlockRoad*, *CallPolice*, and *TurnRedLightOn*, respectively). The security controls that can be enabled to protect the passengers are *CallPolice*, *TurnRedLightOn*, and *WarningDriver*. The latter corresponds to warning the car drivers using road panels, or radio/TV alert messages. Existing vulnerabilities, such as road accessibility and congestions can facilitate potential attacks, such as looting, arson and shooting. The weights assigned to the links between security controls and vulnerabilities indicate the effectiveness of a security control in mitigating the target vulnerability. While the weights of the links between security controls and goal *RegulateVehicle Access* indicate how negatively a security control affects the satisfaction of that goal. Assigning weights require domain knowledge that may come from domain experts and existing evidence–e.g., statistical data [4]. They shall be tuned using sensitivity analysis based on the model output for provided inputs.

The FCN reasoning mechanism computes the value of each node depending on the value of its incoming nodes by using aggregation functions defined based on T-Norm and T-Conorm. A binary search algorithm is enabled by using the Z3 SMT solver [9] for identifying a configuration of security controls that provides the best utility, that is, maximizes the satisfaction of security goals and minimizes the security risk and the negative impacts that security controls have on the satisfaction of other non security goals.

IV. Overview of CarDemo and Demonstration Scenario

CarDemo is built using the service-oriented architecture. The implementation uses Mule ESB [10], an Entreprise Service Bus (ESB) software architecture. The CarDemo offers a set of basic features, such as routing services, viewing of POIs, viewing of traffic condition, and viewing of traffic lights. Thus, it is possible to potentially use the services of the CarDemo for other applications.

The application is depicted by Figure 2, which shows the traffic lights located in Dublin. By clicking on a specific traffic light, a TMS operator can modify its configuration (e.g., number of phases and duration of a phase). The Graphical User Interface (GUI) allows to report emergency situations that occur in the city, such as car accidents, fires, protests, and robberies. Response to emergency situations is among the services offered by CarDemo, which aims at assisting TMS operators in making decisions about the response to these events and reduce their impact. This service suggests

[2]The asset model and threat model for our demonstrator are simple and their main entities are included in the goal model.

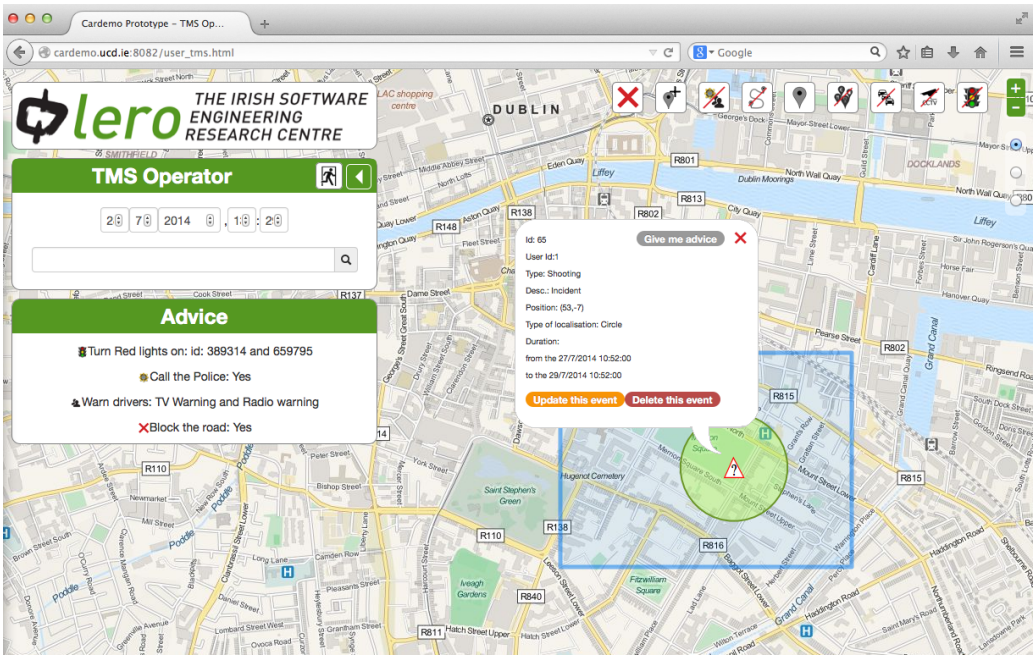

Fig. 3. Output of the recommendation service.

to the TMS specific actions, such as change the traffic light sequences, call the police, block a road.

Scenario. Let consider a event reported (via the Web interface) along with the area where it occurred as depicted by Figure 3. The event is marked by a triangle and the area is marked by a green circle. As a response to this event, a TMS operator invokes the recommendation service by clicking on the button "Give me advice." The blue rectangle represents the area in which the operator thinks it is relevant to act on. The service evaluates the model using data it extracts from other services of CARDEMO such as identification of amenities and traffic lights in the area and displays on the left-hand side of the Web interface a set of actions that shall be performed. They are in the case of this experiment: turn off a traffic light (through the interface presented in Figure 2), call the police to dispatch a patrol and also to block the road and request for TV and radio warning services.

V. CONCLUSION

Given an emergency situation, CARDEMO collects information about the amenities and traffic lights in the area, and uses an adaptive response model to recommend a set of controls to mitigate possible threats. The model is based on weights which should be adjusted in order to provide valid advices using e.g., TMS experts opinions.

ACKNOWLEDGMENT

This work was supported, in part, by Science Foundation Ireland grant 10/CE/I1855 to Lero - the Irish Software Engineering Research Centre (www.lero.ie). This work was also supported by the BMBF within EC SPRIDE, the Hessian LOEWE excellence initiative within CASED, and a Fraunhofer Attract grant.

REFERENCES

[1] "Emergency traffic control and scene management guidelines," Oct. 2008. [Online]. Available: http://www.ce.siue.edu/faculty/hzhou/Information\%20CD/Menu\%20Files/Materials/2-Emergency\%20Traffic\%20Control\%20and\%20Scene\%20Management\%20Guidelines-WDOT.pdf.

[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th ACM/IEEE Design Automation Conference (DAC)*, Anaheim, CA, USA., June 2010, pp. 731–736.

[3] Lero: The Irish Software Engineering Research Centre, "http://cardemo.ucd.ie," 2014. [Online]. Available: http://cardemo.ucd.ie

[4] M. Salehie, L. Pasquale, I. Omoronyia, R. Ali, and B. Nuseibeh, "Requirements-Driven Adaptive Security: Protecting Variable Assets at Runtime," in *Proc. 20th IEEE International Requirements Engineering Conference (RE), 2012*, Chicago, IL, USA, Sept 2012, pp. 111–120.

[5] B. Kosko, "Fuzzy Cognitive Maps," *Int. Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65–75, 1986.

[6] S. Zhou, Z. Liu, and J. Zhang, "Fuzzy Causal Networks: General Model, Inference, and Convergence," *IEEE Transactions on Fuzzy Systems*, vol. 14, no. 3, pp. 412–420, 2006.

[7] A. van Lamsweerde, *Requirements Engineering: From System Goals to UML Models to Software Specifications*. John Wiley and Sons, 2009.

[8] A. van Lamsweerde, "Elaborating Security Requirements by Construction of Intentional Anti-Models," in *Proc. of the 27th International Conference on Software Engineering*, 2004, pp. 148–157.

[9] "Z3," http://z3.codeplex.com.

[10] MuleSoft, "Mule ESB: Most Popular Open Source ESB," 2014. [Online]. Available: http://www.mulesoft.com/platform/soa/mule-esb-open-source-esb