Databases and Information Systems X
A. Lupeikiene et al. (Eds.)

doi:10.3233/978-1-61499-941-6-65

Application of the Reference Model for Security Risk Management in the Internet of Things Systems

Raimundas MATULEVIČIUS [a,1] and Raimundas SAVUKYNAS [b]
[a] *Institute of Computer Science, University of Tartu, J.Liivi 50409 2, 50409, Tartu, Estonia*
[b] *Institute of Data Science and Digital Technologies, Vilnius University, Akademijos str. 4, LT-04812, Vilnius, Lithuania*

Abstract. Security in the Internet of Things (IoT) systems is an important topic. In the previous study we have presented a reference model for security risk management in the IoT systems. In this study we analyse how it can be applied. Specifically we consider an example of the connected vehicle and illustrate how the reference model could help discovering and explaining security vulnerabilities, defining security risks, and introducing security countermeasures.

Keywords. Internet of Things (IoT), information systems security risk management (ISSRM), open web application security project (OWASP), connected vehicle

1. Introduction

Internet of Things (IoT) is a network of connected devices and systems to exchange or accumulate data and information generated by users and embedded sensors in the physical objects [11]. Among the privacy, energy-awareness, environment, and other concerns, security plays an important role, as the (potentially sensitive) data is sent among the various devices and multiple users. In cases where such data is intercepted and used for non-intended purposes, it may lead to the severe damages of the valuable system and/or environmental assets [10,15,19,25,26,29]. There exist a number of surveys related to the IoT security [1,2], security of the IoT frameworks [3,30], or specific components of the IoT systems [4,12,16]. However they lack a systematic approach to manage IoT security risks and reason about the introduced security countermeasures.

In [23] we have proposed a comprehensive reference model for *security risk management in the IoT systems*. We based our proposal on the domain model for the information systems security risk management (ISSRM) [8,20] – thus, we focus on the security risks to the information and data managed in the IoT system. The IoT systems much depend on cloud and Internet computing. Therefore the Web application vulnerabilities and their countermeasure potentially could be considered in the IoT systems, too. In [23]

[1] Corresponding Author: Raimundas Matulevičius, Institute of Computer Science, University of Tartu, 50409 Tartu, Estonia; E-mail: rma@ut.ee

we adapt the vulnerability and countermeasure definitions of the open Web application security project (OWASP) [21] to identify and manage the security risks in the IoT systems. In this paper, we illustrate how this reference model could be applied in order to explain business assets, system assets, and their vulnerabilities, and to introduce security countermeasures. To support our discussion, we analyse connected vehicle system [27,28].

The rest of the paper is structured as follows: Section 2 overviews some related studies. Then in Section 3 we overview the ISSRM domain model. Section 4 presents components of the reference model for security risk management in the IoT systems. This includes the overview of the IoT assets, their vulnerabilities and countermeasures. Section 5 discusses how this reference model is applied in the connected vehicle system. Finally, Section 6 concludes the paper and provides directions for future work.

2. Related Work

Few studies have reported on the IoT security. Most of them focus on the security risks and threats of the IoT. For instance, Basu *et al.* [5] discusses the IoT application design and security challenges. These include the following properties: heterogeneity, interoperability, connectivity, mobility, scalability, addressing, identification, spatiotemporal services, resource constraints, and data interchange. The study characterises security threats such as spoofing, tampering, repudiation, information leakage, elevation of privilege, user privacy, replay attacks and cloning of nodes. Some security framework is proposed to mitigate them. Elsewhere in [7] Benabdes *et al.* explores different methods to address security and privacy requirements (e.g., confidentiality, authentication, integrity, authorization, non-repudiation, and availability) in the IoT systems. The study discusses eavesdropping and denial of service attacks and proposes encryption, hash and digital signature to secure data communication between the IoT devices.

In [9] Fink *et al.* discusses vulnerabilities of the IoT systems and highlight the importance of the privacy and security standards. More specifically it focuses on crime, emergent behavior, scientific and technological, social and regulatory challenges was made. In [13], Hossain *et al.* reports on a series of new security and privacy challenges regarding secrecy, confidentiality, data integrity, and authentication access control in the IoT systems. The study discusses some IoT architecture and interoperability between interconnected networks, security problems and attacks mitigation strategies. Elsewhere in [22], Qiang *et al.* consider the privacy protection, wireless communication, and information security. Authors propose a new IoT security method for processing of the massive amount of data, and for ensuring security and reliability.

In [14] Jing *et al.* classifies security concerns to different levels of abstraction. Specifically, it focuses on the radio frequency identification, wireless sensor network, robust security network technology and proposes solutions to secure them. Similarly, in [17], Mahmoud *et al.* analyzes the general and specific IoT security challenges at different layers of the IoT architecture. On one hand, technological (e.g., wireless communication) challenges include the maintenance of scalability and low consumption of energy. On another hand security challenges are confidentiality, authentication, and integrity. The study reports on the attacks in the perception (e.g., replay attacks, timing, and node capture attacks) and network (e.g., man-in-the-middle attack) layers. Elsewhere, in [18],

Matharu *et al.* describes the IoT architecture consisting of four layers. The authors highlight the importance of the IoT connectivity robustness, interoperability, and standardisation (especially regarding identity management, safety, and security of objects, data confidentiality, and encryption). In [24], Suo *et al.* also discusses the security architecture, features, and requirements at different layers of the IoT system. Hence the authors focus on the key agreement, identity authentication, cloud computing, and authentication at the perceptual, network, support, and application layers.

Zhao and Ge, in [10], proposes a three-layer IoT system structure. Hence the study investigates how security threats (e.g., node capture, fake node, malicious data, replay attack and routing threats) could be performed. The cryptographic algorithms and key management techniques were deployed in order to mitigate those attacks. The compatibility and cluster security problems were resolved using a key agreement mechanism.

Although all studies suggest different IoT security architectures consider various security risks and suggest countermeasures to mitigate them, the state of the art does not suggest a systematic approach for security risk management. In this paper we illustrate how IoT reference model for security risk management could help to explain security risks.

3. Domain Model for Security Risk Management

The ISSRM domain model (see Figure 1) suggests three conceptual pillars to explain secure *assets*, *security risks* and their *countermeasures* [8,20]. Here, the *business asset* is understood in terms of the information, data and processes, which bring value to the organisation. Business assets are supported by the *system assets* (a.k.a., IS assets). *Security criteria* (i.e., confidentiality, availability, and integrity) are the constraints of the business assets and define security needs. *Security risk* is defined as a combination of the *event* and *impact*. Here, *impact* negates the security criterion and harms at least two (one system and one business) assets. Event is defined in terms of *threat* and *vulnerability*. A *vulnerability* is a characteristic of the system assets and it constitutes a weakness of this asset. A *threat* targets the systems assets by exploiting its vulnerability. Threat is defines as combination of the *threat agent*, an active entity who has interest to harm the assets, and the *attack method*, the means used to carry on the threat. Security risk treatment concepts include risk treatment decision, security requirements, and controls. *Security risk treatment* is a decision to treat the identified risk. It is refined to the *security requirements*, which define the condition to be reached by mitigating the security risks. Finally the *controls* implement the defined security requirements.

In this paper we will use the ISSRM domain model to combine constituencies of the IoT system security risks.

4. Security Risk Management in IoT Systems

4.1. Context and Assets

Figure 2 presents an IoT architecture model [6]. Here, the *IoT system* consists of *service* used by the *user*, remote or/and local *storage*, and *computing device*. There exists an

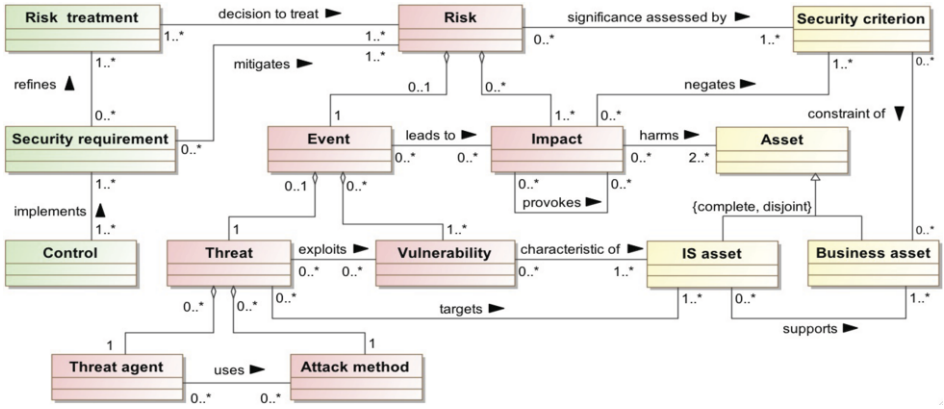

Figure 1. The ISSRM domain model, adapted from [8,20]

IoT device, which interacts with the *computing device*. Different *computing devices* are connected to each other. *IoT devices* manage some *entities*, which can be either on-device and/or network *resources*. *Remote storage* and *network recourses* are placed on the *cloud* environment.

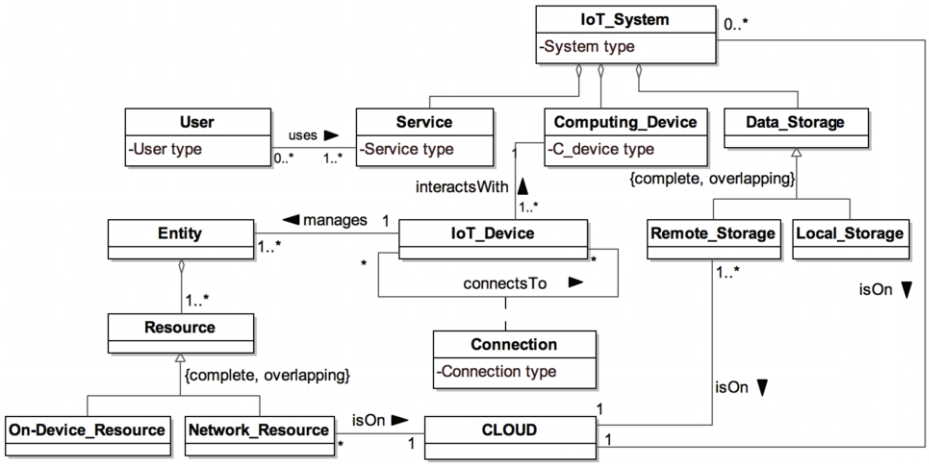

Figure 2. IoT architecture model

The IoT architecture provides the IoT components which correspond to the system and business assets. The IoT asset is anything that is valuable for the IoT system or play an important role in providing functionality and services to users. Like in [8,20] the IoT system assets gain their importance in supporting the business assets. Thus, they can be represented as ground components of information technology such as hardware, software or network.

Business assets are valuable for each IoT system as they represent essential business value such as information, processes, capabilities and skills [8,20]. Besides official definitions, business assets can be commonly represented by the data, which is transferred,

stored or manipulated in the IoT system during the working process. As a result business assets security is defined in terms of security criteria (i.e., confidentiality, integrity or availability).

4.2. IoT Vulnerabilities and Risk Countermeasures

The vulnerability is presented as a weakness in a design flaw or an implementation bug. They allow an attacker to harm applications, users, and other entities that rely on this application. As the IoT systems are using the Web applications, the vulnerabilities of the Web applications could be seen as the potential ones in the IoT systems. Based on the OWASP project [21], in [23], we have discussed ten vulnerability classes potentially related to the different system assets of the IoT system. These vulnerability classes are:

- V#1: *Insecure Web interface*,
- V#2: *Insufficient authentication and/or authorisation*,
- V#3: *Insecure network services*,
- V#4: *Lack of communication encryption*,
- V#5: *Privacy concerns (confidentiality)*,
- V#6: *Insecure cloud interface*,
- V#7: *Insecure mobile interface*,
- V#8: *Insufficient security configurability*,
- V#9: *Insecure software and/or firmware*,
- V#10: *Poor physical security*

To mitigate security risks, where these vulnerabilities can be identified, in [23] we discuss a set of countermeasures. Following the OWASP project [21], these are countermeasures are grouped into five groups:

1. Protocol and network security (i.e., Cm#1: *Secure network services* and Cm#2: *Communication encryption*),
2. Data and privacy (i.e., Cm#3: *Privacy concerns*, Cm#4: *Secure software and/or firmware*, and Cm#5: *Physical security*),
3. Identity management (i.e., Cm#6: *Secure authentication and/or authorisation*, Cm#7: *Secure Web interface*, and Cm#8: *Secure mobile interface*),
4. Trust and governance (Cm#9: *Trust and governance*), and
5. Fault tolerance (Cm#10: *Fault tolerance*).

4.3. Reference Model of IoT Security Risk Management

In Figure 3 we combine IoT system assets, IoT vulnerabilities and the countermeasure to a comprehensive reference model [23] for the IoT security risk management. Firstly, we introduce stereotype System asset to identify explicitly the component which potentially supports the data managed and controlled in the IoT system.

Characteristics of system assets. As discussed in [8,20], vulnerability is *a characteristic of the system assets*. The vulnerabilities listed in Section 4.2 *characterise weaknesses of the system assets* presented in Figure 2. We introduce these vulnerabilities as the attributes of the targeted vulnerable system assets.

For example, *Service* is vulnerable regarding insecure Web interface (V#1), insufficient authentication and/or authorisation (V#2), and insecure mobile interfaces (V#7).

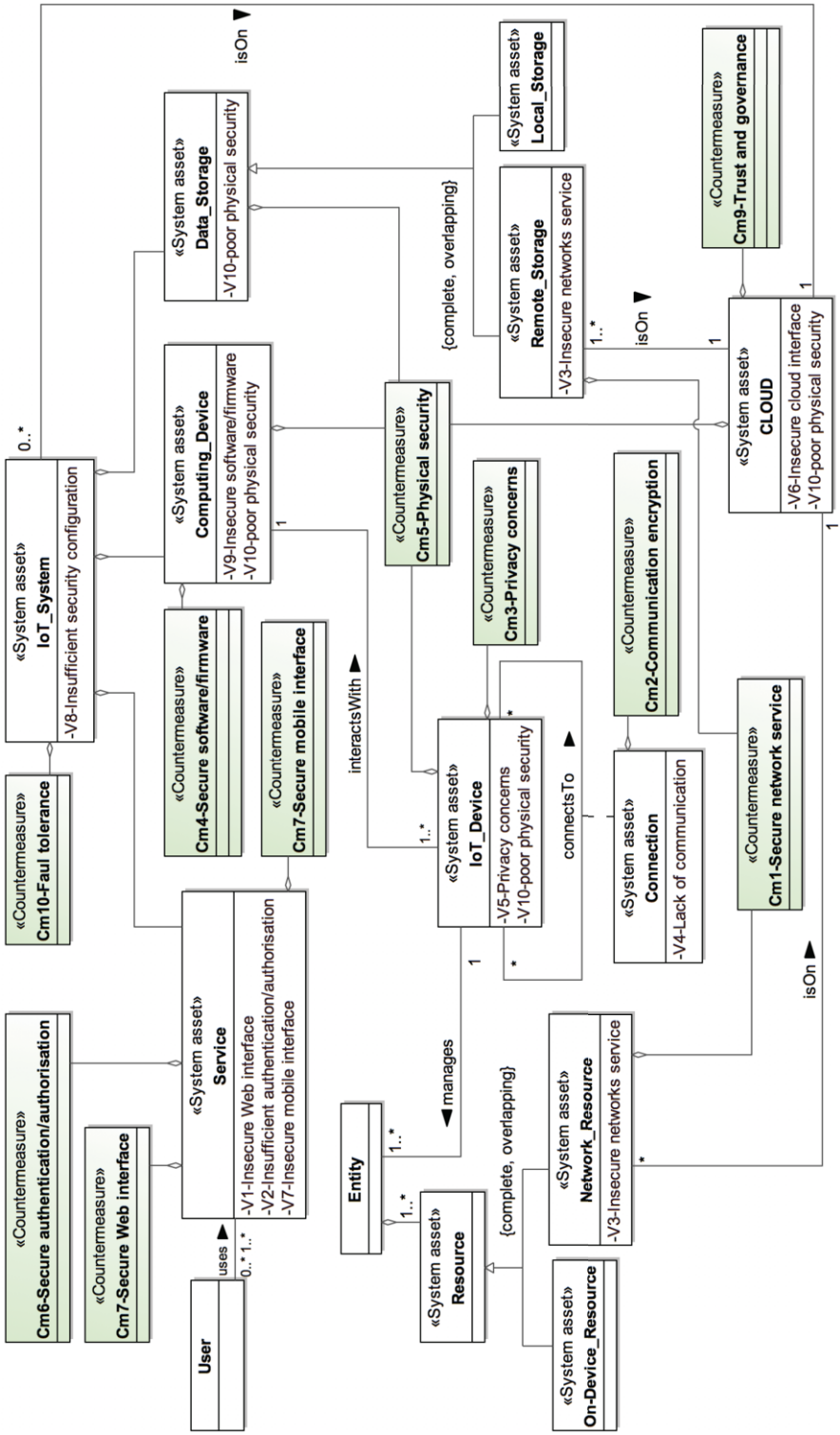

Figure 3. IoT reference model for security risk management

The vulnerability of insecure network services (V#3) could be found in the *network resources* and *remote storage*. A lack of communication encryptions (V#4) could potentially be considered in the *connection* and privacy concerns (V#5) should be considered when managing *IoT devices*. In the IoT systems, *cloud* plays an important role, thus, its interface should be considered regarding the insecure cloud interface (V#6) vulnerabilities. *IoT system* could be explored through the insufficient security configurability (V#8). As the *computing device* is a part of the IoT system, its vulnerabilities regarding the insecure software and/or firmware (V#9) should be also taken into account. Finally, the poor physical security (V#10) could potentially open the gate for the attacker at the *data storage*, *computing device*, *IoT device* and *cloud*.

Countermeasures becomes a part of the IoT system. Security countermeasures are introduced to mitigate the security risks. In Figure 3 we link the security countermeasures (see classes with stereotypes Countermeasure) to the system assets, which can be targeted by the security threat thus exploiting theirs vulnerabilities. Thus, these countermeasure should become a part of the IoT system (e.g., introduced as a part of the various IoT assets), thus reducing the potentiality of the security risk event happening.

Countermeasure on secure network services (Cm#1) mitigate risks with vulnerabilities of insecure network services (V#3), and communication encryption (Cm#2) – vulnerabilities related the lack of communication encryption (V#4). Countermeasures regarding the privacy concerns (Cm#3) help to mitigate security risks with vulnerabilities related to privacy concerns (V#5); secure software and/or firmware (Cm#4) – vulnerabilities related to insecure software and/or firmware (V#9). Countermeasure of physical security (Cm#5) addresses risks with vulnerabilities of poor physical security (V#10). Countermeasures to secure authentication and/or authorisation (Cm#6) mitigate risks with vulnerabilities of insufficient authentication and/or validation (V#2); to secure Web interface (Cm#7) – vulnerabilities of insecure Web interface (V#1); and to secure mobile interface (Cm#8) – vulnerabilities of insecure mobile interface (V#7). Countermeasures regarding the trust and governance (Cm#9) deal with the security risks with vulnerabilities of insecure cloud interface (V#6). Countermeasures regarding fault tolerance (Cm#10) mitigate security risks with vulnerabilities of insufficient security configurability (V#8).

5. Connected Vehicle Example

In this section we will analyse how the proposed security reference model for the IoT systems could support analysis of the security risks. Particularly we will look to the connected vehicle system, described in [27,28]. As defined, a *connected vehicle* uses a network, sensors, and electronic control unit (ECU) to control functions of the vehicle and to connect this vehicle to other system entities (e.g., other connected vehicles, road side equipments, and traffic management centers). This way it exchanges the information about the car location, environment, direction, condition of driving, and status information necessary for vehicle's device control.

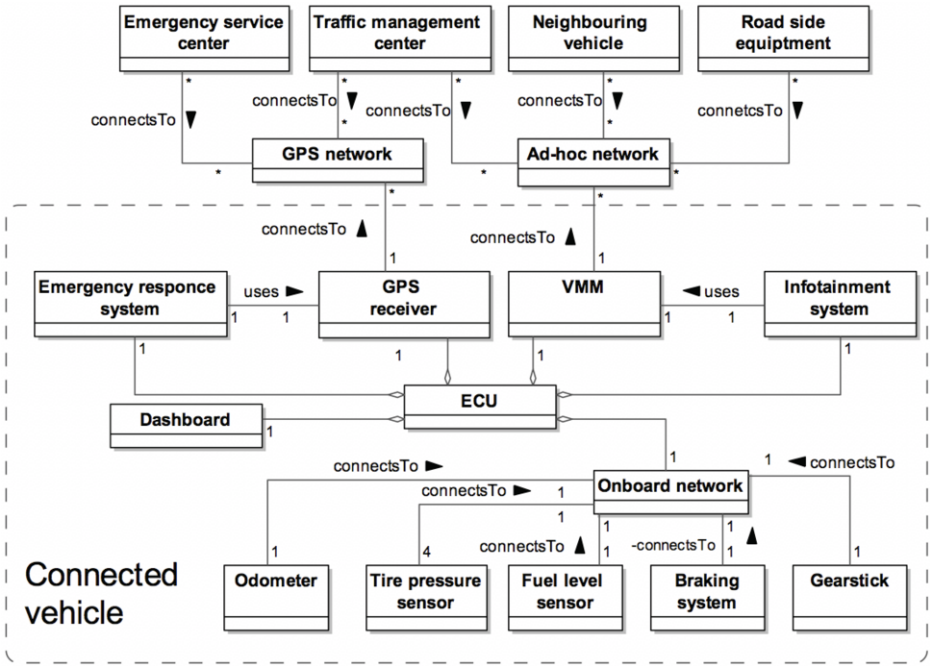

Figure 4. Connected vehicle model

5.1. Context and System Assets

Figure 4 illustrates some major components of the connected vehicle[2] and Table 1 presents a relationship among different system assets and business assets. Hence, a central element in the connected vehicle is the electronic control unit (ECU) for controlling functionalities of this IoT system. ECU includes other components, such as Emergence response system, which could be used to contact some parties for assistance in the emergency situations, Infotainment system used for entertainment and information services, Dashboard used to display information from sensors installed in the connected vehicle. To collect information, ECU is using the Onboard network, which helps to connect and collect sensor information, for example, about the *speed* (from odometer), *tire pressure* (from the tire pressure sensors), *fuel level* (from fuel level sensor), and etc.

The Infotainment system is using the Vehicle Mounted Modem (VMM) to exchange messages with Neighbouring vehicles and Road side equipments. These are connect through *Wi-Fi* communication used in the vehicular ad-hoc networks. In the similar way the Emergency response systems are using the GPS receiver to communicate with Emergency service center through the GPS network.

There is quite a complex design to support various business assets by the system assets (e.g., Table 1 includes only a few major relationships). For example, ECU uses the onboard network to collect *speed recordings* from the odometer. Odometer sensor is connected to ECU through the onboard network. Speed recordings are displayed in

[2]The diagram is developed following discussion given in [27,28]. It potentially could be designed differently if one would consider real connected vehicle.

Table 1. Assets in connected vehicle

Business Assets	System assets	Security criteria
Speed readings	Odometer	Integrity of speed readings
Tire pressure data	Tire pressure sensor	Integrity of tire pressure data
Fuel level data	Fuel level sensor	Integrity of fuel level sensor
Braking service	Braking system	Availability of braking service
Gearing service	Gearstick	Availability of gearing service
Information in emergency situation	Emergency response system	Integrity and availability of information in emergency situation
Infotainment service	Infotainment system	Integrity of infotainment service
Firmware	ECU	Integrity and availability of firmware

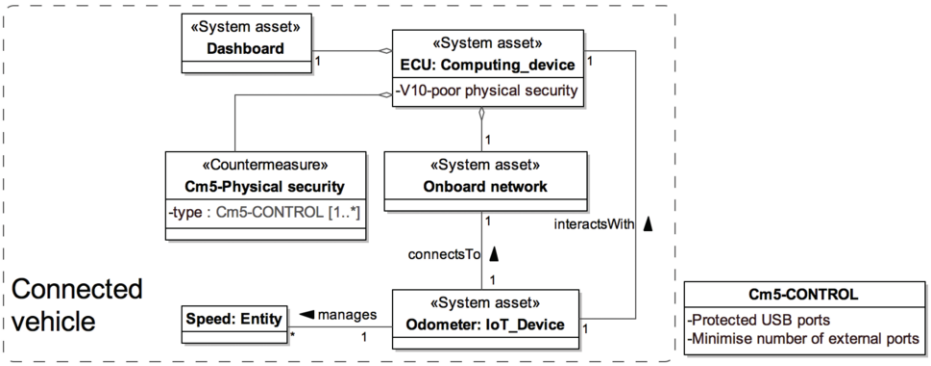

Figure 5. Poor physical security in connected vehicle

the dashboard. This means to support *speed recordings* (i.e., business assets), different system assets (i.e., odometer, ECU, onboard network, and dashboard) are used. Similarly the support for other business assets (e.g., tire pressure data, fuel level data, braking service, gearing service, information in emergency situation, infotainment service, etc) is provided.

5.2. Security Risks

A list of potential security risks for the connected vehicle is discussed in [28]. In this section we will illustrate how the reference model could help explain these risks in the connected vehicle. Lets' consider an extract of the components diagram given in Figure 5. Following Figure 2, the Odometer is an *IoT device*, which manages *entity* (i.e., Speed) and interacts (through the onboard network) with the *computing device* (i.e., ECU). However, as discussed in Table 2, see Risk1, the ECU has a vulnerability (corresponding to *V#10*) regarding the *physical security*. Hence, an attacker can physically change the connected vehicle's ECU and provoke wrong driving decisions. It is interesting to note that in this example we consider the internal IoT device connections to the computing device.

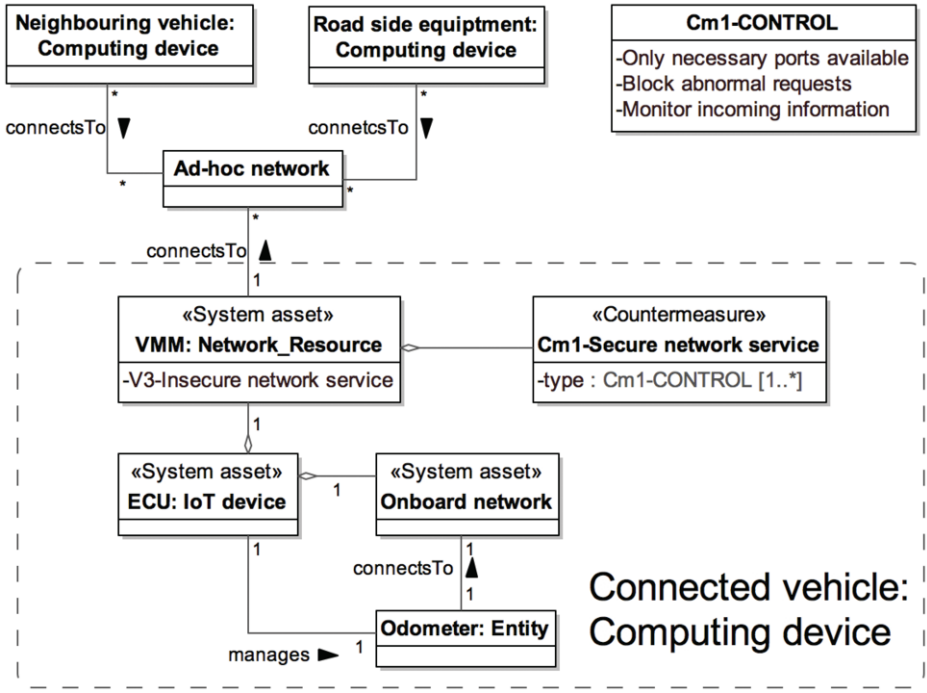

Figure 6. Insecure network communication in connected vehicle

However the connected vehicle itself could be understood as the computing device in the larger scope. In this case it is connected to other computing devices (i.e., connected vehicles, road side equipments and/or traffic management center(s)) as illustrated in Figure 4. Hence the VMM is understood as the *network resource*, which communicates to other devices in order to receive the needed services. If not treated properly (see Risk 2 in Table 2) it could be vulnerable regarding the insecure network services. The attacker could use the insecure VMM in order to alter the *speed readings* thus provoking wrong driving decisions.

Risk 1 and Risk 2 illustrate that the IoT security reference model helps to explicit the targeted system assets and to explain system vulnerabilities. It also guides the redefinition of the analysis scope as illustrated in Figure 5 and Figure 6. Similar security risk scenarios could be observed regarding other system and business assets. Their resulting *impacts* are [28]:

- Negation of integrity of tire pressure data leading to the tire pressure warning in the dashboard and provoking the pull over of tires;
- Negation of integrity of fuel level data leading to the "no signal" in the dashboard and provoking the driver into driving until the vehicle runs out of fuel;
- Negation of availability of the braking service provoking the vehicle accident;
- Negation of availability of gearing service leading to the gearstick locking and provoking the vehicle's immobility;
- Negation of integrity (or availability) of information in emergency situation leading to the falsification of this information;

Table 2. Risks in connected vehicle (negation of integrity of the *speed readings*), adapted from [28]

Concept	Risk 1	Risk 2
Risk	An attacker plugs physically the malicious ECU to the vehicle, alters the speed readings because USB's port(s) can be accessed thus leading to the negation of the integrity of the speed reading and provoking the wrong driving decisions.	An attacker establishes connection between attacker's vehicle (or road side equipment) and target vehicle and alter speed readings at the target vehicle's ECU because of the insufficient control of vehicle's VMM ports and weak monitoring of incoming information at the vehicle's VMM thus leading to the negation of the integrity of the speed reading and provoking the wrong driving decisions.
Impact	- Negation of integrity of the speed readings; - Harm to the vehicle's reliability; - Original speed readings are altered, thus provoking wrong driving decisions.	- Negation of integrity of the speed readings; - Harm to the vehicle's VMM; - Original speed readings are altered, thus provoking wrong driving decisions.
Vulnerability	- Vehicle's USB port(s) can be physically accessed.	- Insufficient control of vehicle's VMM ports; - Weak monitoring of incoming information at the vehicle's VMM.
Threat agent	An attacker capable of developing malicious ECU and physically plugging in the vehicle.	An attacker capable to use his vehicle (or road side equipment) to establish connection to target vehicle and to inject speed readings to target vehicle's ECU.
Attack method	1. Plug (other/potentially malicious) ECU using (physical) vehicle's USB port(s); 2. Alter speed readings received from Odometer; 3. Display altered speed reading at the Dashboard.	1. Establish connection between attacker's vehicle (or road side equipment) and target vehicle; 2. Send (malicious) speed readings to target vehicle's ECU; 3. Alter speed readings at the target vehicle's ECU. 4. Display (altered) speed readings in dashboard.

- Negation of integrity of infotainment service leading to the non-desired infotainment services;
- Negation of integrity (or availability) of the ECU's firmware leading to the misbehave of the connected vehicle.

Table 3. Countermeasures in connected vehicle

Concept	To mitigate Risk 1	To mitigate Risk 2
Security countermeasures	- Vehicle's USB ports should be protected; - Number of external vehicle's USB ports should be minimised.	- Only VMM ports important for the vehicle's functionality should be exposed; - VMM should monitor incoming information; - Abnormal requests/services should be blocked

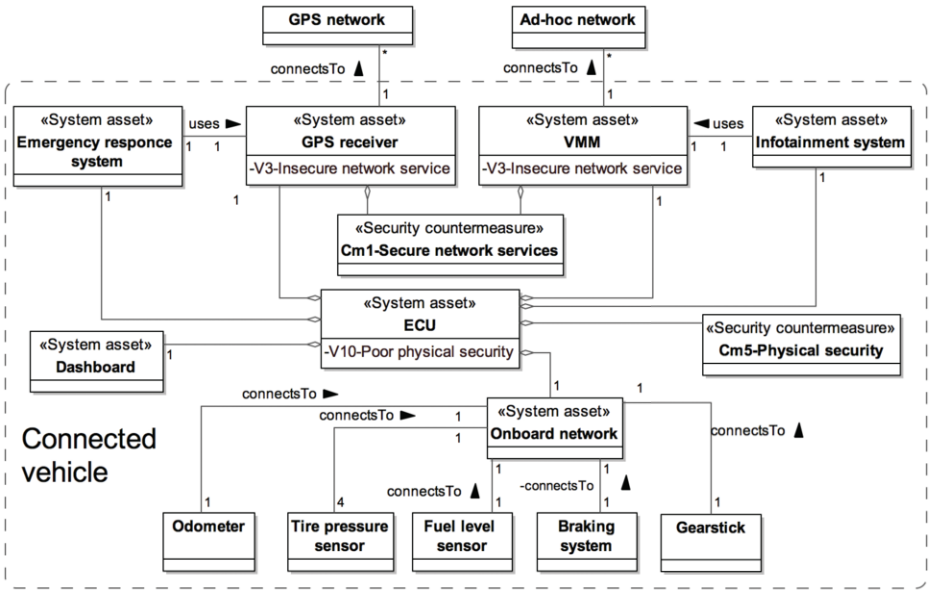

Figure 7. Revised connected vehicle model

5.3. Security Countermeasures

In [23] security countermeasures for mitigating security risks are grouped to different classes. As illustrated in Figure 5, to mitigate Risk 1 one could apply security countermeasures from Cm#5, and to mitigate Risk 2 – security countermeasures from Cm#1. Explicit definition security countermeasures are given in Table 3.

Revised connected vehicle model is given in Figure 7. This model illustrates system assets, their vulnerabilities (following the analysis provided in [28]) and security countermeasures. All these security risk components are introduced following the reference model for the IoT systems (see Figure 3).

6. Concluding Remarks

Following [23], in this paper we have recaptured alignment of the IoT system components to the ISSRM asset [8,20]. We apply this reference model to explain analyses of

the security risks for the connected vehicle [27]. Our analysis is limited to the security risks reported in [28], thus the research of other security risks (e.g., ones illustrated in [10]) could be a natural extension of this study.

The application of the reference model showed that it contains a few limitations. Firstly, it basically covers the system assets and their vulnerabilities, but leaves the analysis of business assets (i.e., data exchanged in the IoT systems, business operations) and their security criteria aside. Regarding the security risk analysis, the reference model concentrates on the vulnerabilities. The further work is needed to highlight the profile of the threat agents, her attack method, as well as the impacts the IoT system and business assets. On the system countermeasure side, we make an assumption that to treat the IoT security risk one takes risk reduction decision; however it is also important to understand consequences of other treatment decision (e.g., risk avoidance, retention or transfer). Finally, in our proposal we do not differentiate between the security requirements and controls. This concern requires further analysis. In the given connected vehicle example, we have used generic ISSRM method guidance to compensate limitations of the security reference model for the IoT systems.

In the future research, also we plan to strengthen the proposed reference model with the definition of the explicit guidelines for the IoT asset, risk and risk countermeasure identification, as well as the method of the security trade-off analysis.

Acknowledgement. This research has been supported by the Estonian Research Council (grant IUT20-55). The authors would like to thank Raman Shapaval for his valuable contribution to this research.

References

[1] M. Abomhara and Koien. Security and Privacy in the Internet of Things: Current Status and Open Issues. In *International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 2014.

[2] F. A. Alabaa, M. Othma, I. Abaker, I. A. T. Hashem, and F. Alotaibib. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88(15):10–28, 2017.

[3] M. Ammar, G. Russello, and Crispo B. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.

[4] M. Banerjee, J. Lee, and K.-K. R. Choo. A blockchain future to Internet of Things security: A position paper. *Digital Communications and Networks*, 2018.

[5] S. S. Basu, S. Tripathy, and A. R. Chowdhury. Design Challenges and Security Issues in the Internet of Things. In *Proceedings of the IEEE Region 10 Symposium (TENSYMP)*, pages 90–93, 2015.

[6] M. Bauer, N. Bui, J. De Loof, C. Magerkurth, A. Nettstrater, J. Stefa, and J. W. Walewski. *Enabling Things to Talk*. Springer, Berlin, Heidelberg, 2013.

[7] R. Benabdes, M. Hamdi, and T. H. Kim. A Survey on Security Models, Techniques, and Tools for the Internet of Things. In *Proceedings of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA)*, 2014.

[8] E. Dubois, P. Heymans, N. Mayer, and R. Matulevičius. *A Systematic Approach to Define the Domain of Information System Security Risk Management*, pages 289–306. Springer, 2010.

[9] G. A. Fink, D. V. Zarhitsky, T. E. Carroll, and E. D. Farquhar. Security and Privacy Grand Challenges for the Internet of Things. In *Proceedings of the International Conference on Collaboration Technologies and Systems (CTS)*, pages 27–34, 2015.

[10] A. Greenberg. Hackers Remotely Kill a Jeep on the Highway - with me in it. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, 2015.

[11] GSMA Connected Living. Understanding the Internet of Things (IoT), 2014.

[12] H. Hellaoui, M. Koudil, and A. Bouabdallah. Energy-efficient mechanisms in security of the internet of things: A survey. *Computer Networks*, 127:173–189, 2017.

[13] M. M. Hossain, M. Fotouhi, and R. Hasan. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In *Proceedings of the 11th IEEE World Congress on Services*, pages 21–28, 2015.

[14] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu. Security of the Internet of Things: Perspectives and Challenges. *International Journal of Wireless Networks*, 20(8):1–30, 2014.

[15] S. Khandelwal. Two Romanians Charged with Hacking Police CCTV Cameras Before Trump Inauguration. https://thehackernews.com/2017/12/police-camera-hacking.html, 2017.

[16] H. Li and Zhou X. Study on Security Architecture for Internet of Things. In *ICAIC 2011, Part I*, volume CCIS 224, pages 404–411, 2011.

[17] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341, 2015.

[18] G. S. Matharu, P. Upadhyay, and L. Chaudhary. The Internet of Things: Challenges and Security Issues. In *Proceedings of the International Conference on Emerging Technologies (ICET)*, pages 54–59, 2014.

[19] L. Mathews. Hackers Use DDoS Attack To Cut Heat To Apartments. https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/, 2016.

[20] R. Matulevičius. *Fundamentals of Secure System Modelling*. Springer International Publishing, 2017.

[21] OWASP. Welcome to OWASP. https://www.owasp.org/index.php/.

[22] C. Qiang, G. Quan, B. Yu, and L. Yang. Research on Security Issues of the Internet of Things. *International Journal of Future Communication and Networking*, 6(6):1–10, 2013.

[23] R. Shapaval and R. Matulevičius. Towards the Reference Model for Security Risk Management in Internet of Things. In *Proceedings of the International Baltic Conference on Databases and Information Systems (Baltic DB IS 2018)*, pages 58–72, 2018.

[24] H. Suo, J. Wan, C. Zou, and J. Liu. Security in the Internet of Things: A Review. In *Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE)*, pages 648–651, 2012.

[25] *Carolina*. Goodbye Spy Toy: Germany Bans My Friend Cayla Doll. https://www.hackread.com/goodbye-spying-toy-germany-bans-my-friend-cayla-doll/, 2017.

[26] The Guardian. DDoS attack that disrupted internet was largest of its kind in history, experts say. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, 2016.

[27] L. van Othmane, A. Al-Fuqaha, E. ben Hamida, and M. van den Brand. Towards Extended Safety in Connected Vehicles. In *Proceedings of the 16th International IEEE Annual Conference on Intelligent Transportation Systems (ITS 2013)*, pages 652–657, 2013.

[28] L. van Othmane, R. Ranchal, R. Fernando, B. Bhargave, and Bodden R. Incorporating Attacker Capabilities in Risk Estimation and Mitigation. *Computers and Security*, pages 41–61, 2015.

[29] S. Weagle. IoT-Driven Botnet Attacks US University. https://www.corero.com/blog/798-iot-driven-botnet-attacks-us-university.html.

[30] X. Yang, Z. Li, Z. Geng, and H. Zhang. A Multi-layer Security Model for Internet of Things. In *IOT Workshop 2012*, volume CCIS 312, pages 388–393, 2012.