Vilnius university
Institute of Data Science and Digital Technologies
L I T H U A N I A

INFORMATICS ENGINEERING (07 T)

INVESTIGATION AND IMPROVEMENT OF MULTIMODAL METHOD FOR INTERNET OF THINGS OBJECTS IDENTIFICATION AND AUTHENTICATION

Raimundas Savukynas

October 2019

Technical Report **DMSTI-DS-T007-19-06**

VU Institute of Data Science and Digital Technologies, Akademijos str. 4, Vilnius
LT-08663, Lithuania
www.mii.lt

Abstract

This technical report analyses a reference model for security risk management in the Internet of Things (IoT) systems and its application capabilities in the connected vehicle. The IoT is a network of connected devices and systems to exchange or accumulate data and information generated by users of and embedded sensors in the physical objects. Among the privacy, energy-awareness, environment, other concerns, identification, and authentication plays an important role, as the 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 damages of the valuable system and environmental assets. The reference model for security risk management in IoT help to discover and explain security vulnerabilities, defining security risks, and introducing security countermeasures.

Keywords: Connected Vehicle System, Electronic Control Unit, Internet of Things, Security Risk Management, Security Reference Model.

Contents

1. Introduction

The 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 [4]. 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 value system and environmental assets [7, 11, 14, 18, 19, 27, 33]. There exist several surveys related to the IoT security [1, 25], the security of the IoT frameworks [3, 31], or specific components of the IoT systems [12, 22, 34]. However, they lack a systematic approach to manage IoT security risks and reason for the introduced security countermeasures.

In [36], 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) [9] and 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. In [36], we adapt the vulnerability and countermeasure definitions of the open web application security project (OWASP) [30] to identify and manage the security risks in the IoT systems. In this paper, we illustrate how this reference model could be applied to explain business assets, system assets, their vulnerabilities, and to introduce security countermeasures. To support our discussion, we analyze connected vehicle system [28, 29].

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 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 characterizes security threats such as spoofing, tampering, repudiation, information leakage, the elevation of privilege, user privacy, replay attacks, and cloning of nodes. Some security framework is proposed to mitigate them. Elsewhere in [6] Benabdes et al. explores different methods to address security and privacy requirements (e.g., confidentiality, identification, 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 [10], 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 were 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, critical security problems, and attacks mitigation strategies. Elsewhere in [31] Qiang et al. consider the privacy protection, wireless communication, and information security. The authors propose a new IoT security method for processing of massive amount of data, and for ensuring high security and reliability.

In [17], Jing et al. classify security concerns to different levels of abstraction. Specifically, it focuses on radio frequency identification (RFID), wireless sensor network (WSN), robust security network (RSN) technology, and proposes solutions to secure them. Similarly, in [23], Mahmoud et al. analyzes the general and specific IoT security challenges at different layers of the IoT architecture. On the one hand, technological (e.g., wireless communication) challenges include the maintenance of the IoT scalability and low consumption of energy. On another hand, the IoT 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 [24], Matharu et al. describes the IoT architecture consisting of four layers. The authors highlight the importance of the IoT connectivity robustness, interoperability, and standardization (especially regarding identity management, safety, and security of objects, data confidentiality, and encryption).

In [37], Suo et al. discusses the security architecture, features, and requirements at different layers of the IoT system. Hence the authors focus on the IoT system key agreement, identity authentication, cloud computing, and authentication in the IoT layers namely perceptual layer, network layer, support layer and application layer.

In [40], Zhao et al. proposes a three-layer IoT system structure and offered some different solutions in each layer. The study investigates how security threats in IoT system structure (e.g., node capture, fake node, malicious data, replay attack, and routing threats in object layer) could be performed. The cryptographic algorithms and key management techniques were deployed in order to solve these attacks. The compatibility and cluster security problems in IoT resolved using the key agreement mechanism.

Although all studies suggest, different IoT security architectures consider security risks and suggest countermeasures to mitigate them, state of the art does not suggest a systematic approach for security risk management. In this paper, we illustrate how the 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 [3, 8]. Here, the business asset is understood in terms of the information, data, and processes, which bring added value to the organization. The business assets are supported by system assets (a.k.a., IS assets). The security criteria (i.e., confidentiality, availability, and integrity) are constraints of the business assets and define security needs. The 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. The event is defined in terms of the current threat and vulnerability. A vulnerability is a characteristic of the system assets and it constitutes a weakness of this asset. A threat targets the system‘s assets by exploiting its vulnerability. The threat is defined as a combination of the threat agent, an active entity who has the interest to harm the assets, and the attack method, the means used to carry on the threat. The security risk treatment concepts include risk treatment decision, security requirements, and controls. This security risk treatment is a decision to treat the identified risk. It is refined to the security requirements, which define a condition to be reached by mitigating the security risks. Finally, the controls implement the defined hight security requirements.

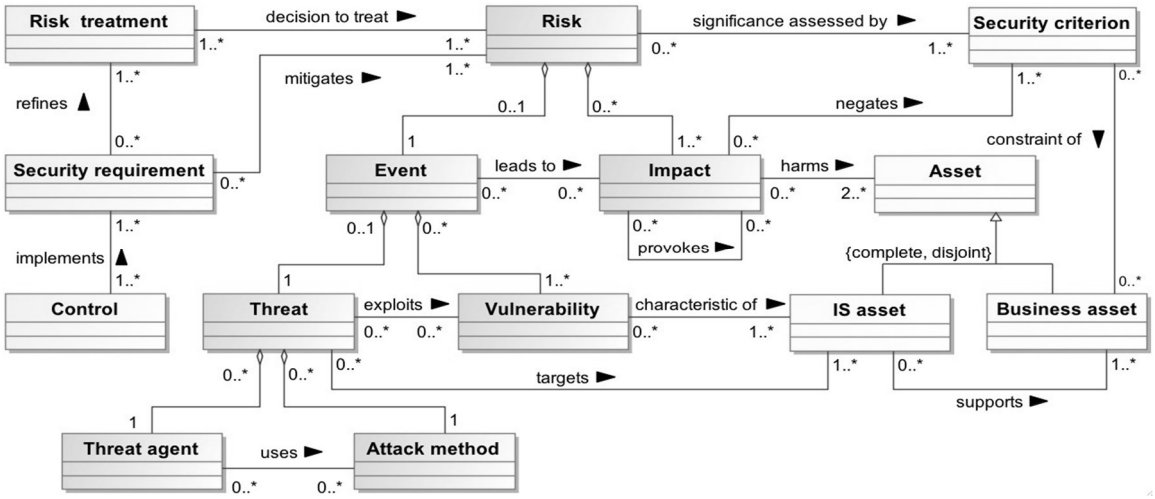

Figure 1. The ISSRM domain model, adapted from [3, 8]

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 [38]. The IoT system consists of service, which interacts with the computing device. Different computing devices are connected to each other. IoT devices manage some entities, which can be either on a device or network resources. Remote storage and network recourses were placed on the cloud environment.

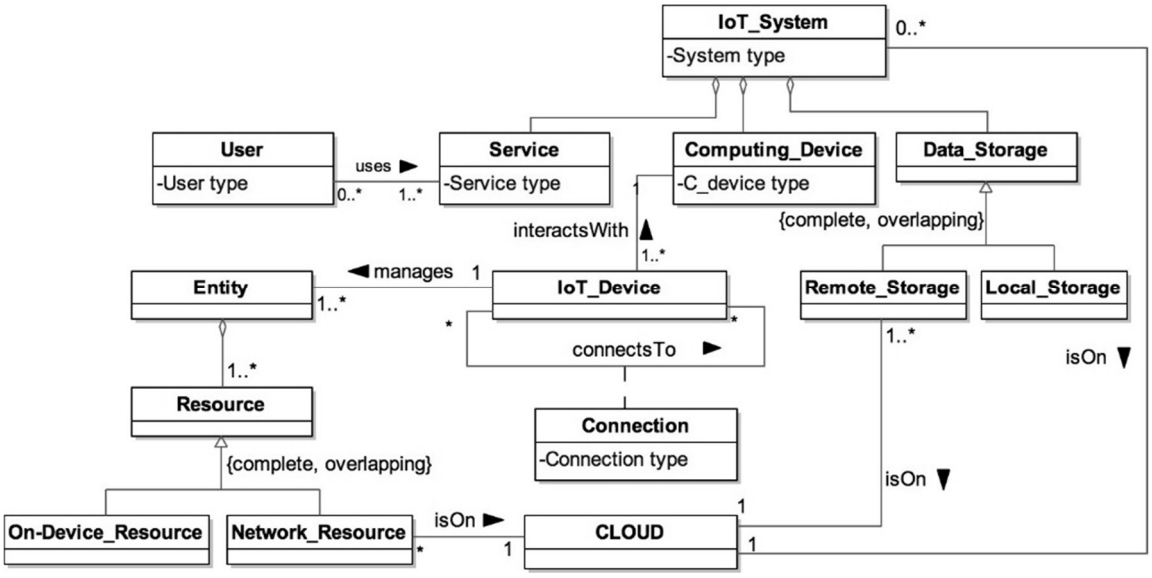

Figure 2. IoT architecture model

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 plays an important role in providing functionality and services to users. Like in [15, 26] the IoT system assets gain their importance in supporting the business assets. Thus, hey can be represented as important ground components of IT 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 [16, 21]. Besides official definitions, business assets can be commonly represented by the data, which was 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.

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 [30], in [36], 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 or authorization;*
- *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 or firmware;*
- *V#10: Poor physical security.*

To mitigate security risks, where these vulnerabilities can be identified, in [36], we discuss a set of countermeasures. Following the OWASP project [30], 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 or firmware*, and Cm#5: *Physical security*).
3. Identity management (i.e., Cm#6: *Secure authentication or authorisation,* Cm#7: *Secure Web interface*, and Cm#8: *Secure mobile interface*).
4. Trust and governance (Cm#9: *Trust and governance*).
5. Fault tolerance (Cm#10: *Fault tolerance*).

4.3. Reference Model of IoT Security Risk Management

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 [30], in [36], we have discussed from all sides the ten vulnerability classes potentially related to different system assets of the IoT system.

Characteristics of system assets. As discussed in [9], vulnerability is a characteristic of the system assets. The vulnerabilities listed in Section 4.2 characterize the 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 authorization (V#2), and highly insecure mobile interfaces (V#7).

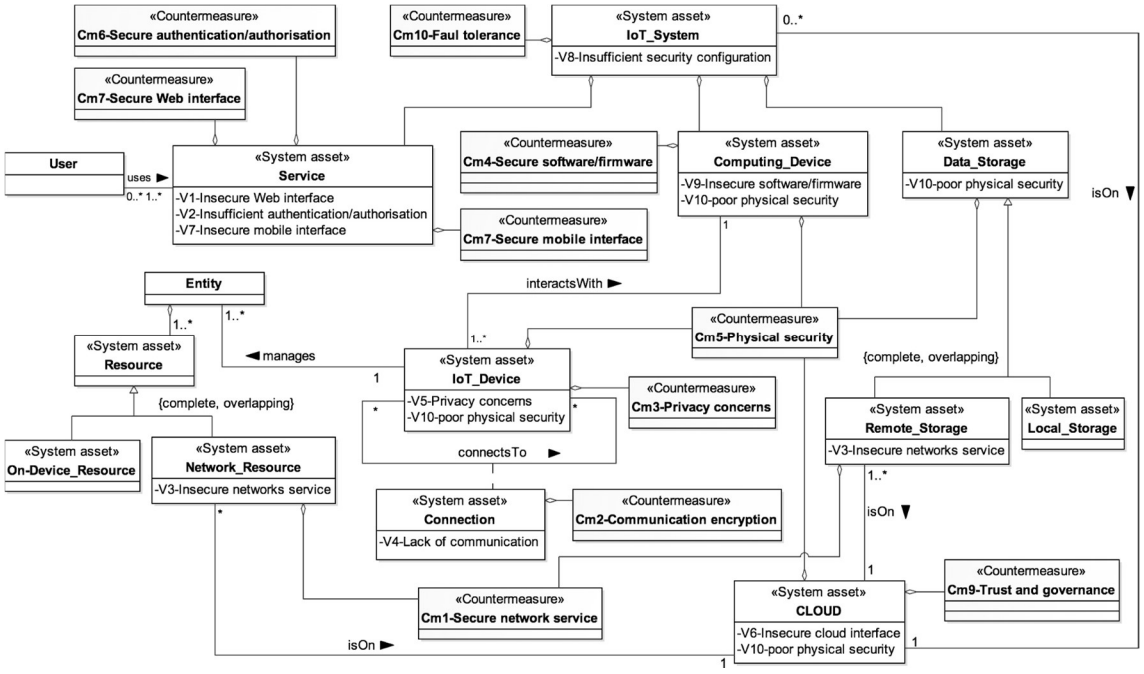

Figure 3. IoT reference model for security risk management

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. The *IoT system* could be explored through insufficient security configurability(V#8). As the *computing device* is a part of the IoT system, its vulnerabilities regarding the insecure software or firmware (V#9) should also be taken into account. Finally, the poor physical security (V#10) could open the gate for the attacker at the *data storage*, *computing device*, *IoT device,* and *cloud*.

Countermeasures become a part of the IoT system. Security countermeasures are introduced to mitigate security risks. In Figure 3, we link the security countermeasures (see classes with stereotypes cuntermeasures) to the system assets, which can be targeted by the security threat, thus exploiting their vulnerabilities. Thus, these countermeasures 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. The countermeasures 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). The countermeasures regarding the privacy concerns (Cm#3) help to mitigate security risks with vulnerabilities related to privacy concerns (V#5), secure software or firmware (Cm#4) – vulnerabilities related to insecure software or firmware (V#9). The countermeasures of physical security (Cm#5) addresses risks with vulnerabilities of poor physical security (V#10). The countermeasures to secure authentication or authorization (Cm#6) mitigate risks with vulnerabilities of insufficient authentication 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). The countermeasures regarding the trust and governance (Cm#9) deal with the security risks with vulnerabilities of insecure cloud interface (V#6). The countermeasures regarding fault tolerance (Cm#10) mitigate different security risks with vulnerabilities of the insufficient security configurability (V#8).

5. Connected Vehicle Example

In this section, we will analyze how the proposed security reference model for the IoT systems could support the analysis of the security risks. Mainly we will look to the connected vehicle system, described in [29, 31]. 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, roadside equipments, and traffic management centers). This way, it exchanges the available information about the car location, current environment, driving direction, condition of the driving, and status information necessary for the vehicle's device control.

5.1. Context and System Assets

Figure 4 illustrates some significant components of the connected vehicle. Table 1 presents a relationship between 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. The ECU includes other components, such as the emergency response system, which could be used to contact some parties for assistance an emergency. The 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 neighboring vehicles and roadside equipment. These are connected through Wi-Fi communication used in vehicular ad-hoc networks. Similarly, the emergency response systems are using the global positioning system (GPS) receiver to communicate with the emergency service center through a GPS network.

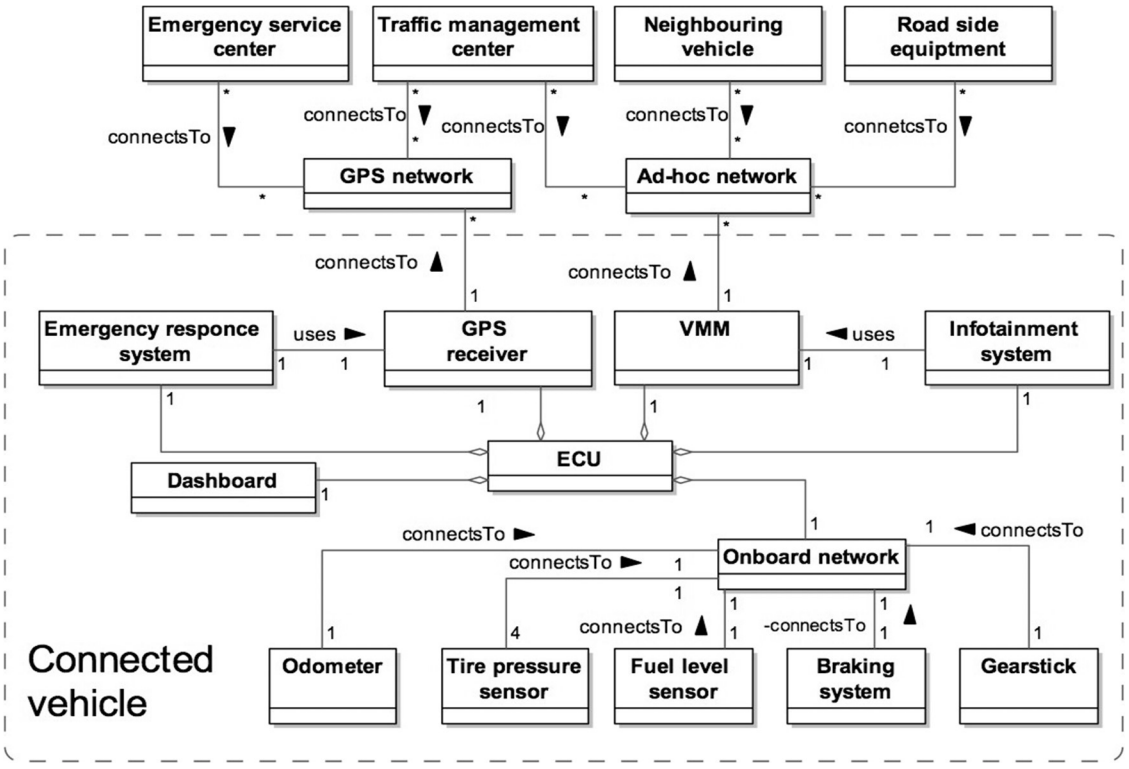

Figure 4. Connected vehicle model

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

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 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

5.2. Security Risks

A list of potential security risks for the connected vehicle is discussed in [29]. In this section, we will illustrate how the reference model could help explain these risks in the connected vehicle. Let's consider an extract of the diagram of the components given in Figure 5. In 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 3, see Risk1, the ECU has a vulnerability (corresponding to V#10) regarding 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 internal IoT device connections to the computing device.

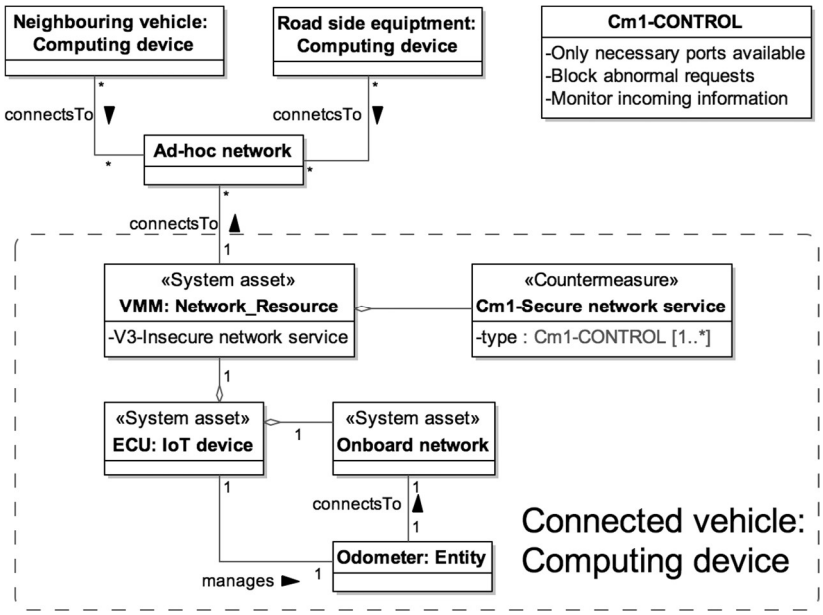

Figure 5. Insecure network communication in connected vehicle

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, roadside equipment, and traffic management center) as illustrated in Figure 4. 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 3) 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.

Table 2. Assets in connected vehicle

Concept	Risk 1	Risk 2
Risk	An attacker plugs the malicious ECU physically 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 roadside 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. • Orginal speed readings are altered, thus provoking wrong driving decisions.	• Negation of integrity of the speed readings; • Harm to the vehicle‘s VMM; • Orginal speed readings are altered, thus provoking wrong driving decisions.
Vulnerability	• The 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 is capable of using a vehicle (or roadside equipment) to establish a connection to the target vehicle and to inject speed readings to target a vehicle ECU.
Attack method	1. Plug (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 a connection between the attacker‘s vehicle (or roadside equipment) and target vehicle. 2. Send (malicious) speed readings to target vehicle‘s ECU. 3. Altered speed readings at the target vehicle's ECU. 4. Display (altered) speed readings in the dashboard.

The Risk 1 and Risk 2 illustrate that the IoT security reference model helps 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 systems and business assets. Their resulting impacts are [29]:

- negation of integrity of tire pressure data leading to the tire pressure warning in the dashboard and provoking the pullover of tires;
- negation of integrity of fuel 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 an emergency leading to the falsification of this information;
- 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 minimized.	• Only VMM ports important for the vehicle's functionality should be exposed. • VMM should monitor incoming information. • Abnormal requests or services should be blocked.

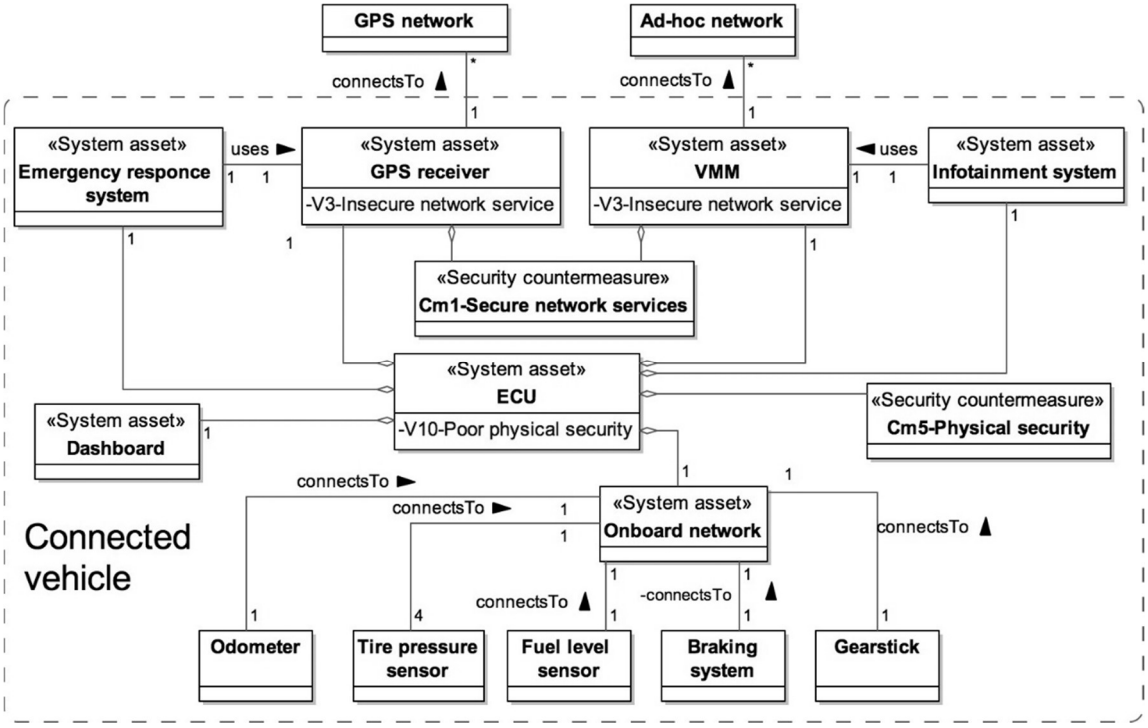

Figure 6. Revised connected vehicle model

5.3. Security Countermeasures

In [36], security countermeasures for mitigating security risks are grouped into 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. The specific definition of security countermeasures is given in Table 4.

The revised connected vehicle model is given in Figure 7. This model clearly illustrates the existing system assets, their vulnerabilities (following the analysis provided in [20]) and security countermeasures. All these security risk components are introduced following the reference defined model for the IoT systems (see Figure 3).

6. Conclusion

Following [36], in this paper, we have recaptured the alignment of the IoT system components to the ISSRM asset [9, 32]. We apply this reference model to explain analyses of the potential security risks for the connected vehicle [29]. Our analysis is limited to the security risks and reported in [39]. Thus the research of other security risks (e.g., ones illustrated in [32]) could be a natural extension of this study.

The application of the reference model showed that it contains a few limitations. It 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. Further work is needed to highlight the profile of the threat agents, her attack method, as well as the impact of the IoT system and business assets. On the system countermeasure side, we assume that to treat the IoT security risk one takes risk reduction decisions. It is also important to understand the consequences of other treatment decisions (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.

References

1. Abomhara, M., Koien, G. M. Security and Privacy in the Internet of Things: Current Status and Open Issues, *in Proc. of the International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Aalborg, Denmark, May 11–14, 2014, 1–8.
2. Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F. Internet of Things security: A survey, *Journal of Network and Computer Applications*, 88 (2017), 10–28.
3. Ammar, M., Russello, G., Crispo, B. Internet of Things: A survey on the security of IoT frameworks, *Journal of Information Security and Applications*, 38 (2018), 8–27.
4. Bastos, D., Shackleton, M., Moussa, F. E. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments, In: *Proc. of the International Conference on Living in the Internet of Things: Cybersecurity of the IoT*, London, UK, March 28–29, 2018, 1–7.
5. Basu, S. S., Tripathy, S., Chowdhury, A. R. Design Challenges and Security Issues in the Internet of Things, In *Proc. of the IEEE Region 10 Symposium (TENSYMP)*, Ahmedabad, India, May 13–15, 2015, 90–93.

6. Benabdessalem, R., Hamdi, M., Kim, T. H. A Survey on Security Models, Techniques, and Tools for the Internet of Things, In *Proc. of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA),* Haikou, China, December 20–23, 2014, 44–48.
7. Chu, G., Apthorpe, N., Feamster, N. Security and Privacy Analyses of Internet of Things Children's Toys*, Journal of IEEE Internet of Things* 6(1), 2018, 978–985.
8. Dazine, J., Maizate, A., Hassouni, L. Internet of Things Security, In *Proc. of the IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, Marrakech, Morocco, November 21–23, 2018, 137–141.
9. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R. A Systematic Approach to Define the Domain of Information System Security Risk Management, in *Proc. of the International Conference on Intentional Perspectives on Information Systems Engineering (IPISE)*, Heidelberg, Germany, 2010. Berlin: Springer-Verlag, 289–306.
10. Fink, G. A., Zarhitsky, D. V., Carroll, T. E., Farquhar, E. D. Security and Privacy Grand Challenges for the Internet of Things, In *Proc. of the International Conference on Collaboration Technologies and Systems*, Atlanta, GA, USA, June 1–5, 2015, 27–34.
11. Hamid, B., Weber, D. Engineering Secure Systems: Models, Patterns and Empirical Validation, *Journal of Computers & Security* 77 (2018), 315–348.
12. Hellaoui, H., Koudil, M., Bouabdallah, A. Energy-Efficient Mechanisms in Security of the Internet of Things: A Survey, *Journal of Computer Networks* 127 (2017), 173–189.
13. Hossain, M. M., Fotouhi, M., Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, In *Proc. of the 11th IEEE World Congress on Services*, New York, NY, USA, June 27–July 2, 2015, 21–28.
14. Yang*, Y., Wu, L.,* Yin*, G., Li, L., Zhao, H.* A Survey on Security and Privacy Issues in Internet of Things*, Journal of IEEE Internet of Things* 4(5), 2017, 1250–1258.
15. Yang, X., Li, Z., Geng, Z., Zhang, H. A Multi-layer Security Model for Internet of Things, *In Proc. of the International IoT Workshop on Communications in Computer and Information Science (CCIS)*, Changsha, China, August 17–18, 2012, 388–393.
16. Yousuf, O., Mir, R. N. A Survey on the Internet of Things Security*, Journal of Information and Computer Security* 27(2), 292–323.
17. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D. Security of the Internet of Things: Perspectives and Challenges*, Journal of Wireless Networks* 20 (2014), 374–377.
18. Kajwadkar, S., Jain, V. K. A Novel Algorithm for DoS and DDoS attack detection in Internet of Things, In *Proc. of the International Conference on Information and Communication Technology (CICT)*, Jabalpur, India, October 26–28, 2018, 1–4.
19. Kees, A., Oberlaender, A. M., Roeglinger, M., Rosemann, M. Understanding the Internet of Things: A Conceptualisation of Business-to-Thing Interactions, in *Proc. of the 23th European Conference on Information Systems (ECIS),* Münster, Germany, 2015, 1–15.
20. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. DDoS in the IoT: Mirai and Other Botnets*, Journal of Computer* 50(7), 2017, 80–84.
21. Kumar, N., Madhuri, J., ChanneGowda, M. Review on Security and Privacy Concerns in Internet of Things, In *Proc. of the IEEE International Conference on IoT and Application (ICIOT)*, Tamil Nadu, India, May 19–20, 2017, 1–5.
22. Li, L. Study on Security Architecture in the Internet of Things, In *Proc. of the International Conference on International Conference on Measurement, Information and Control*, Harbin, China, May 18–20, 2012, 44–48.
23. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures, In: *Proc. of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, December 14–16, 2015, 336–341.

24. Matharu, G. S., Upadhyay, P., Chaudhary, L. The Internet of Things: Challenges and Security Issues, In *Proc. of the International Conference on Emerging Technologies (ICET),* Islamabad, Pakistan, December 8–9, 2014, 54–59.
25. Matulevičius, R.; Savukynas, R. Application of the Reference Model for Security Risk Management in the Internet of Things Systems. In: Lupeikienė, A., Vasilecas, O., Dzemyda, G. (Ed). Databases and Information Systems X. IOS Press, 2019, 65-78.
26. Mena, M. D., Papapanagiotou, I., Yang, B. Internet of Things: Survey on Security, *Journal of Information Security: A Global Perspective* 27(3), 2018, 162–182.
27. Naik, S., Maral, V. Cyber Security - IoT, In *Proc. of the 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, May 19–20, 2017, 764–767.
28. Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols. In: *Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, May 29–31, 2017, 659–666.
29. Othmane, L., Fuqaha, A., Hamida, E., Brand, M. Towards Extended Safety in Connected Vehicles, In *Proc. of the 16th International IEEE Annual Conference on Intelligent Transportation Systems (ITS)*, Hague, Netherlands, October 6–9, 2013, 652–657.
30. Qian, K., Parizi, R. M., Lo, D. OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development, In *Proc. of the International 2018 IEEE Conference on Dependable and Secure Computing,* Kaohsiung, Taiwan, December 10–13, 2018, 1–2.
31. Qiang, C., Quan, G., Yu, B., Yang, L. Research on Security Issues of the Internet of Things, *Journal of Future Communication and Networking* 6 (2013), 1–10.
32. Ren, Z., Liu, X., Ye, R., Zhang, T. Security and Privacy on Internet of Things. In: *Proceedings of the 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Macau, China, July 21–23, 2017, 140–144.
33. Robles, D. E., Robles, R. J. State of Internet of Things (IoT) Security Attacks, Vulnerabilities and Solutions*, Journal of Computer* Reviews 3 (2019), 255–263.
34. Sha, K., Wei, W., Yang, A., Wang, Z., Shi, W. On Security Challenges and Open Issues in IoT*, Journal of Future Generation Computer Systems* 83 (2018), 326–337.
35. Shah, S. H., Yaqoob, I. A Survey: Internet of Things Technologies, Applications and Challenges, *In: Proc. of the 4 th IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, August 21–24, 2016, 381–385.*
36. Shapaval, R., Matulevičius, R. Towards the Reference Model for Security Risk Management in Internet of Things, In: *Proc. of the International Baltic Conference on Databases and Information Systems (Baltic DB&IS)*, Trakai, LT, July 1–4, 2018, 58–72.
37. Suo, H., Wan, J., Zou, C., Liu, J. Security in the Internet of Things: A Review, In: *Proc. of the International Conference on Computer Science and Electronics Engineering (ICCSEE)*, Hangzhou, China, March 23–25, 2012, 648–651.
38. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P. On the Security and Privacy of Internet of Things Architectures and Systems. In: *Proceedings of the International IoT Workshop on Secure Internet of Things (SIoT)*, Vienna, Austria, September 21–25, 2015, 49–57.
39. Virat, M. S., Bindu, S. M., Aishwarya, B., Dhanush, B. N., Kounte, M, R. Security and Privacy Challenges in Internet of Things, In *Proc. of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tamil Nadu, India, May 11–12, 2018, 454–460.
40. Zhao, K., Ge, L. A Survey on the Internet of Things Security. In: *Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS),* Leshan, China, December 14–15, 2013, 663–667.