Security Evaluation of Cyber-Physical Systems in Society-Critical Internet of Things

Viacheslav Izosimov, Martin Törngren
Machine Design, The Royal Institute of Technology, Stockholm, Sweden
viacheslav.v.izosimov@ieee.org, martint@kth.se

***Abstract*— In this paper, we present evaluation of security awareness of developers and users of cyber-physical systems. Our study includes interviews, workshops, surveys and one practical evaluation. We conducted 15 interviews and conducted survey with 55 respondents coming primarily from industry. Furthermore, we performed practical evaluation of current state of practice for a society-critical application, a commercial vehicle, and reconfirmed our findings discussing an attack vector for an off-line society-critical facility. More work is necessary to increase usage of security strategies, available methods, processes and standards. The security information, currently often insufficient, should be provided in the user manuals of products and services to protect system users. We confirmed it lately when we conducted an additional survey of users, with users feeling as left out in their quest for own security and privacy. Finally, hardware-related security questions begin to come up on the agenda, with a general increase of interest and awareness of hardware contribution to the overall cyber-physical security. At the end of this paper we discuss possible countermeasures for dealing with threats in infrastructures, highlighting the role of authorities in this quest.**

Keywords*— *security awareness; cyber-physical systems; attack vectors; commercial vehicles; hardware security

I. INTRODUCTION

Often researchers place weight on technical part of security solutions, with less attention to "human ingredients", system developers and users. Security knowledge and awareness of engineers that implement or install a system can be as critical as the choice of a crypto algorithm and a proper key management infrastructure. The system will not be more secure than the knowledge in security of its creators. Security-awareness of system users and operators are critical to ensure that the system is not compromised. Irrespective of the technical quality, any solution becomes effectively unsecure if the user leaks out passwords or blindly accepts installation of malicious software.

In this paper, our focus will be on smart cyber-physical systems in Internet of Things (IoT) that provide services critical for society. Examples of these smart systems include connected passenger cars, intelligent transportation systems, smart household appliances and alike. We consider them together with their drivers, operators, installation engineers and other persons directly and indirectly involved into their creation and during operation. These systems "live" in the Internet, providing and requesting services. The IoTs are nowadays part of infrastructures in healthcare, energy, transportation and many others. The level of interaction in these infrastructures has increased substantially with advances in development and enhancement of clouding. It raises concerns for robustness and trustworthiness. A fault or a malicious attack on one of system's, even the least critical, components, even a very innocent one at first glance, may affect other, critical, ones.

We will also look into examples of "not yet smart" systems and will advocate that they must be designed with the same level of security requirements as those connected to the Internet. Otherwise, these "not yet smart" systems pose potential serious threats to society when they unintentionally find their ways to the connected world, in situations often unexpected. In a modern society, it is nearly impossible to avoid these connections, due to actions of users, due to system complexity and sometimes due to security negligence of system developers.

Both developers and users play a key role in security of an embedded product as discussed in the Roundtable on Cyber-Physical Security [1]. With respect to applicable research methods, Tariq, Brynielsson and Artman studied the problem of users' security awareness in [2] where they conducted a number of semi-structured interviews in a large telecommunication organization. In our case, we use a similar approach to evaluate security-awareness of developers, engineers and academics, by conducting a number of interviews and surveys. For the users, we browse public reports, media and non-scientific journals as well as study product manuals and installation guidelines, to cover sources of information available to general public. We further study user awareness in a user-centric survey.

To evaluate state of practice in security of existing systems, we also study two practical attacks that are possible, in particular, due to security-unawareness of system developers and users. The attacks involve a connected smart product, a modern commercial vehicle, and an off-line critical facility.

The contributions of this paper are as follows:

- We advocate that security awareness of users and developers of modern embedded systems is essential.
- We evaluate two practical attacks, (i) an app attack on a Bluetooth interface of a modern car and (ii) an attack on an off-line critical facility.
- We highlight importance of hardware security as an essential component of the overall cyber-physical security.
- We suggest a number of countermeasures and discuss roles of authorities to facilitate security-awareness of both users and developers of modern embedded systems.

II. BACKGROUND AND RELATED LITERATURE

Evolving of Internet of Things (IoTs) pose substantial security challenges both technically and with respect to the users and developers. For example, Elkhodr, Shahrestani and Cheung [3] advocated for a number of possible attacks in IoTs, considering such specific IoT aspects as object naming, interoperability and identity management. In [4], Roman, Najera and Lopez highlighted challenges for dealing with security in IoTs, in particular, those related to scalability of solutions and dramatically increased amount of interactions. In some special cases of IoTs, for example, in smart power grids, security was considered on a physical connectivity level [5] and at a system level [6, 7]. In [6], Yilin Mo et al. presented an interesting attack model for smart power grid systems. In [7], a particular case for coordinated data-injection attack on power grid was discussed. Authors suggested a detection mechanism for this attack and pointed out the fact that the attack detection can be computationally sophisticated for a large grid. This is, in fact, one of the greatest challenges in any IoT infrastructure. It is one of the reasons why developers and users become critical. IoT

complexity makes it hard to have full technical understanding of smart product and services. In [8], authors presented guidelines on security processes in industrial automation, where people played a great role. This report is a good reference to practical implementation of IoTs for industrial automation domain.

In IoT systems, "software security" [9, 10, 11, 12, 13], "hardware security" [14, 15, 16, 17, 18] and "communication security" [19, 20, 21, 22, 23, 24] all play an important role. In particular, risks related to software [1, 9, 13] are seen as one of the largest contributing factors to lack of security in the overall system. Complexity, heterogeneity and complex software frameworks make software essentially critical for system security. At the same time, software tools drastically reduce threshold and minimize time needed for an attacker to prepare an efficient attack on a software level. In recent past, however, hardware security [14, 15, 16, 17, 18] started to gain a momentum, not least due to increased hardware complexity, largely distributed development and manufacturing chains. For example, a whole variety of hardware manipulation methods were established, from a simple hardware counterfeit [17] to highly sophisticated Hardware Trojans [18, 15, 16]. This triggered US Government to react and to establish new trade policies for hardware [18]. The third one, communication security was always a great concern for research community [19, 20, 21, 22]. Researchers documented and studied attacks on various communication protocols, network infrastructures and interfaces, on military communications [20], mobile networks [21], wireless [23], peer-to-peer interfaces such as Bluetooth [22, 24] and attacks on supporting functions such as GPS [25].

However, a majority of attacks in IoTs and CPS systems involve more than a single attack "type", are often very sophisticated and done in several steps. Complexity of attacks was outlined in, for example, [26], where a tight connection to physical environment in a stealthy deception attack on CPS systems was pointed out. In cyber-world, a related example is a distributed denial-of-service (DDoS) attack or *flooding attack* [27], where attackers follow an "attack tree" structure, trying different attack paths until either an attack is successful or is detected. In cyber-physical and IoT worlds, attacks are not only complex but they are also very heterogeneous, often with high involvement of human actors in a number of different roles.

III. Security Awareness of Users and Developers

In our interview study, we have evaluated responses from both industry and academia with two questionnaires for academic and non-academic (industry, authorities, etc.) audience. For non-academic respondents, questions were specific about particular products, services and the organization. For academic respondents, questions were made generic, that is, on products and services "in general". In total, we have interviewed 10 non-academic respondents (from transportation, telecom, healthcare and machine industry) and 5 academic (from universities and one research institute). The interviews were conducted in the period from October to December 2014. The interview questions were sent out in advance and most of the respondents had time to prepare their answers (and even ask for permissions from managers). The interviews were performed anonymously with the direct manual textual transcription of the answers such that the answers could not be linked to a particular respondent or their organization, via the voice, pictures, or by any other means. Most of the interviews were performed face-to-face; we had two respondents together in one of the interviews (counted as a single respondent in the study); and one interview was conducted over telephone. Each interview took about one hour, with some, however, lasting for as much as 3 hours and with some as short as 20 minutes. The summary of our interview study is presented in the "Interviews" column in Table I. In particular, only 33% consider valid security methods and, respectively, follow up on new threats. Less than 50% use security standards during technical work (it can be attributed to lack of security standards in many areas). Respondents did not consider hardware-based attacks seriously despite evidences and US export regulations. We, hence, added hardware security to the follow-up conference.

During our work in the interview study, it became clear that industry is attracted to questions of embedded security, while more work is necessary to distribute the security knowledge. Hence, it was proposed to organize a larger industrial event as part of the ICES (Innovative Centre for Embedded Systems, ices.kth.se). The conference, with the topic "IT-security for embedded systems", was finally organized on November 25 in 2015. Academic and industry speakers, knowledgeable in security, were invited. In particular, we invited speakers who could give introduction into hardware security topic. About 100 participants registered, with the majority coming from industry and some from academia and other organizations. We summarized talks of the event, discussed with the speakers, asked questions of interest and conducted our survey study. We also promoted topic of hardware security by asking specific questions and discussing with the conference participants.

During introduction to the conference, main outcomes from our interview study were presented and conference participants were requested to complete survey to re-validate our findings. We distributed our survey questionnaire in the conference room with a short description of the survey. The questionnaire contained a check-box indication for a type of respondent (Industry, Academy or Others), main Yes/No/NA questions, and the last multi-choice question about types of attackers. Survey questions were the same as the interview questions (but adapted for a survey-type questionnaire) except that (a) we added one more question on security information in the user manuals to evaluate opinion of the respondents with respect to the level of users' security-awareness and (b) we explicitly specified types of attackers instead of asking respondents to fill them in.

In total 55 completed questionnaires were returned, with 41 from industry, 8 from academia and 6 from "others" (that included other organizations which could neither fit to industry nor to academia). In columns "Survey" in Table I, we outline results obtained.

It should be noted first the difference between types of respondents in the interview study and the survey. In the interview study, respondents worked with security, did research, were responsible for security in their organizations or had a good understanding of the situation in the own organization. In the case of survey, the audience was broader, which also included respondents with security interest, not necessarily working with security directly. At the same time, the survey results are more statistically significant, compared to the interview study (e.g. 55 against 15). The greatest differences can be found in questions (2), (9) and (10). It seems that respondents of the survey were more uncertain about their security strategies and considered less security standards in business and technical levels. The reason for lower numbers of security standards can be that, during interviews, respondents could clarify what it was

meant with the security standards and could elaborate more, which could have effect. Our final survey result is, nevertheless, alarming, especially for usages of standards.

TABLES I. SUMMARY OF INTERVIEWS (15 RESPONDENTS) AND SURVEY (55 RESPONDENTS – ALL, ACADEMIC AND INDUSTRY), % YES ANSWERS

Topic	Inter-views	Survey (All)	Survey (Acad.)	Survey (Ind.)
1. Security is important	93	**95**	100	98
2. Use a valid and clear security strategy	60	**29**	13	27
3. Consider valid security methods	33	**44**	38	42
4. Classify and identify new threats	66	**45**	50	35
5. Follow up on new threats	33	**46**	63	35
6. Embedded and IT security are equally important	60	**96**	100	98
7. CIA attributes are all important	60	**63**	63	60
8. Safety can be affected by security threats	60	**98**	100	98
9. Use security standards: business level	60	**17**	25	13
10. Use security standards: technical level	47	**12**	13	13

Interestingly, 96% considered embedded and IT security equally important and 98% that safety can be affected by security threats. It was only 60% for both in the interview study. This case can be attributed to way the interviews were conducted, when, during discussion, respondents could bring up their multi-grained view of the problem. In the survey, the question could only result in Yes, No or N/A answers. Usage of valid security methods was slightly increased to 44% (from 33% in the interview study). Still the number is rather low. With respect to threats, for threat classification and following new threats, 45 and 46% were obtained, respectively, which can be considered somewhat similar to the interview study with 66 and 33% (considering similarity of the questions, 66 and 33% would effectively produce average of 50%). Thus, about 50% do not work with the security threats, which is alarming, considering that this is an independent outcome from the interviews and the survey.

We were interested to compare relationship between academic and industrial respondents. The comparison is shown in Table I, "Survey (Acad.)" against "Survey (Ind.)". The results match well except two questions related to classification and following on new threats. For academic respondents, 50 and 63% identify and follow new threats, while for industry, this is only 35%. This makes findings even more alarming, e.g. only 1/3 of industry respondents work with security threats.

We also wanted to study views on the attackers. Initially, the categories of attackers were obtained from the interview study. Several of respondents pointed out advanced persistent threat (APT) as one of the main threats to their products and organizations. In particular, not because of the APT as such but because other attackers (for example, criminal organizations) can utilize holes and backdoors identified or created by APT. APTs are not interested to close these holes since they use the holes for their own purposes. Criminals and criminal organizations were named as one of the most common attackers even for embedded systems according to our respondents. They have relatively large resources and courage to conduct variety of attacks with the purpose to make money out of it. The organizations themselves and employees can also act intentionally or unintentionally as attackers on products of their customers. An employee can attack his/her organization for one reason or another due to, for example, conflict at work or urgent need of money. Individuals with the ability to create dangerous software (e.g. hackers or crackers), both intentionally and unintentionally, can become part of an attack if they themselves use the software (or someone else uses their software to conduct an attack). For example, curious scanning of ports on a PLC (Programmable Logic Controller) of a power station can lead to overload of that PLC and cause a failure of that station with substantial economical consequences.

To our surprise, terrorists were not named as one of the major attack sources. The general claim here was that the physical terrorist attack is still scarier to general public than an online attack from an unknown source. Another reason is also that terrorists are the only attackers who want to happily risk or even miss their lives during an attack, while the online terrorist attack does not offer this possibility, at least, not directly. Further, we extended the list with competitors and users, who might potentially either initiate the attacks or become a part of the attack scenario.

TABLE II. CONSIDERED ATTACKERS BY SURVEY RESPONDENTS (ACADEMIC, INDUSTRY AND USERS), %

Attackers	Acad.	Ind.	Users
1. Advanced Persistent Threat (APT)	13	**7**	**14**
2. Terrorists	25	**20**	**7**
3. Hackers	88	**63**	**68**
4. Users	38	**44**	**14 (21)**
5. Employees (in case of users "Colleagues")	25	**17**	**7**
6. Competitors	50	**46**	**-**
7. Others	38	**17**	**11**
Criminals were pointed out as the most common type of attackers in the interview study (while were purposely omitted in the survey). They were, for example, more "popular" than the "Others" category in the survey. 57% of users also consider that criminals are a common type of attackers. Survey and interview studies are complementary.			

We systematized list of attackers and formed survey questions for evaluation. The results from the survey study are presented in Table II, columns "Acad." and "Ind.". As can be seen, "hackers" are leading with 63% for industry and 88% academia. The second place is competitors, 46 and 50%, respectively. The third place is users, with 44 and 38%. This finding is rather controversial. *Organizations consider their main users as a threat to their businesses and products!* Academic respondents also consider more of other types of attacks (38%) than industry (17%). Advanced Persistent

Threat (APT) is considered as rather lower priority attacker category for both academic and industry respondents, while is ranked high for other organizations (second highest after hackers). Note also that we purposely omitted *criminals*, which were pointed out as the main category of attackers in the interview study, to study the level of influence on the audience in the survey. Interestingly, criminals were not pointed out by any of the respondents (there was a possibility to write additional information) and the "others" is still 22% (considering all 55 respondents). 22% is less than the level of "popularity" of criminals in the interview study. This shows that surveys should be used carefully and results from the survey are necessary to complement with the detailed interviews, highlighting fine-grained aspects in the answers.

Finally, we were interested to know opinion about inclusion of security-related information into user manuals, since according to our opinion, users must be aware of security implications due to smart products that they use. 89% of respondents in the survey study considered that manuals must include security-related information. According to our check on the present manuals, however, manufacturers and service providers, for some reason, do not provide sufficient security related information to the users. This is clearly an indication that possible security risks can arise due to users' unawareness of the fact that the products that they use can be maliciously manipulated or due to resulting lack of knowledge on possible countermeasures. To follow up this question, we have conducted additional survey study targeting users of smart systems.

Our user-related survey included 28 respondents from the younger generation that use smart products every day. The following results were obtained (in % Yes answers):

Do you consider security important for your personal devices and all systems that you use at home and while in public?	96%
Are you aware of security recommendations for these devices?	32%
Do you consider these security recommendations sufficient?	29%
Do you follow these security recommendations?	14%
Do you agree that product user manuals (guides) should provide security information to you?	96%
In your devices, do you consider attacks against privacy more critical than against integrity? (**integrity**: absence of improper system alterations – potentially hazardous)	46%

We could conclude that users are aware about security. However, very small fraction of users is aware of security recommendations for their smart products (32%) and, as the result, only 29% consider these recommendations sufficient and only 14% follow the recommendations. 96% of respondents consider essential providing of security information into the user manuals. Finally, a common misconception is that users are the most concern about their privacy. As our survey illustrates, this is not true. Only 46% consider privacy attacks more critical than integrity attacks. We also added a question about attackers into our survey. Part of the results is depicted in Table II, column "Users". Hackers are on top of the list. Then, in fact, criminals have received 57% (criminals are omitted in the Table). This matches well the interview study outcome. Users consider themselves as attacker as well but only 14% (compare to 44% as perceived by the industry). 21% of respondents consider also that other users are attackers. Advanced Persistent Threat (APT) has obtained 14%. Colleagues and terrorists obtained the same value of 7% each. In addition, we also checked against relatives. 11% of users consider relatives as potential attackers.

IV. Attack Scenarios and Practical Evaluation

The traditional concept with drawing "borders" or "circles" does not work any longer in the IoT world due to enormous complexity, super-connectivity and unlimited computational capabilities to anyone. Thresholds to execute the above attacks are constantly reduced, both in terms of time and knowledge.

Table III illustrates the automotive app attack and the off-line critical facility attack (we have chosen a second variant of this attack focusing on the supplier's network). As it can be seen, the attack on a critical off-line facility takes 7 steps to perform compared to the automotive app attack that takes 10 steps. Moreover, off-line facility's assets can be more interesting for the attacker. The app attack on a modern car is complex and can be difficult to perform, which, however, according to our case study on this attack, is fully feasible. By far, not all the attackers will be interested to accomplish all 10 steps. Some attackers will stop at the info-cluster level (at 8 steps). For some attackers, installation of a malicious app on the driver's mobile phone can be already sufficient (with only 4 steps necessary). We consider that attacks with fewer steps are, in general, more common since they take less effort and less time.

Table III. Attacks Illustration

Smart Car Attack	**Offline Facility Attack**
1. Create app 2. Place app to an app store 3. Social engineering 4. App installation 5. Scanning Bluetooth 6. Update app 7. Enable "right" profile 8. Hijacking info-cluster 9. Scanning gateways 10. Opening CAN bus	1. Identify suppliers 2. Get into suppliers net 3. Development chain modification 4. Wait until update 5. Update equipment 6. Activate code inside 7. Unleash attack

In the automotive scenario, the attacker will use users' lack of unawareness of security in mobile phones and smart cars. Insufficient security awareness of developers (both of the info-cluster and the internal CAN network) will contribute to susceptibility to the attacks. In the off-line facility scenario, suppliers are unaware of connection between security of the facility and security of their network. Maintenance personnel of the facility are unaware of security implication of outsourcing of the maintenance work to the external suppliers. In turn, operators of the facility are not aware that the equipment of the facility has been compromised. They consider the facility as "fully secure" due to disconnection from the Internet and will not be ready, hence, to react in the event of unleashed attack.

Let us consider practical implementation of the smart car attack [28]. The attack was implemented on a Heavy-Duty Vehicle. We have chosen to use Bluetooth on a mobile phone to connect to the vehicle to connect to the internal CAN bus. The app on a mobile phone (downloaded from the Internet) controls the attack. In this evaluation, we have studied both Bluetooth interface and the "critical" CAN susceptibility to the attack. Flooding of the CAN bus was chosen as a final target. The two main ECUs, gateways, were connected to the test bench. Additionally, a laptop with a Bluetooth interface running was employed for testing the specific interface of the infotainment

ECU using the various “open source” Bluetooth test tools available. After testing in the test bench, the same attack was performed on the actual truck to study effects with the regular network load and reaction of the truck driver. The effect is outlined in Table IV. Bus share of some of the ECUs (including safety critical) drops even to 0. In spite of attack execution, the driver could drive the truck and park it safely. The attack generated a great number of safety warnings on the console and it behaved badly, for example, showing no fuel and the speed indicator was "dancing". If these (critical) warning would appear in a real situation, the driver would normally stop the truck immediately. This attack could be also facilited with hardware attack by enabling support on the vehicle side to establish a direct link to external attacker. Once the Bluetooth connection is detected, the hardware can look for a "mother ship" and upload malicious software to the vehicle.

We have not conducted practical implementation of security attack against off-line facility due to safety reasons. However, we studied a possibility of this attack in collaboration with a security expert knowledgeable in the domain. We have chosen a critical facility and followed the hint of a “supplier” attack. For that particular facility, we have, for example, found that the equipment is transported away from the facility for security upgrades. The supplier facility was one level of security lower. Still, we considered it sufficiently protected. However, what we found that the upgrade process (for at least some software modules) was implemented though a sub-supplier located in an East European country, with very limited security protection at the sub-supplier facility. The security update was run over a secure tunnel but through open Internet and, once the sending side would be compromised, could be hijacked and malisious software could be ported into the equipment. Neither of the parties involved into the update process would perceive any difference in the update and the equipment would be then re-installed into the facility, thus, opening it up for a full-scale attack with potentially devastating consequences. In the case the hardware of the equpment is compromised, even with very little embedded functionality, it would easen the attack a lot. Once the hardware detects the Internet connection, it can activate malware to navigate the external attack on the suppliers’ facility from the “mother ship”, with the follow up download of the whole malicious software package. If the hardware malware is large, it can directly attack the facility in the pre-defined conditions.

TABLE IV. TRAFFIC ON THE INTERNAL BUS BEFORE AND DURING FLOODING [28]

Node	Regular bus share %	Attack bus share %	Change	Change % vs. regular
Inf. GW	0,11	82,22	82,11	74645
2nd GW	2	2,01	0,01	0
ECU 1	7,35	0	-7,35	-100
ECU 2	5,71	2,23	-3,48	-61
ECU 3	3,56	0	-3,56	-100
ECU 4	1,28	0	-1,28	-100
ECU 5	8,02	0	-8,02	-100
ECU 6	7,25	6,61	-0,64	-9
ECU 7	0,64	0,69	0,05	8
ECU 8	0,12	0	-0,12	-100
ECU 9	0,58	0,41	-0,17	-29
ECU 10	2,3	0,23	-2,07	-90

V. DISCUSSION

How can we stop attacks at people’s homes and critical IoT (and offline) facilities? Indeed, proposing technically sound security solutions is one possible way forward. However, these security solutions should acknowledge responsibilities of developers and service provides as well as the level of security education of users and operators. Otherwise, even a super-smart security solution can fail due to that classical case of “a password exchanged to a muffin” or unsecure implementations. A number of steps are necessary. At first, a proper attack vector for a product should be determined. Security risks and countermeasures should be suggested and integrated into development. It is beneficial if the independent reviews can be conducted on the level of implementation of countermeasures. Companies and organizations should strive for security culture with security education of personnel, security monitoring and alert response teams. Standards on both technical and business levels should be facilitated and demanded. Manuals and guides for customers should include sufficient information on the product security and actions that must be undertaken in case of security breaching. Products that are imported to the country should be subjected to security evaluation on compliance to basic security principles both technically and in form of proper manuals and installation guides. In particular, it is essential to screen against hardware malware. Users and operators should be regularly updated on the subject of embedded security, by facilitating reporting on embedded and IoT security “issues” and publishing information on security violations. In general, education on embedded security should be taken to each high school classroom, where pupils can lean about embedded security and their own responsibilities as members of the society. Emerging IoT society will not leave any member unattended and everyone can become a victim. The whole society must be prepared to act in the IoT world, with security thinking in mind.

These changes will not happen by themselves and it is a responsibility of authorities to facilitate them. Authorities can impose rules and create facilitating regulations. However, they cannot make any single product secure and make each user or operator aware of security issues in that product. Therefore, acting on the educational level and launching security investigations to demonstrate susceptibility of infrastructural components and certain products can be a possible solution. Another possible solution is to establish a *voluntary security marking* for smart products and services, including control of the supply and manufacturing chains against hardware counterfeit and hardware malware. With issues happening in the security domain and constant reporting on security implications, users’ security awareness should increase and embedded security will become a competitive feature of a product or an infrastructure. In this case, manufacturers and operators will be interested themselves to ensure that they receive this voluntary “security marking” to increase sales, which, in turn, will initiate a positive feedback-loop leading to the overall security increase. However, it has been warned that security marking alone may not work [1] and may create a “false sense of security”. With new threats constantly emerging, the evaluation must include a “dynamic” security aspect with organizations constantly reacting and taking actions to secure products and services against these new threats. Penetrations testing of critical infrastructures and evaluation of processes in development organization can be beneficial to ensure that defects are detected

before they are utilized in malicious purposes or cause safety-critical faulty behavior. Testing should also include screening for hardware-based malware.

VI. CONCLUSIONS

In this paper, we first presented our combined interview and survey study on embedded security with respondents from industry and academia. We also studied security awareness of the users. We presented and studied examples of two possible attack scenarios, against smart car and off-line facility, which we evaluated. We discussed possible countermeasures, based on the fact that the system cannot be better with respect to security than the level of security understanding of its developers and users. There is clearly a gap in security understanding of developers as our study showed, with less than half of the respondents using suitable methods and following up on security threats. Security standards are also lacking, and those that are available are not used. Nearly all respondents (including users), however, consider security important which can drive development of embedded security and help with introduction of appropriate methods and standards. Both users and developers consider important adding security information into the user manuals. However, there is presently a gap in security "education" of the users of smart products and services, with security information often lacking in the manuals, which are supposed to be the main source of users' product and service information.

To conclude, gaps are present in security-awareness of developers and users of smart products and services, as our study confirmed, which contribute to increased security risks in embedded IoT products and services in present and near future. However, opportunities to change the situation are also present, with interest and willingness from developers' side and demand on users' side, and should be utilized for creating a more secure IoT world in future.

ACKNOWLEDGMENT

We would like to thank Swedish Civil Contingencies Agency (MSB) to provide financial support to this research work.

DISCLAIMER

The opinion and views contained in this paper are those of the authors and do not represent the official opinion of Swedish Civil Contingencies Agency (MSB) or Sweden.

REFERENCES

[1] S. Peisert, J. Margulies, D.M. Nicol, H. Khurana,C. Sawall, Designed-in Security for Cyber-Physical Systems, *IEEE Security & Privacy*, 12(5), 9-12, 2014.

[2] M.A. Tariq, J. Brynielsson, H. Artman, The security awareness paradox: A case study, In *Proc. IEEE/ACM Intl. Conf. on Advances in Social Networks Analysis and Mining (ASONAM)*, 704-711, 2014.

[3] M. Elkhodr, S. Shahrestani, Hon Cheung, The Internet of Things: Vision & challenges, In *Proc. IEEE TENCON Spring Conf.*, 218-222, 2013.

[4] R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, 44(9), 51-58, *Computer*, 2011.

[5] Eun-Kyu Lee, M. Gerla, S.Y. Oh, Physical layer security in wireless smart grid, *IEEE Communications Magazine*, 50(8), 46-52, 2012.

[6] Yilin Mo, T.H.-H. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, B. Sinopoli, Cyber–Physical Security of a Smart Grid Infrastructure, *Proc. of the IEEE*, 100(1), 195-209, 2012.

[7] Shuguang Cui, Zhu Han, S. Kar, T.T. Kim, H.V. Poor, A. Tajer, Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions, *IEEE Signal Processing Magazine*, 29(5), 106-115, 2012.

[8] Guide to Increased Security in Industrial Information and Control Systems, *Swedish Civil Contingencies Agency (MSB)*, 2014.

[9] Ann E.K. Sobel, Gary McGraw, Interview: Software Security in the Real World, *Computer*, 43(9), 47-53, 2010.

[10] Ping Wang, S. Sparks, C.C. Zou, An Advanced Hybrid Peer-to-Peer Botnet, *IEEE Trans. on Dependable and Secure Computing*, 7(2), 113-127, 2010.

[11] A. Baliga, V. Ganapathy, L. Iftode, Detecting Kernel-Level Rootkits Using Data Structure Invariants, *IEEE Trans. on Dependable and Secure Computing*, 8(5), 670-684, 2011.

[12] H.M.J. Almohri, Danfeng Yao, D. Kafura, Process Authentication for High System Assurance, *IEEE Trans. on Dependable and Secure Computing*, 11(2), 168-180, 2014.

[13] Yong Li, Pan Hui, Depeng Jin, Li Su, Lieguang Zeng, Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices, *IEEE Trans. on Mobile Computing*, 13(2), 377-391, 2014.

[14] N. Potlapally, Hardware security in practice: Challenges and opportunities, In *Proc. IEEE Intl. Symp. on Hardware-Oriented Security and Trust (HOST)*, 93-98, 2011.

[15] M. Tehranipoor, F. Koushanfar, A Survey of Hardware Trojan Taxonomy and Detection, *IEEE Design & Test of Computers*, 27(1), 10-25, 2010.

[16] N.G. Tsoutsos, M. Maniatakos, Fabrication Attacks: Zero-Overhead Malicious Modifications Enabling Modern Microprocessor Privilege Escalation, *IEEE Trans. on Emerging Topics in Computing*, 2(1), 81-93, 2014.

[17] Vincent van der Leest, Pim Tuyls, Anti-counterfeiting with hardware intrinsic security, In *Proc. Design, Automation & Test in Europe Conf. & Exhibition (DATE)*, 1137-1142, 2013.

[18] S. Mitra, H.-S. P. Wong, S. Wong, Stopping Hardware Trojans in Their Tracks, *IEEE Spectrum*, 2015.

[19] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, C. Assi, Communication security for smart grid distribution networks, *IEEE Communications Magazine*, 51(1), 42-49, 2013.

[20] R. Stillman, C.R. DeFiore, Computer Security and Networking Protocols: Technical Issues in Military Data Communications Networks, *IEEE Trans. on Communications*, 28(9), Part 1, 1472-1477, 1980.

[21] Muxiang Zhang, Yuguang Fang, Security analysis and enhancements of 3GPP authentication and key agreement protocol, *IEEE Trans. on Wireless Communications*, 4(2), 734-742, 2005.

[22] L. Carettoni, C. Merloni, S. Zanero, Studying Bluetooth Malware Propagation: The BlueBag Project, *IEEE Security & Privacy*, 5(2), 17-25, 2007.

[23] Pitipatana Sakarindr, N. Ansari, Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks, *IEEE Wireless Communications*, 14(5), 8-20, 2007.

[24] J.P. Dunning, Taming the Blue Beast: A Survey of Bluetooth Based Threats, *IEEE Security & Privacy*, 8(2), 20-27, 2010

[25] J.A. Larcom, Hong Liu, Modeling and characterization of GPS spoofing, In *Proc. IEEE Intl. Conf. on Technologies for Homeland Security (HST)*, 729-734, 2013.

[26] Cheolhyeon Kwon, Weiyi Liu, Inseok Hwang, Security analysis for Cyber-Physical Systems against stealthy deception attacks, In *Proc. American Control Conference (ACC)*, 3344-3349, 2013.

[27] Jung-Ho Eom, Young-Ju Han, Seon-Ho Park, Tai-Myoung Chung, Active Cyber Attack Model for Network System's Vulnerability Assessment, In *Proc. Intl. Conf. on Information Science and Security (ICISS)*, 153-158, 2008.

[28] V. Izosimov, A. Asvestopoulos, O. Blomkvist, M. Törngren, Security-Aware Development of Cyber-Physical Systems Illustrated with Automotive Case Study, In *Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 818-821, 2016.