Secure Communication in Cyber-Physical Systems

Igor Kotenko[1,2]*, Dmitry Levshun[1,2], Yannick Chevalier[2,3], and Andrey Chechulin[1,2]
[1]SPIIRAS, 39, 14-th Liniya, Saint-Petersburg, 199178, Russia
{ivkote, levshun, chechulin}@comsec.spb.ru
[2]ITMO University, 49, Kronverksky Prospect, St. Petersburg, 197101, Russia
{ivkote, levshun, chechulin}@corp.ifmo.ru
yannick.chevalier@gmail.com
[3]IRIT, 118 Route de Narbonne, F-31062 TOULOUSE CEDEX 9, France
yannick.chevalier@irit.fr

Abstract

The paper considers a new design methodology for organization of reliable and secure data transfer environment in cyber-physical systems, which contain microcontroller-based devices. The key idea of the design methodology is in providing of most rational solution to improve the data transfer environment according to functional and non-functional requirements and limitations to security and reliability. This solution will became trusted only after verification process checking its correctness and compatibility. If a cyber-physical system is dynamic and contains various mobile devices, the design process of such system will determine additional requirements and limitations to its data transfer environment. The application of the design methodology is presented for I2C network of Arduino-based devices that are used for interaction with external event sources in the Integrated Cyber-Physical Security System.

Keywords: Cyber-Physical Systems Security, Data Transfer Environment, Design Methodology, Microcontroller-based Devices

1 Introduction

Each cyber-physical system represents complex structure which contains a lot of various elements [6]. Cyber-physical systems can be distributed, decentralized and / or self-organized, and also can contain a variety of connected and disconnected mobile devices. As a consequence, there are many different techniques for development of such systems. Some of them are focused on software, some on hardware, and some on highly specialized applications (cars, railway transport, robotics, etc.). The main challenge of such design methods is that usually the security of a resulted system is not one of their goals [9]. When one tries to design a trusted, secure and reliable data transfer environment in cyber-physical systems, the task becomes even more complicated. One of the available solutions is the Trusted Platform Module (TPM), but sometimes it cannot be used. For example, a cyber-physical system may contain devices, and their hardware part cannot be changed, or the requirements to develop the system contain demands that will allow to use only cheap and energy efficient devices with low computing power.

This paper presents a solution based on a tradeoff between resources and protection a new design methodology which is aimed to provide a reliable and secure data transfer environment in cyber-physical systems that contain devices based on microcontrollers. The presented solution is a continuation of previous investigations devoted to the development of a methodology for data transfer environment design [6],[9],[10]. The key idea of this methodology is to suggest the most rational solution for improving

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 10 (September 15, 2018)
*Corresponding author: SPIIRAS, 39, 14-th Liniya, Saint-Petersburg, 199178, Russia, Tel: +7(812)328-26-42, Url: `http://comsec.spb.ru/`

the data transfer environment in accordance with functional and non-functional requirements for security and reliability. This solution will be considered as a trusted only after the verification process, which will verify its correctness and feasibility. The example of the proposed design methodology is based on the Arduino platform network which uses the I2C protocol for communication. This example represents the part of an integrated cyber-physical security system operating with external sources of events. The remaining sections of the paper contain the analysis of advantages and disadvantages of the proposed methodology, as well as the scope of its application. In addition, possible directions for further research are presented.

2 Related Work

The most common way to verify the data transfer environment for compliance with specified requirements for reliability and security is to verify the protocols and the algorithms for data transfer. Various tools have been developed to verify data transfer environments. The most widely used tools are ProVerif [3], Tamarin Prover [4] and AKiSs [8]. These automatic verifiers are aimed at working with the cryptographic primitives of various protocols and data transfer environments, but they also have limitations when working with strong properties of authentication algorithms and resource-intensive solutions. Verification approaches can be divided into two groups: (1) verification of the model and (2) verification of the prototype of the analyzed object. In turn, models can be divided into analytical and simulation ones. Verification of the analytical models is aimed at checking the composition of elements and their compliance with requirements. Verification of the simulation model is aimed at testing the interaction of the composition of elements, which allows one to verify the model for correctness and prevent the formation of incompatible solutions.

The results of the verification process of the data transfer environment can be used later to determine the level of trust to it. The level of trust is the degree of conformity of the security and reliability of the generated solution with the reference solution. Algorithms for calculating the level of trust are applicable in various areas, for example for security analysis of Internet of things [13], fraud transactions prevention [11] or securing the mobile communication network of VANET vehicles [12]. It is obvious that the security and reliability of the analyzed solution will be less if compare with the reference one. Comparative analysis can be made based on various aspects of reliability and security, allowing one to obtain a relative rating for each of them. Based on the relative ratings, an integral assessment is calculated, which determines the level of trust of the data transfer environment. At the same time, the trust levels are usually associated with a model of the attacker against which it is necessary to protect the developed communication environment.

Thus, different solutions can be used to verify the data transfer environments and calculate the level of trust to them. That is why one of the most important tasks in improving our design methodology was the integration of effective algorithms of verification and determining the level of trust. At the same time, these algorithms should be able to process the models of the data transfer environment used by our design methodology.

3 General Approach

The workflow of our improved methodology for development of the secure data transfer environment can be divided into two main stages: (1 the formation of the data transfer environment models and (2) the verification of models (see Figure 1). The stage of model formation consists of three main steps, the main task of these steps is to transform the representation of the analyzed data transfer environment into

the developed model, to compare its functionality with the specified requirements and limitations, and to change the model in accordance with the results of the comparison.

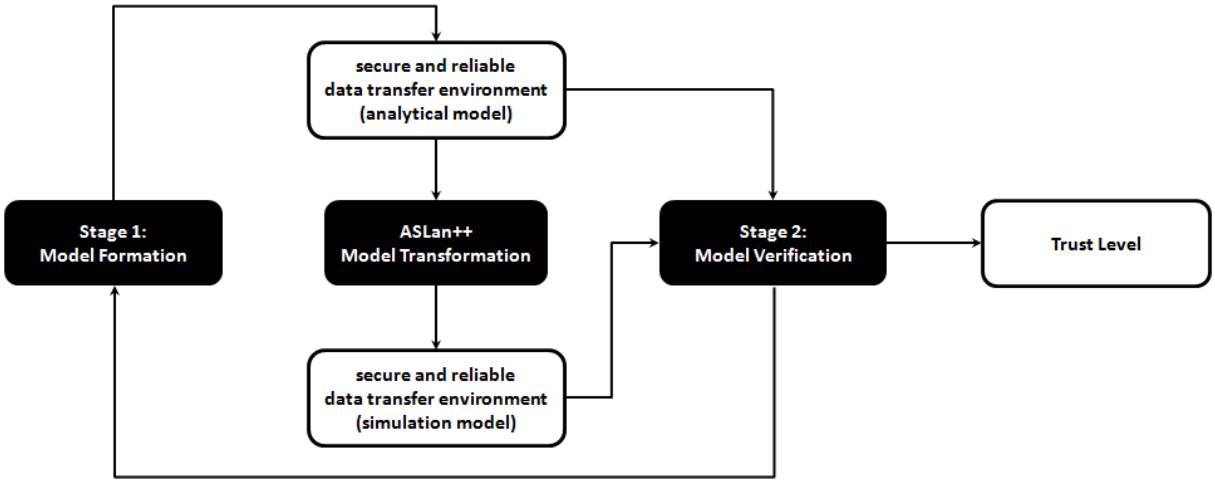


Figure 1: The improved methodology for designing a secure data transfer environment

Step 1. Converting the requirements and the specified limitations for the data transfer environment into a formalized form based on functional and non-functional requirements and limitations. As a rule, the functional requirements and limitations are converted into ones for the availability of the data transfer environment or specific capabilities, for example, dynamic addressing of system devices. Non-functional requirements and limitations include ones related, for example, to the computational complexity of the final solution.

Step 2. Analysis of the involved data transfer protocols and their algorithms, logical interfaces and rule sets. Carrying out such an analysis is necessary to identify the functional capabilities of the data transfer environment and the conditions necessary for its full operation. The obtained data allows one to form the model of the initial state of the data transfer environment. After it the comparison of the results of step 1 (*what do we want?*) and step 2 (*what do we have?*) will allow one to formulate the query to the expert knowledge base on step 3 (*what can we add?*).

Step 3. Usage of the expert knowledge related to the existing protocols and their algorithms, logical interfaces and rule sets for their subsequent application in the data transfer environment in order to ensure the proper level of reliability and security. Expert knowledge is specified in the relevant database and represents the description of the blocks the elements of the model, each of which can be used as a replacement or addition to other blocks. An example of such blocks is given in the next section of the paper. As a result of this step, the introduction of new blocks into the model of the initial state of the data transfer environment will form a new model of the data transfer environment. In this case, the new model of the data transfer environment will fully satisfy the requirements formulated in step 1, and therefore will be transferred to the verification phase. However, if the process of forming a new model of the data transfer environment is impossible, the methodology will return to the step 1 to update the requirements.

At the verification stage, verification of feasibility and correctness is carried out, as well as an assessment of the trustworthiness of the two models of the data transfer environment: analytical and simulation. The analytical model represents the composition of elements and nesting (hierarchy) of the individual elements of the data transfer environment, which allows one to check individual elements in the verification process and to remove incompatible solutions. However, the analytical model does not allow one to describe the dynamic links between the elements of the model and the sequence of their interaction in the

process of functioning. Therefore, in order to verify that the model preserves functionality and verify its compliance with non-functional requirements and limitations in the interaction of elements, the analytical model of the data transfer environment is to be transformed into a simulation model. In the framework of our design methodology, the analytical model of the data transfer environment is transformed into a simulation model based on the ASLan ++ language [14].

As the level of trust here we understand the degree of conformity of security and reliability of the generated models with the reference solution based on crypto processors (TPM). The degree of conformity with the reference solution is determined by the models of the attacker and threats [5]. Obviously, the security and reliability of the solution, based on the design methodology, will usually be less than the reference solution. At the same time, it will be sufficient to meet the requirements and more rational from the point of view of the imposed limitations. The comparison is made on various aspects of reliability and security, allowing one to obtain a relative rating for each of them. For the data transfer environment, the following aspects are taken into account: the resistance of the algorithms of authentication, encryption and pseudo-random number generation Later on, based on the relative assessments for each of them, the integral assessment is calculated, which determines the degree to which the model of the data transfer environment corresponds to the reference solution.

Note that if, as a result of the verification process, it is discovered that the model obtained at the stage of formation is not correct or not realizable, an assessment of the level of trust will not be carried out. Instead, the methodology will move to the stage of model formation to make the necessary changes to the model of the data transfer environment and the subsequent verification process.

4 Experiments

For the experimental verification of the developed design methodology, a network of devices of the Arduino platform, based on the I2C protocol, was realized. These devices are used for the interaction of a complex system of cyber-physical security with external sources of events [7].In accordance with the requirement for the data transfer environment, the functional and non-functional requirements and limitations were formulated on the first step of the first stage of the design methodology.

Step 1. Functional requirements: reliable transfer of messages up to 160 bytes in size; encryption of transmitted data; mutual authentication of connected devices. Non-functional requirements: minimization of computational complexity; allowable payload volume is not less than 70 % of the data packet; the amount of data stored is no more than 25 % of the available memory of the device.

Step 2. The connection at the hardware level is supported by a two-wire TWI interface [1], which provides reliable transfer of 1 byte of information on the physical layer of the communication protocol. In addition, for Arduino platform microcontrollers, there is a freely available Wire.h library [2], which provides reliable transfer of 32 bytes of information on the link layer of the communication protocol. By default, the addressing of slaves in the I2C network is static - the device address is set in its firmware (permissible address range belongs to the interval [8; 127]).

Step 3. The basic version of the I2C protocol needs to be expanded by dynamically addressing slave devices, enabling reliable transfer of unlimited-sized messages, device authentication, and encryption of transmitted data. In addition, the initialization algorithm needs improvement.

Data collected as a result of the second step of the design phase allowed one to form an analytical model of the initial state of the data transfer environment (see Figure 2).

The analyzed data transfer environment provides ability in the I2C network the following functionality: to configure the initial configuration of devices depending on the role of the device; to set and determine the role of devices; to generate packets for data transfer; to specify the response of slave devices to the requests of the master device, depending on the role of the device, to the I2C bus and to

read data from it; and also to work with several master devices within the same data bus. Functional requirements and non-functional limitations are follows: to build a environment for transmitting data of the physical layer for working with the SDA data line and the SCL clock line.

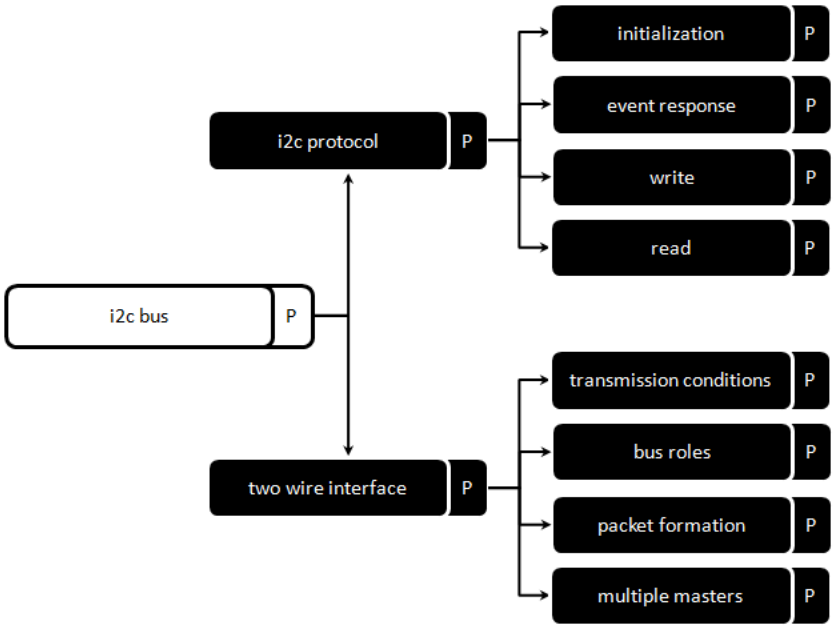


Figure 2: Analytical model of the initial state of the data transfer environment

In the future, based on the information about the requirements and limitations provided in step 1, the analytical model was added to form the analytical model of a reliable and secure data transfer environment in step 3 (see Figure 3). As a result of the analysis of functional requirements, the technique concluded that the basic version of the I2C protocol needs to be expanded by dynamically addressing slave devices, enabling reliable transfer of messages of unlimited size (basic I2C does not transmit messages larger than 32 bytes), device authentication and encryption of transmitted data, as well as improving the initialization algorithm. At the same time, the solutions used should correspond to non-functional limitations related to the computational complexity of the final solution, the minimum allowable payload volume, and the maximum allowable amount of stored data.

Expansion of the set of algorithms of the data transfer protocol will entail changes in the properties of the data transfer environment. The provided functionality of the data transfer environment in the I2C network is as follows: to configure the initial configuration of devices depending on the role of the device; to set and determine the role of devices; to form packets for data transfer; to specify the response of slave devices to the requests of the master device, depending on the role of the device; to write data to the I2C bus and read data from it; to dynamically address slave devices; to transmit messages of unlimited size; to organize mutual authentication of devices; to provide encryption of transmitted data; and also to work with several master devices within the same data bus. At the same time, functional and non-functional requirements and limitations remained the same: to build the environment of data transfer of the physical layer for working with the SDA data line and the SCL clock line.

The new analytical model and the simulation model obtained on its basis pass to the second stage of the design methodology the stage of verification of models of the data transfer environment. At the same time, verification of the analytical model allows to reveal the vulnerabilities of the developed system in relation to the certain models of violators and specific attacks. For example, verification allows one to detect and repair shortcomings that allow an attacker to attack based on sending incorrect network packets

and buffer overflow, cryptographic analysis of encrypted messages, impact on the authentication system, attacks on the update system. The verification of the simulation model allows one to identify vulnerabilities and errors, as well as determine the resistance to attacks on channels of device interaction, including attacks on resource depletion and load overload through channels. For example, verification can detect and eliminate shortcomings that allow an attacker to listen to communication channels, intercept, modify and forge transmitted data, as well as denial of service attacks.

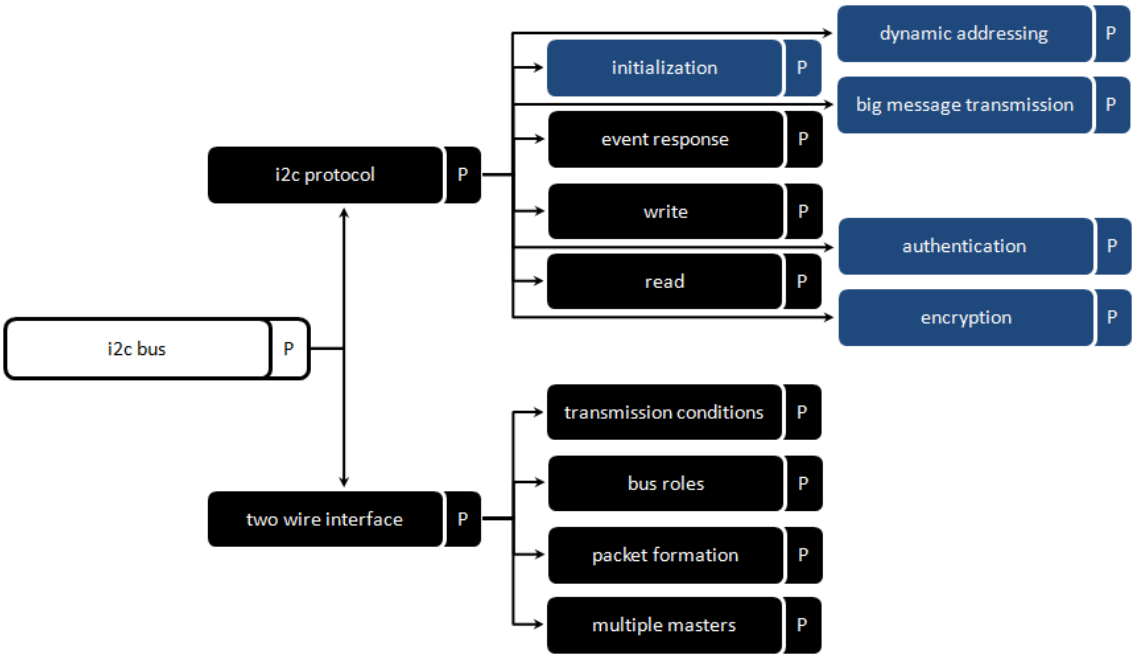


Figure 3: Analytical model of reliable and secure data transfer environment

Thus, through verification of the analytical and simulation models, the correctness and realizability of the solutions were provided, and their reliability and security with respect to the attacker of the appropriate level are guaranteed. This means that as a result of the methodology implementation, the data transfer environment was designed that is trusted with respect to this level of attacker.

5 Discussion

Expanding the developed methodology for designing the secure data transfer environment by applying approaches to verification and determining the level of trust has made it possible to improve the quality of the solution. Verification algorithms work with the analytical model to check the composition of elements and nesting (hierarchy) of individual elements of the data transfer environment, while verification algorithms when working with the simulation model check the sequence of execution of the algorithms, change their parameters and dependencies between them. This is necessary to detect and eliminate incompatible or unsafe solutions, as well as to take into account the influence of emergent properties on the correspondence of the data transfer environment to non-functional requirements and limitations, which allows us to further assess the overall level of trust in the designed data environment.

It is important to note that the main task of the design methodology has remained the same: to provide developers with an automated tool for designing a secure data transfer environment in cyber-physical systems, without involving security experts. Note that the methodology is not aimed to fully

replace expert opinions. Typically, an expert in the security of cyber-physical systems containing microcontrollers, knowing about existing best and highly specialized solutions, will be able to form alternatives at a qualitatively higher level. On the other hand, this approach can be useful to the expert as a tool for automating some of routine tasks, as well as the source of decisions that are different from his (her) subjective preferences.

6 Conclusion and Future Work

This paper demonstrates the improvement of the previously developed design methodology of a secure data transfer environment in systems containing devices based on microcontrollers [6],[9],[10]. This improvement is based on the addition of a new phase of the methodology the verification phase of the data transfer environment for compliance with the requirements for reliability and security. Also this new phase will allow one to calculate the level of trust of the analyzed data transfer environment.

Experimental verification of the proposed design methodology was carried out to develop a secure data transfer environment for the devices based on the Arduino platform that use the I2C protocol for communication. Also it is shown that this methodology also can be applied for development of the data transfer environment for mobile cyber-physical devices.

In the further investigation, it is planned to perform experiments to apply a new version of the design methodology to the various use cases and to improve the analytical and simulation models of data transfer environments. It is also planned to expand the already existing expert knowledge base and analyze and classify the impact of emergent properties on functional capabilities and non-functional limitations.

Acknowledgments

The work was partially funded by the Russian Foundation for Basic Research (projects 16-29-09482 and 18-07-01488), the budget project No AAAA-A16-116033110102-5 and the Grant of the President of the Russian Federation No. MK-314.2017.9.

References

[1] ARDUINO. Official documentation of the TWI hardware interface on the forum for Arduino platform developers. `https://playground.arduino.cc/Main/WireLibraryDetailedReference#hardware`, [Online: accessed on August 19, 2018].

[2] ARDUINO. Official documentation of the Wire.h library on the site for Arduino platform developers. `https://www.arduino.cc/en/reference/wire`, [Online: accessed on August 19, 2018].

[3] B. Blanchet. Automatic verification of security protocols in the symbolic model: The verifier ProVerif. In A. Aldini, J. Lopez, and F. Martinelli, editors, *Foundations of Security Analysis and Design VII*, pages 54–87. Springer, 2014.

[4] C. Cas. Symbolic security analysis using the tamarin prover. In *Proc. of the 2017 Formal Methods in Computer Aided Design (FMCAD'17), Vienna, Austria*, pages 5–5. IEEE, October 2017.

[5] V. Desnitsky, I. Kotenko, and A. Chechulin. An abstract model for embedded systems and intruders. In *Proc. of the 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing (PDP'11), Ayia Napa, Cyprus*, pages 25–26. SEA-Publications. SEA-SR-29, February 2011.

[6] V. Desnitsky, D. Levshun, A. Chechulin, and I. Kotenko. Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 7(2):60–80, June 2016.

[7] I. Kotenko, D. Levshun, and A. Chechulin. Event correlation in the integrated cyber-physical security system. In *Proc. of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM'16), St. Petersburg, Russia*, pages 484–486. IEEE, May 2016.

[8] S. Kremer. Official site of active knowledge in security protocols (AKiSs) project. `http://akiss.gforge.inria.fr/`, [Online: accessed on August 19, 2018].

[9] D. Levshun, A. Chechulin, and I. Kotenko. Design lifecycle for secure cyber-physical systems based on embedded devices. In *Proc. of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'17), Bucharest, Romania*, pages 277–282. IEEE, September 2017.

[10] D. Levshun, A. Chechulin, and I. Kotenko. A technique for design of secure data transfer environment: Application for I2C protocol. In *Proc. of the 1st IEEE International Conference on Industrial Cyber-Physical Systems (ICPS'18), St. Petersburg, Russia*, pages 789–794. IEEE, May 2018.

[11] T. Price and J. Lewis. Automatic execution of authentication actions at high trust levels. `https://www.tdcommons.org/dpubs_series/750`, [Online: accessed on August 19, 2018], October 2017.

[12] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle. Trust on the security of wireless vehicular ad-hoc networking. *Ad Hoc & Sensor Wireless Networks*, 24(3–4):283–305, February 2014.

[13] S. Sicari, A. Rizzardi, L. A. Grieco, and A. C. Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164, January 2015.

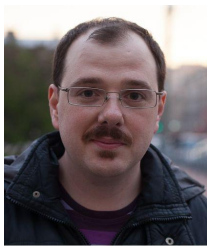
[14] D. von Oheimb and S. Mödersheim. ASLan++ — a formal security specification language for distributed systems. In *Proc. of the 9th International Symposium on Formal Methods for Components and Objects (FMCO'10), Graz, Austria*, volume 6957 of *Lecture Notes in Computer Science*, pages 1–22. Springer-Verlag, November-December 2010.

Author Biography

Dmitry Levshun graduated with honors as a specialist (equal to master degree) in Computer Security at ETU "LETI" in 2017. Currently a PhD student at ITMO University and a Junioiur research fellow at the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). His research interests include Cyber-Physical Systems Security, Design of Secure Cyber-Physical Systems, Modelling of Cyber-Physical Systems and Microcontroller-based Devices.

Yannick Chevalier is a former mathematics and computer science student of ENS Lyon. He has received a PhD from University Nancy 1 in 2003, and is since 2004 an associate professor at University Toulouse 3. He has co-authored 13 journals and 27 conference papers, and has participated in the European AVISS, AVISPA, and Avantssar Projects. His work was cited more than 2000 times according to Google Scholar.

Igor Kotenko graduated with honors from St.Petersburg Academy of Space Engineering and St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is Professor of computer science and Head of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. He is the author of more than 350 refereed publications, including 12 textbooks and monographs. Igor Kotenko has a high experience in the research on computer network security and participated in several projects on developing new security technologies. For example, he was a project leader in the research projects from the US Air Force research department, via its EOARD (European Office of Aerospace Research and Development) branch, EU FP7 and FP6 Projects, HP, Intel, F-Secure, etc. The research results of Igor Kotenko were tested and implemented in more than fifty Russian research and development projects.



Andrey Chechulin received his B.S. and M.S. in Computer science and computer facilities from Saint-Petersburg State Polytechnical University and PhD from St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in 2013. In 2015 he was awarded the medal of the Russian Academy of Science in area of computer science, computer engineering and automation. At the moment he holds a position of leading researcher at the Laboratory of Computer Security Problems of SPIIRAS. He is the author of more than 70 refereed publications and has a high experience in the research on computer network security and participated as an investigator in several projects on developing new security technologies. His primary research interests include computer network security, intrusion detection, analysis of the network traffic and vulnerabilities.