ROMANIA - MINISTRY OF EDUCATION
PETROLEUM-GAS UNIVERSITY OF PLOIEȘTI
DOCTORAL SCHOOL

DOCTORAL THESIS

- SUMMARY -

RESEARCH REGARDING SECURITY OF CONTROL SYSTEMS

Supervisor
Prof. Nicolae PARASCHIV, Ph.D., Eng.

Author
Emil PRICOP, Eng.

Ploiesti
2017

Table of Contents

Introduction and thesis structure

Most control systems now integrate increasingly high computing processing power and provide multiple communication capabilities across local networks and even on the Internet. Specific developments in control systems engineering were focused, among other things, on improving performance, including their reliability, and using optimal control algorithms. Recently, research and developments have also been geared towards ensuring the security of automated systems.

Control systems have become in the last years more and more frequently the targets of various cyber-attacks, including the ones with worms and viruses as vectors. The purpose of malicious actions is to disturb or interrupt the correct operation of the systems, especially of those that are key components of critical infrastructures. In this context, some of the total number of attacks can be identified as terrorist threats or even acts of an electronic war, with high impact and consequences often affecting more than one country. These are only the main reasons for what the increasing of systems security is a very challenging and current topic of research that benefit from the interest of both industry, defense organization, research institutes and academic community.

The main objective of the research is to identify and develop robust and high-performance methods and techniques for improving the control systems security.

The research done in the doctoral stage was oriented in three main directions, corresponding to the following focus points of the thesis:

- development of innovative methods for analysis, evaluation and estimation of the security status of a given system;
- development of a robust authentication method for the data source in an industrial network;
- development of a high precision access control system designed for hardware or software resources, especially those that are components of critical infrastructures.

The research was conducted by various methods as follows:

- bibliographic and Web studies;
- analysis of security reports generated by security companies and governmental organizations, such as NATO Cooperative Cyber Defence Centre of Excellence;
- experimental investigations in laboratory;

- investigation using real systems for collecting attacks related data (honeypots).

During the research stage of the doctoral degree, the need for best practices and information exchanges in the domain of systems security was identified. In this context, the thesis author initiated in 2013 the International Workshop on Systems Safety & Security (IWSSS), which is a real idea exchange forum in the field at its 5th edition in 2017 (details are available on www.iwsss.org).

The doctoral thesis is structured in seven chapters that are briefly described in the following paragraphs.

❖ The first chapter of the PhD thesis presents the main identified vulnerabilities, possible attack types and security issues associated with control systems. Within this chapter, the two fundamental aspects of ensuring systems security are emphasized, namely physical and logical access control to resources and protection from attacks, malware, viruses and worms.

❖ The second chapter of the doctoral thesis describes in detail the issues of implementing of robust and efficient mechanisms for physical and logical resources of the protected systems. An extensive bibliographic study was done and main features of biometric person identification systems based on fingerprint and/or iris analysis were presented.

❖ The third chapter focuses on the study of methods for systems protection from cyber-attacks. Two different but complementary approaches were identified, namely using firewalls for limiting the connections from unsecure networks and honeypots for analyzing the context and deceiving a potential attacker. The author demonstrates the interest of attackers for automation systems connected to the Internet and for industrial protocols, by using honeypot systems installed on real servers. By analyzing honeypot data, the author proves the increasing need for securing industrial control systems.

❖ The fourth chapter of the PhD thesis is dedicated to the development of three original methods proposed by the authors for:

- evaluation of the profile for a given attacker type;
- estimating the likelihood (probability of appearing) of a cyberattack initiated by an attacker with known profile, targeting a particular system;
- estimating the probability of a successful attack given the system characteristics and attacker profile.

The author introduced the attacker profile score and the degree of interest of a given system. Also, there is presented an automate method for vulnerabilities identification on a particular system by using a vulnerability scanner.

- The fifth chapter of the PhD thesis focuses on solving a major security issues faced by most industrial communication protocols – the lack of an authentication mechanism for data sources. A mechanism for authentication of sensors connected using Modbus/TCP protocol is presented and validated in a laboratory setup.

- The sixth chapter presents a complex access control systems for hazardous areas in industrial systems, based on biometric person identification using fingerprint analysis. The system is presented in a conceptual approach, as functioning specifications and algorithms. The key component of the proposed system is the *biometric RFID card*, an RFID tag with a special memory structure proposed by the thesis author.

- The seventh chapter of the thesis is focused on presenting the final conclusions and original scientific contributions of the author. This section includes the publication list in which the results of the author's research have been disseminated. The chapter concludes by presenting the future possible research directions in the field of security of systems.

- The doctoral thesis is concluded with a bibliography that contains 71 references and a webography which contains 60 referenced placed in citation order.

General conclusions

Control systems security has become a priority for both academia and industry since they are key components of the critical infrastructures. It is important to mention that more often the control systems components are interconnected in various industrial networks that are becoming targets of cyber terrorist and cyber war actors. The impact of control systems compromising could be devastating, for example a malfunctioning automation system that controls a power plant or a power distribution (power grid) system may paralyze the entire economy of a country.

Control systems security is a very complex domain that targets not only the classical security aspects, such as authentication, data confidentiality, integrity and non-repudiation, but also protection against malware (viruses and worms), unauthorized access and defense from hackers and attackers. A very important aspect is related to physical access control to the automation infrastructure.

The main vulnerabilities, possible attack methods and common security issues associated to industrial control systems are presented in the first chapter of the doctoral thesis. The main security vulnerability identified by bibliographic studies and by consulting the security reports generated by various companies is *the lack of any authentication mechanism for the source of data in industrial networks,* especially in the case of data coming from sensors or controllers.

The evidence of threats that were present in the personal computers domain, but now are shifting to target industrial control systems is emphasized in the thesis. The computer viruses and worms are now modified to target automation equipment such as PLCs (the well-known case of Stuxnet worm) and to spread by using industrial communication protocols.

The vulnerabilities identified by the author of this PhD thesis and presented in the first chapter can be exploited remotely, over the network and the Internet, or locally, having physical access to the resources of the target system. The research presented in the next two chapters of the thesis is focused on controlling the access to physical and logical system resources, securing data transfers and protecting against cyber-attacks.

A bibliographic study and a presentation of the main features of personal biometric identification systems were realized in order to establish the state of the art for developing innovative, robust and high performance access control systems. The uniqueness, the lower complexity of the used sensors, the performances of the existing algorithms, the lower cost of the necessary equipment, and the greater acceptance by the users allowed the development of a large number of applications where persons are identified by fingerprint analysis methods. The technology is mature and stable so, in the thesis author opinion, it could be used to successfully implement powerful authentication systems for access control in command and control facilities and protected areas of critical infrastructures components. Iris image analysis is another biometric technology with high precision and performances. Unfortunately, the technology cost is high and the big number of difficulties in iris scanning makes this biometric method to be use only in facilities that requires the highest degree of protection.

Protection from cyberattacks is the main topic of the third chapter of the PhD thesis. The research emphasize that a secure system has a maximized availability, which is reached by limiting any attempt of a DoS (Denial of Service) or DDoS (Distributed Denial of Service) attack. Firewalls and honeypots are the two solutions for achieving this objective that were identified by the thesis author.

The firewalls are recommended in order to separate the industrial network from the company standard computer network and to create DMZs (demilitarized zones) where servers that provide public services should be places. By using this approach, even if one of the exposed servers is compromised, the attacker cannot access entities from the local computer or industrial networks.

Honeypots have a dual role in ensuring security of industrial control systems. They can be viewed both as means of information collection regarding sources and deployment mechanisms of cyberattacks and as trap devices that mimic the operation of a real system, that induce attackers interest.

During the doctoral research stage, the honeypots were used for collecting data associated with cyber-attacks and attempts of attacks against control systems and industrial networking protocols. The results obtained show an increased interest of the attackers for this category of technical systems and make the need of securing these entities obvious.

In the author opinion, the honeypots are not only information collecting instruments, but also high efficiency methods for deceiving a potential attacker. A real cloud of "cyber-fog" can be created by deploying a large number of honeypots around the protected system. By using this approach the probability of identifying the real system is diminished, also increasing the time and effort required to successfully conduct the potential attack.

The fourth chapter of the PhD thesis is focused on the development of three original methods for evaluation of the profile for a given attacker type, estimating the likelihood of a cyberattack initiated by an attacker with known profile against a system and estimating the probability of a successful attack given the system characteristics and attacker profile. The proposed methods uses fuzzy logic and rules sets developed by the thesis author based on his own experience achieved during the doctoral research stage and from collaboration with security companies.

In order to estimate the likelihood of a cyber-attack against a control system, a rule-based fuzzy inference system was designed and implemented in MATLAB®. The system analyzes two inputs: the *vulnerabilities level* of the systems and the *degree of interest* that the system show to a protential attacker.

The *degree of interest* is a concept introduced by the thesis author to quantify in a lexical variable (with values “low”, “medium” and “high”) the number of cyber-attack attempts on a honeypot that mimics the protected (analyzed) system.

An inference system based on fuzzy logic was designed and implemented to estimate the success probability of an attack. The system analyzes three inputs: attacker profile score, the level of vulnerabilities and the level of existing countermeasures (system protection). The attacker profile score is also a concept introduced by the author to allow the quantification of an attacker's "abilities" by assessing the level of knowledge, available technical resources, and motivation. The vulnerability level of a system can be evaluated by specialized applications, vulnerability scanners, that were described extensively in the fourth chapter of the PhD thesis.

By using the fuzzy systems described above, the author concluded that the likelihood of cyberattacks is significantly affected by the level of system security vulnerabilities and less by its degree of interest. The success probability of a given attack is influenced by the vulnerabilities level and by the attacker abilities. The thesis author consider that implementation of adequate protection measures allows to reduce the attack success probability to an acceptable level.

The fifth chapter of the doctoral thesis focus on the design and implementation of a method for authenticating sensors connected by using Modbus/TCP industrial network protocol. The author of the thesis conducted a bibliographic study regarding Modbus and Modbus/TCP protocols specifications. The study results lead the author to the conclusion that sensor authentication is required in order to ensure a good system security. This conclusion is demonstrated experimentally, by using a laboratory setup to initiate and deploy a man-in-the-middle (MITM) attack against Modbus/TCP protocol.

In order to solve the security issue presented above, the author of the doctoral thesis proposed a sensor authentication method that is based on introducing a sensor signature (hash function) in the TCP Options fields of TCP/IP packets transferred by the sensor to the network. The proposed method has been implemented and validated as a laboratory demonstrator. The demonstrator confirmed the correct premise of the method and that its usage does not affect the performances of the network. It should be noted that the proposed method works with all the equipment already connected to the network, assuring backward compatibility.

The sixth chapter presents a complex access control systems for hazardous areas in industrial systems, based on biometric person identification using fingerprint analysis. The system is presented in a conceptual approach, as functioning specifications and algorithms. The key component of the proposed system is the *biometric RFID card*, an RFID tag with a special memory structure proposed by the thesis author.

Original scientific contributions

The following sections contains a summary of the original contributions and developments realized by the author and presented in extenso mainly in the last three chapters of the thesis.

1. There was realized a bibliographic study of high complexity, which allowed the author to develop a complete image regarding the state of the art in the systems security field.
2. The author installed, configured and tested honeypots (Conpot & T-Pot system) in real conditions, in order to prove the attacker interest on industrial control systems connected to the Internet and to collect data on the dynamics of unauthorized access attempts or attack attempts.
3. The control systems were treated as information systems in regard of data processing.
4. The author introduced two concepts: *attacker profile* and *attacker profile score.* The *attacker profile score* is used to quantify the attacker abilities by evaluating his knowledge, resources and motivation.
5. Rules set for defining the attacker profile score was proposed in the thesis.
6. The concept *degree of interest of a system* was introduced in order to quantify (by using a lexical value) the number of attack attempts on a given honeypot.
7. The risks associated to pen-testing on a given systems were identified and described.
8. A fuzzy logic system for automated evaluation of profile attacker score based on his attributes (knowledge, technical resources and motivation) was developed and tested in MATLAB®.
9. A fuzzy logic system was developed in MATLAB® to estimate probability of apparition of a given attack against an industrial control system. The proposed fuzzy

logic system evaluates the probability by considering the degree *of interest for potential attackers* and *the vulnerabilities level* of the evaluated system.

10. A fuzzy logic system for assessing the probability of attack success was developed and tested. The proposed system evaluates the attack success probability by analyzing three inputs: *attacker profile score, systems security vulnerabilities level* and *existing countermeasures level.*
11. The possibility of intercepting data transmitted via the Modbus/TCP protocol to run a Man-In-The-Middle or spoofing attack was demonstrated in the laboratory.
12. A robust mechanism for authenticating sensors connected by using Modbus/TCP protocol has been developed and tested.
13. An access control system for hazardous areas in industrial installations or operating consoles was proposed at the conceptual level. The system is functioning by using live biometrics (fingerprint analysis) and comparing the resulting biometric template to the one stored on a special RFID card, called *biometric RFID card.*
14. A special memory structure for the *biometric RFID card* was proposed in order to store three fingerprint templates along with information on the user access rights and personal data.

Results dissemination

The results obtained during the doctoral research stage were disseminated in recognized publications and conferences as follows: a book published by Springer Verlag as editor, co-author of three chapters included in this book, 16 articles of which 8 Thomson- Reuters Web of Science (ISI), 6 articles published in the IEEE Xplore database, and 2 articles in the ProQuest Central international database, 2 patents granted and 2 patent applications under evaluation at the State Office for Inventions and Trademarks – Romania. A complete list of these publications is presented in chronological order, organized by category.

A. Books and book chapters published by international publishers

1. **Pricop E.**, Stamatescu G. (editors), *Recent Advances in Systems Safety and Security*, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1;
2. Fattahi, J., Mejri M., **Pricop E.**, - *The Theory of Witness-Functions*, chapter in Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 1-19;
3. Rădulescu G., **Pricop E.**, Nicolae M., Roșca C. – *Using Modelling and Dynamic Simulation Techniques for Systems' Safety and Security*, chapter in Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 57-77;
4. **Pricop E.**, Mihalache S.F., Fattahi J. – *Innovative Fuzzy Approach on Analyzing Industrial Control Systems Security*, chapter in Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 223-239;

B. Papers indexed by Thomson-Reuters - Web of Science (ISI Papers & ISI Proceedings)

1. Paraschiv N., **Pricop E.** – *Adequacy testing of some algorithms for feedforward control of a propane propylene distillation process*, Revista de Chimie, vol. 67, no. 7, July 2016, pp. 1363-1369, ISSN: 0034-7752 (**ISI Paper, IF: 0,973**);
2. Fattahi J., Mejri M., **Pricop E.**– *Tracking Security Flaws in Cryptographic Protocols using Witness-Functions*, IEEE International Conference on Systems, Man & Cybernetics (SMC) 2015 Proceedings, pp. 1189-1196, doi: 10.1109/SMC.2015.213 (**ISI Proceeding**), Hong Kong, 2015;
3. **Pricop E.**, Zamfir F., Paraschiv N. – *Feedback control system based on a remote operated PID controller implemented using mbed NXP LPC1768 development board*, Journal of Physics: Conference Series, Vol. 659, Article number: 012028, doi: 10.1088/1742-6596/659/1/012028, IOP Publishing, 2015 (**ISI Proceeding**);
4. **Pricop E.**, Mihalache S.F. – *Fuzzy approach on modelling cyber-attacks patterns on data transfer in industrial control systems*, 3rd International Workshop on Systems Safety & Security – IWSSS 2015 - Proceedings of the 7th International Conference on

Electronics, Computers & Artificial Intelligence – ECAI 2015, vol. 7, SSS-23 - SSS-28, nr. 2/2015 – ISSN: 1843-2115; ISBN: 978-1-4673-6646-5 (**ISI Proceeding**)

5. **Pricop E.**, Mihalache S.F. – *Assessing the security risks of a wireless sensor network from a gas compressor station*, 2nd International Workshop on Systems Safety & Security – IWSSS 2014, București, România - Proceedings of the 6th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2014, vol. 5, pag.45-50, ISBN: 978-1-4799-5478-0 (**ISI Proceeding**)
6. Ionescu O., **Pricop E.** – *On the design of a system for airport protection against terrorist attacks using MANPADS*, International Conference on Systems, Man and Cybernetics - SMC 2013 Proceedings, pag. 4778-4782, ISBN 978-0-7695-5154-8, Manchester, UK, 2013 (**ISI Proceeding**)
7. **Pricop E.** – *On the design of an innovative solution for increasing hazardous materials transportation safety*, International Workshop on Systems Safety & Security for Automotive, Passengers & Goods Protection – IWSSS 2013 - Proceedings of the 17th International Conference System Theory, Control and Computing (ICSTCC 2013), 2013, Sinaia, Romania, pag. 624-629, ISBN: 978-1-4799-2228-4 (**ISI Proceeding**)
8. Ionescu O., **Pricop E.**, Paraschiv N. – *The management of health & safety issues related to the wearing of protective clothing by using RFID technology,* The 2nd International Conference on Economic, Education and Management – ICEEM 2012 Proceedings, Shanghai, China, Volume 1, pag. 495, ISBN 978-988-19750-3-4 (**ISI Proceeding**)

C. Papers published in IEEE Xplore

1. **Pricop E.**, Fattahi J., Paraschiv N., Zamfir F., Ghayoula E. - *Method for authentication of sensors connected on Modbus TCP*, Proceedings of the 2017 4th International on Control, Decision and Information Technologies (CoDIT'17), Barcelona, Spania, 2017 (Paper accepted for publishing in **IEEE Xplore)**
2. Zamfir F., Paraschiv N., **Pricop E.** - *Performance analysis in WiMAX networks using Random Linear Network Coding*, Proceedings of the 2017 4th International on Control, Decision and Information Technologies (CoDIT'17), Barcelona, Spania, 2017 (Paper accepted for publishin in **IEEE Xplore)**
3. **Pricop E.**, Mihalache S.F., Paraschiv N., Fattahi J., Zamfir F. – *Considerations regarding security issues impact on systems availability*, 4th International Workshop on Systems Safety & Security - Proceedings of the 7th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2016, Vol. 8, No. 4/2016, ISSN: 1843-2115, doi: 10.1109/ECAI.2016.7861110, 2016, Ploiești, România (**IEEE Xplore, Scopus**)
4. Fattahi J., Mejri M., **Pricop E.** - *Authentication by Witness Functions* 2016 IEEE Trustcom/BigDataSE/ISPA Conference Proceedings, pp. 1990-1997, doi: 10.1109/ TrustCom.2016.0304, Tianjin, China, 2016 (**IEEE Xplore, Scopus**)
5. Fattahi J., Mejri M., Ghayoula R., **Pricop E.** - *Formal reasoning on authentication in security protocols*, IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2016 Proceedings, pp. 282-289, doi: 10.1109/SMC.2016.7844255, Budapesta, Ungaria, 2016 (**IEEE Xplore**)
6. Ghayoula E., Fattahi J., Ghayoula R., **Pricop E.**, Stamatescu G., Chouinard J.-Y., Bouallegue A. – *Sidelobe Level Reduction in Linear Array Pattern Synthesis Using*

Taylor-MUSIC Algorithm for Reliable IEEE 802.11 MIMO Applications, IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2016 Proceedings, pp. 4700-4705, doi: 10.1109/SMC.2016.7844973, Budapesta, Ungaria, 2016 (**IEEE Xplore**)

D. Papers indexed in international scientific databases

1. **Pricop E.** – *On the design of a monitoring and alarming system for hazardous goods transportation by ships***,** Scientific Bulletin "Mircea Cel Bătrân" Naval Academy, vol. 18, no. 1, pp. 235-239, Constanța, România 2015 (**ProQuest Central**);
2. **Pricop E.** – *Security of industrial control systems – an emerging issue in Romania national defense*, Scientific Bulletin "Mircea Cel Bătrân" Naval Academy, vol. 18, no. 2, pp. 142-147, Constanța, România 2015 (**ProQuest Central**);

E. Granted patents and patents currently under evaluation procedure

1. *Biometric RFID card structure and method for personal data storage on the RFID Card* Patent RO 123364 B1 / 28.10.2011, issued by the State Office for Patents and Trademarks, Romania
   Authors: Melinte Toader, **Pricop Emil**, Lorentz Adrian, Andron Liviu
2. *Security system for protecting civil airports against terrorist attacks with soil-air missiles* Patent RO 129740 B1 / 30.06.2016, issued by the State Office for Patents and Trademarks, Romania
   Authors: Ionescu Octavian Narcis, **Pricop Emil**, Ionescu Gabriela Cristina
3. *Automatic system for monitoring the wearing of mandatory protection equipment in areas with high hazard potential* – under evaluation procedure
   Patent application no. 129906 A0, published in the Official Intellectual Property Bulletin no. 11/2014 of the State Office for Patents and Trademarks, Romania
   Authors: Ionescu Octavian Narcis, Crăciun Daniel, **Pricop Emil**
4. *Wireless sensors system for montoring the destruction attempts on strategic infrastructures for electrical energy distribution* – under evaluation procedure
   Patent application no. 129850 A0, published in the Official Intellectual Property Bulletin no. 10/2014 of the State Office for Patents and Trademarks, Romania
   Authors: Ionescu Octavian Narcis, Ionescu Gabriela Cristina, **Pricop Emil**

During the research stage of the doctoral degree, the need for best practices and information exchanges in the domain of systems security was identified. In this context, starting with 2013, the author of the PhD thesis organized "*International Workshop on Systems Safety & Security - IWSSS*", an annual scientific event that benefited from the presence of prestigious researchers from Romania as well as from abroad. The papers presented at each edition of 2013-2016 were published in the IEEE Xplore database and indexed in the prestigious Thomson Reuters - Web of Science (ISI) database.

Future research directions

The research conducted in this doctoral stage is just the beginning of an activity with a high complexity degree in a niche domain – the security of technical systems in general, with a special focus on those who coordinate the operation of critical infrastructures.

The current international context, characterized by the increase in attacks targeting critical infrastructures and technical systems, by the development of viruses targeting industrial equipment (PLCs, SCADA systems, etc.), indicates that the security of technical systems must become a priority of the researchers and decision-makers including the ones acting in the national defense field. It is very important to mention that control systems security was defined as a priority in the United States of America since 2013, when the Obama Administration has formulated cyber security regulations for critical infrastructures. The North Atlantic Treaty Organization also set up an excellence research center in Tallinn - CCD COE - the Cooperative Cyber Defense Center of Excellence in order to study and develop methods of protection against cyber-attacks.

The possible research and development directions, that can be considered in the future for increasing the security of industrial control systems, are briefly presented in the following paragraphs.

- Extending and implementing in a real environment of the proposed method for authentication of the sensors connected in Modbus/TCP networks. The laboratory demonstrator developed during the research stage used a static clear text for authentication, but in the future a TOTP (Time One Time Password) hash should be used for authenticating the sensors.
- Developing other methods and techniques for authenticating the source of data in industrial networks, for the most commonly used protocols such as Profibus, Fieldbus, Profinet etc., based on the proposal defined for Modbus/TCP.
- Development of high interaction and context-aware honeypots that are able to reconfigure themselves in real time in order to fully mimic the behavior of a real system and to completely deceive a potential attacker, to collect a large amount of data regarding all the attack mechanisms followed by the trapped attacker.
- Implementation at the demonstration and then industrial level of an access control system based on the concept (biometric RFID card) introduced in chapter 6 of the doctoral thesis.
- Improvement of automated methods (or vulnerability scanners) by developing facilities to assess the impact of vulnerabilities not included in existing databases.

- Development of robust methods for assessing the security impact on systems availability.
- A method to define the availability coefficient K_D to extend the actual approach that takes into consideration only reliability and mentenabiliy, to include and assess the systems security impact.
- Developent of the methods proposed in the PhD thesis for estimating the likelihood of a cyber-attack to take into consideration the context by analyzing various data sources available on the internet and by importing real-time data from honeypots.