An Architecture for the Analysis and Management of Security in Industrial Control Systems.

Laurens Lemaire, Jorn Lapon and Vincent Naessens

KU Leuven, Department of Industrial Engineering
Gebroeders Desmetstraat 1, 9000 Ghent, Belgium
firstname.lastname@cs.kuleuven.be

Abstract. The security of Industrial Control Systems (ICS) has become an important topic. Attacks such as the Stuxnet worm have shown that inadequately protecting control systems could have disastrous consequences for society.
Our research focuses on the creation of a tool that aims to enhance the security of Industrial Control Systems. It will be possible for system owners and operators to model their control systems in our tool. Using formal methodologies, the tool can extract a list of vulnerabilities in the system. Users can reason about the effects on system security of component changes or newly discovered vulnerabilities.

1 Problem

Industrial Control Systems (ICS) are used for managing industrial processes. These systems are responsible for controlling and regulating a large number of processes such as the distribution of gas and electricity, following up nuclear reactors, or managing traffic lights. In the last decades, ICS have seen many changes. In the past they were isolated, proprietary systems. Now they mostly use commercial off-the-shelf components, integrated with back-end systems that are often connected to corporate networks and the internet.

This evolution has made ICS easier to use. At the same time it has weakened the security and exposed the systems to remote attacks. To make things worse, ICS are rather static and use components and technologies that are quickly outdated with regards to security. Several attacks on ICS systems have made the news in recent years. The most known example is Stuxnet [1,2], a worm that infected a nuclear plant in Iran, and severely slowed down the nuclear program of the country [3]. Other notable ICS incidents include the Slammer worm disabling the David-Besse nuclear power plant in Ohio [4], the Maroochy Shire sewage spill in Australia [5], and discovery of worms and Trojan backdoors like Duqu [6] and Night Dragon [7] that gather information about control systems to make future attacks like Stuxnet possible.

Attacks on these systems can be very damaging for society. A lot of attention has been given to ICS security, and governments are aware that new security

measures must be taken. This can be done from various angles: public awareness, laws, technology, etc. Organisations such as ISA, NIST, and ISO are defining standards regarding security in industrial control systems [8].

2 Aims and Objectives

The objective of this research is to create a tool for the analysis of security in ICS. We develop a new approach to automatically draw conclusions regarding system security. It is also possible to generate suggestions that provide decision support. Important considerations during this research are: efficiency and flexibility of the architecture, quality of the achieved results, and practical usability.

We aim to develop a model that takes into account the specific requirements of ICS. Existing models for IT systems cannot be used since ICS have different architecture and security properties (Confidentiality, Integrity, Availability in IT versus Safety, Reliability, Availability in ICS). Attackers of ICS can range from disgruntled employees to governments, our attacker model should be able to capture them all.

3 Contributions to State-of-the-Art

Tools for modelling control systems or assessing their security have been developed. Homeland Security has created CSET, the Cyber Security Evaluation Tool [9]. CSET checks compliance of a system with a chosen security standard through a question and answer method. It does not provide an architectural analysis, and it also does not allow the user to reason about compromised components and their effects on system security, which our tool does.

The KTH in Stockholm has developed CySeMoL, the Cyber Security Modelling Language [10,11]. This tool estimates the probability that attacks succeed against an enterprise system. It does not suggest system improvements to reduce this probability, or point out the weaknesses that make the attacks possible. It allows users to change their system architecture and view the resulting changes on the attack probabilities, but only the attacks defined by the tool designers are considered. CySeMoL has to be updated when new attacks are discovered. In our tool, when new vulnerabilities are discovered, it suffices to change the security properties of the affected components in the system model. This can be done by the user and does not require the program to be updated. For computing the attack probabilities, CySeMoL assumes that the attacker is a penetration tester who only has access to public tools, and only tries to attack the system for one week. Previous ICS incidents like Stuxnet have shown that attackers are much more powerful. Our attacker model will reflect this.

ValueSec has redesigned Lancelot [12], a tool previously used for security evaluation of ICT systems in the financial sector. It is now a risk management platform that enables users to analyse security risks and their business implications for the energy smart grid and SCADA (Supervisory Control And Data Acquisition) environment. SCADA systems are a subset of ICS [8]. Lancelot

asks a user to define the system's assets and to associate risk profiles to them. It then does a security analysis to detect risks and compliance issues, and prepares mitigation plans to deal with the risks that are found. Risk in Lancelot is defined as "the potential damage that can be caused when something goes wrong with an asset or when someone/something takes advantage of an asset's vulnerabilities". It is assumed that the user of the program already has knowledge of the vulnerabilities in his system. Lancelot does not help with identifying vulnerabilities.

There are several other tools to conduct risk assessment, but they also assume that the vulnerabilities are already known [13]. Risk assessment methods usually start with a meeting between the risk assessment team and the system engineers [14]. During this meeting they brainstorm about possible vulnerabilities that the system could have. Our tool provides an automation of this phase and the results could hence be used as input for a risk assessment method. When using our tool, a system engineer only has to enter the system architecture, assign the relevant security properties to components, and the vulnerabilities are extracted automatically.

4 Research Methodology

The first months of the project were dedicated to a literature study about the current situation in Industrial Control Systems. Research was done on current modelling techniques, standards and guidelines related to ICS security, ICS architectures, etc.

The next step was to create a first model and test it on a simplified ICS. The systems are modelled using the Inductive Definition Programming framework (IDP) [15,16]. A control system is entered as a network of components to which security properties are assigned. A logic-based theory using induction rules then allows the tool to automatically infer vulnerabilities and corresponding attacks that could occur in this system. Changing the security properties allows users to reason about scenarios in which attackers have breached or compromised certain components. It is also possible to model the consequences of system changes, newly discovered bugs, applied patches, etc.

This initial model was tested on a wind turbine case study. The results have been submitted to a conference as a first paper.

The model will be reworked to include an attacker model and distinguish between vulnerabilities and attacks. New functionalities to improve ICS security will be added to the tool, for instance decision support allowing the user to give a desired security property and presenting him with the optimal component configuration to achieve this. Input and output handling for the tool will be improved upon. Ways to automatically add ICS-CERT vulnerabilities posted on the website into the tool's logic theory will be explored. The result of the vulnerability extraction will be compatible with risk management tools such as CORAS.

Lastly, the model will be tested on multiple case studies.

5 Contributions to the field of Engineering Secure Software and Systems

Our research involves analysing the security in Industrial Control Systems. An important aspect of engineering secure systems is the verification of such systems. This is where our tool can help. When a new component for ICS is developed with certain security properties, our tool can model a complete system to assess the impact of this component on system security.

References

1. A. Matrosov, E. Rodionov, D. Harley, J. Malcho. *Stuxnet Under the Microscope*. ESET 2011.
2. N. Falliere, L. O. Murchu, E. Chien. *W32.Stuxnet Dossier Version 1.4*. Online: `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`, 2011.
3. R. Langner. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. 2013.
4. K. Poulsen. *Slammer worm crashed Ohio nuke plant network*. Online:
5. M. Abrams, J. Weiss. *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia*. IFIP, Volume 253, Critical Infrastructure Protection, 2008. `http://www.securityfocus.com/news/6767`, 2003.
6. Symantec. *W32.Duqu: The precursor to the next Stuxnet*. Online: `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf`, 2011.
7. McAfee. *Global Energy Cyberattacks: "Night Dragon"*. 2011.
8. K. Stouffer, J. Falco, K. Scarfone. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82, 2011.
9. Homeland Security. *Cyber Security Evaluation Tool (CSET): Performing a Self-Assessment*. `http://ics-cert.us-cert.gov/Assessments`.
10. T. Sommestad, M. Ekstedt, H. Holm. *The Cyber Security Modeling Language: A Tool for Vulnerability Assessments of Enterprise System Architectures*. IEEE Systems Journal, 2013.
11. T. Sommestad, M. Ekstedt, L. Nordström. *A case study applying the Cyber Security Modeling Language*. CIGRE 2010.
12. J. M. Prez, D. Machnicki. *ValueSec D5.3 - Description of developed tools and data*. ValueSec, 2013.
13. G. A. Francia, III, D. Thornton, J. Dawson. *Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems*. 2012.
14. *The CORAS Method*. Online: `coras.sourceforge.net`. 2013.
15. J. Wittockx, M. Mariën, M. Denecker. *The IDP system: a model expansion system for an extension of classical logic*. LaSh'08, Leuven, Belgium, November 2008.
16. J. Wittockx, M. Mariën. *The IDP system*. Online: `http://www.cs.kuleuven.be/~dtai/krr/software/idpmanual.pdf`, 2008.