Securing Communication in Cyber-Physical Systems using Steganography and Cryptography

Laura Vegh [1] , Liviu Miclea [2]
Technical University of Cluj-Napoca, Faculty of Automation and Computer Science, Romania
E-mail: [1]laura.vegh@aut.utcluj.ro, [2]liviu.miclea@aut.utcluj.ro

***Abstract*—In a time where technologies come and go, when most of the areas of our lives are rely one way or another on electronic devices and the internet, security is a crucial aspect, always needed. Technologies may rise and fall, but the area of security remains necessary at all times. For this reason the research for new algorithms, new and improved methods is constant. Cyber-physical systems are designed as a network of interconnected devices with physical input and output and represent a new direction in the information systems world. In the present paper we present a solution for the security of communication in cyber-physical systems with hierarchical access by combining cryptography and steganography.**

***Keywords*—cryptography, steganography, cyber-physical systems, hierarchical access, multi-agent systems**

I. Introduction

Protecting the information transmitted throughout a system, contained within a message has always been an area of interest. Nowadays, taking into consideration the rapid advancing of technology, securing the information is becoming more important than ever. Information systems are more and more complex, used in various applications in which the smallest leak of information can be fatal. As a result, current research is focusing more and more on finding a system that can offer a balance, a combination of physical and computational elements. Such systems are called cyber-physical systems (in short, CPS) and are usually projected as a network of interconnected devices and not as separate devices [13].

The term cyber-physical systems suggest the interaction between the real world and the information systems, this being their main characteristic. CPS are not just desktop applications nor are they traditional real-time systems, they bring an addition to the classical systems – their cyber and physical components are integrated for learning and adaptation, self-organization and performance [14]. Because of the many additions they bring to the classical information systems, cyber-physical systems are used in various applications. A few examples are the control of critical infrastructures, transportation and medical devices. It is only natural that with such complex systems arises the need for increased security. Of course, the distinguishing aspect when talking about the security of CPS will be their application area, different areas will bring different structures of the systems and thus security will also be addressed differently.

Speaking in general terms, there are various ways to ensure the security of a system. The best known and probably the most used method is cryptography, specifically algorithms using the public-key infrastructure such as Advanced Encryption Standard (AES), Diffie-Halman or ElGamal, to name a few. As a definition, one can say cryptography is the art of protecting a message by altering its form in such a way that it becomes unreadable without the key to decode it. The encrypted message is still visible to any third party, but cannot be read without being decrypted first.

A different method to secure data is steganography. In contrast to cryptography, steganography does not imply changing the form of the message but rather hiding it in such a way that its existence cannot be perceived. There are several types of steganography – the difference between them being given by the way in which the message is hidden. We cannot speak of the best form, as each method has its role and place accordingly to the type of system to which it is being applied.

From a general perspective, there are two types of steganography: technical and linguistic. Technical steganography is the one that uses images, audio or video files and even networks to hide a message. Image steganography is the most popular of them, since it is easier to use. On the other hand, linguistic steganography refers to the method being applied on text – hiding information inside a text. Probably the most used way to hide information within a text is by adding blank spaces at the end of that text based on the fact that most file editors will overlook a blank space at the end of the file.

A rather new approach in terms of system's security and also the one used in this paper is to combine cryptography with steganography. When using cryptography alone, the message is encrypted, its form is changed and a key is needed to decrypt it. Once that key is found by a malicious third party, the information is compromised. With steganography, the message's existence is hidden but the form is not changed. Once someone realizes there is a hidden message in whatever file was used to hide it, the information is again compromised. However, if the two methods are combined, the security level is much higher as both steganalysis and cryptanalysis need to be performed in order to find the original data. A strong security level as described above is what systems such as CPS need due to their critical application areas [3].

II. Related Work

Steganography and cryptography represent two methods for ensuring security that have been used for several years now. Like everything else in the information technology area, the two are in continuous research and improvement. Combining these methods within the same system is a relatively new direction but we can find several outstanding works in literature. One such work is presented in paper [4]. The authors propose a system that will improve the least significant bit (LSB) method, which is probably the most popular

978-1-4799-2385-4/14/$31.00 ©2014 IEEE

steganographical method. The described system has a private key transmitted between the sender and the receiver and used to extract the hidden message.

In the area of combining steganography with cryptography is the system described in [7]. This time, the key necessary to decrypt the message will also be embedded in the steganographic file. The authors of paper [11] propose a security system with three modules: one module for cryptography, another one for steganography and finally a third module for the security of the system as a whole. The encryption algorithm used is AES. In short, the idea is to first encrypt the data and to later hide the encrypted form in a steganographic file. The same technique, but with different algorithms can be found in papers [5][13][6].

In paper [9] the method used for securing data depends on the type of the communication. Thus, in the case of self-communication – storing digital data, using only steganography is considered to be sufficient. For one-to-one communication or the exchange of information between two parties both cryptography and steganography are used.

Paper [1] uses linguistic steganography, more specifically the word shift coding protocol, which is combined for better security with the well known encryption algorithm AES. The idea behind the paper is simple – providing an additional layer of protection to a communication network.

III. Proposed Model

The model proposed in the current paper aims at finding a new solution for securing a cyber-physical system. We have chosen to use both cryptography and steganography within a hierarchical system. Details about the structures chosen to implement the model and the algorithms that were used will be presented in the following paragraphs.

A. *Agent-based modeling for cyber-physical systems*

An agent can be defined as a software entity capable to act with a certain degree of autonomy, having decision-making capacities. Multi-agent systems have distinguishing characteristics such as having no global control system, decentralized data or the fact that every agent has incomplete information in order to solve a task. Because there is no global control system, each agent has only a 'local view', in other words no agent can see the entire information in the system. Cyber-physical systems are a rather new paradigm, bringing together all the physical and the cyber elements in order to create a more complex and robust system. It is due to their complexity that their design is an ongoing challenge – the cyber and physical components have significant difference between them, bringing different requirements when modeling a CPS. Agent-based modeling is a promising way to overcome the problems brought by CPS design due to the agents' flexibility and their decision making capabilities.

B. *Hierarchical system*

Hierarchical systems are somewhat different than the classical systems in which all parties have equal access to the data. In the case of hierarchical systems, access to data is restricted, a very important aspect especially when discussing security. Information cannot be viewed by all the parties involved, it can only be viewed by those who have access to it. This aspect is very useful when it comes to modeling real-life application, such as medical facilities or e-learning applications. In these cases and not only, information should be naturally restricted according to the position of the user. Taking as an example a medical facility, a nurse might not have access to all the information a surgeon has for instance. This can easily be modeled using hierarchical systems.

The hierarchy can be established in many ways. In the present paper, we propose a model in which the hierarchy is established using an encryption algorithm with divided private key. This means, that each users receives a certain private key and with it he can decrypt and view only those messages to which he has access.

The encryption algorithm used is an extension of the ElGamal algorithm [15] – a classical public key type of algorithm in which one user, the sender, will use the public key to encrypt a message while the other user, the receiver uses the private key for decryption. The algorithm relies on powerful mathematical structures to ensure a good level of security being based on a cyclic finite group. ElGamal with differentiated decryption on K+1 access levels [10] resembles the original algorithm being based on the same type of mathematical structure. We will not go into further detail regarding the mathematical structures and formulas used as they do not represent the main subject of our paper. However, the algorithm explained in detail can be found at [10].

An important aspect is that the algorithm is based on the idea that the information is a set of messages. As a result, each user has access to certain messages in the set according to his access level. The levels can be viewed as a tree structure, where the root of the tree is the user with the highest access level, being able to view all the messages in the set, while the leaves are the users with the lowest access level and are able to see only one message from the set. Another distinguishing aspect in this algorithm is that the leaves are the users which perform the encryption. Also, decryption can be performed only if there is a direct chain from the user trying to decrypt a message to the leaf which performed the encryption. Figure 1 illustrates a hierarchical structure as described above, with four degrees of access, i.e. k=3.

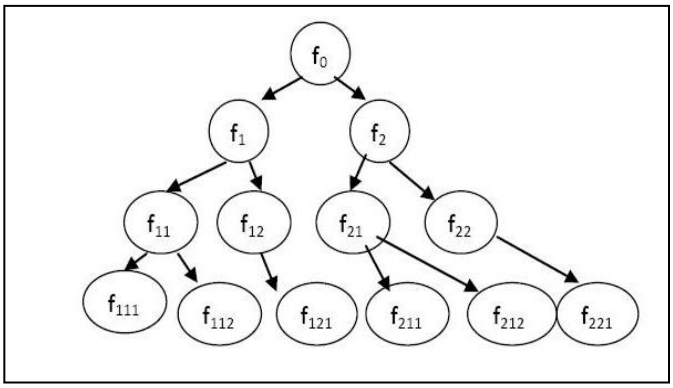

Figure 1. Hierarchical structure

As with any ElGamal algorithm the one presented in this paper has three main phases: key generation, encryption and decryption. In this case however, the key generation is more than just a simple phase of the algorithm as it sets the entire tree structure.

For the implementation of the entire model we have used the Java language and the JADE agent platform which provides all the tools necessary to develop a complex multi-agent system and is FIPA compliant.

The system itself was implemented using three distinct classes: one class called KeyManager represented the agent which will start the entire system by starting the agents, generating the keys and distributing them; another for the agent represented the root of the system and finally a class for all the other agents in the tree structure. This distinction between the root and the other agents was made because the root has access to any message therefore no verification of its rights is needed when decrypting a message. The KeyManager agent is a separate entity from the tree structure; its role is solely to generate the tree and attribute the access rights and shuts down when these tasks are completed. After the keys are generated, respecting the mathematical structures imposed by the algorithm, the next step is to distribute them to the agents in the system.

In terms of programming, it should be noted that all main actions performed by the agents are implemented as 'behaviors'. An agent behavior can be seen as an event handler, a method which describes how an agent will react to an event. There are several behaviors made available in JADE, but for this system we have used *SimpleBehavior* – executed only once and *CyclicBehavior* – executed continuously, as long as the agent is 'alive' and used here to receive messages. Also, the distribution of the keys is performed as the operation of sending a message. Agents will know they received a key and not a simple message by checking the 'conversation id', a feature of JADE agents.

Regarding the access rights, the private keys and automatically the position of a user in the tree structure are the main factors that tell whether or not a user has right to view a certain message. However, in the present model, we have added another step. Even though according to their keys all the ascendants of a leaf have access to the message encrypted by it, if the sender of the message decides intends that message only for a certain level all the levels below it will be denied access. Looking back at the example in Figure 1 for better understanding, if we have a message intended only for agent f_1, its descendant f_{11} for instance will be denied access even though the encryption was performed by f_{111}. This step is not mandatory, the outside sender chooses whether or not a message can go to all that have the key for decryption or if it is intended for a certain level only.

C. Encryption and Decryption

The operations of encryption and decryption, even though at the center of the system's functionality are relatively easy to implement and use. An approximate view of how the system works can be pictured as follows: an external user wants to send information to the users on a certain level. The data is first sent in its unencrypted form to the users with the roles of encrypting it, in our case the leaves. After securing the data, each leaf will send it to its direct ascendant from that specified level.

When an encrypted message is received, before beginning the decryption process, one must first perform a check-up to make sure there is a direct chain from the sender to the receiver. This is a request of our algorithm and even though the implementation was carried out in such a way that a message should not be received by the wrong agent, this verification takes very little execution time in comparison to performing a decryption with the wrong key. If a chain is not present, the decryption is impossible and the agent is automatically denied further access to that message. If a chain exists, the receiver has the necessary private key to perform decryption.

D. Steganography

Defined as the art of hiding a message, steganography has been used for a very long time and for a while it seemed to be taking a backseat to the new emerging security methods such as cryptography. However, during the past years, the continuous development of the information systems and their increasing need for solid security has brought steganography back into researchers' attention. There are many ways to hide a message. It is mostly common to divide steganography in two types: technical and text. The technical one involves hiding the secret information in stego-files such as images, audio or video.

Text steganography, the method chosen in the present paper, refers to hiding information within a text. Linguistic methods are divided into several categories depend on how the stego-text is manipulated in order to hide the message. One such category are format-based methods. They use the physical formatting of text and usually modify the text by adding white spaces, deliberate misspelling or resizing the text. Another method is the random and statistical generation, which is used to avoid comparison with the original text and practically means generating your own cover text.

In the present paper, we have chosen to secure communication in our cyber-physical system using both cryptography and steganography. The encryption algorithm described in the previous chapters, helps model a hierarchical system. Due to the critical nature of CPS application areas, we have chosen to add a new security layer to the system. Steganography was added at the message level. Once encrypted, the message is considered secured. However, should any of the agents be compromised, a part of the message would also be compromised. Each user in the system has a different private key and they cannot be easily computed one from the other. However, the mathematical algorithm for computing them is similar, therefore if one user becomes compromised, the security of the entire system is at risk. For better security, steganography was added to the encrypted message.

The text used to hide the message is created by the system and the code used to form it is changed after every 30 minutes. This time span can be easily changed according to the needs of the system – if we have a system that needs to be running for days without taking up as little resources as possible, the time interval should be bigger. However, if the system is only running for hours, the time interval can be even shorter. Other factors that might force a change of the interval are a known high risk for the system to be attacked frequently.

The text code is formed based on the knowledge that the message to be hidden will be a very large number, on up to 1024 bits, it will never have any letters or special characters, due to the encryption algorithm that has been used. From here, the code is simply generated by assigning a word to each number, from 0 to 9. In order to get a less suspicious code, when generating these words, one should take into consideration the area of application of the CPS. For example, if we are modeling a system for a medical care facility, the words chosen should be from the medical field. This is not mandatory, but it is better if we consider the moment when a malicious third party should intercept this messages. Words that fall in the system's activity domain have a better chance of not raising suspicions than simple random words.

After performing the encryption, the leaf-user will take the steganography code and will start hiding the message. Each number will simply be transformed into its equivalent word and added to a text file. For ease of usage, after each word one white space will be added. We chose to use text files due to the dimension of the encrypted message, which combined with our steganography approach, might result in a text too large to fit into a simple String. Once the message is hidden it can be sent to the receiver agents. At the receiver's side, the first thing to do will be to check for the link with the sender, as described in the previous chapter. Once this operation is performed and the existence of the link is performed, the receiver will begin extracting the encrypted message. This means performing the hiding operation backwards. Knowing the steganographical code, each word is transformed back into a number, until the encrypted message is revealed. From here, the decryption operation will follow as previously explained.

IV. CONCLUSIONS

The system proposed in the present paper brings a new approach to the security of cyber-physical systems. The encryption algorithm used – ElGamal with differentiated decryption with (K+1) degrees of access, allows us to create a secure hierarchical system. The communication is secured with both encryption and steganography. The model used protects data not only from unwanted external access, but it also limits the number of users who can view from inside the system. Modeling the cyber-physical system in a hierarchical manner is very practical with respect to several real-life applications where the access to information should be restricted based on someone's position within the system.

The tree structure used to represent the hierarchy is not unique in current research. Other systems such as the one presented at [12] are based on tree-like architectures. Unlike the systems already developed, our system brings a new perspective by having an agent outside the tree generate and distribute the keys. Having an outside entity generate the hierarchy contributes to bringing our system closer to a real-life application and is more suitable for the design of cyber-physical systems.

REFERENCES

[1] Abdelraham Altigani, Bazara Barry, "A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and word shifting protocol", International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), 2013

[2] Laura Vegh, Stelian Flonta, Liviu Miclea, "Secure multi-agent system using the ElGamal decryption algorithm with (K+1) degrees of access", The 6th International Conference on Security for Information Technology and Communications, Bucharest, Romania, June 2013

[3] Riadh W. Y. Habash, Voicu Groza, Kevin Burr, "Risk Management for Power Grid Cyber-Physical Security", British Journal of Applied Science & Technology, Volume 3, Issue 4, July 2013.

[4] Mamta Juneja, Parvinder Sandhu, "An improved LSB based Steganography with Enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems, Hong Kong, China, January 2013

[5] Arun Kumar Shakar, "Enhancing the Data Security Features of Communication by Means of Media Files through Improvising the Cryptographic and Steganographic Techniques", ASM's International E-Journal of Ongoing Research in Management and IT, 2013

[6] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Aprilie 2013

[7] Chander Kant, Rajender Nath, Sheetal Chaudhary, "Biometrics Security using Steganography", International Journal of Security, Volume 2, Issue 1

[8] M. Grace Venice, Prof. Tv. Rao, "Hiding the Text Iinformation using Steganography", International Journal of Engineering, Research and Application, Vol. 2, Ian-Feb 2012, pp. 126-131

[9] Tayana Morkel, "Image Steganography Applications for Secure Communication", Dissertation Thesis, University of Pretoria, May 2012

[10] S. Flonta, V. V. Patriciu, L. C. Miclea, "Metode criptografice pentru sisteme structurate", U.T. Press, Cluj-Napoca, 2011

[11] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for Data Hiding using Cryptography and Steganography", International Journal of Computer Applications, 2010

[12] V. Valli Kumari, D.V. NagaRaju, K. Soumya, K.V.S.V.N. Raju , "Secure Group Key Distribution Using Hybrid Cryptosystem", Machine Learning and Computing, pp. 188-192, February 2010.

[13] Partha Pal, Rich Shantz, Kurt Ruhloff, Joseph Loyall, "Cyber-Physical Systems Security – Challenges and Research", BBN Technologies, Cambridge, Available at: http://cimic.rutgers.edu/positionPapers/CPSS_BBN.pdf

[14] Dr. Clifford Neuman, "Challanges in Security for Cyber-Physical Systems", Available at: http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf

[15] ElGamal Encryption: http://en.wikipedia.org/wiki/ElGamal_encryption