J. Lopez, J. A. Montenegro, and R. Roman, “Service-Oriented Security Architecture for CII based on Sensor Networks”, *2nd International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU06)*, pp. 1-6, 2006.
NICS Lab. Publications: https://www.nics.uma.es/publications

# Service-Oriented Security Architecture for CII based on Sensor Networks

Javier Lopez, Jose Antonio Montenegro, Rodrigo Roman
Computer Science Department, E.T.S. Ingenieria Informatica
University of Malaga, Spain
{jlm, monte, roman} @lcc.uma.es

## Abstract

*The extraordinary growth of the Information Society is originating a high dependency on ICT. This provokes that those strongly interrelated technological infrastructures, as well as the information systems that underpin them, become highly critical, since their disruption would lead to high economical, material and, sometimes, human loss. As a consequence, the protection of these Critical Information Infrastructures is becoming a major objective for governments and companies.*
*In this paper, we give an overview of the main challenges and open research issues on Critical Information Infrastructure security, and introduce an on-going research project that, using wireless sensor networks as an underlying technology, is dealing with those problems. Our research project focuses on the development of protection, control, evaluation, maintenance and verification mechanisms, integrated into a secure service-oriented architecture.*

## 1. Introduction

On the other hand, more and more intelligence and autonomy go in components/systems at lower and lower scale: (i) large scale systems of casually networked and evolving real-time embedded devices, like wireless sensors; (ii) mobile codes in heterogeneous and mobile environments, (iii) volatility of networks and service infrastructures, etc. Therefore, security issues in the digital environment are becoming global.

In such scenario, a new mega-infrastructure is emerging from the convergence of infrastructures of different industry sectors and the Internet. The concept of Critical Infrastructure is arising. The challenges on protecting those Critical Infrastructures are numerous and complex, since problems in individual and homogeneous systems evolve into problems in heterogeneous environments, where the security and resilience of the overall system and its parts must be assured before, during and after any operation. In order to provide solution to some of those problems, we have recently started a research project called CRISIS (CRitical Information Infrastructures Security based on Internetworking Sensors).

Thus, the purpose of this paper is to introduce the main challenges in the protection of *Critical Information Infrastructures* and how our research project is actually coping with them. The rest of this paper is organized as follows. In section 2 we define the CII and justify why *Wireless Sensor Networks* technology is suitable to provide security in those scenarios. In section 3 we provide a very useful background on CII and WSN, and remark some open research issues that we address in Section, where we present our ongoing project. Finally, we conclude the paper in section 5.

## 2. Critical Information Infrastructures and Wireless Sensor Networks

According to the European Commission, *Critical Infrastructures* consist of *“those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical Infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services”* [5]. As pointed out by the Commission, some critical elements in these sectors are not strictly speaking ’infrastructure’, but are in fact, networks or supply chains that support the delivery of an essential product or service. Key sectors of modern society that are vital to the national security and the essential functioning of industrialized economies are dependent on a spectrum of highly interconnected national (and international) software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the aforementioned Critical Infrastructures, and is hence called *Crit-*

*ical Information Infrastructures* (CII).

Secure and reliable operation of these information networks is fundamental to national and international economy, security, and our quality of life, and what is worst, the interconnected nature of networks means that single, isolated disturbances can cascade through and between networks with potentially disastrous consequences. Therefore, it is essential to guarantee the security of information that is considered of critical importance, from a political, economic, financial or social standpoint. One may think that Information Security provisions such as authorization, authentication, encryption, and other basic security services must be added to current communications protocols. However, the solution is not that easy. The complexity of the Critical Infrastructure scenarios and applications is so high that it becomes strongly necessary to provide advanced security technologies.

An essential step in the research of Critical Information Infrastructures is a comprehensive assessment to determine which underlying communications technologies and security options are appropriate for utility operations. In this sense,it is very important to point out that CII are characterized by unique requirements for communications performance, including timing, redundancy, centers control and protection, and equipment control and diagnostics. Because they are complex and dynamic infrastructures, they have many layers, and are vulnerable to many different types of disturbances. Although strong centralized control is essential to reliable operations, CII require multiple high-datarate communication links, a powerful central computing facility, and an elaborate operations control center. All of them are especially vulnerable when they are needed most -during serious system stresses or disruptions.

However, for deeper protection, intelligent distributed control is strongly required to keep parts of the network operational. It is commonly agreed by network experts that Wireless Sensor Networks (WSN) is the technology that better fulfills features like the ones required by CII. In fact, WSN can be applied to a large number of areas, and its applications are continuously growing.

WSN are composed of hundreds or thousands of inexpensive sensing devices with computational and communication resources, and provide a useful interface to the real world with their data acquisition and processing capabilities. Sensor nodes are densely deployed either very close or inside the object to be observed. Inside a WSN, every node is totally independent, sending data and receiving control packets from a central system called base station, usually managed by a human user, what fits with the aforementioned requirement of operation control center for CII. The purpose of a sensor is very specific: measure the physical information (such as temperature, sound, movement, etc.) of its surroundings. A typical sensor node such as MICA [10] has a 8Mhz microprocessor with 128Kb of program flash memory and 512Kb of serial flash memory. As a result, both hardware modules and communication/configuration protocols are highly specialized.

In spite of this, due to the extreme constraints of the devices, a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations.

Because of these problems, one may argue that it would be a better solution for CII scenarios to use another technology rather than WSN. However, there is no better technology available at this moment. Moreover, experts agree on the high benefits that this new technology can provide to the many different facets of Information and Communications Technology. Therefore, many believe that it is only a matter of starting developing security solutions for sensor networks, in the same way as years ago the scientific community started developing security solutions currently under use for typical networks. As a result, it is essential to achieve a successful deployment of secure sensor nodes solutions for the protection of CII.

## 3. Background and open research issues

The protection of Critical Information Infrastructures is a very novel research topic. Therefore, there are many open research issues. Moreover, as it is easy to figure out, the challenges in this field are influenced by its interdisciplinary nature, where problems in individual and homogeneous systems evolve into complex problems in heterogeneous environments. In such heterogeneous environments, it is crucial to provide a set of policies and methods to allow an effective and secure interaction of the elements of a CII, both internal and external. In the literature we can find works focusing on the creation of high-level policies (like the work of Hammerli [6] on the relationship between CII organizations), but little research has been put into areas such as the security policies of a CII. On the other hand, resilience and robustness are important matters of a CII. This one must be resilient and robust against any type of problem or attack, and must be able to react and protect itself in real time. There are some tools that can help in the mitigation of these problems by alerting and helping the human user [4]. Different solutions, like Intrusion Recovery Systems, could help with this matter, though they have not been applied yet.

Also, alerts and warnings are certainly important questions that must conform a basic part of a CII. Warning systems help the human user and the information system to react against possible difficult situations before (or after) they occur. This is a hot topic that will be greatly useful for a CII. However, it is usually not feasible to test and obtain results about a CII without endangering the operation of the entire system itself. As a result, it becomes imperative to create models and simulations that show how the system should behave in presence of problems. Although there are a couple of interesting works in the literature, like those by Rinaldi [13] and Wolthusen [19], this is not a well-developed topic yet.

It is interesting to mention the importance of the ability to manage and assess the risks that a CII can face throughout its existence. It is of vital importance to analyze an infrastructure and quantify the possible problems in order to correctly model the protection system. At this moment, risk management and quantification in CII are in a very early stage, and only recent works are available in the literature like those ones by Sahinoglu [15] and Adar et al. [1].

Last, but not least, it is important to point out that the knowledge of the structure and behavior of the individual elements of the CII does not mean a complete understanding of how the CII could work as a whole. Simulating and analyzing these large and complex systems is a real challenge because of their nonlinear and time-dependent behavior. Little work has been done regarding this issue. Among those few, we highlight [16].

As for Wireless Sensor Networks, the challenges that this area faces are numerous. As previously mentioned, the major problem that avoids the application of sensor networks to real-world scenarios is the lack of security of its components and protocols. Existing sensor nodes are able to incorporate software-based security primitives such as symmetric key encryption and Message Authentication Codes (MACs) with minor overhead in terms of CPU, energy and memory footprint, as shown by Karlof et al. in their paper about TinySEC [9]. Although the computational and memory requirements of public key cryptography are high and these techniques has been disregarded during the last two years, new results show that the great advantages introduced by public key cryptography can also succeed in the area of wireless sensor networks. All the security primitives need to store a set of secret keys inside every node. Thus, key management systems are compulsory. Deploying, storing and maintaining a set of keys over a fixed group of nodes in a scalable manner is a hot research topic. However, there are only a few interesting solutions, like the one included in the work by Camtepe et al. [3]. The interesting and genuine case of maintaining the keys for group of sensor nodes that is created in real-time, remains unresolved yet.

The security of network-level services such as routing and aggregation is still at its infancy. There are many routing algorithms and protocols, like the one by Al-Karaki et al. [2] that solve problems like addressing, connectivity, coverage, fault tolerance, and scalability. However, almost all the existent routing protocols do not consider security as an issue during their initial design, even if there are a wide range of attacks that can manipulate the routing subsystem, like was shown by Karlof et al. in [8]. Aggregated data, as routing packets, can be easily attacked by a malicious adversary.

Nowadays, there are no auditing procedures for wireless sensor networks. As a result, the field of intrusion detection systems and intrusion prevention systems lacks to be well developed in these scenarios. Only a few solutions exist, and are incomplete, like the one by Da Silva et al. [18], or untested, like the work by Roman et al. [14]. Other open areas of research [17] include tolerating the lack of physical security, managing the secure location of nodes or groups of nodes, optimizing the security infrastructures in terms of resources (energy and computation) and managing the threats to the privacy of both the information infrastructure and the sensed objects [12].

## 4. Development of a Service-Oriented Security Architecture for Critical Information Infrastructure Protection

As we have seen, there are many challenges in the field of Critical Information Infrastructure Protection, involving complex problems such as defining policies and methods for secure interaction between entities, assuring resilience and robustness of the overall system, deploying warning and alert systems, creating models and simulations, and defining tools that could quantify the scope of possible problems. The underlying infrastructures of those CII, such as Wireless Sensor Networks, have numerous challenges as well.

We have started a project named CRISIS (CRitical Information Infrastructures Security based on Internetworking Sensors). That project will not be able to completely solve the situation mentioned above, but it could improve it and provide a ground for both future research projects and commercial solutions. Our on-going project focuses on the design of Security solutions for Critical Information Infrastructures by means of the development of protection, control and evaluation mechanisms. Wireless sensor networks are introduced as a main technological platform for this task because that technology facilitates a distributed control and allow the different components of the network to remain operative, even in crisis situations. In order to guarantee the faultless interoperability of the protection, control and evaluation mechanisms, new security services are being created. These services will be integrated into a Service Oriented Architecture (SOA) [11], specifically devised for Critical Infrastructures, with the aid of a trust management model designed for this purpose. The functionality of the Architecture is going to be verified in different ways. On one hand, we are designing and developing management and maintenance systems embedded into the Architecture, such as early warning, dynamic reconfiguration and Auditing systems. On the other hand, with the aim of providing support for the infrastructure, we are developing tools for decision support and, risk analysis and management.

### 4.1. Supporting Services

At a low level, our Architecture is mainly composed of wireless sensors hardware platforms, namely MICA [10]. At this point of the project, we are identifying and defining the software components needed to provide basic mechanisms for the creation of security services. These software components will allow the deployment, supervised or automatic, of the control infrastructure. They will also allow the access, in a scalable and efficient way, to the information acquired by the sensors system and adjacent subsystems. Additionally, it is necessary to maintain in a simple way (with or without supervision) the information infrastructure. Therefore, we are specifying components that allow the access and modification, in a secure manner, of the behavior of the network, but also to access and monitor the state of the elements of the infrastructure.

On the other hand, at high level we are specifying mechanisms for providing an appropriate interoperability of the elemental mechanisms. These integrated elements will establish the foundation of a SOA . This requires the creation of security policies adapted to the new Critical Infrastructures context (mainly, those policies based on the management of user and device attributes). At the same time, these security policies require the correct specification of the associated middleware. We also need to determine the functional interdependences and the interfaces for the interchange of information among the components of the Architecture. We are going to create specific interfaces, following the design rules applied by the standards.

Finally, we are designing mechanisms that will facilitate the interoperability among the different services of the CII Architecture, following the SOA specification. Additionally, we are identifying the external services required for the appropriate operation of the CII Architecture, as well as the entities that provide them. Once created, we will design mechanisms and protocols that will allow the transparent use of external services to the users of the Critical Infrastructure. In order to define the interoperability services, we are considering standards such as XML.

### 4.2. Trust Management Model

Whenever there is an interaction among applications, entities, etc., Trust Management becomes a fundamental issue in the Security area. There are many formal or computational trust models, but no one has been specially designed for complex scenarios like those ones that CII conform, where the dependency among applications and entities is extremely high. For this reason, we have to integrate security services such as Authentication, Authorization and Delegation for the design of a basic trust management model where it will be easy to further add new composed services.

In order to avoid uncontrolled accesses to CII services, we are defining and designing *Advanced Authentication Services*. At a low level, we are creating a key management system for the sensor nodes that allow the storage, distribution and maintenance of the keys, both for static groups of nodes and groups formed in real time. We will provide a framework that guarantees confidentiality and integrity of communications among sensors, and services for the advanced authentication of each of the elements of the network. For that goal, we are specifically adapting to the field of sensor networks public key cryptographic algorithms based on elliptic curves. At a high level, and though the standard solution for distributed authentication, PKI (Public Key Infrastructure), is an off-line mechanism, the infrastructures foresee in this project will take us to design on-line mechanisms in order to support emergency situations.

We are also defining *Authorization Services* with different security levels, since devices with different capabilities (processing, memory and bandwidth) will coexist in the CII. In order to accomplish this, we are designing an Intelligent Authorization Gateway that will be able to translate the different authorization mechanisms that coexist in the Critical Infrastructure. Also, when establishing this service, it will be necessary to consider the evolution towards ubiquitous environments. Therefore, we are designing a Distributed Authorization System that, integrated with the previous gateway, will allow legitimate users to have access to any resource. At the same time, resource owners will be able to control how resources are used. The *Delegation Service* is a complementary service to the Authorization one, extending the latter with the scalability property. Therefore, we are defining a Delegation Description Language, and will implement a tool for visual modeling, establishing in this way advanced control mechanisms so that the delegation process is supervised. Fostering that goal, we are analyzing standardized mechanisms, like PMI (Privilege Management Infrastructure) [7].

These three services and the trust management model allow us to define essential composite services such as Information Sharing, Aggregation, and Privacy. In case of crises and large-scale disruptions, national critical infrastructures must coordinate and cooperate in order to cope with any ongoing problems. Therefore, we are developing an Information Sharing Service that will allow any center in the infrastructure to exchange critical information with internal or external trusted entities. On the other hand, since the amount of available data (both in normal operations and during a crisis) is usually very high, we are developing an Aggregation Service that will manipulate and transform the data flow into smaller pieces of information that could help humans and computers in taking useful decisions. Finally, it is interesting to identify those points of the CII where anonymity of users should be preserved, but also those that, because its special relevance, anonymity should be avoided.

## 4.3. Secure Control System

For the sake of protecting a CII, it is indispensable to provide a secure control system that will allow both human supervisors and the computer infrastructure to control its operation and detect and react against any problems that could happen. Such control system must have monitoring and maintenance services, such as Early Warning Systems, Dynamic Reconfiguration Systems, Auditing procedures and forensic techniques.

The main task of an Early Warning System (EWS) is to identify, detect and react against possible problems before they become a threat for the CII. These problems can range from a simple malfunction or degradation of an element of the CII to an intrusion done by an external or internal entity. Therefore, we are designing a EWS that will analyze the information provided by the underlying architecture in order to infer the actual behaviour of its elements. As a result, it will provide the appropriate information, right on time, to the human analysts, supporting them in the decision process. In this way, all scattered human resources can be treated as one scalable virtual response team, accessing to precise and reliable information whenever they need it. Also, the EWS will automatically react against any potential threats, based on internal intrusion prevention systems on the sensors, system policies, and the experience gained by itself in previous decisions. Finally, the EWS will check the reliability and continuity of service of the underlying communication infrastructure to allow seamless business continuity, albeit at the price of affordable performance degradation. It will incorporate the possibility of (dynamically) assigning both priorities and performance thresholds for the different communication infrastructure services, allowing them to take the appropriate measures to achieve the best possible balance among the potentially conflicting goals of service availability.

One of the main characteristics of a CII is to keep the provision of services even in the worst conditions. For this reason, it is necessary that the different components of a CII are self-sufficient to react under difficult operational conditions that may be a threat for providing basic services. Thus, a Dynamic Reconfiguration System (DRS) is being designed and implemented as a set of mechanisms in a high and a lower level. The DRS will allow the different components of the CII to re-configure itself in an automatic way. The events generated by the EWS will prompt the reconfiguration mechanism.

Regarding maintenance, every system needs a continuous support to ensure a correct performance during its work life. Consequently, we are defining monitoring schemes for the hardware components and services of the CII. Based on these schemes we will design and develop specific auditing procedures that will allow us to find possible problems within the activities developed by the services of the CII. These procedures will work off-line and complementarily to the EWS. They will also allow us to correct wrong operations of the components and/or optimise the performance of the CII services.

However, no infrastructure is totally safe against external or internal threats, and even protected CII will suffer from problems that will hinder their normal operations or (even worse) halt the entire system. For this reason, we are also creating and deploying forensic techniques and procedures that will provide investigators with the most accurate information regarding failures. This information will be a valuable feedback for future procedures and, in some cases, will lead to a quickly and accurately identification of a malicious operation. These techniques and procedures will provide detailed guidelines for accessing the information contained in the underlying architecture and mechanisms for detecting any past irregular behavior.

## 4.4. CII Testing and Evaluation Framework

This Critical Information Infrastructure framework would be incomplete without the testing and evaluation of the CII. For this reason, at a lower level, we are designing and developing a tool that allows us to verify the security of the interconnections between systems in the CII. For this purpose, we will select a significant enough set of protocols and interfaces in order to validate the strength of the developed tool.

At a higher, behavioural level, a Decision Support System (DSS) aids both human users and automatic systems in the process of making decisions regarding the actual or future status of the CII, recognizing its stability under a certain context, its ability to adapt to this context, and the onset of irreversible trends. In the context of CII, the DSS must feature a simulation model in order to study the dynamics and interactions of the CII without actually changing it. These changes could endanger the operation of the system itself.

For the previous reason, we are designing and developing a Simulation-based DSS that will be based on the properties of individual nodes, the overall system and its context (for instance, an electricity system consumes less during the night than during the morning), interconnections between nodes. It will also be based on faults and intrusions to which the system is susceptible, such as failures and faults in the system components, environment-related events, and human errors and intrusions. The input of the simulator will range from statistical and symbolic probabilities to real-time data, with the aim of facilitating the recreation of past, actual or even possible future events. Also, all the properties of this model will be represented in a formal notation in order to facilitate automated analysis.

## 5. Conclusions

In this paper, we have discussed why the security of Critical Infrastructures and its information infrastructures must be guaranteed in order to protect the well-being of a nation and its citizens, and how technologies such as Wireless Sensor Networks are essential for fulfilling the requirements and features of those Critical Infrastructures. Additionally, we have introduced our on-going project, CRISIS, which focuses on the protection of Critical Information Infrastructures using Networked Sensors.

## References

[1] E. Adar, A. Wuchner. *Risk Management for Critical Infrastructure Protection Challenges, Best Practices & Tools*, First Intern. Workshop on Critical Infrastructure Protection, pp 90-100, November 2005.

[2] J. N. Al-Karaki, A. E. Kamal. *Routing techniques in wireless sensor networks: a Survey*. IEEE Wireless Communications, Vol. 11 Issue 6, pp 6-28, 2004.

[3] S. A. amtepe, B. Yener. *Key Distribution Mechanisms for Wireless Sensor Networks: a Survey*. TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department, 2005.

[4] L. Carlier, L. Dhaleine, P. Genestier, C. Lac and B. Savina. *Emergency and Rescue: Methodology and Tool for Alert Activation and Crisis Management*, Informatik2003, Lecture Notes in Informatics, 2003.

[5] Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism*, COM (2004) 702 final, Brussels, 20 October 2004.

[6] B.M. Hammerli. *CIIP Task Description and a Proposal for a Substitute of National C(I)IP Policies*, 1st International Workshop on Critical Infrastructure Protection, pp 51-61, 2005.

[7] Information technology: Open systems interconnection. The Directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509, 2000.

[8] C. Karlof, D. Wagner. *Secure routing in wireless sensor networks: attacks and countermeasures*. 1st IEEE Intern. Workshop on Sensor Network Protocols and Applications, pp 113-127, 2003.

[9] C. Karlof, N. Sastry, D. Wagner. *TinySec: a link layer security architecture for wireless sensor networks*. Second Intern. Conf. on Embedded Networked Sensor Systems, pp 162-175, 2004.

[10] Crossbow Technology, Inc. Wireless Measurement Systems. http://www.xbow.com.

[11] S. Jones, M. Morri. *A methodology for service architectures*. OASIS Draft.26th October 2005

[12] C. Ozturk, Y. Zhang, W. Trappe, M. Ott. *Source-location privacy for networks of energy-constrained sensors*. 2nd IEEE Workshop on Software Techn. for Future Embedded and Ubiquitous Systems, 2004.

[13] S. M. Rinaldi. *Modeling and Simulating Critical Infrastructures and Their Interdependences*. 37th Hawaiian International Conference on system Sciences, 2004.

[14] R. Roman, J. Zhou, J. Lopez. *Applying Intrusion Detection Systems to Wireless Sensor Networks*. IEEE Consumer Communications & Networking Conference, 2006.

[15] M. Sahinoglu. *Security Meter: A Practical Decision-Tree Model to Quantify Risk*, IEEE Security & Privacy, vol. 3, n.3, pp.18-24, 2005.

[16] W. Schmitz. *Modelling and Simulation for Analysis of Critical Infrastructures*, First GI Workshop on CIP, within Annual Meeting Informatik, 2003.

[17] E. Shi, A. Perrig. *Designing Secure Sensor Networks*. IEEE Wireless Communications, V.11, n.6, pp 38-43, 2004.

[18] A. Da Silva, A. Loureiro, M. Martins, L. Ruiz, B. Rocha, H. Wong. *Decentralized Intrusion Detection in Wireless Sensor Networks*. 1st ACM Intern. Workshop on Quality of Service & Security in Wireless and Mobile Networks, 2005.

[19] S. Wolthusen. *Modeling Critical Infrastructure Requirements*. 5th IEEE SMC Information Assurance Workshop, 2004.