C. Alcaraz and J. Lopez, "FACIES: online identification of Failure and Attack on interdependent Critical InfrastructurES", *European CIIP Newsletter*, vol. 7, pp. 11-13, 2013.
NICS Lab. Publications: https://www.nics.uma.es/publications

FACIES: *online identification of Failure and Attack on interdependent Critical InfrastructurES*

FACIES aims to protect water treatment systems and their control systems against accidental or intentional incidents such as failures, anomalies and cyber-attacks with a particular emphasis on stealth attacks.

In September 2012, the European online identification of Failure and Attack on interdependent Critical InfrastructurES (FACIES) project was launched to find suitable methodological solutions for cyber and physical defense of Critical Infrastructures (CIs) in general. The project, funded by the European Commission's 7th Research Framework Program (FP7) within the prevention, preparedness and consequence management of terrorism and other security related risks program, highlights the current situation through a set of theoretical analyses and practical experimentation in a testbed.

The testbed, with a particular focus on water treatment systems and their control systems, exhibits how changes in specific CIs can seriously affect other interdependent infrastructures, such as energy systems, dams, market, environment or public health.

Why the Water Sector?

Water systems are, in common with other critical systems, susceptible to adverse events that can have a dramatic impact on the safety of our society, its social welfare and economy, with a certain degree of emotional repercussions and distrust. Compromising the security of control systems and damaging the underlying infrastructure, is to indirectly attack social sensibility and to put on edge, governments, industries and citizens, who are the main consumers and beneficiaries of water supply. Therefore, they become the main end-victims of cyber or physical attacks.

According to the latest reports published by the Control System Cyber Emergency Response Team (ICS-CERT) in 2009 [1][2][3], the number of incidents in the respective critical sectors has increased over the last few years. In the particular case of the water sector: 3 incidents were registered in 2009 with 33% compared to other sectors; 2 in 2010 with 4%; 81 in 2011 with 31%; 29 in 2012 with 15%; and this year 8 incidents with 4% in total.

> Situational awareness consists of "*the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*". R. Endsley, 1995.

The spread of a consequent effect depends on a set of factors: (i) scope of the effect measured in terms of geographical extension, loss or unavailability of assets and services; (ii) magnitude of the effect measured according to the degree of the effect or propagation towards other CIs; and (iii) restoration time, which is established, starting from the initial loss of an element until it regains its initial states, whilst preserving its essential properties. The effect on the water sector may not be, a priori, so shocking as a lack of electric power services, but the consequences can become equally drastic in time.

Situational Awareness

Responses to hardware or software failures, anomalous perturbations or cyber-attacks can require information of a context to understand, at a high-level, what a domain and its infrastructures may be experimenting at a given moment [4]. This degree of knowledge can require the orchestration of small evidences related to the context, to interpret and illustrate a specific situation, such as location, identity, physical events, time, etc. This information is generally perceived by sensory devices and massively managed by collectors, such as dedicated servers, remote terminal units/Programmable Logic Controllers (PLCs) or gateways.

However, the management of big data is not a trivial task. Depending on the context, the characteristics of such a context and its architectural complexities, it is necessary to carefully select some of the existing methodologies for detection of anomalies and intrusion. In any case, the solutions should be effective, rapid and lightweight since supervision and acquisition requirements cannot be sacrificed or violated at any time. This effectively means a tradeoff between security and operational performance should also be questioned at this point and always.

An anomaly is something that deviates from what is standard or expected, and can become the evident symptom to watch for in unrecognized behavior pattern prototypes, likely linked to specific cyber-attack sequences. Applying anomaly and intrusion detection techniques in critical contexts can become a challenge to be met, where a high degree of knowledge of the situation is needed to exhaustively or perhaps, partially explain a problem.

Most of these problems are primarily caused by deficiencies and vulnerabilities registered in the underlying system. Some common exposures to vulnerabilities in

control systems are for example: incomplete or inefficient security policies and access control, deficient protection in the perimeter where security systems (e.g. firewalls or intrusion detection systems) are based on inaccurate rules/patterns, interoperability issues and conflicts, abuse and use of weak security credentials based on username-password with high visibility and low update using insecure cryptosystems, vulnerable TCP/IP-based protocols, implementation bugs, non-segregation of functions, interferences or industrial noise, strong dependence on third-parties' components, and so on.

Any failure or anomaly may open up breaches in security and bring about numerous security risks. Indeed, attackers may take advantage of a given situation to lead a set of non-iterative or coordinated cyber-threats, such as: false injection, to falsify reading values/alarms, hide real values of signalization, manipulation of assets and configurations, memory corruption, denial of services, impersonation, etc.

Governance, best practices, recommendations, policies, maintenance, training, auditing, and accountability are certainly key elements to mitigate these cyber issues. Still, specification and commissioning of both methodologies and lightweight approaches, and the exploration of new research fields and technologies are also necessary. Investigation on situational awareness could for example complement the majority of these goals, becoming in itself a useful tool for prevention and mitigation.

Stealth Attack and Mitigation

Being aware of stealth attacks and addressing topics of protection against them is nowadays a challenging exercise. A stealth attack consists of quietly operating a set of techniques to drive a set of malicious actions that compromise critical nodes with a low visibility. The attacker, capable of dynamically moving across the entire system, normally tries to hide evidence that can reveal his/her presence.

An example of precisely this type of threat was the Stuxnet worm in 2010. It was considered the first malware designed specifically for writing, reading and localizing critical sections in the PLCs of Siemens without leaving activity evidences. Although Stuxnet is a clear example of how to beat the system unnoticed, typical stealth attacks have, as their ultimate goal, the manipulation of the state estimation while preventing the control system from being warned of bad data.

Unmasking stealthy and invisible actions is consequently a difficult mission, but not impossible. For example, it is possible to protect a state estimator by applying cryptographic techniques (e.g. to encrypt the number of state variables) or correlation methods. Through FACIES we intend to address all of these cyber issues in addition to considering some other measures to quantify and qualify anomalies, compare physical and software evidences, manage interdependencies, and quantify situations through weights. Obviously, defining patterns or schemes to ascertain the influence of stealthy actions can become a tricky job since it could require a prior learning phase to understand the context and classify normality settings.

> Now that we have the right tools, it's time to learn to defend ourselves, validating defense solutions to face stealth attacks. The time is now. It's our time.

Differentiating a normal (but unrecognized) situation from an abnormal situation involves specifying boundaries/regions. Anomaly detection is an open research area that still faces many investigative problems, especially when it is applied to critical contexts to [5]:

- Appropriately manage high rates of false alarms; either false positives or false negatives.
- Define the concept of normality and adapt it to the application domain. In this case, in contexts related to water treatment and control.
- The normality concept can vary as these types of infrastructures generally work over long time periods.
- Differentiate between anomaly and noise so as to properly remove the noise from the data.
- Differentiate between causal anomalies and anomalies provoked by malicious actions.

Moreover, the prototypes of patterns are in the majority of cases unknown to staff members. They do normally know when and where to establish the limits of the normality concept, how in reality, to apply it, and why. The lack of knowledge of this can even hamper the training procedures and labeling sometimes requiring an initial investigation to examine the context and determine where, when and how to establish the boundaries. This study could even require an analysis on levels of criticality associated with each subdomain, modeling or simulation of inter-dependencies, valorization of architectural complexities and analysis of information so as to illustrate a general skeleton of the context, thereby distinguishing a normal from an abnormal event.

About Cyber-Physical Exercises in Testbed

In order to implement the objectives of FACIES and experiment with cyber-physical exercises to validate defense solutions, the University Campus Bio-Medico of Rome (UCBM) under the coordination of Professor Roberto Setola, has configured a testbed for FACIES (Figure 1).

Fig. 1.- Testbed for FACIES

The testbed, based on four water tanks, a water reservoir, automatic and manual valves, pumps and (flow, pressure and level) sensors, is monitored 24/7 by a Proficy HMI (Human-Machine Interface)/SCADA (Supervisory Control and Data Acquisition)–iFIX software, offering support to operate 200+ nodes. All the knowledge of the context is centralized in a Modicom M340 PLC, which is responsible for transferring

commands from iFIX to values/pumps, and collecting (flow, pressure and level) reading values from sensors.

Several cyber exercises on the testbed will principally focus on testing the robustness and resilience of the solutions against falsification attacks and integrity of data, availability of resources and stealth attacks, exploring the abilities of the testbed to detect intrusion, warn of the situation and self-heal to continue the services in the worst case scenario.

The FACIES Consortium is based on four partners, each of whom is entrusted with a particular task. For the physical part, those responsible are as follows:

- UCBM as the coordinator of the project and responsible for configuring and maintaining the testbed, in addition to addressing modeled stealth attacks, and recovery.
- RadioLabs from Italy focuses on topics of analysis and evaluation of impact and consequences in highly interdependent systems, and fault detection.
- University of Cyprus (UCY) in charge of the modeling and simulation of interdependent networks, as well as the analysis of behaviors and impact.

For the cyber part, the entire Consortium heavily relies on:

- The Network, Information and Computer Security (NICS) Lab. at the University of Malaga (UMA) which is responsible for addressing cyber-threats, intrusion and anomaly detection, stealth attacks awareness, and reaction strategies.

For more information about the structure of FACIES, its Consortium, goals and technical documentation, please visit our website at http://facies.dia.uniroma3.it

Are we going in the right direction?

Optimistically, we believe that the direction we are taking is correct, but somewhat pessimistically we also believe that there is still a long way to go. Support from governmental and industrial entities are essential to proceed with these types of practical exercises over the coming years. Ideally the scientific community should be encouraged to expand their research and learn more from these systems, exploring new technologies and exploiting existing/new research fields to evaluate protection measures. These fields could be for example controllability, observability, secure location privacy, trust management, reputation, prevention and reaction through dynamic and intelligent solutions.

> The secret to us not deviating from the right path is to stay motivated, but in some way it is also necessary to feel that we are being supported.

Knowledge sharing and motivation are the means to keep on this path, where closer collaboration is, unfortunately, still needed. Trust is the secret to succeeding in overcoming a problem, but certainly this is impossible if such collaboration does not exist.

References

[1] U.S DHS, ICS-CERT, incident response summary report, 2009-2011, September 2011, http://www.uscert.gov, Last access on Sept., 2013.

[2] U.S DHS, ICS-CERT, ICS-Monitor – Malware Infections in the Control Environment, Octr/Nov/Dec 2012. http://www.uscert.gov, Last access on Sept., 2013.

[3] U.S DHS, ICS-CERT, ICS-Monitor – Brute Force Attacks on Internet-Facing Control Systems, June 2013, http://www.uscert.gov, Last access on Sept., 2013.

[4] C. Alcaraz, and J. Lopez, Wide-Area Situational Awareness for Critical Infrastructure Protection, IEEE Computer, vol. 46, no. 4, pp. 30-37, 2013

[5] V. Chandola, A. Banerjee and V. Kumar, Anomaly Detection: A Survey, ACM Computing Surveys, vol. 41, no. 3, Article 15, pp. 15-58, July 2009.

Cristina Alcaraz

C. Alcaraz is a Marie-Curie Postdoctoral Researcher on CIP at the NICS Lab. of the University of Malaga and at the Royal Holloway, University of London under the Marie-Curie COFUND programme "UMobility" co-financed by UMA and the EU 7th FP (GA 246550). She is an editorial member of several international journals, such as the ECN, being responsible for the young section working on the CIP field.

e-mail: alcaraz@lcc.uma.es
URL: https://www.nics.uma.es/alcaraz

Javier Lopez

Full professor in the Computer Science Department at the University of Malaga, and Head of NICS Lab. His research activities mainly focus on information security and CIP, areas where he has led several international research projects. Prof. Lopez is Co-Editor in Chief of IJIS journal, and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: jlm@lcc.uma.es
URL: https://www.nics.uma.es/jlm