Towards Secure Monitoring and Control Systems: Diversify!

Domenico Cotroneo[1,2], Antonio Pecchia[1,2], Stefano Russo[1,2]
[1]Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI)
Università degli Studi di Napoli Federico II
via Claudio 21, 80125, Naples, Italy
[2]Critiware S.r.l.
Incipit, Complesso Univ. M.S. Angelo, via Cinthia, 80126, Naples, Italy
{cotroneo, antonio.pecchia, stefano.russo}@unina.it

I. Rationale

Cyber attacks have become surprisingly sophisticated over the past fifteen years. While early infections mostly targeted individual machines, recent threats leverage the widespread network connectivity to develop complex and highly coordinated attacks involving several distributed nodes [1]. Attackers are currently targeting very diverse domains, e.g., e-commerce systems, corporate networks, datacenter facilities and industrial systems, to achieve a variety of objectives, which range from credentials compromise to sabotage of physical devices, by means of smarter and smarter worms and rootkits. **Stuxnet** is a recent worm that well emphasizes the strong technical advances achieved by the attackers' community. It was discovered in July 2010 and firstly affected Iranian nuclear plants [2]. Stuxnet compromises the regular behavior of the supervisory control and data acquisition (SCADA) system by reprogramming the code of programmable logic controllers (PLC). Once compromised, PLCs can progressively destroy a device (e.g., components of a centrifuge, such as the case of the Iranian plant) by sending malicious control signals. Stuxnet combines a relevant number of challenging features: it exploits zero-days vulnerabilities of the Windows OS to affect the nodes connected to the PLC; it propagates either locally (e.g., by means of USB sticks) or remotely (e.g., via shared folders or the *print spooler* vulnerability); it is able to modify its behavior during the progression of the attack, and communicates with a remote command and control server. More importantly, Stuxnet can remain undetected for many months [3] because it is able to fool the SCADA system by emulating regular monitoring signals.

The novelty of a Stuxnet-like *attack model* is the impairment of the **monitoring and control system**, which plays a critical role to ensure proper operations of a variety of systems, including industrial processes/plants, smart grids [4], and data centers of a grid- or cloud-computing infrastructure. Attacking a SCADA system can definitively lead to severe consequences, both economical and societal. For example, what if an attacker overloads a power distribution system by breaking into a power grid? What if environmental sensors of a cloud facility are maliciously compromised? Stuxnet has shown that SCADA systems are vulnerable to cyber attacks, and that attackers may physically damage critical infrastructures in the near future. Nevertheless, it is hard to tell whether there is a real chance to fully secure a SCADA system: as for regular computer systems, the variety of monitoring and control hardware/ software components (e.g., sensors, actuators, OSs, PLCs management tools) is inherently vulnerable because of residual exploits, intentional misuse, or bad operator practices (such as plugging in an infected media or writing down a password).

This work discusses the role of **diversity** as a mean towards secure monitoring and control. The intuition underlying the proposal is that diversity can be leveraged to raise the effort it takes to conduct a successful attack (in terms of attack resources and time) *to such a level so as to make it pointless to attempt an attack at all*. For example, let us consider an attack that requires compromising two machines in order to be successful. If the machines are identical, it suffices to compromise one machine and then repeating the exploit for the other, i.e., the chance of a successful attack P_{SA} to the system is related to the chance of compromising just one machine ($P_{SA} \approx P_M$). When the machines are different, P_{SA} is smaller because it becomes somewhat related to chance of compromising each machine *separately* (i.e., $P_{SA} \approx P_{M1} \times P_{M2}$): succeeding is harder and time-consuming. Diversity is not used here to replicate components. We claim that a monitoring and control system, when possible, can smartly combine diverse technologies to significantly increase the effort to conduct a successful attack. Key aspects, issues and future research directions are briefly discussed in the following.

II. Assessing the Impact of Diversity

Diversity is a valuable mean to achieve the mentioned objective; however, the complex nature and dynamics of Stuxnet-like attacks make it difficult to assess the actual impact of diversity from a cyber security perspective. We propose a three-step attack modeling and evaluation approach *(i)* to identify the components that can be potentially diversified in a given SCADA system, and *(ii)* to evaluate to what extent a given diversity degree can actually impact the effort it takes to fulfill an attack. The proposal drives a balanced approach between secure system design and diversification costs. Fig. 1 depicts the steps of the proposed modeling and evaluation approach.

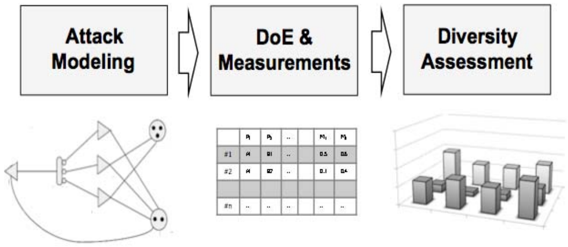

Figure 1. Proposed modeling and evaluation approach.

The goal of the proposal is to estimate how a set of **security-oriented indicators** varies when diverse HW/SW components are used in the system. Example of security indicators are: *(i) Time-To-Attack*, i.e., the time between the beginning and completion of an attack; *(ii) Time-To-Security-Failure* [5], i.e., the time between the beginning of the attack and the perceived attack manifestation; *(iii) compromised ratio*, i.e., the number of compromised components at time *t* with respect to the total number of components. Key characteristics of each step are:

- **Attack Modeling**. Progression of an attack, in terms of the stages the attack undergoes before success (e.g., *initial*, *activated, root access, network propagation, device impairment*) is formalized by means of a model. Potential modeling approaches include, for example, Bayesian networks, Petri-nets, or attack trees. For each stage, we identify the system HW/SW components (e.g., OS, firewall, programs, devices) that impact the probability of the attack to move to the next progression stage. For example, the chance to accomplish the sample *root access* stage may depend on the underlying OS version; similarly, the *device compromise* stage might be harder to fulfill if the device targeted by the attack is someway resilient to malicious control signals.
- **Design of Experiments (DoE) & Measurements**. We assess security indicators when diverse components are introduced in the system. Impact of diversity is emulated by varying the success probabilities involved at each attack stage. For instance, the *root access* stage might have a success probability P_1 when operating system OS_1 is used, or P_2 in case OS_2 is used ($P_1 \neq P_2$). Probability values reflect the availability of tools and/or exploits that can be leveraged to accomplish a given stage. Probability values are established either by means of previously documented attack history, or by emulating malware samples in a controlled environment (e.g., *honeypots*), or by performing a sensitivity analysis. Given the large number of HW/SW components that can be potentially diversified in a real system, the choices of probability values and related combinations, measurement of security indicators is driven by a DoE approach. DoE allows narrowing the number of configurations to assess. Security indicators are measured by running the attack model against each configuration identified by means of DoE.
- **Diversity Assessment**. In this step it is assessed how the adoption of diverse components impacts security indicators. To this aim, we plan to use ANalysis Of VAriance (ANOVA) techniques, which make it possible to allocate the variability of the security indicators (measured across the different system configurations established in the previous step) to the component(s) responsible for such variability. This step allows identifying the system HW/SW components that impact security indicators, and thus valuable to diversify in the real system implementation.

We are in the process of instantiating the proposed framework to assess the resilience against Stuxnet-like attacks of the cooling system of the SCoPE data center at the Federico II University of Naples (www.scope.unina.it). A system model encompassing control/monitoring nodes and PLCs has been developed by means of the stochastic activity networks (SAN) formalism. A preliminary sensitivity analysis indicates that the use of a small, strategically distributed, number of highly attack-resilient components can significantly lower the chance of bringing a successful attack to the system.

III. Conclusions and Future Work

We discussed the principles underlying a modeling and evaluation approach conceived to support a diversity-based design for more secure monitoring and control in a distributed system. We aim to improve the approach both from the attack- and system-perspective by introducing a wider set of threat models, such as Duqu and Flame, and by modeling the impact of a wider set of components, e.g., sensors, actuators, firewall. The approach will be used to assess and improve attack-resiliency of real-world critical infrastructures.

Acknowledgments

This work has been supported by the TENACE PRIN Project (n. 20103P34XC) and by the MINIMINDS PON Project (n. B21C12000710005) funded by the Italian Ministry of Education, University and Research.

References

[1] C. Leita, “A data-driven approach to generate threat intelligence”, Talk at Hot Topics in Secure and Dependable Computing for Critical Infrastrucutres, SDCI 2012

[2] N. Falliere, L. O. Murchu, E. Chien, “W32.Stuxnet Dossier”, Symantec Security Response, 2011

[3] A. Kolesnichenko, P. de Boer, A. Remke, E. Zambon, B. R. Haverkort, “Is Quantitative Analysis of Stuxnet Possible?”, QEST: Fast Abstracts, 2011

[4] “Guidelines for Smart Grid Cyber Security”, Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. NIST Report, 2010

[5] B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, K.S. Trivedi, “Modeling and Quantification of Security Attributes of Software Systems”, Int’l Conf. on Dependable Systems and Networks, 2002