2014 Asia-Pacific Services Computing Conference

False Logic Attacks on SCADA Control System

Weize Li, Lun Xie*, Daqian Liu, Zhiliang Wang
School of Computer and Communication Engineering
University of Science and Technology Beijing
Beijing, China
Correspondence Author: xielun@ustb.edu.cn

***Abstract*—A cyber security incident in SCADA systems can cause the disruption of physical process, and may result in significant economic loss, environmental disasters or even human casualties. To exploit the feature of the physical process and find the potential attacks, this paper presents and analyzes a new class of cyber-physical attacks, named false logic attacks, against the logic of control process in SCADA systems. In addition, it proposes a model for false logic attacks, which is useful for analyzing how attacks can affect the physical system. An experiment is performed to illustrate the concepts, and the effect of false logic attacks are also discussed.**

Keywords—SCADA; security; cyber-physical attack; false logic attack

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems have been widely used to continuously monitor and control physical processes in modern Critical Infrastructures (e.g., power plants, water plants, smart grids, etc.) [1], and their secure operations are therefore of paramount importance to national security, public safety and economic vitality [2]. In this paper, the focus is on the interaction between cyber security and the physical process controlled by the SCADA system.

A. SCADA Cyber-Physical Security

SCADA systems are usually composed of a set of networked devices, such as sensors, actuators, controllers and communication devices, and their fundamental materials about the components and network topologies can be found in [3]. SCADA systems gather real-time data from remote units and issue commands to remote stations or field devices to control the physical process, following the elaborate strategies. Based on this, a cyber security incident in them can cause the disruption of physical systems, and may result in significant economic loss, environmental disasters or even human casualties. The goal of this paper is to exploit the feature of the physical process and find the potential cyber-physical attacks, which can disrupt the control process or damage the physical system by cyber assaults.

The control process in SCADA system can be thought of as a combination of parameter values, execution time and sequential logic. Lots of research has been done on security analysis of parameter values in SCADA systems, such as data integrity attacks [4]-[9], which modify output values of sensors or input values of actuators within acceptable limits. The main motivation behind our work is the observation that a highly-skilled attacker can utilize the sequential logic of the control, and achieve his aim of disrupting the physical process before the intrusion is detected. Taken this possibility into consideration, we present a potential class of cyber-physical attacks on SCADA control system, named false logic attack.

B. Related Work

There have been some similar studies. Bigham et al. [10] introduced an approach to build up a normal model of SCADA data by looking for invariants between the different data readings. However, the approach focused on the mathematical relationships. Carcano et al. [11]-[13] described a kind of attack composed of a set of commands, which are licit when considered in isolation on a single-packet basis. It can disrupt the correct behavior of the system when executed in particular operating states. Mitchell and Chen [14]-[16] considered the attacks that violated the behavior rules of different components, which have state constraints between each other at runtime. Yang et al. [17] proposed a correlation detector based on this consideration that the switching state of a specific device correlates with relevant measured values. These prior studies all consider the constraints or interactions between different system state variables. However, unfortunately, there is no discussion about the execute logic of control commands. Based on the prior work cited above, the state constraints of different components and sequential logic of commands are both considered in our work.

C. Contributions and Outline

The paper proposes a model for false logic attacks, which is useful for analyzing how attacks can affect the physical system, and describes an example scenario that illustrates the feasibility and effect of false logic attacks. The main contribution of this paper is that we exploit the sequence logic feature of the control process in SCADA system, and present a new type of potential threats, namely false logic attacks.

The paper is organized as follows. A description of false logic attacks is introduced in Section II, while the feasibility of attacks is discussed in Section III. Then, a model of false logic attacks is provided in Section IV., and attack experiments are presented in Section V. Finally, the paper concludes in Section VI.

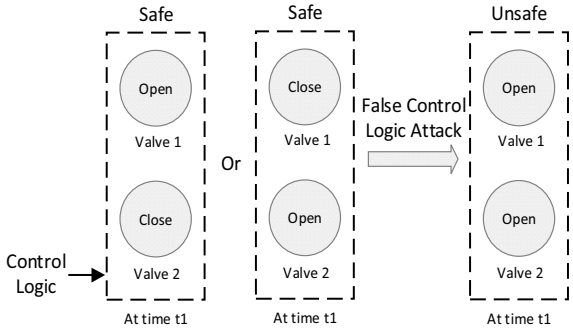
978-0-7695-5381-8/14 $31.00 © 2014 IEEE
DOI 10.1109/APSCC.2014.27

II. FALSE LOGIC ATTACKS

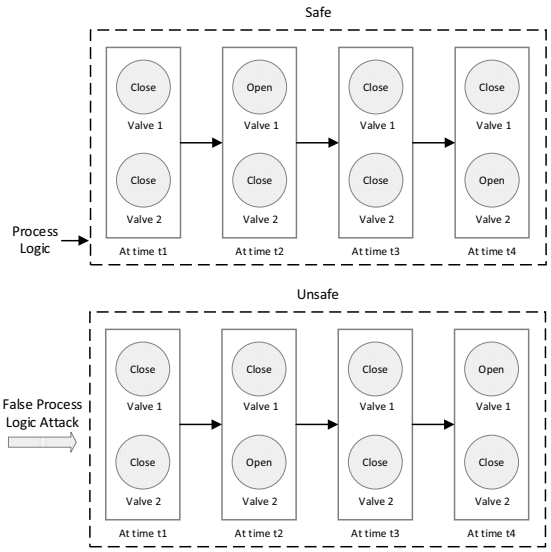
When we take into account the "false", it can be classified into two kinds: (1) the incorrect data value; and (2) the incorrect execution logic of control commands. The former is what the false data injection attacks [18] concentrate on, and the latter is what the false logic attacks focus on.

To be specific, we consider two modes of false logic attacks on SCADA systems: the false control logic attack and the false process logic attack. We define the control logic as a constraint relationship between different system components at some point, and the process logic as a constraint relationship between the control logic at some point and the next. Both of the two attacks are based on licit control commands, and can be able to disrupt the system operations and influence the physical process.

In order to simplify the problem, we only consider the binary parameters of actuators in this paper, such as the switching state. For example, valve open and close commands are common in SCADA systems. When considered in isolation on a single-command basis, open and close are both licit for a valve. However, it is not true for two or more valves, especially when there are logic constraints be-tween each other. For example, there are two valves (valve 1 and valve 2). The two constraint conditions for them are: (1) they cannot both be in open state, and (2) valve 1 should be open before valve 2. The false control logic attack and the false process logic attack on two valves are respectively illustrated in Fig.1 (a) and Fig.1 (b). The violation of constraint conditions can drive the physical system into an unsafe state.



(a)



(b)

Figure 1. Examples of two modes of the logic attack. (a) The false control logic attack. (b) The false process logic attack.

III. FEASIBILITY OF ATTACK

In the past, SCADA systems were believed to be secure because they used proprietary protocols and isolated networks [19]. Nowadays they are at high risk of cyber threats for two reasons: 1) With the increase of interconnected devices, their vulnerabilities [20] are exposed and available to highly-skilled attackers [7]; 2) The use of standard hardware and software components makes traditional security vulnerabilities and attack methods target SCADA systems too [21].

There have been some confirmed cases of attacks [22] and incidents [23] on SCADA systems, such as "Stuxnet", "Duqu" and "Flame". The Stuxnet worm is a good case as a proof of concept that physical devices controlled by SCADA systems can also be controlled by adversaries. The experiments for three stealthy attack scenarios have been performed in a secure control systems testbed [24]. The results show that it is feasible for an attacker to modify the control actions or sensor measurements from their real values to the corrupted signals. So it is also possible for the attacker to disrupt the sequence logic of physical process under control.

To implement a false logic attack on SCADA control system, there are two basic requirements:

1) The requirement for physical process

- There are two or more control components (e.g., switches, relays, valves, etc.) constraint with each other.
- The control commands or system states are finite in number.
- The control process is periodic.
- The controlling operations are with strict sequence requirement.

- The control flow in the network can be regarded as a representation of the evolution of the system.

2) The requirement for the attacker

- The intent of the attacker is to disrupt the physical process or damage the physical devices.
- The attacker gets sufficient knowledge and background information, such as the system topology, and is able to alter the data exchanged between the plant and the controller in networked control system.

IV. MODELING FALSE LOGIC ATTACKS

A. System Model

In a simplified SCADA control system [5] as shown in Figure 2, sensing data and control data are both critical to the stable operation of physical system. However, the latter play a decisive role and have a direct impact on the physical process. Therefore, in this paper we only consider the control data, specific the binary parameters of actuators. It is also important to study other types of parameters, but we leave this for future work.

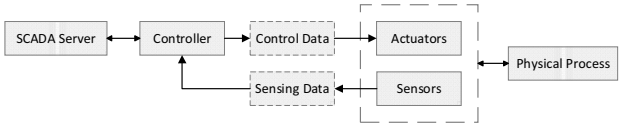


Figure 2. Simplified Control Model of SCADA Systems

The physical process is modeled by a 4-tuple:

$$P = (A, V, E, R) \tag{1}$$

where

- $A = \{a_1, ..., a_n\}$ is a finite set of actuators, which have binary parameters, such as a switch, a valve or a relay, and there are constraints between each other.
- $V = \{V(a_1), ..., V(a_n)\}$ is a finite state set of actuators, where $V(a_i) = \{0, 1\}$ for every $i \in \{1, ..., n\}$.
- $E = \{e_1^n, ..., e_m^n\}$ is the finite set of all the observations, and each observation $e_i^n = (V_i(a_1) \ ... \ V_i(a_n))^T$ corresponds to a stable state of the actuators, namely the control logic we have defined. The $i \in \{1, ..., m\}$ is the index representing the observation sequence of a given process cycle of the system.
- $R = \{r_1, ..., r_m\}$ is a finite set of transition relation. For each e_i^n, $i \in \{1, ..., m-1\}$ in E, there is a r_i in R. $r_i = \langle e_i^n, e_{i+1}^n \rangle$ denotes the transition from e_i^n to e_{i+1}^n, namely the process logic we have defined. Note that the considered control process is cyclic, then there is a transition $r_m = \langle e_m^n, e_1^n \rangle$.

All the modeling work described above is based on the assumption that the control process has not yet been attacked, and all the observed sequences can be regarded as a representation of the normal system behavior.

B. False Logic Attack Model

There are two kinds of false logic attacks defined. A false control logic attack and a false process logic attack. Let $V_t(a_i)$ be the control state of actuator i at time t. A false control logic attack vector $\tilde{e}_t^n$ is defined as

$$\tilde{e}_t^n = \left(V_t(a_1) \ ... \ \tilde{V}_t(a_i) \ ... \ V_t(a_n)\right)^T \tag{2}$$

where

$$\tilde{V}_t(a_i) = \begin{cases} V_t(a_i) & for\ t \notin T_a \\ \sim V_t(a_i) & for\ t \in T_a \end{cases} \tag{3}$$

and when $t \in T_a$, $\tilde{e}_t^n \notin E$. $T_a = [t_s, t_e]$ denotes the duration of the attack, t_s and t_e are the start time and end time respectively.

A false process logic attack is described by

$$\tilde{r}_t = \langle e_i^n, e_t^n \rangle, \quad e_i^n \in E \tag{4}$$

with

$$e_t^n = \begin{cases} e_{i+1}^n & for\ e_{i+1}^n \in E, t \notin T_a \\ e_j^n & for\ j \neq i+1, e_j^n \in E, t \in T_a \end{cases} \tag{5}$$

In brief, a false control logic attack is performed by injecting illegal control logic states, and a false process logic attack is launched by modifying the order of legal control state sequences. In the next section, an experiment has been done to illustrate the two false logic attacks.

V. 5 EXPERIMENTS AND RESULTS

To test the attacks, we setup an experiment platform. As shown in Fig.3, there are three switches and all of them are controlled by a Programmable Logic Controller (PLC), which uses PROFINET as its communication protocol to the SCADA server. Commands are issued by the SCADA server to the PLC according to a simple control strategy of the switches. In order to mimic the behavior that attacks net-work devices, we construct a Cortex-A8 based appliance, which is located proximal to the PLC and used to intercept packets and modify the control commands of switches.

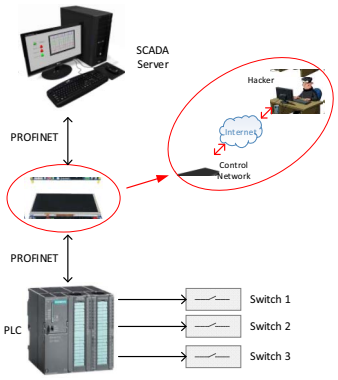


Figure 3. System diagram of the experiment platform

Using the notation presented in part IV, the three switches can be donated by $A=\{s_1, s_2, s_3\}$. Because of the control strategy, the normal sequence is

$$E=\{e_1^3, e_2^3, e_3^3, e_4^3, e_5^3, e_6^3\}=\left\{\begin{pmatrix}0\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$$

where 0 and 1 mean the open and closed state of switches respectively, and the transition set is

$$R=\{r_1, r_2, r_3, r_4, r_5, r_6\}$$
$$=\{\langle e_1,e_2\rangle,\langle e_2,e_3\rangle,\langle e_3,e_4\rangle,\langle e_4,e_5\rangle,\langle e_5,e_6\rangle,\langle e_6,e_1\rangle\}$$

Consider the false control logic attack vector $\tilde{e}_3^3=(1\,0\,1)^T$ and the false process logic attack vector $\tilde{r}_2=\langle e_2^3, e_5^3\rangle$, Fig.4 provides a clear picture of the observations without attack and with attacks.

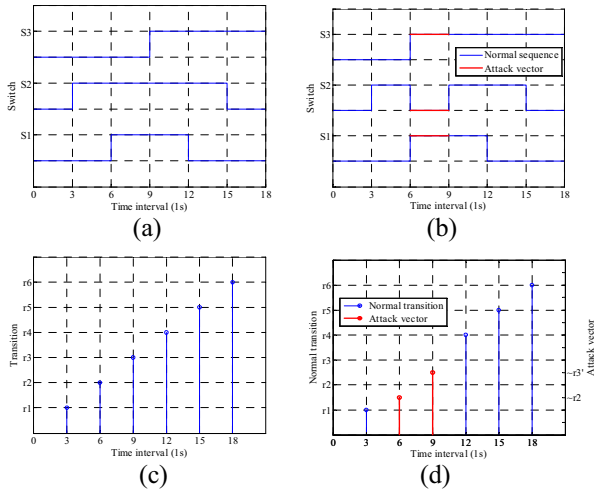


Figure 4. Observations of the switching state without attack and with attacks. (a) Normal control logic. (b) With false control logic attack. (c)Normal process logic. (d) With false process logic attack.

It is shown that a false control logic attack can violate the constraint conditions in a short period of time, and a false process logic attack will result in a secondary effect $\tilde{r}_3^{'}=\langle e_5^3, e_4^3\rangle$. The neglect of such abnormal status may ultimately lead to a serious accident. The two attacks can be stealthy before they achieve their goals. However, unfortunately, even if the operator notices the abnormal state change in the SCADA server, the control process has been already disturbed.

VI. CONCLUSION

In this work, we have introduced the concept of false logic attack and discussed the feasibility. An attack model was proposed and two kinds of false logic attack was illustrated using an experiment platform. For the false logic attack is based on the licit commands, traditional Intrusion Detection System (IDS) is not able to effectively protect the physical process. Thus, there is a need for the sequence logic feature-based Intrusion Detection Systems (IDS) to keep the operation parameters under continuous monitoring. For future work, we intend to study the method of detecting false logic attack in SCADA control systems. Considering the actual situation, it is also interesting to extend the attack model by studying other types of control parameters.

ACKNOWLEDGMENT

This work is supported by National Key Technologies R&D Program of China (No. 2014BAF08B04), National Natural Science Foundation of China (No. 61170115).

REFERENCES

[1] M. Brundle and M. Naedele, "Security for process control systems: An overview", IEEE Security & Privacy, vol. 6, pp.24-29, November/ December 2008.

[2] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling", IEEE Trans. on Sys., Man and Cybernetics, Part A: Sys. and Humans, vol. 40, pp. 853-865, July 2010.

[3] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim—A framework for building SCADA simulations", IEEE Trans. on Smart Grid, vol. 2, pp. 589-597, December 2011.

[4] Y. L. Huang, A. A. Cárdenas, S. Amin, Z. S. Lin, and H. Y. Tsai, et al., "Understanding the physical and economic consequences of attacks on control systems", Int. J. of Critical Infrastructure Protection, vol. 2, pp. 73-83, October 2009.

[5] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system", 2010 IEEE Power and Energy Society General Meeting, pp. 1-6, July 2010.

[6] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid", 2011 IEEE Power and Energy Society General Meeting, pp. 1-6, July 2011.

[7] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, and C. Y. Huang, et al., "Attacks against process control systems: risk assessment, detection, and response", Proc. of the 6th ACM symp. on inf., computer and commun. security, pp. 355-366, March 2011.

[8] Y. L. Mo, R. Chabukswar, and B. Sinopoli, "Detecting Integrity Attacks on SCADA Systems", IEEE Trans. on Control Sys. Technol., vol. 22, pp. 1396-1407, July 2014.

[9] A. P. Premnath, J. Y. Jo, and Y. Kim, "Application of NTRU Cryptographic Algorithm for SCADA Security", 2014 11th Int. Conf. on Inf. Technol.: New Generations, pp.341-346, April 2014.

[10] J. Bigham, D. Gamez, and N. Lu, "Safeguarding SCADA systems with anomaly detection", Computer Network Security, 2003, pp. 171-182.

[11] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, "State-based network intrusion detection systems for SCADA protocols: a proof of concept", Critical Inf. Infrastructures Security, 2010, pp. 138-150.

[12] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera, "Modbus/DNP3 state-based intrusion detection system", 2010 24th IEEE Int. Conf. on Advanced Inf. Networking and Appl., pp. 729-736, April 2010.

[13] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, and I. N. Fovino, et al., "A multidimensional critical state analysis for detecting intrusions in SCADA systems", IEEE Trans. on Ind. Inf., vol.7, pp. 179-186, May 2011.

[14] R. Mitchell and I.R. Chen, "Behavior rule based intrusion detection for supporting secure medical cyber physical systems", 2012 21st Int. Conf. on Computer Commun. and Networks, pp. 1-7, July/August 2012.

[15] R. Mitchell and I.R. Chen, "Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications", IEEE Trans. on Smart Grid, vol. 4, pp. 1254-1263, September 2013.

[16] R. Mitchell and I.R. Chen, "Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications", IEEE Trans. on Sys., Man, and Cybernetics: Sys., vol. 44, pp. 593-604, May 2014.

[17] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, and E. G. Im, et al., "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks", IEEE Trans. on Power Delivery, vol. 29, pp. 1092-1102, June 2014.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids", ACM Trans. on Inf. and Sys. Security, vol. 14, pp. 13, May 2011.

[19] R. R. R. Barbosa, and A. Pras,"Intrusion detection in SCADA networks", Mechanisms for Autonomous Management of Networks and Services, 2010, pp. 163-166.

[20] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks", Computers & Security, vol. 25, pp. 498-506, October 2006.

[21] I. Garitano, R. Uribeetxeberria, and U. Zurutuza, "A review of SCADA anomaly detection systems", 2011 6th Int. Conf. on Soft Computing Models in Ind. and Environ. Appl., 2011, pp. 357-366.

[22] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems", 2011 Int. Conf. on Internet of Things and 4th Int. Conf. on Cyber, Phys. and Social Computing, 2011, pp. 380-388.

[23] B. Miller and D. Rowe. "A survey SCADA of and critical infrastructure incidents", Proc. of the 1st Annual conf. on Res. in inf. Technol., 2012, pp. 51-56.

[24] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems", Proc. of the 1st int. conf. on High Confidence Networked Sys., 2012, pp. 55-64.