Research Journal of Applied Sciences 10 (8): 407-410, 2015
ISSN: 1815-932X

Probability Analysis of Critical State of Production Network Based on Simplified Model for Connection Between Enterprise Network and Production Network

[1]Jaroslav K. Smirnov, [1]Viktoria I. Halimon, [1]Oleg V. Prostitenko,
[2]Igor S. Konstantinov, [2]Sergej A. Lazarev and [2]Konstantin A. Rubcov
[1]St. Petersburg State Technological Institute (Technical University),
Moskovsky Prospect 26, 190013 Saint-Petersburg, Russia
[2]Belgorod State University, Pobedy St. 85, 308015 Belgorod, Russia

Abstract: The integration of the corporate resource planning systems in industrial networks requires connection of the network infrastructure of the production network to the network infrastructure of the corporate network. The main objective of this study is focusing attention on the danger of use of the standard methods with the use of firewalls for organization of the production network protection as well as comparison of probabilities of emergence of the system critical states in respect of the three connection options: without additional protection with the use of a firewall and with implementation of the proprietary two-layer concept.

Key words: PLC, production networks security, ERP, IDMZ, infrastructure

INTRODUCTION

Integration of the ERP (Enterprise Resource Planning) systems requires connection of the corporate network to the production network or an enterprises (Khalimon and Smirnov, 2014). At that for the branches of industry with advanced requirements to reliability of the data obtained (such as pharmaceutical one) such connection may be extremely dangerous as it may affect the quality of the product on which in its turn a human life depends (Akimova, 2007).

PROCEDURE

The problems arising by connection of the corporate and production networks of an enterprise are described in details in the study (Khalimon and Smirnov, 2014). This is why in this study, only the main of them are outlined:

- The necessity of compliance with the GMP (Good Manufacturing Practice) requirements as the result the necessity of validation and complicated system commissioning
- The virus threat of the Programmable Logic Controller (PLC)
- Incorrect PLC operation as the result of errors in the system design
- Critical vulnerabilities in the PLC of the production lines
- The necessity of the 'deep' integration with the production lines PLC due to the data limitation in the SCADA (Supervisory Control and Data Acquisition) systems
- Organization of the data synchronization system

The methods of connection, their advantages and disadvantages are specified in the study (Khalimon and Smirnov, 2014). Possible methods of connection:

- Connection ignoring the safety issues where the industrial equipment is combined into a single sub-network that is connected to the corporate network without additional safety measures
- A safe technology with the use of DMZ (Demilitarized Zone) ensuring limitation of the network traffic through a firewall executed on the basis of the standard network equipment
- A safe topology proposed by the researchers of the study on the basis of a PLC and a gateway that arranges the transferred traffic and the volume of information, so that the gateway organization may be described as two-player

MAIN PART

The CISCO company offers a safe technology with the use of DMZ that may include a few firewalls at different network levels. However, such solution does not make the topology to be two-layer, since the equipment and the software of firewalls are similar, therefore, the

Corresponding Author: Jaroslav K. Smirnov, St. Petersburg State Technological Institute (Technical University), Moskovsky Prospect 26, 190013 Saint-Petersburg, Russia

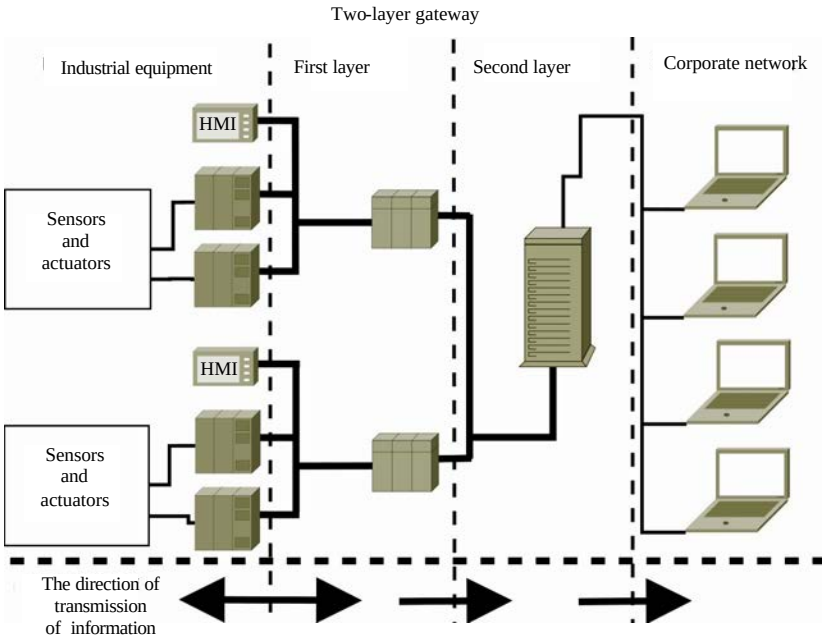

Fig. 1: The structure of the two-layer data gateway

methods of attacks are similar, too (Konstantinov *et al*., 2014; Anonymous, 2008). The structure of a two-layer data gateway is presented in Fig. 1.

The first gateway layer is the PLC that is in charge of the collection of data from the industrial equipment. Depending on the tasks solved a few PLCs may be used for data collection.

The second layer of two-layer architecture is the server with an operating system on the basis of the Linux core. For organization of collection, processing and transmission of data by this server the software complex 'Instrumental system of the data processing and transmission from the production equipment to the corporate network' (ICAT) has been designed. This software allows creating drivers for the equipment used at the first layer and running the data processing algorithms. The data transmission is initiated by the server which ensures efficient safety. Limitation of data transmission between the second layer and the corporate network is set at the level of the core component netfilter with the use of iptables application (Yang, 2007).

Let's consider the model used for comparison of the proposed architectures. The model of estimation of the probability of emergence of the critical system state is provided in the study (Khalimon and Smirnov, 2014). Within this study, it was decided to change this model a little. Let's consider the system status as a Markoff process with a discrete state and continuous time (Ventzel, 1991; Imamverdiyev, 2014).

For the sake of simplicity, we assume that the probability by the target attack of the industrial equipment is identified. Based on this assumption it is accepted that the industrial equipment is always in the conditions of a target attack. The resulting state matrix is presented by Eq. 1:

$$S = \{S_1 \quad S_2 \quad S_3\} \tag{1}$$

Where:

S_1 = Normal operation of the corporate network

S_2 = The corporate network is hacked, i.e., unauthorized access to one or more computers of the corporate network was gained

S_3 = The node connecting the production and corporate networks is hacked, i.e., the unauthorized access to the production network equipment was gained which is critical and may affect the quality of the output product

For this state model the transition matrix may be constructed. This matrix is presented by Eq. 2:

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} \tag{2}$$

Where:

P_{11} = Vulnerabilities in the corporate network not found

P_{12} = Hacking of the corporate network by intruders

P_{13} = Third-party virus in the production network of an enterprise

P_{21} = Elimination of vulnerability in the corporate network of an enterprise

P_{22} = Persistence of vulnerability in the corporate network of an enterprise
P_{23} = Breaking of equipment connecting the corporate and the enterprise networks
P_{31} = Elimination of vulnerability in the corporate network
P_{32} = Elimination of vulnerability in the equipment connecting the corporate and the enterprise networks
P_{33} = Persistence of vulnerability in the enterprise network

The calculation of probabilities for the presented systems will be performed on the basis of the model for different methods of connection of the production network to the enterprise network. In the case if the connection model without additional safety measures is used the presented model degenerates into the two states since no auxiliary equipment ensuring separation from the industrial equipment is available. For this system the state matrix is presented by Eq. 3:

$$P_{NAIVE} = \begin{pmatrix} 1-P_{inj1} & P_{inj1} & 0 \\ 0 & 0 & 1 \\ P_{fix1} & 0 & 1-P_{fix1} \end{pmatrix} \quad (3)$$

Where:
P_{inj1} = Identifying vulnerability in the corporate network
P_{fix1} = Elimination of vulnerability in the corporate network

For the model proposed by the CISCO Company (the method of connection to a firewall) direct penetration of a virus in a computer of the corporate network does not result in failures in the equipment operation. For this system the state matrix corresponds to Eq. 4:

$$P_{CISCO} = \begin{pmatrix} 1-P_{inj1} & P_{inj1} & 0 \\ P_{fix1} & 1-P_{fix1}-(P_{BD2}+P_{HE2}-P_{BD2}\times P_{HE2}) & P_{BD2}+P_{HE2}-P_{BD2}\times P_{HE2} \\ P_{fix1} & P_{fix2} & 1-P_{fix1}-P_{fix2} \end{pmatrix} \quad (4)$$

Where:
P_{inj1} = Identifying vulnerability in the corporate network
P_{fix1} = Elimination of vulnerability in the corporate network
P_{fix2} = Elimination of the firewall vulnerability
P_{BD2} = Embedding of vulnerability by the firewall producer
P_{HE2} = Human error by setting of the firewall

In case of the model of the two-layer connection gateway proposed by the researchers as well as the model proposed by CISCO, the direct penetration of a virus in a computer of the corporate network does not result in failures in the equipment operation. For this system, the state matrix is presented by Eq. 5:

$$P_{DL} = \begin{pmatrix} 1-P_{inj1} & P_{inj1} & 0 \\ P_{fix1} & 1-P_{fix1}-P_{VUL2}\times P_{GW2} & P_{VUL2}\times P_{GW2} \\ P_{fix1} & P_{fix2} & 1-P_{fix1}-P_{fix2} \end{pmatrix} \quad (5)$$

Where:
P_{inj1} = Identifying vulnerability in the corporate network
P_{fix1} = Elimination of vulnerability in the corporate network
P_{fix2} = Elimination of vulnerability in the production network
P_{VUL2} = Identifying vulnerability in the data collection PLC
P_{GW2} = Gateway vulnerability

The numerical evaluation of the designed model was performed. Based on the report provided by the company positive technologies, the probability of identification of vulnerability in the corporate network ensuring total control over the infrastructure makes 50%, P_{inj1} (Anonymous, 2013, 2014).

Based on these assumptions and the information presented in (Tsibulevsky, 1977; Gertman, 2004; Reason, 2000), it was accepted that P_{HE2} = 5.8/23.5%, P_{BD2} = 15% and P_{GW2} = 15%. At the same time, it is impossible to adequately estimate the probability of appearance of back doors in the network equipment as legislation of some countries obliges to embed them in the equipment which may be taken into account by the attempt of the unauthorized access (Cross, 2014).

The vulnerabilities known to PLC Siemens used for the system design are not critical to this architecture. The vulnerabilities detected for S7-1200 have been eliminated (Siemens, 2011). In this case, P_{VUL2}≈5%. In the study (Ponomarev, 2008) for estimation of the probability of the vulnerability elimination the following assumption for proposed: the probability of the vulnerability emergence is equal to the probability of the vulnerability elimination. This assumption has been taken into account in this research. Thus, the following transition matrices were obtained:

$$P_{NAIVE} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0 & 0 & 1 \\ 0.5 & 0 & 0.5 \end{pmatrix}$$

Table 1: Probabilities of occurrence of the critical state of the system designed

Method of connection	S_1	S_2	S_3
System without safety measures	0.4	0.2	0.4
CISCO option	0.5	0.39-0.35	0.11-0.15
Two-layer connection gateway	0.5	0.498	0.002

$$P_{CISCO} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.3 \div 0.15 & 0.2 \div 0.35 \\ 0.5 & 0.2 \div 0.35 & 0.3 \div 0.15 \end{pmatrix}$$

$$P_{DL} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.496 & 0.0025 \\ 0.5 & 0.0025 & 0.4975 \end{pmatrix}$$

The calculation of probabilities for the obtained transition matrices was performed with the use of the Kolmogorov equation (Ventzel, 1991; Imamverdiyev, 2014). The final probability of transition into a critical state is presented in Table 1.

SUMMARY

The study provides the analysis of occurrence of a critical state according to the simplified model of the safe connection of the industrial equipment information system to the corporate system of an enterprise. The danger of use of the standard methods of the firewall application in the network infrastructure of a corporate network has been proved. Based on the results of calculations the conclusion as to applicability of the two-layer connection gateway ensuing maximum safety may be drawn.

CONCLUSION

Based on the calculations, it may be concluded that the model of connection without additional safety measures is not applicable for enterprises requiring the low risk of occurrence of a critical state. At the same time, the model proposed by the study, researchers surpasses the model proposed by CISCO and may the recommended for use at the pharmaceutical and other critical enterprises.

REFERENCES

Akimova, G.P., 2007. Methodological Approach to the Determination of Effect of the Human Factor on the Performance of Information Systems. ISA RAN, 29: 102-112.

Anonymous, 2008. Cisco Systems and Rockwell Automation. Ethernet-to-the-Factory 1.2 Design and Implementation Guide. San Jose, Milwaukee.

Anonymous, 2013. Positive Technologies. Statistics of vulnerabilities of the corporate information systems for the years 2011-2012. Moscow: Positive Technologies.

Anonymous, 2014. Positive Technologies. Statistics of vulnerabilities of the corporate information systems (2013). Moscow: Positive Technologies.

Cross., 2014. Exploiting Lawful Intercept to Wiretap the Internet, pp: 18.

Gertman, B., 2004. Human Error and Available Time SPAR-H. Workshop on Temporal Aspects of Work for HC1.

Imamverdiyev, Y.N., 2014. The GM (1,1) Markoff model for forecasting the software vulnerabilities. Issues of Information Technologies, pp: 26-37.

Konstantinov, I., J. Chashin and S. Lazarev, 2014. Simulation of the Software-defined Network for a high-performance computing cluster. J. Res. App. Sci., 9 (10): 704-706.

Khalimon, V.I. and Y.K. Smirnov, 2014. The Model of the Reliable System of Connection of the Production Equipment to the Corporate Network for a Pharmaceutical Enterprise. The Bulletin of the St. Petersburg of the State Technological Institute (Technical University), 26 (52): 95-101.

Ponomarev, A.A., 2008. Topical Issues of the Information Technologies Safety. Solution of the Task of the Estimation of the Time of the Data Protection System Penetration, Krasnoyarsk.

Reason, J., 2000. Human Error: Models and Management. BMJ, 320: 768-770.

Siemens, A.G., 2011. Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU. Siemens Security Advisory: SIEMENS-SSA-625789.

Tsibulevsky, I.E., 1977. Failing Responses of a Human Operator in a Control System. Automatics and Tele Mechanics, 6: 112-144.

Ventzel, E.S., 1991. Theory of Random Processes and Engineering Applications Thereof. Moscow: "Nauka", pp: 128-141.

Yang, G., 2007. Research on Linux firewall based on Netfilter/Iptables. Computer Engineering and Design, 17: 22.