Cybersecurity Threats to P&C Systems

Yuly Bay[1, a)], Yana Malkova[1, b)] and Anna Buran[1, c)]

[1]*National Research Tomsk Polytechnic University, 634050 Tomsk, Russia.*

[a)]Corresponding author: tbf@list.ru
[b)]yamalkova96@gmail.com
[c)]aburan@tpu.ru

Abstract. Vulnerabilities introduced into the hardware and software by P&C system manufacturers are typically difficult for the EPU's P&C engineers to discover and patch. The most common cybersecurity flaw is a vulnerability that provides the means to inject malicious code into the P&C system software. The primary reason to consider this type of attack is that it can allow an individual to bypass the access control restrictions set by the developer or EPU's P&C engineer. P&C system engineers should review all wireless remote access to the P&C system. Depreciate wireless access using WEP encryption and their interface to the P&C system network declared "untrusted". Lastly, P&C managers should not view these vulnerabilities of P&C assets independently as a successful cyber-attack typically involves exploitation of a chain of vulnerabilities present on various assets. Consequently, there is a need to model and analyze the entire sys-tem-of-systems to estimate the relative security of a threat scenario.

INTRODUCTION TO DEVELOPMENT VULNERABILITIES

Vulnerabilities introduced into the hardware and software by P&C system manufacturers are typically difficult for the EPU's P&C engineers to discover and patch. The most common cybersecurity flaw is a vulnerability that provides the means to inject malicious code into the P&C system software [1].

The primary reason to consider this type of attack is that it can allow an individual to bypass the access control restrictions set by the developer or EPU's P&C engineer. For instance, to gain complete control of a protection relay from a remote location or to escalate user privileges to "administrator" on a protection relay. Typically, administrator privilege includes the capability to change the privileges of other users.

Code injection attacks can be realized as binary code injection attacks or source code injection attacks.

BUFFER OVERFLOW

A binary code injection attack involves insertion of malicious code in a binary program to alter how the program behaves, and is often carried out through buffer overflow [2].

A few reasons behind this are the lack of security awareness of the P&C system software developers and the great complexity of today's commodity software.

The consequence of successful buffer overflow attacks is typically denial of service or gained privileges.

CODE INJECTION

Code injection classes include the following vulnerabilities/weaknesses [3]:

1. cross-site scripting
2. SQL injection
3. LDAP injection
4. mail command injection

International Youth Scientific Conference "Heat and Mass Transfer in the Thermal Control System of Technical and Technological Energy Equipment" (HMTTSC 2019)
AIP Conf. Proc. 2135, 020013-1–020013-3; https://doi.org/10.1063/1.5120650
Published by AIP Publishing. 978-0-7354-1878-3/$30.00

5. null-byte injection
6. operating system commanding
7. path traversal
8. remote file inclusion
9. server side injection
10. extensible markup language (XML)
11. external entities
12. XML Injection
13. XQuery Injection

Source code injection attacks involve interaction with P&C system applications written in programming languages that do not require compilation; e.g. JavaScript, Hypertext (PHP) and Structured Query Language (SQL). Consequently, this attack type primarily concerns web applications. Common vulnerabilities of this category include cross-site scripting (XSS) and SQL injection [3]. XSS involves adding malicious JavaScript code to existing web applications which then enables any visitor (or visitor specified by the attacker) of the particular application.

VULNERABILITIES INTRODUCED DURING DEPLOYMENT AND MAINTENANCE

There can be various vulnerabilities introduced during the deployment and management of the P&C system that need attention. A common type of vulnerability concerns enabled software services that are either not utilized or are unknown to the P&C engineers responsible for the security of the P&C system.

Software functionality not utilized or is unknown to the P&C engineer is a problem as it can allow the attacker to compromise the P&C system. These types of services are often vulnerable because no one is concerned about them. An example of a service often employed. Another example of a service unknown to the P&C engineer could be a file transfer protocol (FTP) server that enabled to allow remote data access to P&C system files for a user, without consent from the P&C engineer.

REMOTE ACCESS TRUST ISSUES

P&C engineers, technicians and managers, including processes control, and the cybersecurity technology they use must declare transparent levels of trust for any exchange of data to take place. For this reason, the means used to configure and maintain P&C equipment such as IEDs, RTUs, or PLCs that are reachable from outside the substation need to be declared untrusted.

FIREWALL CONFIGURATION ERRORS

Assuming that the firewall within the substation is in a gateway or local area network (LAN) routers, appropriately configuring a firewall is a difficult task for the P&C engineer due to the complexity of the firewall rules [4]. This is a significant effort not only for deployment commissioning for site acceptance test (SAT), but for maintenance throughout the lifecycle of the substation automation system. If the firewall is at an external interface to the substation (for example, the control center or a remote engineering center), then configuring the firewall is not a P&C engineers responsibility. However, the P&C engineer must be confident that the firewall configuration is correct because of the trust invested in its security. To gain this confidence, SAT and maintenance testing should always include verification that the firewall configuration is correct. Regardless of where the firewall is located, frequent misconfigurations provide the means for an attacker to reach vulnerable P&C system components and their data.

INADEQUATE ACCESS CONTROLS

Poorly specified access controls can result in giving a P&C system user too many or too few privileges. For example, providing administrator access to an individual or to a group of individuals who should only have read-only access. Write access to change settings is a serious violation of security policies for access control. Overly restrictive access control can also result in problems due to services not properly shut down or sensitive credentials shared among personnel. P&C system engineers should routinely review who has what access control privileges and ensure they properly align with those privileges associated with their job role and responsibilities.

SOCIAL ENGINEERING

It is important to remember that a cyber-initiated attack does not need to involve malicious code. Successful cyber-fraud often happens due to critical P&C system information simply being (unknowingly) exposed without proper security awareness training [5]. P&C system engineers should be extremely cautious in their discussion with suppliers of P&C system technologies. It is far too common to get into deep technical discussion of how a new technology would improve the functional capability of the EPU's P&C system on a web-sponsored meeting or at a conference or workshop [5]. Routine awareness training updates will sharpen the P&C system engineer's sensitivity to social engineering security issues.

NETWORK TRAFFIC ANALYSIS AND MANIPULATION

An attacker that is able to listen to and record data in transit has the potential capability to conduct a number of different attacks. For in-stance, the attacker could replay previously sent messages and thus fool the system operators regarding the state of the power system. Or, the attacker could alter the message and resend them to execute a man-in-the-middle attack. P&C system engineers should review all wireless remote access to the P&C system. Depreciate wireless access using WEP encryption and their interface to the P&C system network declared “untrusted”. Lastly, P&C managers should not view these vulnerabilities of P&C assets independently as a successful cyber-attack typically involves exploitation of a chain of vulnerabilities present on various assets. For instance, many social engineering attacks involve emails containing links to websites with exploit kits. In essence, an attacker must accomplish two tasks:

1) social engineer personnel to access the link in the email, and
2) exploit a vulnerability in the web browser (often a buffer over-flow) of the connecting individual [5].

Consequently, there is a need to model and analyze the entire system-of-systems to estimate the relative security of a threat scenario.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Education and Science of the Russian Federation under the governmental grant “Science” No 13.5852.2017/8.9 (Development of the concept for comprehensive validation of calculating modes and processes in electric power system and tools of its realization).

REFERENCES

1. Ju. Thome, L. KhinShar, D. Bianculli and L. Briand, J. Syst. Softw. **137**, 766–783 (2016).
1. E. Leon and S. D. Bruda, Procedia Comput. Sci. **83**, 1301–1306 (2016).
2. N. Palsetia, G. Deepa, F. A. Khan, P. S. Thilagam and A. R. Pais, J. Syst. Softw. **122**, 93–109 (2016).
3. D. Li, H. Guo, J.Zhou, L. Zhou and J.W. Wong, Comput. Secur. **80**, 134–154 (2016).
4. F. Mouton and L. Leenen, Comput. Secur. **59**, 186–209 (2016).