Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 30-31, 2008

Vulnerability Test Framework for Ethernet based Network of Digital Control System

Oh Eung-Se, Yang Sung-Ok, Jung Chang-Kee
Korea Electric Power Research Institute, Munji-Ro 65,Yuseong, Daejeon, Korea 305-380
{esoh, lover, jck}@kepri.re.kr

1. Introduction

As an industry digital control system has become the more relied on network technologies, stakeholders of the system get more awareness and demand for secure and dependable communication system (CS) performance of their control system [1]. But, due to its complexity and un-interruptible mission, tests of the CS are typically performed at test-beds that physically and functionally replicate real system. This paper suggests practical test framework of vulnerability test for digital control system's CS which uses Ethernet technologies.

2. Vulnerability Test Process

In this section, generic test processes are described to test CS networks. Simplified DUT (Devices Under Test) and test devices setup scheme is shown in Figure 1. Pre-test condition and test coverage concerns are also described.

2.1 Test Setup

Before execute CS vulnerability test, DUT and test devices setup (hardware and software) should be completed. The DUT's network shall be in normal operation mode or ready to operable configuration. Any non-periodic communication traffics or DUT abnormal conditions should be removed.

Test devices have the ability of monitoring and transferring of DUT output data. Real-time packet capturing is more preferable test devices feature. Test devices also have the ability to scan any open port of DUT and to generate sets of test protocol frame or packet as described in section 3.

During tests, DUT may undue fail or freeze that requires DUT reboot. Test devices have DUT power off-on cycling capability using normally closed(NC) relay contacts.

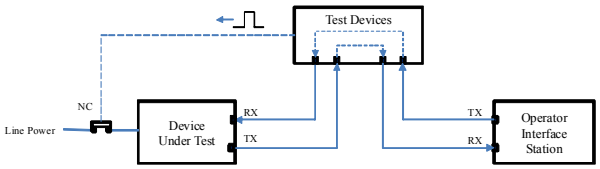

Figure 1. CS Vulnerability Test Setup

2.2 Open Port Probing

After test setup is completed, DUT is activated and testing device runs to scan to find any open port exist on the DUT. Consequent vulnerability tests will go through those founded open port only. Generally, DUT is embedded system that has limited computer resources, port probing may take the DUT to abnormal operating state.

Industry CS may have proprietary protocol implementation that uses not well known ports. From this, complete range of TCP/UDP port scan (0 to 65535) is more preferable to check any private port exist on DUT.

2.3 Testing

Main vulnerability uncovering tests are executed after CS open port probing is completed. Sets of storm traffics will send to previously identified open port. Testing these open port only reduces testing time greatly.

If previous probing ranges are partial, tests performed using these probing ports also generate partial results and tester should be aware of these limitation.

3. Test Protocols and Methods

CS vulnerability test covers very wide range of test spectrum from out-of-date to state-of-the-art network technologies. Following section describes selected sets of test protocol and test methods that are practical to apply real CS vulnerability test and summarized at Table 1.

3.1 Test Protocol

Address Resolution Protocol (ARP) is one of well known lower layer protocol. It converts hardware network address (MAC) to IP address or vice versa. Ethernet based control system has unique IP address and, from that sense, implementation of ARP is very probable.

Internet Control Message Protocol(ICMP) is a network layer protocol. In control system, this standard protocol may be used for network connection diagnostic (ping test) and reconfiguring purpose.

Transmission Control Protocol (TCP) or User datagram Protocol (UDP) is a transport layer protocol that delivers data to and/or from user application or services.

Some complicate and deluxe control systems may have web service functions, Hypertext Transfer Protocol

(HTTP) can be applied as layer-7 test protocol for these systems.

Table 1. Test Protocols/Methods and OSI Layers[2]

OSI Layer Model	Test Protocol	Test Method
L7-Application	HTTP	(TBD)
L4-Transport	TCP, UDP	TCP Storm, UDP Storm
L3-Network	IP, ICMP	ICMP Storm
L2-Data Link	ARP	ARP Storm
L1-Physical	-	-

3.2 Test Method for Each Protocol

Test methods of Ethernet based CS network covers vast network technology spectrum and continuously evolve to more effective and economical perspective. As same context to other type of system test, exhaustive CS vulnerability test is an unachievable goal in real world.

Almost all digital control systems are embedded computer system with real-time functionality, that means, deterministic data deliveries through CS is critical function of the system. Another different features of control systems with IT computer system is a limited system resources such as CPU performance, memory size, etc. [3]

Sending many packets from test devices to DUT for each protocol may exhaust DUT resources and can easily deliver DUT to well known Denial-of-Service (DoS) state.

To test these critical point, various storm generation methods are well developed for these protocols. For further effective vulnerability check, invalid combination methods of frame or data field can be used in parallel during these storm tests. These invalid frames or packets can contribute to exhaust DUT resources more rapidly.

4. Conclusions

To test industry control system's communication network vulnerability, practical and cost effect test framework is suggested.

Tester must consider of test feasibility (cost) and the results real effectiveness. Form these base, sets of test protocol suite and available test methods are selected.

After these tests, evaluations of each test results with respect to system risks should performed.

Throughout all these test and consequent any security hole hardening process, system owner always have sound balances between network security concerns and counter-measures cost expenditure [4].

REFERENCES

[1] KINS/GT-N27, Regulatory Guide: Cyber Security of Instrumentation and Control Systems in Nuclear Facilities, 2007
[2] RFC-1122, Requirements for Internet Hosts – Communication Layers, 1989
[3] ANSI/ISA-TR99.00.01, Security Technologies for Industrial Automation and Control System, pp 73-75, 2007.
[4] ANSI/ISA-99.00.01, Security for Industrial Automation and Control Systems Supplement Part 1: Terminology, Concepts, and Models, p 54, 2007
[5] Ethernet: The Definitive Guide, O'Relly, 2000