Cyber Security Penetration Test for Digital Safety I&C Systems

C. K. Lee, D. H. Kim, K. C. Kwon, H. K. Joo, J. S. Song
Korea Atomic Energy Research Institute, I&C & HF Research Div.,
1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Republic of Korea
**Corresponding author: cklee1@kaeri.re.kr*

1. Introduction

In the Korea Nuclear I&C Systems Development project the platforms for plant protection systems are developed, which function as a reactor shutdown, actuation of engineered safety features and a control of the related equipment. Those are fully digitalized through the use of safety-grade programmable logic controllers (PLCs) and few types of communication network. However the Regulatory Guide 1.152 (Rev. 02) was published by the U.S. NRC in 2006 [1] and it recommended the application of a cyber security to the safety systems in the Nuclear Power Plant (NPP). Therefore to incorporate the new licensing requirement, a cyber security risk assessment is performed for the platforms. Then the vulnerabilities identified by the risk assessment are validated by penetration test. This paper summarizes test scenario, test results and their incorporation into system design.

2. Backgrounds of Cyber Security in NPP

With the use of digital computers and communication networks the issues on cyber security were raised about 10 years ago, and the scope of application has now been extended from safety I&C system to the systems important to safety, plant security system and emergency preparedness system since publishing a new Reg. Guide 5.71 this year [2]. While each country has published its own regulatory guide in association with this topic, there is actually no international standard for the use in NPP design, and it is the only one that IEC began to develop a standard last year. Up to now most technologies are coming from information technology (IT) industry and these are being customized for the use in other industries. For an example, NIST, a national research institute in the U.S.A. published many reports on the application of cyber security to supervisory control and data acquisition (SCADA) system. Even if these are very useful in SCADA system, the differences in design concepts between NPP I&C system and SCADA system can lead us to a different design in the application of cyber security technology. Nevertheless, it is fortunate to hear that national research institutes in America have been continuing the associated studies in recent years.

3. Cyber Security Risk Assessment

To incorporate the cyber security into the design of the platforms for plant protection systems, first a cyber security risk assessment is conducted with preparing a detail implementation plan for strengthening the level of cyber security for the platforms whose security model is in Fig. 1. The assessment consists of an asset analysis, a threat analysis, a vulnerability analysis, a risk analysis and penetration test, and an analysis of security controls or defensive techniques, etc [3].

Asset analysis evaluates the importance of assets from the viewpoint of confidentiality, integrity and availability, which are top-tier properties for the cyber security. In threat analysis, the risk elements which have potential to attack the vulnerabilities existing in the real systems are identified. Vulnerability analysis identifies the weak points against all types of anticipated cyber attack and 27 items are identified for platforms. Then the risks are calculated with a simple equation and prioritized by the value that is a severity of affection to the safety and availability of system. The identified risks are validated through the penetration test by authorized hacker to confirm the possibility of occurrence in real world. Finally appropriate security controls (or defensive techniques and strategies) for each risk are recommended.

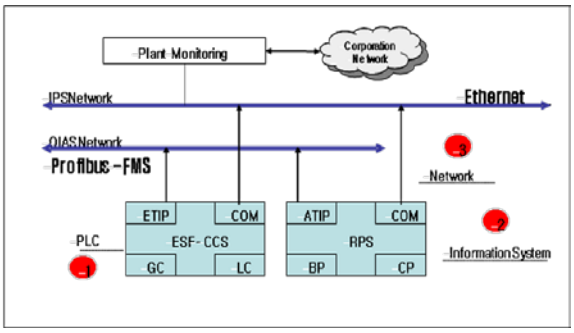

Fig. 1. Cyber Security Model for Platforms

4. Penetration Test

The aims of a penetration test are to identify the threats of concern, to confirm vulnerabilities and the potential of risks identified in the risk assessment, and to complement the review of security controls [4]. If an attack during a test is successful, the vulnerability or risk is verified and security controls are identified to mitigate the associated security exposure.

The attack points for test as shown in Fig. 2, and the attack scenario for each risk in Table 1 are selected based on the identified threats and vulnerabilities and the discussion between system designers and hackers

4.1 Test Conditions

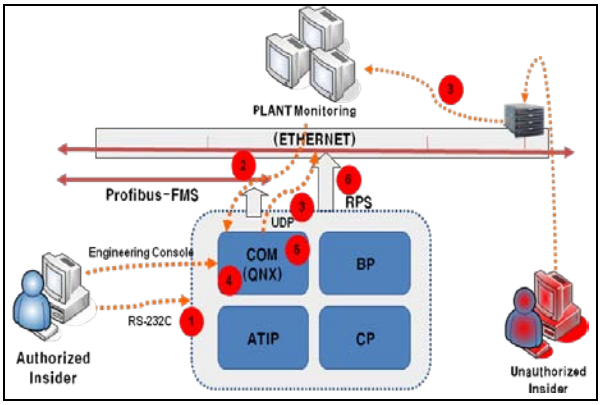

Fig. 2. Vulnerable Points and Penetration Paths

Table 1: Intrusion Test Plans for Scenario

	Scenario	Risk
1	Transfer of a large amount of traffic within PC and PLC by warm virus	Denial of service (DoS) in PLC System
2	Transfer of a large amount of traffic to COM by warm virus	Denial of service in COM System
3	Transfer of a large amount of packet from COM to MCR by warm virus	Denial of service in information system within MCR
4	Executing malicious codes in COM sys.	Exposure of COM control and user account
5	Attack for modification of MMI program	Tampering (modification) of monitoring program
6	Modification of packet data being transferred from COM(QNX) to MCR	Mis-operation of IPS

- Test is conducted by authorized hackers on the prototypes. In fact it is expected that on-line penetration test will not be allowed in NPP.
- Penetration path from outside to PLCs of processors via Profibus was not tested, because it was assessed at that time that it is hard to attack through this path.
- Plant monitoring system in the main control room (MCR) is connected for the test.

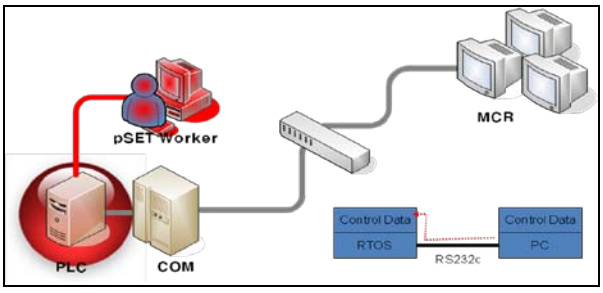

Fig. 3. Penetration Test : Scenario No. 1

4.2 Test Results

1) Scenario 1 (see Fig. 3): PLC CPU load was increased abnormally.
2) Scenario 2: COM was infected by PC traffic and this then caused monitoring errors.
3) Scenario 3: Transfer delay in network and connection of large sessions were confirmed.
4) Scenario 4: Unauthorized one could get the control authority of COM due to lack of authentication means.
5) Scenario 5: Attack was not successful.
6) Scenario 6: Modification of data transferred from COM to MCR information systems via UDP was successful.

4.3 Defensive Techniques and Strategies

Recommendations from the test are summarized.
- pSET PC connected to PLC should be checked periodically to see if it is infected by malicious codes like warm, and the recommended policies for pSET PC are as following;
  * Access control and exclusive use of pSET for programming PLC software.
  * Testing data integrity and infection by warm or malicious codes.
  * No other PC connection to PLC and management of unauthorized connection.
- In response to the attacks of Denial of Service or malicious codes to COM, following activities are recommended.
  * Periodic check of infection of information systems.
  * Use of firewall or IDS or IPS.
  * No connection of Internet or use of solutions.
  * Maintaining the list of processes so as not to execute the unnecessary services.
  * Establishment of cyber security policies for information systems which are same as those of pSET.
- To perform the following activities in response to the packet data modification between COM and MCR.
  * Check of data integrity.
  * Use of data encryption to protect from tapping, data forging and data modification.
  * Establishment of security policies for networks.
  * Isolation of safety system networks from nonsafety system networks.

5. Conclusions

Through the penetration test we could confirm the threats and vulnerabilities identified by the assessment. For most of the risks, the penetration test was successful, but in scenario 5 the attack was failed. Through the analysis we could identify the weak and robust points on the platform. And we established defensive strategies and techniques based on the recommendations from the test. Finally it is desirable to establish a cyber security test facility for NPP I&C equipment.

REFERENCES

[1] U.S. NRC, Reg. Guide 1.152, Criteria for Use of Computers in Safety Systems of NPP, Rev.02, 2006.
[2] U.S. NRC, Reg. Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[3] C. K. Lee et al, Cyber Security Risk Assessment for the KNICS Safety Systems, Transaction of KNS Spring Meeting, Geyongju, Korea, May 29-30, 2008.
[4] Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006.