Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 25-26, 2007

An Attack Model Development Process for the Cyber Security of Safety Related Nuclear Digital I&C Systems

Parvaiz Ahmed Khand, Poong Hyun Seong
Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,
371-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea
parvaiz@kaist.ac.kr, phseong@kaist.ac.kr

1. Introduction

In nuclear power plants (NPPs), the redundant safety related systems are designed to take automatic action to prevent and mitigate accident conditions if the operators and the non-safety systems fail to maintain the plant within normal operating conditions [1]. Presently, there is trend of connecting computer networks of commercial NPPs to corporate local area networks (LANs) to give engineers access to plant data for economic benefits. An increase in plant efficiency of a couple percentage points can translate to millions upon millions of dollars per year [2]. The nuclear industry is also moving in the direction of installing digital controls that would allow for remote operation of plant functions, perhaps within a few years [2]. However, this connectivity may also cause new security problems such as: in 2003, a computer worm named as slammer penetrated a private computer network at Ohio's Davis-Besse nuclear plant and disabled a safety monitoring system called a safety parameter display system (SPDS) [2,3]. Moreover, the present systems were developed with consideration of reliability and safety rather than security. In present scenario, there is a need to model and understand the cyber attacks towards these systems in a systematic way, and to demonstrate that the plant specific procedures and the imposed security controls adequately protect the systems from analyzed cyber security attacks.

Attack trees provide a systematic, disciplined and effective way to model and understand cyber attacks towards any type of systems, make it possible to understand risks from deliberate, malicious intrusions from attackers, and make security decisions. Using attack trees the security of large systems can be modeled by considering a security breach as a system failure, and describing it with a set of events that can lead to system failure in a combinatorial way. The attacks towards the system are represented in a tree structure, with an attack that can significantly damage the system operation as a root node and different ways to achieve that attack as leaf nodes. The structure, syntax and semantics of attack trees can be seen in [4].

In attack trees, the leaf nodes can take many kinds of values to evaluate different aspects of system security. For example, the possible/impossible value can be assigned to enumerate all sets of possible attacks that achieve the attack goal, probability values to evaluate the probability that the attack goal can be achieved, cost value to evaluate the minimum cost needed to reach attack goal, and the special equipment value to obtain the most probable attack sets with no special equipment required.

Although it is possible to implement security controls almost any type of attack, it is not practical to protect everything. Attack trees also provide a systematic way to model security controls and plant specific procedures as a safeguard against attacks, and check their effectiveness.

In this paper, we will present a process for developing an attack model for the cyber security of safety related nuclear digital I&C systems using attack trees.

2. Methods and Results

To develop the attack model, the steps involved are shown in figure 1. For steps 1 and 2,, we have considered a conceptual model of a digital safety related system (figure 2), the IT environment of the system (figure 3), and general steps involved in an attack process (figure 4).

1. Understand the system and its IT environment,
2. Understand the general attack process,
3. Develop the attack model using attack trees,
4. Add the security controls in the attack model

Figure 1. Steps involved in attack model development process

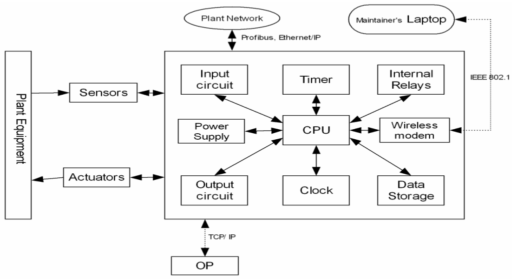


Figure 2. Conceptual model of a digital safety related system

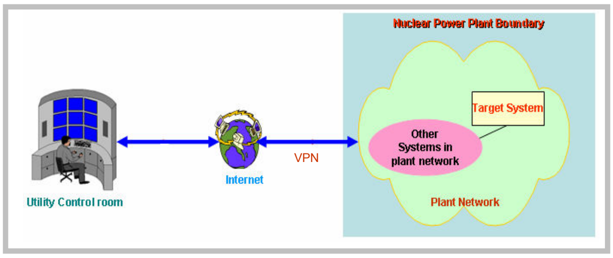
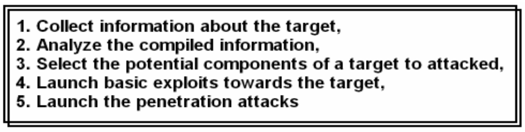


Figure 3. An illustration of the IT environment of the system



1. Collect information about the target,
2. Analyze the compiled information,
3. Select the potential components of a target to attacked,
4. Launch basic exploits towards the target,
5. Launch the penetration attacks

Figure 4. General steps involved in an attack process

The attack model was developed in the form of an attack tree; the attack tree development process is shown in figure 5. A higher level attack tree is shown in figure 6, and the refined nodes are shown in figure 7.

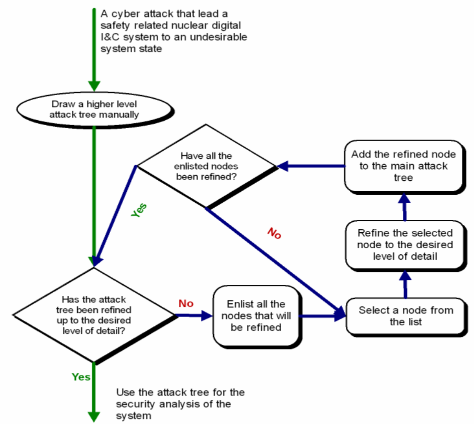

A cyber attack that lead a safety related nuclear digital I&C system to an undesirable system state
Draw a higher level attack tree manually
Have all the enlisted nodes been refined?
Add the refined node to the main attack tree
Yes
No
Refine the selected node to the desired level of detail
Has the attack tree been refined up to the desired level of detail?
No
Enlist all the nodes that will be refined
Select a node from the list
Yes
Use the attack tree for the security analysis of the system

Figure 5. The attack tree development process

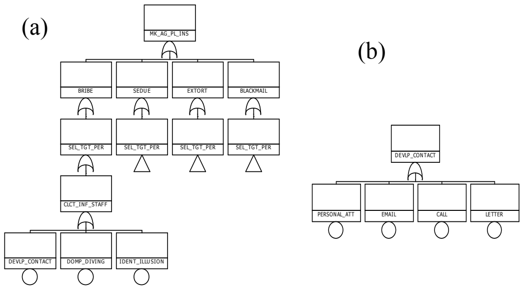
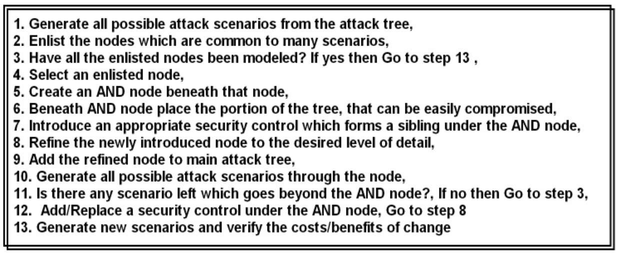


Figure 7. (a) A refined node of higher level tree
(b) A refined node of (a)

The process of modeling security controls in the developed attack tree is shown in figure 8.



1. Generate all possible attack scenarios from the attack tree,
2. Enlist the nodes which are common to many scenarios,
3. Have all the enlisted nodes been modeled? If yes then Go to step 13 ,
4. Select an enlisted node,
5. Create an AND node beneath that node,
6. Beneath AND node place the portion of the tree, that can be easily compromised,
7. Introduce an appropriate security control which forms a sibling under the AND node,
8. Refine the newly introduced node to the desired level of detail,
9. Add the refined node to main attack tree,
10. Generate all possible attack scenarios through the node,
11. Is there any scenario left which goes beyond the AND node?, If no then Go to step 3,
12. Add/Replace a security control under the AND node, Go to step 8
13. Generate new scenarios and verify the costs/benefits of change

Figure 8. Modeling the addition of security controls

3. Conclusion

An attack model for the cyber security of safety related nuclear digital I&C systems was developed using attack trees. The model provides a systematic, disciplined and effective way: (i) to model and understand cyber attacks towards the safety related nuclear digital I&C systems, (ii) to help in understanding the risks from deliberate, malicious intrusions from attackers, (iii) to help in demonstrating that the plant specific procedures and the imposed security controls adequately protect the systems from analyzed cyber security attacks, and (iv) to make security decisions.

REFERENCES

[1] Commission on Engineering and Technical Systems (CETS),"Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues", http://books.nap.edu/catalog.php?record_id=5432#orgs

[2] Kevin Poulsen, " Slammer worm crashed Ohio nuke plant network", SecurityFocus 2003, http://www.securityfocus.com/news/6767

[3] David Moore et. Al., "Inside the slammer worm ", Security & Privacy Magazine, IEEE, www.cs.ucsd.edu/~savage/papers/IEEESP03.pdf

[4] David M. Nicol et. Al., "Model-Based Evaluation: From Dependability to Security", IEEE Transactions on Dependable and Secure Computing, Vol. 1(1), 2004

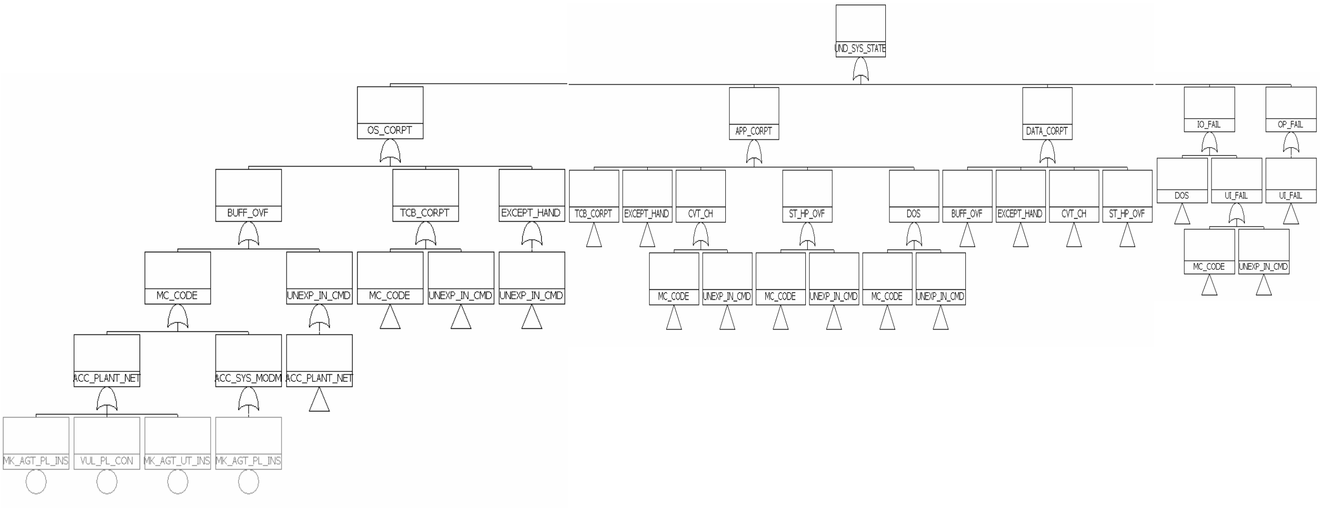


Figure 6. The higher level attack tree for the safety related nuclear digital I&C system