A CYBER-CAPABILITY MODEL FOR COMPROMISE OF I&C SYSTEM FUNCTIONS AT NUCLEAR FACILITIES

J. Li
Tsinghua University
Beijing, China
Email: lijianghai@tsinghua.edu.cn

M. T. Rowland
Sandia National Laboratory
Albuquerque, USA

M. Hewes
IAEA
Vienna, Austria

Abstract

IAEA Nuclear Security Series No. 20 recommends the use of risk informed approaches that takes into account a current assessment of nuclear security threats (i.e. threat actors having motivation, intention, and capability to attack a State's nuclear security regime). This assessment requires an understanding and analysis of the cyber-capabilities to determine the security requirements. This analysis can be supported by modelling threat actor capabilities required to compromise instrumentation and control (I&C) system function via cyber-attack. IAEA Nuclear Security Series No. 33-T para 2.21 provides an ordered list of the four potential consequences of compromise on I&C system function. These potential consequences are the basis on which to define the computer security requirements for the I&C system functions (i.e. computer security level).

This paper proposes a three-level adversary cyber-capability model for use in evaluation of potential consequences and their likelihood of occurrence. In this model, the threat actor capabilities lead to a classification into one of three groups. They are 'IT hackers', 'ICS hackers', and 'nuclear process hackers'.

IT hackers have knowledge and understanding on how to compromise information technology and could initiate or target cyber-attacks on I&C systems that are likely to be limited to disruptive effects (i.e. failure) than causing more severe consequences as per NSS No. 33-T. This is due to the IT hackers not being aware of the specialized characteristics of industrial control systems required to initiate these more severe consequences.

On the next level representing increasing capability (i.e. risk), ICS hackers have the all of the capabilities as IT hackers (having acquired the general knowledge of information technology) as well as specific knowledge of industrial control systems.

The most capable threat actor, representing the highest risk, nuclear process hackers have the same capabilities as ICS hackers, but also have gained the access and understanding of the detailed process information at nuclear facilities that they have targeted.

In this model, the different types of attacks are associated with each of the different types of threat actors. Application of this model, reveals that consequences increase in severity as the threat actor behind the compromise progresses from lower threat level (i.e. IT hackers) to the highest threat level (i.e. nuclear process hackers). The three-level model proposed in this paper could also be utilized in development of a more sophisticated model used to develop the cyber design basis threat (cyber-DBT) of nuclear facilities.

1. INTRODUCTION

The instrumentation and control (I&C) systems are often essential for facility safety, consequently an understanding of nuclear safety can assist in assessing risk, developing computer security measures for the I&C system, assessing potential conflicts between safety and security, and determining how such conflicts could be resolved. For example, adversaries could sabotage a facility through a cyber-attack on the facility's I&C systems, resulting in potential safety and security consequences. Such attacks might cause failures of I&C systems or might cause I&C systems to operate in ways that differ from their intended behaviour or their analysed failure modes [1].

IAEA Nuclear Security Series No. 20 [2] states that “A nuclear security regime uses risk informed approaches”. According to NSS20 [2], these risk informed approaches take into account (1) the State’s current assessment of threat actors, (2) attractiveness and vulnerability of targets, (3) characteristics of the targets, and (4) potential harmful consequences. The assessment of threat actors who have motivation, intention, and capability to attack nuclear security regime requires an understanding and analysis of the cyber-capabilities to determine the cyber security requirements. This analysis can be supported by modelling threat actor capabilities required to compromise I&C system function via cyber-attack.

IAEA Nuclear Security Series No. 33-T [3] para 2.21 provides an ordered list of the four potential consequences of compromise on I&C system function arranged from best to worst case. These potential consequences are the basis on which to define the computer security requirements for the I&C system functions (i.e. computer security level).

This paper proposes a three-level adversary cyber-capability model for use in evaluation of potential consequences and their likelihood of occurrence to support the assessment of cyber risk of I&C systems at nuclear facilities.

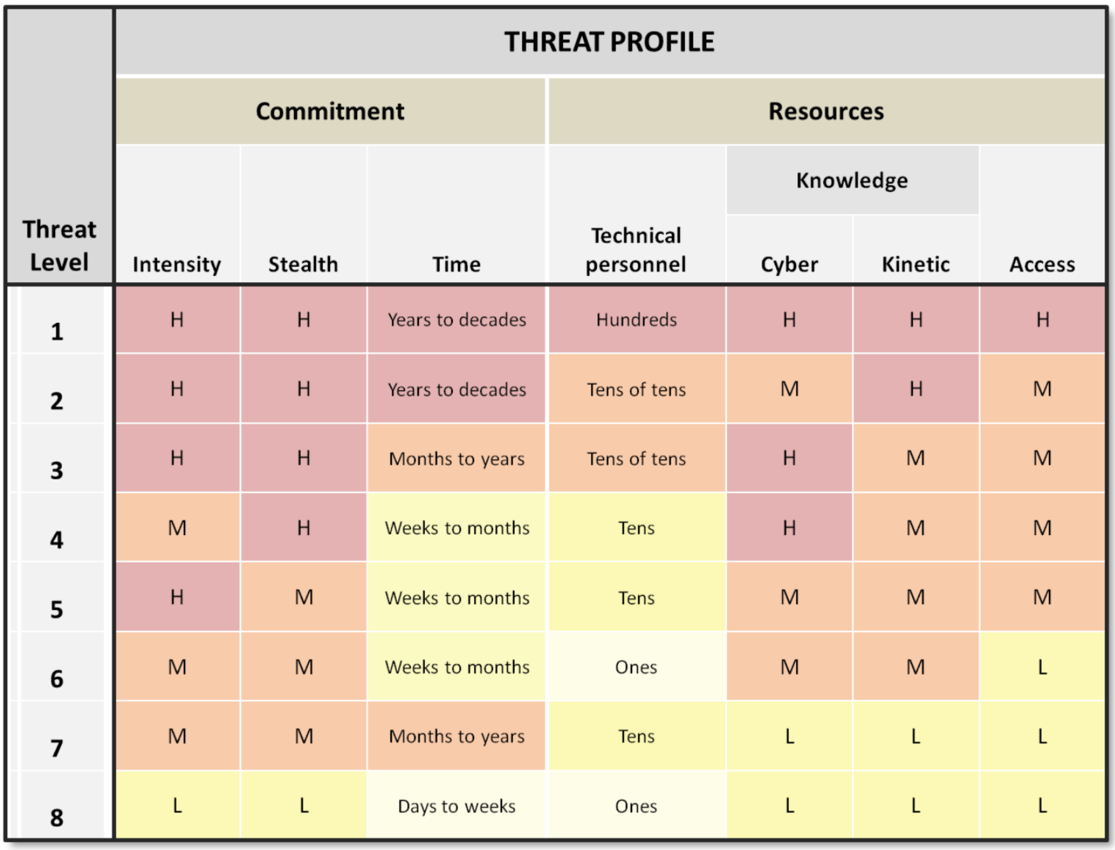
Applications of a three level capability model that provide a hierarchy of the threat actors that can support:

- Development of test cyber scenarios;
- Consequence evaluation and risk assessment;
- Identification of data type required for protection.

2. RELATED WORKS OF THREAT ACTOR CAPABILITY MODELS

Currently, the cyber threat actors are often labelled with the notions of script kiddies, criminals, hacktivists, nation states, and cyber terrorists. These semi-descriptive labels reinforce preconceived notions regarding motivation and resources [4, 5]. [5] provides details on a Generic Threat Matrix (in Table 1) that has a greater number of attributes and levels than the one proposed in this paper.

TABLE 1. THREAT PROFILE [4, 5]



Threat Level	THREAT PROFILE						
	Commitment			Resources			
					Knowledge		
	Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
1	H	H	Years to decades	Hundreds	H	H	H
2	H	H	Years to decades	Tens of tens	M	H	M
3	H	H	Months to years	Tens of tens	H	M	M
4	M	H	Weeks to months	Tens	H	M	M
5	H	M	Weeks to months	Tens	M	M	M
6	M	M	Weeks to months	Ones	M	M	L
7	M	M	Months to years	Tens	L	L	L
8	L	L	Days to weeks	Ones	L	L	L

The threat profile detailed in [4, 5] depends upon motivation (i.e. commitment) and resources, but does not address capability fully which addresses skills and abilities. Further, the development and discovery of malware toolkits (e.g. ZeuS, Gameover ZeuS) and frameworks (e.g. CRASHOVERRIDE) have the boundary to lower the threshold of knowledge, skills, and abilities as well as the level of commitment in intensity and time required for an adversary to complete scenarios with probability and consequences associated with Threat Level 1. For example, [6] states the following Key Takeaways for CRASH OVERRIDE:

- CRASHOVERRIDE is not unique to any particular vendor or configuration and instead leverages knowledge of grid operations and network communications to cause impact; in that way, it can be immediately re-purposed in Europe and portions of the Middle East and Asia.
- CRASHOVERRIDE is extensible and with a small amount of tailoring such as the inclusion of DNP3 protocol stack would also be effective in the North American Grid.
- CRASHOVERRIDE could be extended to other industries with additional protocol modules, but the adversaries have not demonstrated the knowledge of other physical industrial processes. [6]

The last point in particular is key, as the knowledge of the physical industrial process that is under automated digital control is the barrier to adversary in successfully achieving the consequence. Therefore, a threat actor model lacking of the capability modelling that is specific to nuclear security is inadequate for the I&C systems at nuclear facilities.

In this paper, the capabilities of threat actors, including the knowledge and skills they have, are modelled into three levels. This model that emphasis on the capability of threat actors, especially on the knowledge of physical nuclear process, could support for the cyber risk assessment, the scenario testing, and the protection establishment.

3. THREE LEVEL ADVERSARY CYBER-CAPABILITY MODEL

In the three level capability model, the cyber threat actor capabilities lead to a classification into one of three “hacker” groups. They are IT hackers, ICS hackers, and nuclear process hackers (see fig. 1 below). This paper assumes that the highest risks (potential consequences) are associated with compromise of I&C systems resulting in the consequence in operation of nuclear facilities. The motivation of three level classification is rooted from three domains of knowledge or skills related with cyber security of nuclear facilities. They are:

- A. information technology (IT) skills;
- B. industrial control systems (ICS) skills;
- C. nuclear process information and operation knowledge.

The three hacker groups are assumed to have different levels of capabilities. IT hackers have mastered the domain A. ICS hackers have mastered the domains of A and B. And nuclear process hackers have mastered the domains of A, B, and C.

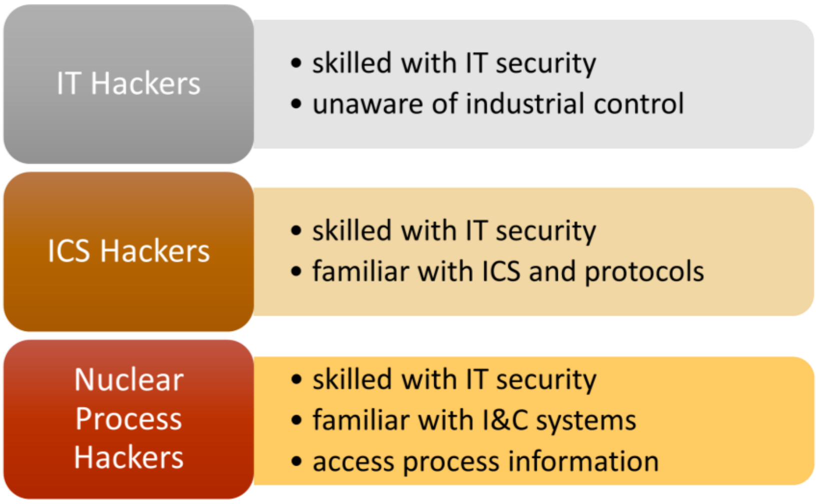

IT Hackers
• skilled with IT security
• unaware of industrial control
ICS Hackers
• skilled with IT security
• familiar with ICS and protocols
Nuclear Process Hackers
• skilled with IT security
• familiar with I&C systems
• access process information

FIG. 1. Three Level Capability Model.

3.1 IT Hackers

IT hackers have knowledge and understanding on how to compromise information technology (IT) and could initiate or target cyber-attacks on I&C systems that are likely to be more disruptive (i.e. failure) than causing more severe consequences as per NSS 33-T [3]. This is due to the attribute that IT hackers are not aware of the specialized characteristics of industrial control systems. The assets most likely to be compromised are servers, workstations (running common operating systems; Unix, Linux, MS Windows) and commercial ICT network infrastructure (that support common ICT protocols and services; TCP/IP, FTP, HTTP, Telnet). The potential for an attack from IT hackers resulting in failure is due to the integration of ICT equipment and protocols within I&C systems (e.g. supervisory computers, historians, TCP/IP). IT hackers lack the capability to compromise or purposefully and directly impact the function of the customized I&C system or its environment.

3.2 ICS Hackers

ICS Hackers have all the capabilities of the IT Hackers (having acquired the general knowledge of information technology). It is important to note that ICS Hackers and IT Hackers may have differing proficiency in the application of these capabilities. ICS Hackers also have the capability to compromise specific OT equipment, such as Programmable Logic Controller (PLC), and Distributed Control System (DCS). This includes knowledge and understanding of distinct industrial control protocols, such as Modbus/TCP, Siemens S7, OPC UA.

The vulnerabilities of all the assets of the industrial control systems could be exploited by the ICS hackers. They are also able to manipulate the network data packets of ICS protocols. In this way, they can compromise I&C systems to cause undesirable and abnormal behaviour or actions [3]. However, the ICS Hackers lack the understanding of the specificities of nuclear facility environments to evade or mitigate other protective actions or design features that provide for nuclear safety.

Even so, these attacks also could affect the communication of I&C systems and disrupt the normal operation of controlled physical equipment or process. ICS hackers are able to manipulate ICS data packets, including tampering with the data fields within the packet payload. The malicious operation in the packet payload by ICS hackers poses more serious threat than the malicious actions available to IT hackers (e.g. tampering of TCP/IP header within ICS networks).

This paper assumes that ICS hackers can significantly impact a nuclear facility where there are no cyber security measures in place, but cannot result in sabotage of these facilities that result in unacceptable radiological consequences (URC) [7].

3.3 Nuclear Process Hackers

On the level representing the highest risk, nuclear process hackers have the same capabilities as ICS hackers, but also have the access and understanding of the detailed process information at nuclear facilities. The process information includes the process dynamics, the control logics, fail-safes, the normal range of physical quantities, and the information presented on the Human-Machine-Interface (HMI). With the process information, hackers can initiate more advanced attacks having the potential to lead to severe impacts upon the facility (i.e. sabotage resulting in URC). The original control logics may be replaced by the malicious ones. The set points of the process may be altered out of the normal range. The anomalies in one subsystem may spread to other subsystems via process dynamics. The information presented to operators may be falsified (i.e. spoofed) for hiding an attack or misleading the operators to either prevent them taking action or perform erroneous actions.

4. THE APPLICATIONS OF THE THREE LEVEL CAPABILITY MODEL

4.1 Development of Test Cyber Scenarios

The three level capability model can be used for developing test cyber scenarios performed on the I&C systems. Three typical test scenarios are proposed based on the three level capability model,

- Scenarios 1: The denial of service by IT hackers;

- Scenarios 2: The packet injection by ICS hackers;
- Scenarios 3: The feedback spoofing by nuclear process hackers.

The goal of denial of service (DoS) scenario is to interrupt the communication between the Programmable Logic Controller (PLC) with the Human-Machine Interface (HMI). A type of DoS attack could prevent the HMI either sending commands to or querying measurements from the PLC. Hence, the operators lose control of the I&C system. To develop such a DoS attack, no specific knowledge about the target I&C systems is required. An IT hacker could brutally generate a large amount of insignificant packet to take away the bandwidth and interrupt the normal communication.

The goal of packet injection scenario is to stop the PLC while it is working. A packet injection attack could forge a malicious packet containing the device stopping command and inject it into the ICS network. This packet conforms to the ICS protocols that they appear to be part of normal communication. Packet injection of stopping the PLC requires the understanding of ICS systems; thus it can only be initiated by the ICS hackers.

The goal of feedback spoofing scenario is to falsify the feedback data to mislead the operators. A type of the man-in-the-middle (MITM) attack could secretly alter the communication between the control stations and the HMI. Then the third party can capture the feedback data from sensors and send them back to operators after modifications. The nuclear process information is required to modify these feedback data for the specific misleading purpose. Therefore, only the nuclear process hacker could develop such type of attack.

4.2 Consequence Evaluation and Risk Assessment

The risk assessment of the I&C systems requires the evaluation of potential consequences and their likelihood of occurrence. The potential consequences of a compromise of I&C system include not only the failure mode of not working, but also the abnormal behaviour beyond expectations. An ordered list of the four potential consequences of a compromise on I&C system function is provided by IAEA Nuclear Security Series No. 33-T para 2.21[3]. When arranged from best to worst case, they are no effect, fails, observable unexpected behaviours, and indeterminate (unobserved alteration). The likelihood of these consequence can be assessed based on the capacity model, in order to support the security requirement determination.

Table 2 uses the ordered list of consequences and the three level capacity model to provide a qualitative assessment of the likelihood of these consequences resulting from an adversary having opportunity to compromise vulnerable and unprotected I&C systems in a nuclear facility.

TABLE 2. LIKELIHOOD OF CONSEQUENCES AS PER THE THREE LEVEL CAPABILITY MODEL

Capability\Consequence	No effect (Resilient)	Fails	Observable unexpected behaviors	Indeterminate
IT hackers	often	most often	less often	rarely
ICS hackers	less often	often	often	rarely
Nuclear process hackers	rarely	often	often	most often

This table can be verified by the typical scenarios developed in the Section 4.1 of this paper. The communication interruption scenario by IT hackers only makes the HMI fail to receive feedbacks or send out commands. However, since the IT hacker are lack of specific knowledge about the I&C systems, it is unlikely for them to make the HMI to perform unexpected behaviours. While, the ICS hacker having the knowledge of the I&C systems are able to cause unexpected behaviours in the I&C systems, such as the PLC stopping. To cause the consequence of indeterminate which is unobservable alteration, the detailed process information is required, which is the capacity of the nuclear process hacker. The feedback spoofing by nuclear process hackers is one example, the consequence of which is unobserved to the operator.

4.3 Identification of Data Type for Intrusion Detection

To detect the intrusions caused by hackers with different capabilities, different types of data are required. The types of data required depends on what hackers are able to impact. The more capable the hackers are; the more data types are required.

For IT hackers, they are able to manipulate the header of packets, rather than the payload of packets which requires specific knowledge of the ICS protocols. Thus, the data type required for detection of intrusion by IT hackers is the IT data. For examples, the five-tuple of TCP/IP packers (i.e. source IP address, source port, destination IP address, destination port, and transport protocol), the network traffic flow, or the statistics of the communication conversations and network endpoints. Most of conventional intrusion detection systems (IDS) are based on these types of data.

For ICS hackers, they are able to manipulate the ICS data while hiding within authorized IT data packets (thereby increasing the difficulty to detect the intrusion via IT data inspection). The ICS data are the data in line with the ICS protocols. They are for example the function code of ICS protocols, the register address to be written and read, and the operation data value. These data are usually encapsulated in the data payload of packets. And they could be retrieved by the techniques of deep packet inspection (DPI). Taking the packet injection scenario for example, the malicious data packet sent from the HMI to the PLC is as normal as other packets if only the headers of packets are inspected. However, the function code of stopping the control device in the payload is quite unusual when in the working condition. Thus the ICS data of the function code can indicate the malicious operations by the ICS hackers.

For nuclear process hackers, they are able to manipulate not only the ICS data, but also the nuclear process variables. For example, the set points can be modified to a certain value to increase the pressure beyond the limits. Or in the scenario of feedback spoofing, the true feedback of abnormal water level is tampered into a feedback of normal level in order not to trigger alarms. All the above operations seem legal from the view of IT behaviour or ICS control. Unless the process variables are incorporated for intrusion detection, the malicious operations by the nuclear process hackers are difficult to detect.

TABLE 3. DATA TYPES FOR INTRUSION DETECTION

Hackers groups	Test Scenarios	Data Type	Examples
IT hackers	DoS	IT data	Five-tuples of TCP/IP packets, the traffic flow.
ICS hackers	Packet Injection	ICS data	Function codes, register address, and operation data values
Nuclear process hackers	Feedback Spoofing	Process data	Process variables such as temperatures, pressures, controls commands, set points.

5. CONCLUSIONS AND FUTURE WORK

The three level adversary cyber-capacity model is proposed in this paper. This model emphasizes the threat actors' capabilities to compromise I&C system functions at nuclear facilities. The three level classification is based on three domains of knowledge or skills that are IT skills, ICS skills, and nuclear process knowledge. The model can be applied to support the cyber risk assessment, the test scenario development, and the count measure development. A further more sophisticated model can be used to develop the cyber design basis threat (cyber-DBT) of nuclear facilities.

REFERENCES

[1] ROWLAND, M.T., DUDENHOEFFER, D.D., and PURVIS, J.S., "Computer Security for I&C Systems at Nuclear Facilities", 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2017), San Francisco, CA, June 11-15, 2017.

[2] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Series No. 20 (2013).

[3] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Nuclear Security Series No. 33-T (2018).

[4] MATESKI, M., TREVINO, C.M., VEITCH, C.K., MICHALSKI, J., HARRIS, J.M., MARUOKA, S., and FRYE, J., Cyber Threat Metrics, Sandia Report SAND2012-2427, 2012.

[5] DUGGAN, D. P., THOMAS, S. R., VEITCH, C. K. K. and WOODARD, L. Categorizing Threat: Building and Using a Generic Threat Matrix, Sandia Report SAND2007-5791, 2007.

[6] DRAGOS INC., CRASHOVERRIDE Analysis of the threat to Electric Grid Operations, Dragos Inc. v. 2.20170613, 2017.

[7] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities, Nuclear Security Series No. 27-G (2018).