Cyber-Security –

Best-Practices dealing with Automated Protection and Visualization

Mr. Ismael L. Garcia, P.E.
Senior Technical Advisor, Office of New Reactors-DEI
U.S. Nuclear Regulatory Commission
11545 Rockville Pike, Rockville, MD 20852-2738
Ismael.Garcia@nrc.gov

Purpose: The purpose of this paper is to make available to industry information concerning best-practices related to Cyber-Security. The information discussed herein is based on best-practices that private industry abroad is adopting in order to improve their defensive posture against cyber-attacks.

Background:

a. One of the biggest challenges facing cyber defenders today is keeping up with attackers who have developed automated mechanisms to morph malware, distribute attacks, and continually alter signatures, domain names, and IP addresses. Defending against cyber-security threats such as hacks, leaks, and exploitation is a complex problem, compounded by the ever increasing interconnectivity of computing devices. For example, future growth prediction ranges up to 50 billion Internet enabled devices by 2020 [1], which presents a new set of challenges and risks to the internetworked ecosystem. With the expansion of fully autonomous systems throughout the world, there is an increase need to explore the possibilities of automated cyber-attack identification, categorization, and response.

b. Despite the potential implementation of an automated method(s) for defending against cyber-attacks, the human operator needs to remain in the loop to perform many cognitively intense activities [2]. For example, a human operator would need to discover incidents that do not fit a given automated attack detection profile, evaluate automated alerts for true and false positives, or assess the operational impact of a cyber incident. Despite the fact that computers can keep track of many objects, humans remain more capable of higher-level comprehension, reasoning, and anticipation. The large number of logs and alerts that could be generated on computing devices calls for visualizations that can augment human performance of cyber operations as those shown in Figure 1 below. Information visualization is a proven method to help make sense of large, complex problems. Specifically, cyber security visualization allows users to explore and navigate large security data sets to identify salient features, build context for investigations, or to identify suspicious activity requiring mitigation. However, it is possible that not all the visualization tools provide the necessary and sufficient information to effectively and efficiently respond to a cyber-attack.

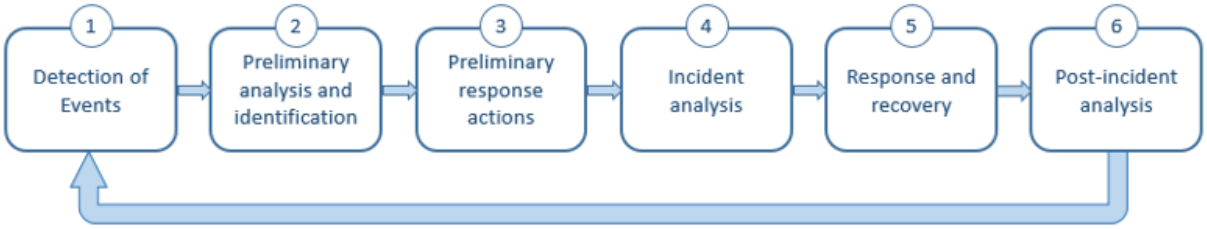

Figure 1 Cyber-incident handler's responsibilities [3]

c. This paper discusses best-practices that should be taken into consideration when developing methods for automated cyber-attack protection. Furthermore, this paper also discusses best-practices for designing cyber visualization tools that provide all the necessary and sufficient information in support of the cyber-incident handler's responsibilities.

Discussion:

a. Best Practice #1 (Cyber-security visualization):

1) Figure 2 below shows a structured method for designing cyber visualizations [2]. The main objective of methodology discussed herein is to convey the information required for a cyber operator to decide on the nature of event activity presented in alerts and to process event tickets or alert queue more efficiently and effectively, relying largely on current data rather than historical analysis. Specifically, the methodology discussed herein supports very early cyber analysis tasks (e.g., "Detection of Events" and "Preliminary analysis and identification" as shown in Figure 1) which are accomplished in near real-time, under high volume data intensity. Decisions are often made in seconds during the early stages of cyber-attacks to avoid alert queue overflow, which could result in malicious activity going unresolved.

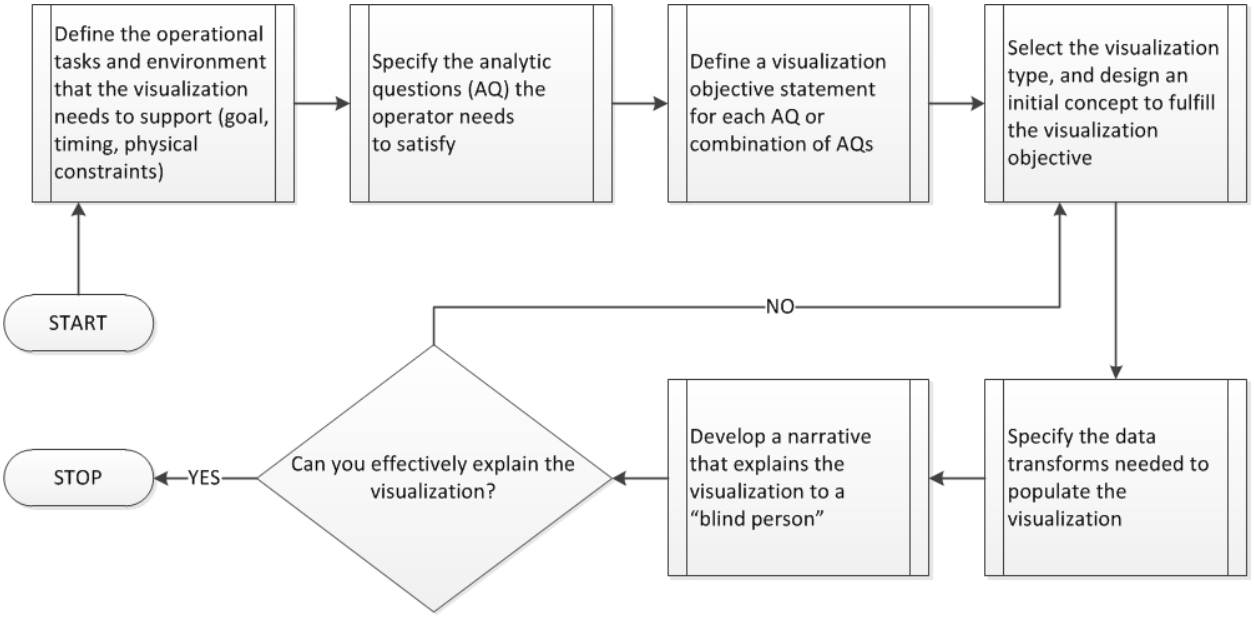

Figure 2 Methodology for designing cyber security visualizations

2) Some guidance associated with the proposed methodology include:

   i. Prior to designing cyber security visualizations, it is necessary to define the operator decisions that the visualizations must support and the information requirements that the operator must satisfy in order to make these decisions.

   ii. Only after understanding what the operator needs to know to do his or her job, developers can design visualizations to provide that information in an easily consumable and actionable form.

   iii. Define the list of analytic questions the operators need to satisfy in response to a cyber-attack. An example of an analytic question would be: "*Is there a significant deviation in the number of events being reported during the recent time period and what is typically observed?*" The resulting visualization objective could be: "*To depict the current event activity (volume, intensity, and type) as compared to some 'normal' baseline (defined as a range of activity), so that any data plot outside of that baseline range can be immediately seen as a deviation from normal that warrants investigation*."

   iv. While in the process of specifying the data transforms needed to populate the visualization, raw data must be processed into structured form and

selected based on the criteria established as part of the visualization objective.

v. If a given visualization cannot be effectively explained verbally by its developer then, the more likely the visualization will not be easily interpreted by the end users.

vi. It is useful to consider the cyber operator's work in terms of the decisions they make, rather than specific stages or tasks. Such guidance allows for removing any assumption that a cyber operator has already been exposed to information obtained in a prior activity as those shown in Figure 1.

b. Best Practice #2 (Cyber-attack protection automation):

1) Establish good cyber security hygiene, such as implementing established best practices for cyber risk management, removing known system weaknesses and misconfigurations, and patching known vulnerabilities [1]. [Note: Data indicates that most cyber-attacks are not based on new and sophisticated techniques but instead on well-known, publicly available vulnerabilities.]

2) Use of network architecture models that operate on a decentralized versus centralized approach. Centralized approaches such as that as shown in Figure 3 below fail to provide adequate cyber-protection due to the need to have perfect visibility throughout a networked ecosystem[2]. Specifically, traditional information security models are static and derive from traditional physical security models, where a stationary perimeter surrounds the protected information systems [1]. However, the perimeter disappears when users require increased connectivity to third parties and others outside the organizational perimeter.

To mitigate the potential consequences associated with a centralized network approach, new security models that operate in a de-perimeterized ecosystem via a decentralized network architecture such as that shown in Figure 4 could allow the system to respond faster than is possible with a centralized model. That is, a decentralized network architecture allows for identifying potential cyber threats and responding immediately and instinctually as necessary as discussed in the next principle.

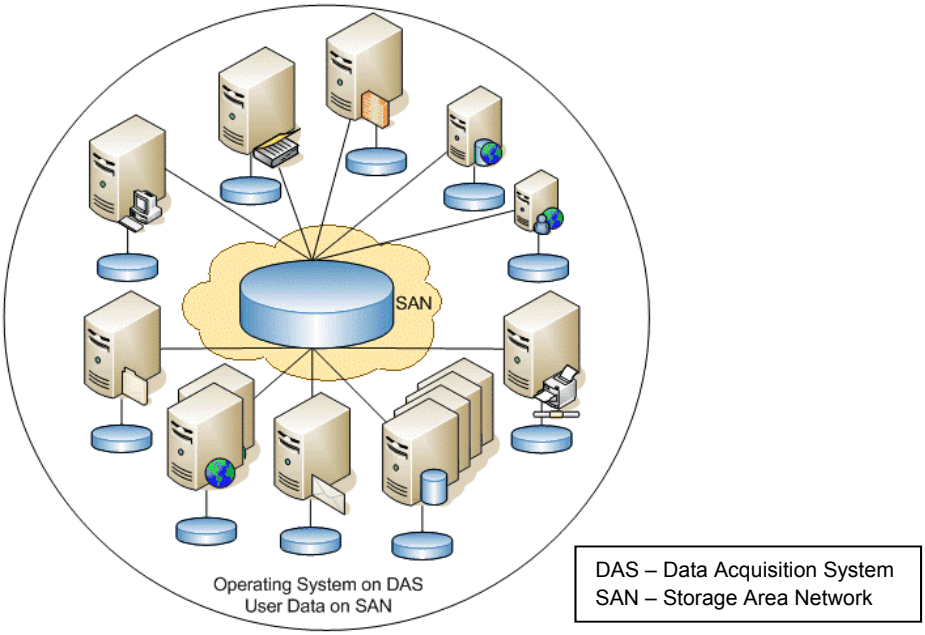

Figure 3 Notional fully-centralized architecture

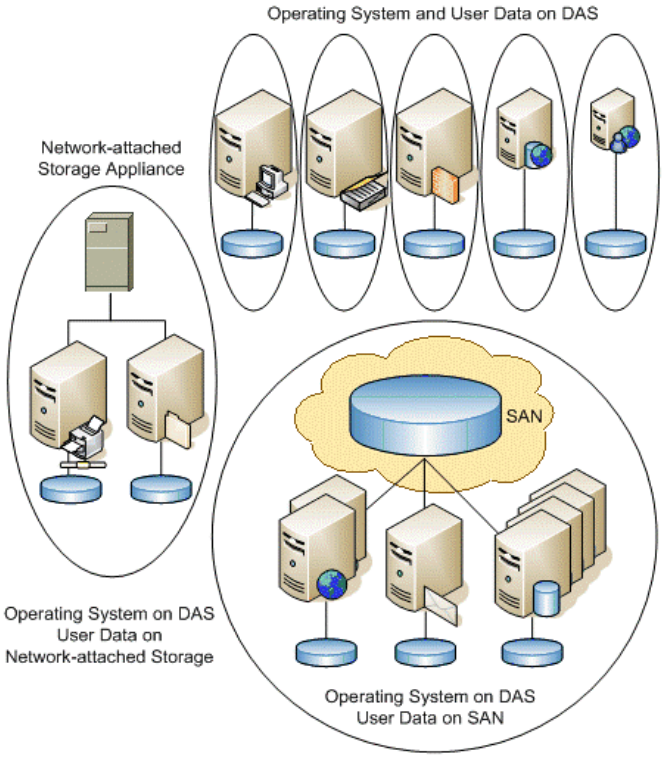

Figure 4 Notional fully-distributed network architecture

3) In addition to implementing network diversity and a distributed network architecture as discussed above, implementation of the following network system characteristics would help mitigate the risk of complex attackers via an equally complex and responsive defensive system:

Characteristics[1]	Basis/Rationale[1]
Network nodes should be able to modify their defensive posture [1] and activities through local interactions within their environment and no central system. Examples of defensive posture and activities include: • Blocking IP addresses, ports, sites • Disabling services • Increasing security by checking for updates more frequently and moving to a higher security state • Slowing the reaction and response time and eventually tightly restrict communications with the rest of the environment • Taking a node offline until the system is patched or fixed	Nodes respond rapidly to weaknesses and anomalies faster than would be performed by a human or centralized system. Traditional security managers stage their upgrades over days, or weeks, or more. However, if one node detects an anomaly to address by a planned update, the priority of patching that system should change. An increase in the defensive posture would reduce the risk of a cyber-attack in the largest attack surfaces.
As the defensive posture increases for the affected network nodes, their level of "nervousness" [1] will decrease thus returning the system to a normal state.	The "nervousness" or "paranoia" [1] level of the network host modifies the attack surface sensitivity.
All network nodes should rely on the same set of simple cyber-security rules.	Promotes having a set of shared security goals and rules to communicate among nodes in a de-centralized network system. Enables a stable, resilient, and harmonious environment among the network.

Conclusion: There may be different approaches when protecting against cyber-attacks. The best-practices discussed herein are not to be construed as a requirement or regulation. Instead, this paper provides information for two viable technical protection alternatives related to: (1) developing methods for automated cyber-attack protection; and (2) designing cyber visualization tools that provide all the necessary and sufficient information in support of the cyber-incident handler's responsibilities. Nonetheless, the approach taken for effectively protecting against cyber-attacks should be justified for suitability for the particular application.

References

[1] "ANTS: A Biologically-Inspired Model for Agile Cyber Defense," E. Crane

[2] "Mixed Method Approach to Identify Analytic Questions to be Visualized for Military Cyber Incident Handlers," L. Buchanan, A. D'Amico, and D. Kirkpatrick

[3] U.S. Department of Defense, Chairman of the Joint Chiefs of Staff Manual, Cyber Incident Handling Program: CJCSM 6510.01B, 10 July 2012 (Directive Current as of 18 December 2014)

Glossary

Attack surface - The total sum of the vulnerabilities in a given computing device or network that are accessible to a hacker. Attack surfaces can be divided in to a few categories: (1) the network attack surface; (2) the software attack surface; and (3) the physical attack surface.

Critical Digital Asset (CDA) - A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network.

Critical system (CS) - An analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.

Cyber-attack - The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve physical or logical threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CSs integrity, availability, or confidentiality or the attempt to cause an adverse impact to a safety, security, and emergency preparedness function. Further background on cyber-attacks which are up to and including DBT, can be found in Sections 1.1(c), 1.2, and 1.5 of Regulatory Guide 5.69, and the cyber-attack may occur individually or in any combination. [Note: Consistent with 10 CFR 73.54(a), a licensee must provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the a design basis threat, as described in 10 CFR 73.1. Consistent with 10 CFR 73.54(a)(1), licensees must protect from cyber-attacks digital computer and communication systems associated with certain categories of functions and support systems and equipment, which, if compromised, would adversely impact the safety, security, and emergency preparedness functions of a nuclear facility. These functions include safety-related and important-to-safety functions, security functions, and emergency preparedness functions (including offsite communications). These functions must be protected from cyber-attacks that would adversely impact the integrity or confidentiality of data and software; deny access to systems, services, or data; or provide an adverse impact to the operations of systems, networks, and associated equipment.]

Incident - Occurrence, caused by either human action or natural phenomena that may cause harm and that may require action.

Internet Protocol (IP) address - A numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

Malware - Malicious software designed to infiltrate or damage a CDA, without the Licensee/Applicants consent. Malware is taken to include computer viruses, worms, Trojan horses, Root kits, spyware and adware.

Network - Group of components that share information or interact with each other in order to perform a function.

Node - A connection point that can receive, create, store or send data along distributed network routes. Each network node -- whether it's an endpoint for data transmissions or a redistribution point -- has either a programmed or engineered capability to recognize, process and forward transmissions to other network nodes. In internet and intranet networks, most physical network nodes are host computers that are identified by an IP address."

Patch - A fix for a CDA or software program where the actual binary executable and related files are modified.

Threat - Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.

Vulnerability - Feature, attribute or weakness in a system’s design, implementation, or operation and management that could render a CDA open to exploitation or safety, security, and emergency preparedness function susceptible to adverse impact.