**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: Module 3 Review Questions

Brian Russel Davis, brian\_davis@brown.edu

Question 1: Choose what you consider to be the 3 most important Basic System Security Technologies from the readings and explain your decisions (in at most 200 words).

Access control by far is the most important aspect of Basic Security Systems. Access to files, applications, network resources, credentials and all of the other jewels that make up an organization’s assets often the target of attackers. Without smart access control, an attacker will have free reign to steal, destroy and hide inside a network. It follows therefore that limiting or eliminating peer to peer connections is critical. It is almost impossible to guarantee an employee’s credentials will not be compromised. If an attacker can pivot through an organization by using open and poorly secured peer to peer connections, it will be next to impossible for a centralized network analytics monitoring software to catch illicit activity.

The second most important mitigation is routine patching of software within the enterprise. More often than not attackers exploit vulnerabilities in Operating Systems, Productivity Software, Network Software or any piece of software that is widely distributed throughout the organization. Since many of these tools are used with the intention of sharing files or access, it is easy for an attacker to exploit a vulnerability and then hide illicit activity within the normal course of user interaction.

Third, on my list is the segregation of networks and functions. As the IAD states, “plan for the

possibility of a successful intrusion and design the network architecture and management procedures to separate segments based on role and functionality”. Assuming that an attacker will gain access to a network is probably the best defensive posture for any security team. Traditional “moat builders” secure the perimeter but fail to set up intelligence rules of applications, servers, and services to safely communicate with each other.

Question 2: Identify 3 topics from the Basic System Security Procedures and the Secure Network Operations readings that you consider most important to protect your network. Pick one topic and provide a synopsis of it (in at most 200 words).

Networks are hard to manage, especially in a time when IoT is becoming more and more popular. A network engineer tasked with monitoring network traffic will instantly be overwhelmed with activity with no idea of who, what or where to look to find malicious activity. Setup up rules around DNS, routing, and intricate firewalls don’t solve the problem. Attackers pivot through these rules and use the tools meant for protection against the organization. The best tool to inject in the midst of all of this is human permission and authentication. Tools set up to authenticate people should be designed to keep asking for permission and authentication that verifies the action that is being taken is an action really being taken by a user, especially when the activity is abnormal. In the readings many of the attacks that are mentioned involve an attacker intercepting communication or spoofing the communication of a user. Most of this can be stopped by using encryption that starts with a physical object like physical encryption keys, two-factor authentication, and other personal credentials. This first step serves to prove that agent making a request is doing so with a valid encryption key. If the attacker is in the network and has compromised the private key, resources listening to a compromised request may not be able to invalidate request on the key alone. At this point, the network should have rules that analyze where a user is logging in from, the actions they are attempting to make and whether any of that activity falls outside of the normal activity for the user. The abnormal activity should generate a notification to the user. Once again the most important tool here is the attempt to bring the activity to the attention of a real person outside of the automated process. Human intelligence is the best tool in the network because when humans are trained to analyze the activity, activity from an attacker will be noticed and stopped.