Automated insider threat detection system using user and role-based profile assessment:

We can see that the method described in this article will catch anomalous intrusive insider-threat behavior. What if the behavior insider-threat behavior, but it is not anomalous. For example, an employee is completing the same activities each day, but they are also compromising the business each day with these activities. As another example, an entire role of employees could be compromising the organization with the same behavior and it would not raise a flag as anomalous. Is there a way to combat this? Is there a way to combat insider threat behavior that does not appear anomalous?

Towards Autonomic Security Management of Healthcare Information Systems:

This article talks a lot about protecting HIS systems from attack since they, for the moment seem to be more vulnerable to attacks. It lists a few reasons why HIS’s are seemingly much more vulnerable, but are there more reasons that we can think of? Another question I have regards this articles approach to solving the vulnerabilities of an HIS system. It considers outside attacks, but what if, like one of the other articles we read this week, we have an insider threat or an inside attacker? Do we think this is less likely in these types of systems?

A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions:

This article relays to us numerous aspects regarding stealth malware including an account of percentages of attacks across operating systems. We can see that Microsoft Windows family of operating systems maintains the large majority of the attacks. The article discusses some possible explanations of why this might be, but what are some other reasons that Microsoft might be at the top of this list? What are some of the major differences between Microsoft Windows and other operating systems? What might Microsoft do differently in the future to combat this? Are some of the mitigation techniques and solutions in this article applicable to this question?