Ryan Christopher
MET CS695 – Assignment 3

1. Summarize extra security threats and requirements when implementing BYOD (bring your own device), focusing on smartphones only.

Bring Your Own Device, while necessary for many roles and organizations, comes with a substantial list of security hurdles that demand consideration. Smartphones in particular come with a wide variety of security concerns where requirements should be enforced by an entity when attempting to safely implement BYOD.

One factor to consider when implementing BYOD in employee smartphones is the wide range of manufacturers, operating systems, protocols supported, and hardware age that make up the smartphone market. To name a few, there are manufacturers such as Apple, Samsung, and Google who manufacture devices running iOS and Android that support different protocols depending on when they were released. In addition, there is a growing subset of active devices that no longer receive updates due to their age in an attempt by companies to get users to purchase devices more frequently. By including more configurations of devices, there is an increased security threat as there is more difficulty in ensuring that each combination of hardware and software for each type of smartphone can meet the minimum security requirements for the hospital. The benefit of the doctors and nurses being able to access work-related information regardless of their location comes with the risk that these devices are not secure enough for communicating with the hospital's systems. Regardless of the security of the hospital's systems, if the smartphone devices that are accessing patient information are susceptible to attacks via their network connection, protocols used, or outdated software, then the entity's information can be compromised as well.

To combat this risk, a requirement can be established where employees must use a device that is no older than a set date such as 4 years, and use operating systems that provide frequent security updates such as iOS or Android.

Another important aspect of BYOD is the lack of asset management as personal devices are impractical to enroll or set up with the remote management software that enterprise devices are given. If there is a vulnerability detected or device found to be compromised, there is no method to immediately push changes to all employee personal smartphones or lock one specific personal smartphone without remote management that is normally viable through enterprise asset management systems.

2. Investigate the Samsung Knox solution by reading the whitepaper. Also, discuss how Samsung Knox addresses the threats/requirements identified in Question 1.

Samsung Knox was introduced in 2013 as an answer to the growing security concerns of smartphones in enterprise settings. While the service appeals more to smartphones that are enterprise assets, there are a number of features that apply to address the threats and enforce the requirements that would be needed for the implementation of BYOD.

To address the vulnerability of out-of-date operating systems and applications, Samsung notes that Knox makes use of a "Hardware-based Root of Trust" which stores verified signatures of applications that are approved to run. This helps guarantee that the correct, up to date applications are being used on devices.

Knox also includes a Linux kernel-level protection feature that monitors which applications run with superuser privileges with a "hyperviser-based protection feature" preventing unauthorized applications or unknown scripts from escalating their privileges. In the event that a system is compromised, Knox uses a "verified boot" to prevent any malicious programs from re-installing, and can certify whether or not a system has been booted with unauthorized code through the "Knox Warranty Bit."

These measures help counteract the vulnerabilities that appear with the growing number of combinations that smartphones have of software and application versions, as well as preventing bad actors from having malicious code stay and spread to other devices on a network.

With network security in mind, Samsung has Knox follow strong encryption protocols, where Wi-Fi connections use IKEv2 and a hybrid connection using symmetric and asymmetric encryption with AES and ECC. This helps to secure network communications from bad actors by using current protocols that have been tested by organizations such as NIST.

Samsung also makes a note to discuss the asset management capabilities of Knox including automatic enrollment and over-the-air updates to firmware. Named "Knox E-FOTA" for "Enterprise Firmware Over-the-Air," the service can force firmware updates on devices that are enrolled in an organization's Enterprise Mobility Management system when security patches are released. As a result, there is a lower likelihood for a device in the EMM to become compromised due to an exploit carried out on outdated firmware once vulnerabilities are found.

The Knox platform can also log unsafe domain access, where devices attempting to gain unauthorized access are made visible to the organization before access is given. According to Samsung, the reports contain the app name, blocked domains, and timestamp of when access was denied.

Knox helps to address many of the issues present in smartphones interacting with enterprise systems as addressed in question 1. With the features provided and requirements that can be enforced, these security threats become more controlled. While most of these features are offered through enterprise devices and not personal devices, the services provided make a compelling argument for entities to standardize their mobile hardware and software in the goal of achieving mobile device security.