JHU Information Assurance Analysis
Module 6 Assignment

1 Ransomware

What is ransomware? How does ransomware work cryptographically? In your opinion are mobile devices more prone to ransomware attacks than desktops, why or why not? What are some of the defenses that can be employed to defend against ransomware?

2 Bluesnarfing & Bluejacking

What is bluesnarfing and bluejacking? How do they compromise bluetooth technology? In your opinion with the increasing number of Internet of Things (IoT's) being IP addressable and being able to connect to smart devices/phones, will these and other Bluetooth types of attacks increase? Support your answer.

3 Mobile Application Scanning

Static & Dynamic analysis scanning methods are a popular method to use against mobile devices. Static analysis includes assessing the security of Android or I-Phone Apps, detecting app clones, automating test case generations, or uncovering non-functional issues related to performance or energy. Dynamic analysis includes testing & evaluating a program by executing data in real-time. Discuss **two (2) static** and **two (2) dynamic** tools used for mobile applications? With respect to cost & implementation, is there any differences between them? Discuss any cloud solutions which exist for performing this type of analysis?

4 OWASP Mobile Vulnerabilities

Go to the following link; https://owasp.org/Top10/ You will see a list titled **Top 10:2021 List** on the left hand side of webpage**.** Then review the ICS-CERT FY 2016 Annual Assessment Report Sections 2.1 & 3.2 found here; https://www.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf as well as review pgs 7-15 and Figure 11 & Figure 12 on pg 13 & pg 14 respectively in the attached Dragos pdf. (found in assignment section of CANVAS).

How do the ICS vulnerabilities differ from typical IT/enterprise web based application vulnerabilities? Pick **two (2)** mobile 2021 vulnerabilities (i.e., A01 through A10) that you feel are the most significant and explain why they are and how they can be guarded against?

Read "Top 10 Mobile Risks- Final List 2016 found here; https://owasp.org/www-project-mobile-top-10/2016-risks/

Which mobile OS are attacks more successful against: Android or iOS, and why?

5 Application Program Interfaces (API's)

A foundational element of innovation in today's app-driven world is the API. APIs are a critical part of modern mobile, SaaS and web applications and can be found in customer-facing, partner-facing and internal applications. By nature, APIs expose application logic and sensitive data becoming targets for attackers. Pick **two (2)** items from the **"API Security Top 10 2019"** list that you feel are the most significant and explain why they are and how they can be guarded against? Click on Blue API to drill down further. API list can be found here; https://owasp.org/www-project-api-security/

6 Protecting Work Information System & Data

Many organizations provide standard image laptops, require secured VPN connections using HID tokens, run VDI & RDP software from a trusted device, and allow BYOD's. Pretend you're the CIO of a fortune 500 company. Describe to me in 3 to 4 paragraphs your method/plan on how you would implement a BYOD policy. Have your plan focus on protecting the security of the company's assets, systems, and sensitive/proprietary data, and PII/PHI of the employees for when BYOD's are used at work and off-site/home. BYOD's are considered any mobile device. Have your plan cover work situations/environments for outbreaks/pandemics (i.e., COVID-19).

Please make sure to answer all the questions and site your sources. Submit in either PDF or Word document format to Module 6 assignment in CANVAS. Might have to copy and paste links.