Rebound Security – Mobile Device Use

Kelsey Cator

Candie Estrada

M. Fitzhugh

[kyc@students.columbiabasin.edu](mailto:kyc@students.columbiabasin.edu)

[redyesyami@yahoo.com](mailto:redyesyami@yahoo.com)

Candieestrada@hotmail.com

CSIA 330-8373 Wireless Security

Winter 2020

**Problem Statement**

Our group has been tasked by Rebound Security’s CEO, Eric Robinson, to answer questions he has on his employee’s guest wireless use. Mr. Robinson is especially interested in mobile device management solution. This is a type of software used to monitor, manage and secure employees’ mobile devices that are deployed across the company. The utilization of this type of software can help prevent unsecure access to the company’s network.

Our group will be using data provided by Mr. Robinson, Microsoft’s Excel, and the Internet to research and provide answers for the following fourteen questions below.

1. What is a mobile device management (MDM) solution? What risks does its use address?
2. List the top three product offerings in the MDM market. Which one is the industry leader and why?
3. Show the ownership breakdown by company and employee and unknown. What is the risk with the "unknown" category?
4. What is the most common platform in use? What is the most common model?
5. In the 'Compliance Status' column, what is the difference between "rooted" and "jailbroken"?
6. Show the breakdown for all the 'Compliance Status' categories.
7. What does the 'Enrollment' column mean and what is its risk implication?
8. What department is in greatest need of security training regarding device use?
9. Which category of devices present a significant technical risk to Rebound Security and why?
10. All the listed devices may connect to Rebound Security's guest wi-fi network, which is public. So, why are all the known IP addresses ('Wi-Fi IP Address' column) private then?
11. Using limited data available, how many broadcast addresses does Rebound Security use? List your assumptions about the network configuration.
12. From the data provided, which platform appears to be the most "secure" and why?
13. From your research online, which platform appears to be the most "secure" and why?
14. Based on the data presented, what specific policy recommendations would you make to Rebound Security (e.g. Do not allow rooted devices)?

**Solution**

1. What is a mobile device management (MDM) solution? What risks does its use address?
   1. In order to better understand mobile device management solution and its risks, our team used our best resource, the internet, to better understand what it is and why it is important.
2. List the top three product offerings in the MDM market. Which one is the industry leader and why?
   1. Our team was able to find multiple product offerings in the MDM market. We found the top three offerings and then found which one is the industry leader. After finding the industry leader we were able to find out why it deserved such a title.
3. Show the ownership breakdown by company and employee and unknown. What is the risk with the "unknown" category?
   1. Our team used the Excel worksheet to show the breakdown of ownership. After understanding what we were looking at, we were able to find the risk of the unknown category.
4. What is the most common platform in use? What is the most common model?
   1. We used the Excel sheet provided to find the most common platform and most common model used. We specifically used a formula to help provide this information. The formula used for most common platform was =INDEX(C2:C847,MODE(IF(C2:C847<>"",MATCH(C2:C847,C2:C847,0)))). The formula used for most common model in use was =INDEX(E2:E847,MODE(IF(E2:E847<>"",MATCH(E2:E847,E2:E847,0)))).
5. In the 'Compliance Status' column, what is the difference between "rooted" and "jailbroken"?
   1. In order to find the difference between rooted and jailbroken our team scoured the internet for definitions. We then took these definitions and compared them to the information in the compliance status column.
6. Show the breakdown for all the 'Compliance Status' categories.
   1. Our team used the Excel worksheet to show the Compliance status of each device. By looking at the Compliance status column we found out how many of each device listed was Compliant, Jailbroken, Rooted or Not available. We took the total devices and divided them by the amount of each category to get the percentages presented.
7. What does the 'Enrollment' column mean and what is its risk implication?
   1. A google search of ‘Enrolled cellphone devices’ was made to gather information about what Enrolling devices allows a company to see or manage on the device as well as certain risks having an unenrolled device would cause. We compared the Excel sheet to the total unenrolled devices and compared potential risks the company might have by not enrolling all devices into the network.
8. What department is in greatest need of security training regarding device use?
   1. In order to see which department is in greatest need of security training we analyzed the Excel spread sheet and we compared how many devices were unenrolled in the companies network as well as jailbroken and rooted devices and crossed referenced it with the department which concluded the Marketing department needing to tighten up the security of their respected devices.
9. Which category of devices present a significant technical risk to Rebound Security and why?
   1. We concluded that Unenrolled devices present a greater risk to Rebound Security because of searching risks of unenrolled devices as well as the benefits of having enrolled devices in the company’s network.
10. All the listed devices may connect to Rebound Security's guest wi-fi network, which is public. So, why are all the known IP addresses ('Wi-Fi IP Address' column) private then?
    1. Prior knowledge as well as searching the internet for private IP Addresses allowed us to conclude that Routers/ Access Points have their own private IP addresses that are commonly used.
11. Using limited data available, how many broadcast addresses does Rebound Security use? List your assumptions about the network configuration.
    1. To find how many broadcast addresses Rebound Security uses based on the limited data available, we first imported the data into Excel. We then sorted the data by the “Wi-Fi IP Address” column. From there, we deducted what broadcast addresses were used based on which IP address were in use—we assumed every IP address that shared the same first 3 octets were of the same broadcast group; counting every group to find the total number of broadcast addresses. Our assumption about the network configuration is that the subnet mask is 255.255.255.0.
12. From the data provided, which platform appears to be the most "secure" and why?
    1. Our team used Excel to sort the data by the Compromised column in descending order to see which platforms were compromised. Once the data is sorted, all data containing a compromised device can be copied into new columns. From there, the COUNTIF function can be used on the Platform column using “Android” and “Apple”. The platform with the most compromises would be considered least secure, while the platform with the least compromises would be considered most secure.
13. From your research online, which platform appears to be the most "secure" and why?
    1. Our team used the search engine, Google, to find articles about which platform is most secure, and why.
14. Based on the data presented, what specific policy recommendations would you make to Rebound Security (e.g. Do not allow rooted devices)?
    1. Our group went over the data presented and used the Internet to search for suitable policy recommendations and why they should be used.

**Results**

1. What is a mobile device management (MDM) solution? What risks does its use address?
   1. Mobile device management is a type of security software used to monitor, manage and secure mobile devices. The use of such software is used to address the risk of employees who bring their own devices to use on a company’s network. This way they can manage and control these devices when they have problems.
2. List the top three product offerings in the MDM market. Which one is the industry leader and why?
   1. Microsoft’s Intune, Blackberry Enterprise Mobility Suite and Jamf Pro are the top three product offerings. Blackberry is currently leading the worldwide market for mobile device management. They are industry leader because they offer clear visibility as well as control of a user’s mobile devices. Their MDM facilitates complete data protection coupled with industry compliance (Heralkeepers, 2020).
3. Show the ownership breakdown by company and employee and unknown. What is the risk with the "unknown" category?
   1. The risk with the unknown category is that it is uncertain what type of device this is. It is unknown if it a company owned device, or an employee owned device. The risk is that this could be an attacker’s device infiltrating the network.
4. What is the most common platform in use? What is the most common model?
   1. The most common platform in use is Apple. The most common model is the iphone.
5. In the 'Compliance Status' column, what is the difference between "rooted" and "jailbroken"?
   1. Jail-breaking is usually done on Apple devices, it is the process of removing limitations put in place by the manufacturer. Rooting is the process of gaining administrator access to a device. After rooting the user can grant specific applications access to root permissions which allows them to do almost anything they want with the operating system. Rooting is generally done on Android devices.
6. Show the breakdown for all the 'Compliance Status' categories.
   1. **Complaint Status Break Down**

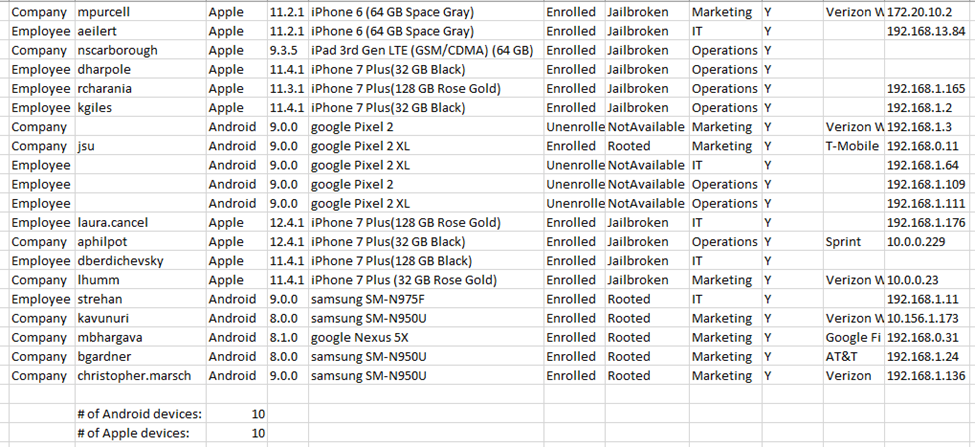
Complaint Devices: 686/ 846 = 81%

Jailbroken Devices: 15/846 = 0.02%

Rooted Devices: 9/846 = 0.01%

Not Available: 136/846 = 16%

1. What does the 'Enrollment' column mean and what is its risk implication?
   1. The Enrollment column showcases all the devices that are Enrolled in Rebound Security. Enrolling a device gives the company permissions such as being able to view Application details, phone number of the device, device model and manufacturer, device owner, name, serial number and IMEI. It also allows to check the device status, as well as check for malware, jailbreaking, and allows the company to bulk configure the devices with updated security protocols. Enrolling a device created an MDM certificate which communicates with the network which makes the device more secure. An enrolled device allows to limit the risk of Device loss, as well as keep track of BYOD devices since it is officially enrolled into the Rebound Security network.
2. What department is in greatest need of security training regarding device use?
   1. The marketing department is in greatest need of security training.
3. Which category of devices present a significant technical risk to Rebound Security and why?
   1. Unenrolled devices present the most technical risk to Rebound security because these devices are not in Rebounds Security network therefore information of Compliance are not available since they’re not registered in the system.
4. All the listed devices may connect to Rebound Security's guest wi-fi network, which is public. So, why are all the known IP addresses ('Wi-Fi IP Address' column) private then?
   1. The routers and access points used by Rebound Security have the private IP Addresses which is what is showcased even if the guest wi-fi is being used.
5. Using limited data available, how many broadcast addresses does Rebound Security use? List your assumptions about the network configuration.
   1. From the limited data available and our assumption of the network configuration that the subnet mask is 255.255.255.0, there are 61 broadcast addresses that Rebound Security uses.
6. From the data provided, which platform appears to be the most "secure" and why?
   1. From the data provided, it appears that neither platform is more secure than the other. As seen in the screenshot of the sorted data below, there is an equal number of compromised devices from both devices, showing that neither is more secure than the other. It’s worth noting that almost all of the compromised devices are either jailbroken or rooted.



1. From your research online, which platform appears to be the most "secure" and why?
   1. According to Rafter, iOS is considered most secure, making the Apple platform the most secure. He goes on to state that, “Apple doesn’t release its source code to app developers, and the owners of iPhones and iPads can't modify the code on their phones themselves. This makes it more difficult for hackers to find vulnerabilities on iOS-powered devices” (Rafter, n.d.).
2. Based on the data presented, what specific policy recommendations would you make to Rebound Security (e.g. Do not allow rooted devices)?
   1. One policy recommendation our group would recommend to Rebound Security is “Do not allow root devices.” We make this recommendation because there are 20 compromised devices being used. As Snyder points out, that a rooted device exposes company data to new threats. These threats include malware, which may have been unknowingly installed on the rooted device (Snyder, n.d.). Another policy recommendation would be “Automatic Update.” There are many devices that are not running the current OS update. According to ZOHO Corp., the disadvantages of running an outdated OS are: “additional tech support for devices running lower versions of the OS; enterprise apps must support these OS versions; and unavailability of vital device/security features which are specific to particular OS versions.”

**References (APA format)**

Beal, V. (n.d.). MDM - mobile device management. Retrieved from <https://www.webopedia.com/TERM/M/mobile_device_management.html>

ErikjeMS. (2019, April 24). What is Microsoft Intune device enrollment - Microsoft Intune. Retrieved from <https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment>

Heralkeepers. (2020, February 3). Mobile Device Management (MDM) Market 2020 Global Analysis, Industry Size, Share Leaders, Current Status by Major Key vendors and Trends by Forecast to 2023. Retrieved from https://www.marketwatch.com/press-release/mobile-device-management-mdm-market-2020-global-analysis-industry-size-share-leaders-current-status-by-major-key-vendors-and-trends-by-forecast-to-2023-2020-02-03?mod=mw\_quote\_news

Hoffman, C. (2017, June 20). What's the Difference Between Jailbreaking, Rooting, and Unlocking? Retrieved from <https://www.howtogeek.com/135663/htg-explains-whats-the-difference-between-jailbreaking-rooting-and-unlocking/>

Jain, M. (2019, November 6). Microsoft Intune brings mobile threat defense to unenrolled BYO devices. Retrieved from https://techcommunity.microsoft.com/t5/enterprise-mobility-security/microsoft-intune-brings-mobile-threat-defense-to-unenrolled-byo/ba-p/966734

Preimesberger, C. J. (2020, February 27). Top Mobile Device Management Companies. Retrieved from https://www.eweek.com/mobile/top-mobile-device-management-companies

Rafter, D. (n.d.). Android vs. iOS: Which is more secure? Retrieved from https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html

Snyder, J. (2020, January 21). What Are the Security Risks of Rooting Your Smartphone? Retrieved from https://insights.samsung.com/2019/05/29/what-are-the-security-risks-of-rooting-your-smartphone/

ZOHO Corp. (n.d.). Automate OS Updates. Retrieved from https://www.manageengine.com/mobile-device-management/help/os\_update\_management/mdm\_automate\_os\_updates.html