RMU Network Security Analysis

Austin Patnesky, Zarek Rush, Eric Miller

Robert Morris University

Secure System Design

12/4/2024

Introduction

To initiate our network mapping process, we conducted a thorough physical walkthrough of the campus, systematically examining each building to understand the physical layout and identify any issues or holes in the network setup. This allowed us to estimate the number of users expected to utilize the network throughout the day. During the physical assessment, we pinpointed the locations of access points and server rooms and made informed assumptions regarding their configurations. Additionally, we evaluated the physical security measures in place, such as the presence and positioning of security cameras, identification of open and unsecured ports, and the use of ID card readers. We also ensured that server rooms and equipment rooms were securely locked. Following the collection of this physical data, we shifted our focus to the virtual aspects of the network. We reviewed user and group policies, determined accessible resources and sites, assessed network segmentation, evaluated the Wi-Fi security protocols in use, identified the DNS servers being utilized, and confirmed whether Multi-Factor Authentication (MFA) was required for all users. Having compiled this comprehensive information, we are now prepared to present our findings and provide security recommendations for RMU's network.

Network Requirements

As with any network, or system, requirements are necessary to reign in our design and stay focused on the task at hand. The following table consists of our updated requirements for the RMU Network. The requirements are broken down into four fundamental aspects of a network: Physical, virtual, software, and networking.

Requirement Number 1 : Physical 2 : Virtual 3 : Software 4 : Networking	Requirement	Rational	Additional Notes
1.1	The network shall further implement ID readers	ID readers ensure people are who they say they are	Would possibly have to combat RFID readers
1.1.2	The network shall have these readers be up to date with all clients.	ID readers must be able to work for those who need to use them with proper permissions	
1.1.3	The network shall have user groups for ID readers	This makes sure that only certain users may access sensitive areas	
1.1.4	The network shall have the ID readers lock doors to sensitive areas	Protects sensitive data and equipment from threats	
1.2	The network shall have secure physical ports	Many computers and ethernet ports have their ports open	Many ports were open in classrooms and labs
1.3	The network shall a way to destroy sensitive documents	The university deals with sensitive information and it must be dealt with	Could be a shredder or electronic device killer

		properly	
1.4	The network shall have multiple servers	Allows for data of multiple types to be stored securely and network segmentation	
1.4.1	The network shall have multiple types of data servers	Allows for better network segmentation and separation of duties	
1.4.2	The network shall segment these servers	Network segmentation eliminates possible movement across the network	
2.1	The network shall have virtual desktops with current software	These desktops currently have outdated software on them which could lead to possible attack vectors	currently using AWS AppStream 2.0 and 1.0 running old software
2.2	The network shall have secure accounts	User accounts hold sensitive information and this should be kept safe	
3.1	The network shall have up-to-date software	Prevents possible threat actors	Problem with current virtual desktops
3.2	The network shall use software to protect the network	Using software such as antivirus software or an IPS would only increase security	Prevents threat actors (assumption)
4.1	The network shall have multiple subnets	allows for network segmentation	Ensures separation of duties
4.2	The network shall be comprised of multiple smaller network groups	allows for the multiple network groups	

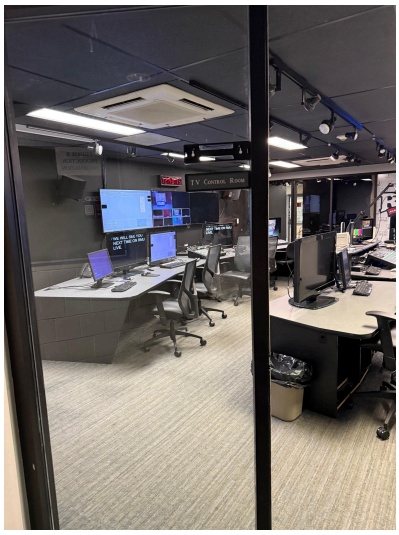
4.2.1	The network shall have a basic secured network segment	Allows for basic network usage while still being secure	student network
4.2.2	The network shall have a subnet for faculty and admins	The faculty and admins would have different permissions on the network then students	
4.2.3	The network shall eliminate expired users	Takes away an account that may be an access point for an attack	
4.3	The network shall have secure banking connections	Because of the food courts across the campus, the network must protect users' banking information	
4.4	The network shall have a clear policy	Users and staff need to know what they can and cannot do	
4.4.1	The network shall have the policy be consistently updated	The policy must be updated to deal with the nature of the ever-evolving network	

On-Site Security Assessment

While virtual risks are important to protecting the network, the physical and on-location aspects of the network are just as important. As mentioned previously, the team walked around campus to see what security the network was currently employing and what could be implemented in the future. The overall physical security of the campus was a mixed bag, with doors to server rooms, closets, and rooms containing expensive equipment all being locked, but at the same time, other doors were wide open or just not locked. This was especially an issue with doors that were to be unlocked via ID card, as nearly every door that was supposed to be secured by this was not locked. The only door secured via these ID card readers that worked was the one leading to the esports gaming room. This is a big issue as some of these doors lead to computer labs, workspaces, and more.

Another big flaw dealing with the security of the network, or how the network is to be used, is the lack of findable policy for what can be done on the network. The last policy that can be found relating to the network was created in 2016 containing severely outdated information. What users can and cannot do on the network must be expressed, as this will allow RMU a valuable piece of evidence if they ever face an attacker in court. The only findable policy about RMU's network was found here: https://www.rmu.edu/sites/default/files/it-site-docs/policies/RMU-IT-SEC-01InformationTechnologyAcceptableUsePolicy.pdf

Continuing with the problem of unlocked doors, doors leading to hardware with direct access to RMU accounts were left open with the systems running, which could lead to threats sneaking in and deploying malicious software or hardware on these devices, allowing them to do all manner of possible attacks. This was particularly bad in the Patrick Henry building where almost every office door was kept open, the door to the media center was unlocked, and more. It should be noted that storage doors and unlabeled doors were kept locked.

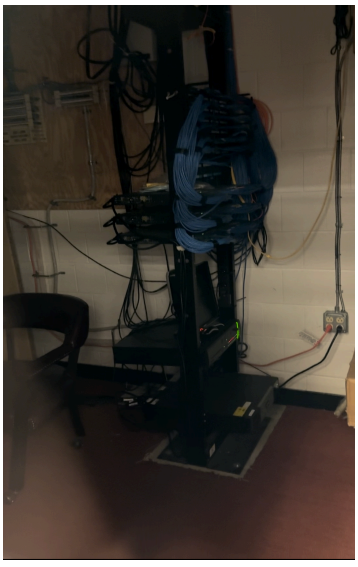


Another possible issue we came into contact with was the amount of open ethernet ports and external system ports in every building. While we could not test this, it is possible that these ports lead as a physical way to access the network. If the network does not have the proper access controls attackers could use these ports as a way to attack the network. There was even an instance of an object covering these ports, perhaps trying to hide them from users.

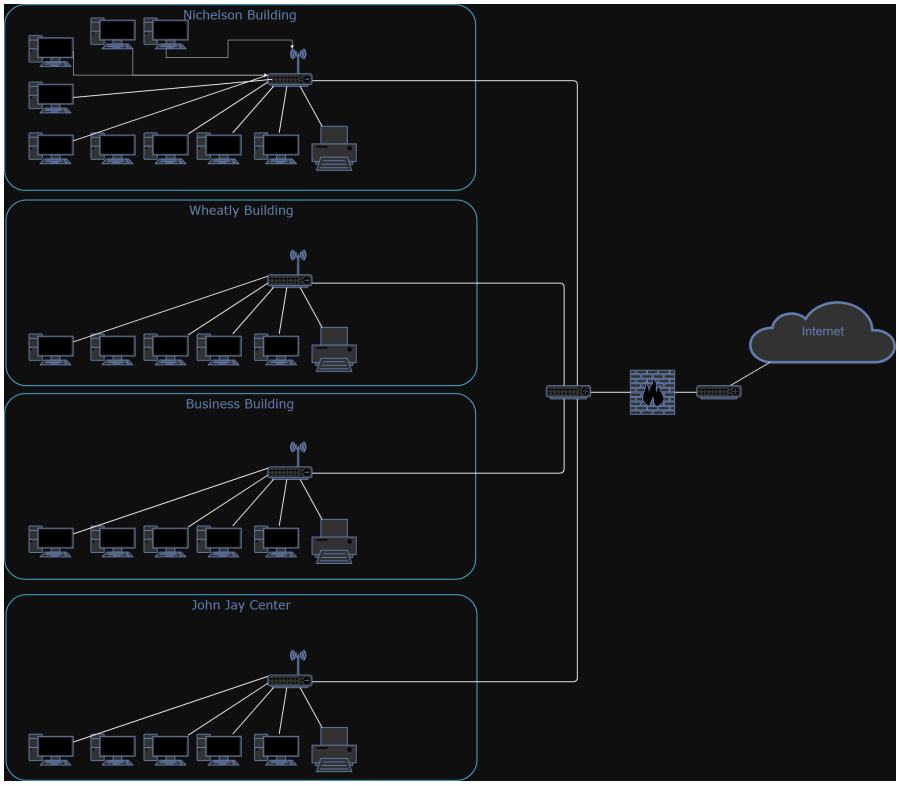
Open ports on hardware can be used for USB drives or other malicious hardware access, allowing for malicious use against hardware, accounts, or the network. Pair this with the previously mentioned computers left logged-in credentials and open the door, and an attack could easily occur.

The lack of ways to destroy sensitive data on the campus needs to be fixed as well. While walking through the campus, the only way to destroy sensitive data was found, and it was an old paper shredder. This is simply not enough for hundreds of faculty, students, and other workers. Not only do more of these shredders need to be installed, but ways to destroy sensitive data of electronic drives need to be put in place. While the team is guessing that RMU does not have a device like this, they need to have access to one if they don't. In the new age of technology, banking information, health information, and private information are all being stored on RMU's hardware. At some point, the university is going to need to destroy this hardware as this information must not be able to get out.

Other than these vulnerabilities, it seems as though RMU takes good care of its physical security. Most doors besides the ones found in the Patrick Henry building and those locked by ID card readers were locked, keeping nosy intruders out. The team even found what seems to be a hardware closet of some kind disguised as a study room in the library to hide the hard from attackers. Access points were located in each classroom but located on the ceiling to prevent tampering. It should be noted that the team did not find many cameras in these buildings, which may be a vulnerability itself.

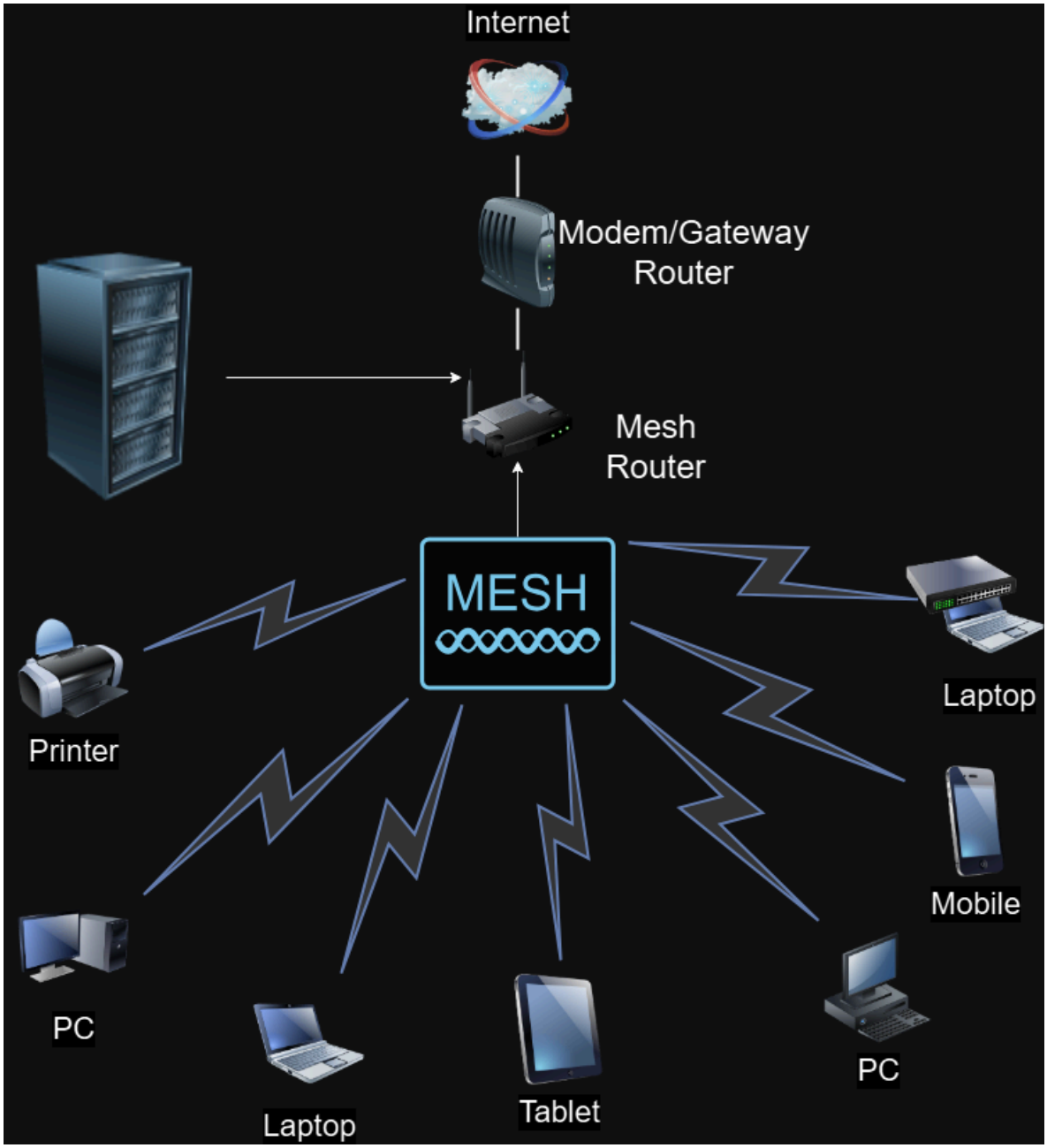


Physical Map



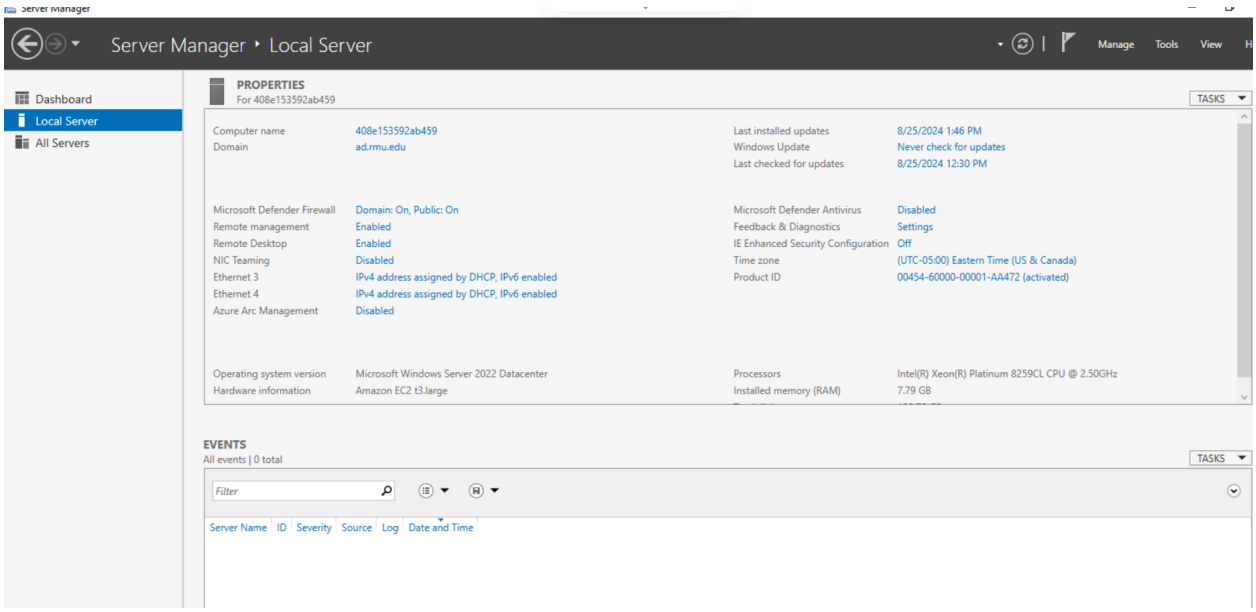
Our findings for our physical map are as follows. We have grossly simplified our map to Academic buildings only, as the dorms are not a part of the RMU network. To further simplify our diagram, we have also made every computer client you see represent 10 actual clients, printer clients represent 2 for every client listed. This is all in an effort to not overcomplicate our design while still leaving the same impact. It is also important to note that the Nicholson building is the biggest building containing 4 floors, the library, advisor offices, as well as two food courts.

Virtual Map



Our virtual Map is also simplified for the sake of not creating an eye sore as well. From our findings, Robert Morris uses a mesh network that connects to everything. So, as listed, every client connects to the mesh network which lets us connect to the modem, or default gateway, that then gives us access to the internet.

Remote Access



The RMU network also uses remote access. Through Amazon Web Services(AWS), we are allowed to connect to a RMU virtual desktop from anywhere in the world. We also found that you are reset every time that you are disconnected from the network. There is an option in AWS to have your specific desktop and data save between uses, but that is not active here. As depicted, we also found that AWS through RMU uses three different user groups. What must be noted about these virtual workstations is that they contain outdated hardware, and are running on the soon-to-be end-of-life Windows 10. While these are virtual workstations running off a server, it is harder to attack the network or cause serious damage through these VMs, but it is possible. We were even able to access the server managing software on these VMs to discover more information about them. With what we discovered about this workstation, the team wondered why the university was using these Amazon AWS systems over Microsoft Azure virtual desktops.

Vulnerabilities

- Network is not segmented
    - All of the Wi-Fi networks are on the same DNS server and network
- Only one DNS server for the whole network
- All internet segments have unencrypted DNS servers
- Most card readers were being used for decoration instead of intended purpose
- Multi-Factor Authentication is not enforced for all users
- Passwords are not forced to be changed, allowing the same passwords to be kept for a long time
- Computer and ethernet ports are left unsecured
- The virtual desktops have outdated software on them
- Windows 10 (which is soon to be end of life)
- All accounts on the network are roaming accounts
- The network does not have an updated policy of what users can and cannot do
- The lack of ways to destroy sensitive data on the campus

Trade Study

	AWS AppStream 2.0	WINNER Microsoft Azure virtual desktop
Rankings	64	25
4. Platforms Supported	4 (16)	2 (8)
3. Support	3 (9)	1 (3)
2. Price	3 (6)	2 (4)
5. Feautures	3 (15)	2 (10)
5. Integrations	3 (15)	1 (5)
1. Perfomance	2 (2)	1 (1)
1. Reliability	1 (1)	2 (2)

Reasoning

After completing the Trade Study our team came to the final conclusion that switching to the Microsoft Azure Virtual Desktop version would be a better fit than AWS Appstream. Since the Microsoft Azure Virtual Desktop was more optimal for a bigger network, and supported more platforms, the price was better when bought in bulk, there were tons of more features and integrations, and the performance and reliability were very similar to AWS Appstream anyway so it seemed like the obvious choice.

Recommendations/ Conclusion

In conclusion, the team does not think the university needs to completely discard the network and start new changes for security purposes are needed. For the most part after the assessment, we would say that the network is pretty good and does its intended purpose. However, with that being said the team still does believe that there are a lot of security concerns that can be fixed with our proposed recommendations.

For the on-site aspect of the network, the team recommends implementing and further improving the ID card readers. These readers, if implemented correctly, can be more secure than any normal lock, blocking lockpicking from occurring. These readers could also allow for better group segmentation, allowing a certain group of people or students access to certain rooms. These readers could also keep a log of who entered at what times, allowing for the university insight into who might have been in a certain room if something has occurred such as stolen goods or an attack on the network.

RMU must also not only rework its policy about network use but must incorporate a regularly scheduled revisit to this policy. Technology is an ever-evolving field, with new and exciting things always coming out, but because of this, the university must stop possible attacks from future technology before they can occur. These revisits of the policy must also remove old policies that are no longer relevant to the current way the network is currently being used.

While it is difficult to force people to close doors, staff must recognize the dangers of leaving systems unguarded. Training the staff and faculty that unguarded hardware, especially hardware that they have data on, will encourage them to stop this behavior. Training may not be necessary, but some sort of announcement or poster letting faculty know to keep their systems guarded would greatly prevent this issue.

While the team does not know if RMU has an intrusion prevention system as a part of the network, due to the amount of open ethernet ports located the team strongly encourages this. An IPS system would not only detect malicious traffic from these devices but block it and any traffic from the source address. While the network could simply deactivate these ports, many of them are being used by university systems and this would cause an issue with those systems. Committing to this option would mean connecting all the university computers to a wireless connection, which is less reliable than a wired connection, which is why the team recommends an IPS.

While the team also does not know if RMU has ways to destroy sensitive data, if they do not they should have a way to achieve this. As a private college, hundreds of students' sensitive information is collected such as banking information, healthcare information, and more. If this kind of data were recovered, found, or stolen from devices or physical media, not only would the student or faculty be in danger, but RMU as well as they could be found responsible for the data leak. To combat this, sensitive data shredders for physical media, and some form of crushing unit will be used to destroy the electronic device or hard drive holding the sensitive data.

Our team also decided that it would be best if RMU segmented their network more to control the traffic flow and enhance security. The main thing we want to focus on is segmenting the RMU-Secure Wi-Fi network and the RMU-Guest Wi-Fi network since they should not be on the same network at all. By doing this we can ensure people connecting to the Guest network can’t escalate from there and gain access to resources that they shouldn’t be able to. This makes it easier for the network administrators to be able to improve network performance, enhance the network security, reduce network traffic, have easier network management, and control network growth.

The team also recommended that Multi-Factor Authentication be enforced for everyone on the network. Since I do know that most people do have it I think they just have to roll out another update and ensure everyone has received it and are prompted to do so to enhance network security further.

Lastly, the team decided that it would be better if RMU switched to the Microsoft Azure Virtual Desktop version over the AWS Appstream. Since the Microsoft Azure Virtual Desktop was more optimal for a bigger network, and supported more platforms, the price was better when bought in bulk, there were tons of more features and integrations, and the performance and reliability were very similar to AWS Appstream anyway so it seemed like the obvious choice.