My Internship Experience

Chase Seider

Kyndryl Architect Internship

CYSE 368

Summer 2023

Table of Contents

Introduction

The difficulties I faced while trying to find a 2023 summer internship were more than I could have ever expected. Online schooling from covid-19 was not the best way for me to learn and I ended up changing my major from Computer Science to Cybersecurity after hitting the brick wall of online Calculus 2. Because of this, I was a bit behind when I transferred to ODU (Old Dominion University) from my community college and did not end up getting an internship during the 2022 school year. As a senior with no prior internship experience, it was very hard to compete in the intern market. However, after I sent over 200 applications out, I finally started hearing back from some great companies. One of them being Kyndryl. They offered me an internship position as a mainframe architect. One of the main things I was told was how much importance they put into cybersecurity and that they would love someone with a cybersecurity skillset to work with their team. At first, I was hesitant about accepting the offer because I was looking for a pure cybersecurity internship, but after doing my research I realized how much the architect experience would help me with cybersecurity! Going into this internship, I hoped to learn three main things. Those were a deeper understanding of computer systems and architecture, the architectural mindset, and how I could implement these into my cybersecurity skillset. A good architect needs to have both a deep understanding of computer, network, and storage systems, and the ability to adopt an architectural mindset so they can design fast, efficient, and cost-effective systems. I believe that implementing cybersecurity skills and ideas into an architectural mindset will give me the ability to not only design and implement safe and efficient system architecture, but also give me then a deeper understanding of computer architecture that is needed to secure systems, networks, and storage.

My start at Kyndryl

Kyndryl is a global technology services company and the world's largest provider of IT infrastructure services. The company designs, builds, manages, and modernizes enterprise IT infrastructure. Being just a couple of years old, Kyndryl was a spinoff from the giant tech company IBM and its infrastructure services department. Because of this, Kyndryl brings world-class technology skills and talent from IBM to a new customer-oriented business model. Some of the main services they provide include cloud computing, applications, and data, core enterprise and zCloud, digital workspace, network and edge computing, and security and resilience.

Kyndryl is a focused, independent, and customer-oriented company that is dedicated to helping customers navigate the advancement of the digital age. Because of their spin-off from IBM, they were able to become a more versatile company that uses multiple technology platforms. This has allowed them to create partnerships with companies like Microsoft and Red Hat. This gives them the freedom to offer their customers the best solutions no matter what the vendor. Because of this, they are trusted by some of the world's largest corporations such as Broadridge Financial, Coca-Cola, and Dow.

One thing that is constantly pushed throughout the company is the focus of "The Kyndryl Way." This set of values is applied to the entire culture of Kyndryl and is what separates them from other IT service companies. According to the company, "The origin of The Kyndryl Way was our desire to offer customers, investors, partners, and employees an experience of mutual benefit and success." This workplace culture includes six main values. Their employees are Restless, Empathetic, Devoted, Flat, Fast, and Focused. These values dictate everything from how the company and employees interact with customers, to the whole way the company is organized.

My orientation at Kyndryl started as a whole week of what felt like a college classroom setting. We had a lot of speakers that presented what the company was, what they do, their split from IBM, and "the Kyndryl Way." It made me realize how important values were to the company because we heard about "the Kyndryl Way" over and over for that first week. The company was incredibly supportive of the interns. They even offered to pay for any certifications we wanted to get while interning for them. After the first week, we were given our own office space and started to work with our respective teams. The architect interns got started by training on an IBM training application called zExplore. This application got us introduced to the world of mainframes and how to navigate and work on them. As a cybersecurity student, I was also given training opportunities on cybersecurity and mainframe security.

Management

The management environment at Kyndryl was both effective and confusing at times. Because we were interns, we had multiple managers that we had to look up to. We had our site leader, our internship manager, and our Mainframe Architect manager. When there were no conflicts between managers, the system they had in place worked well, but after the first conflict, I realized there was no communication between the managers. The internship manager wanted us to focus on internship activities like speakers that would come in or fun events that they would set up for us. At the same time, my Architect manager wanted me to focus on my architectural training and the projects that I was working on. Because of this, there were times when each manager was telling me to do something that directly went against what the other one wanted. When I mentioned this, instead of talking to each other they communicated through me, which did not help the situation at all. By themselves, these managers were great people and did an exceptionally excellent job with their departments, but there are communication problems between departments sometimes.

Focusing on the management of the architect team and my manager Pat Stannard, I loved the way that he managed his team. He genuinely cared about every member of his team and did everything he could to allow the interns to learn and be successful. He was highly available to the team and encouraged everyone to reach out to them if they had any problems or questions that needed to be answered. There were many times when I had a question or needed something to be explained and he would take 10-15 minutes out of his busy day to help me and get me where I needed to be. He was focused on teamwork and the bond between the architect team.

Every week he had “The art of innovation” meeting with the team where he encouraged everyone to share their ideas of what we could do differently and how we could improve both our work and our work environment. Once a month he would host an hour-long virtual happy hour where everyone could hop on a call for an hour while drinking and bonding. This department is going to stay with me as one of the best teams I have ever worked on.

My work

I started by shadowing my mentor who is a mainframe architect that has worked for both IBM/Kyndryl for the last 40 years. Mark was a fountain of knowledge and I learned so much about not only mainframes but also computer architecture in general. One of the things I did while shadowing Mark to work on a lot of his architectural paperwork for him. This included gathering mainframe information into Excel sheets, assigning IP addresses to the different mainframe ports, and helping document customer needs. Mark did an excellent job of explaining to me why mainframes are so important to the world today and the reasons they are still used. One thing about mainframes that caught my eye was how secure they are. Mainframes are the first computer that I have seen that can have fully encrypted data both at rest and in transit without impacting system speed at all. Because their architecture lacks vulnerable endpoints, they are also very secure in nature. It is extremely hard for someone to get into a mainframe system. The biggest risk of mainframe security is dealing with an inside job. Shadowing Mark taught me so many things, and I was so able to take a big load off his shoulders while he focused on more important matters.

Some of the work that gave me the most hands-on experience and learning opportunities were the Use Case Scenarios that we were given. (**See Appendix A**) Three different use cases were given to us throughout the internship. These use cases were created by members of the architect team using their real experiences and used to give us a problem and the necessary information to solve it. Because they include confidential customer and Kyndryl information, I can only talk about the first use case that we did. The first use case involved upgrading a company's z14 mainframe to a z16 mainframe. We were given descriptions of what the company needed and tasked to use the online IBM tool eConfig to create the order for the mainframe with all the specifications that we thought the company would need. I was told to have an extra focus on security when designing the z16 to fit my cybersecurity skillset. Included in the appendices of this paper is the documentation that I wrote up for this use case describing all the choices I made and why they are important. I am going to talk in detail about the security I added to this mainframe and leave the rest with the documentation. There were two main optional components that I added to the customer's mainframe to add security to the mainframe. The first component included adding the RACF (Resource Access Control Facility) component to the mainframe. This is an Access Control manager that gives the tools to manage user access to critical resources on the mainframe. Access control is a huge step in any cybersecurity plan, and this was a requirement for the mainframe. The next security piece that I added was two Crypto Express co-processor cards to the mainframe. These I/O attached cards are used for implementing cryptographic functions throughout the mainframe. Not only can they encrypt and decrypt data at

rest, but also all data while it is in transit throughout the mainframe. These kinds of training are necessary for Kyndryl because the main talent behind Mainframes is getting older and retiring. If new people are not trained and given the knowledge from experienced mainframe architects, there will be no one to work on the machines that help run the world.

Another big project that I worked on was a group presentation on a company called MainTegrity to the whole architect team. (**See Appendix B**) We were tasked with researching the company, their product called FIM+, and why it could be beneficial for Kyndryl to partner with them. We met with the CEO of MainTegrity multiple times throughout this process to make sure our data was accurate. This project was my favorite internship because it related to cybersecurity, and I understood a lot of the concepts that were at play here. MainTegrity created an application called FIM+ which stands for File Integrity Monitoring. File Integrity Monitoring is an internal control or process that validates the integrity of z/OS system files, application software, configuration parameters, and log files by comparing current files contents to a known desired baseline. FIM+ also alerts us to changes that may have occurred because of your files being compromised. It does this by using the concept of hashing. FIM+ scans a resource set on the mainframe and creates a hash value from the data. This value is sent to the FIM server and then gets stored in the FIM Secure Vault as the baseline value for that resource set. When a resource set needs its integrity validated, it scans a resource set, gets a hash value, and compares it to the baseline value that was stored in the Secure Vault for the scanned resource set. If the hash values match up, then the data is secure. If they do not match up, the data has been edited or compromised. Hashed resource sets can be unlocked and edited using the FIM+ application. Once unlocked and edits have been made, it can be saved and rehashed which is then added back as the baseline for that resource set. I have learned a lot about field integrity and hashing data during my cybersecurity classes at ODU and I was able to successfully present this information in front of the architect team and executives of the company. This was important for Kyndryl and the architect team because my manager believes this is a missing link in mainframe technology for mainframe security. Kyndryl is highly likely to partner with MainTegrity and their FIM+ product so Kyndryl customers will have access to more security.

Towards the end of the internship, I was tasked with researching how mainframes and the Azure cloud could work together. (**See Appendix C**) What I found is that most cloud providers view mainframes as a “legacy” technology. They want to migrate all customers off the mainframe and onto the cloud. However, this is not the right way to go forward in the future. Instead of trying to figure out which computing technology is better than the other, we can compare what each technology is better at doing. Mainframes are the best of the best when it comes to running applications that require an extreme amount of I/O processing. Cloud computing cannot realistically handle the amount of processing power than mainframes have in their current state. However, not every application needs to be hosted on a mainframe. These applications can be run more efficiently and at a cheaper cost on cloud-based systems instead. Choosing the right platform for the right workload is a key idea of a hybrid cloud environment. When an on-premises system and the cloud work together, this is called a hybrid cloud. A hybrid cloud takes the strengths of both on-premises and cloud environments by using them together instead of going all in one. One big way these technologies work together is by integrating cloud

services into mainframe systems. Microsoft and Kyndryl, two big tech companies, teamed up to create data pipelines that build connections between mainframes and the Azure cloud. This allows mainframe customers to transfer their data to the cloud and use key cloud-based applications and services including machine learning, AI, and data replication. This means data originally on the mainframe can now be used in Azure. I had to create a presentation to present to the company executives and explain why our partnership with Microsoft was so important.

Putting my skills to use

Throughout the internship, I have used my Cybersecurity skills in many ways. The most notable example is our group presentation on MainTegrity. Through an informative PowerPoint presentation to the architect team, we talked about a disruptive topic on MainTegrity and FIM+, a security software used to protect data sets on a mainframe. In this presentation, I focused on the security aspect and diagramed how exactly the software protects data sets on mainframes. File Integrity used by the MainTegrity team involves using the technique of hashing to perform file integrity monitoring of data. Hashing is an important topic I learned through my cybersecurity classes and is a technique used in data authentication and security. Hashing involves a one-way function that takes an input such as a file or a string, and outputs a string of characters of a fixed size that is unique to the input. Because of this, only the input should return the exact hash value. This is used for file integrity because if the files have not been altered then if you have the files, they should return the same hash key as the first time. Cryptography is a security technique that is used in many different security systems out there. Because of this, I was able to apply my knowledge of Cryptography to mainframe security.

Access control is a big topic that I have learned throughout my courses at ODU. Mainframes have an optional Access Control application called RACF that I got to get some hands-on experience with. RACF protects resources by granting access only to authorized users of the protected resources. RACF retains information about users, resources, and access authorities in special structures called profiles in its database, and it refers to these profiles when deciding which users should be permitted access to protected system resources.

ODU did an excellent job preparing me for this internship. From my programming, networking, and cybersecurity classes, just about everything was used in this internship. This gave me a good opportunity to get hands on experience in the field which is the best way for me to learn. Learning about mainframes over these twelve weeks hammered in the fact that cybersecurity is going to be important no matter the type of technology. Any type of business I end up working for is going to have a need for cybersecurity. Another thing that I realized is that I can take my cybersecurity skills into a job that is not necessarily purely cybersecurity. For example, if I were to become a mainframe architect, my knowledge and skills in cybersecurity would help me design more secure systems from the ground up. This foundational addition of cybersecurity is a massive increase to security on the system.

The internship outcome

The first learning objective I had going into this internship involved getting a deeper understanding of computer systems and architecture. Throughout this internship I got training and hands on experience about the ins and outs of mainframes and how these work. Even though this internship had a heavy focus on mainframes and the cloud, it taught me the different systems that go into computer architecture whether it is a basic desktop computer, cloud computing, or mainframes. There are so many things that happen at the architectural level of computing. Everything from processors, binary, data transfer, and microcode means that when you design a system, you must understand how these systems work together.

This leads to my second learning objective, the architectural mindset. Having an architectural mindset was described to me as being able to create a solution for the customer that is cost effective and efficient. There are many factors that come into play when creating a solution for a system and every single customer is going to have differing needs. This means you must have a deep understanding of architecture to have the flexibility to help these unique customers. As I have said before, this is the learning objective that cybersecurity really plays a big part in. Being able to design a solution while keeping in mind the cost, effectiveness, and security is a big step forward in the architectural mindset. Security should be considered on every level of a system. With this philosophy, solutions will be more secure right away and customer systems and data will be safer.

The most motivating thing about this internship was the opportunity to learn about a technology that I knew nothing about. Mainframes were just a thing from movies before I started this internship. Now I know that the entire world runs on mainframes. Just the fact that I have been able to learn about this has been an amazing experience for me. The most discouraging facts about this internship was how the internship program outside of the architect team was run. There were many conflicts between different assignments from the architect team and the internship team. The data science interns were assigned a data science project and the mainframe architects were assigned to the same project with them. It was really disheartening to have to put all my effort into a project that both did not interest me and did not involve my cybersecurity skills or what I have learned about mainframes.

The most challenging parts of this internship were the use cases I worked on and my research assignment. The use cases gave us customer information and wanted us to either design a mainframe, DASD storage, or VTS depending on the use case. We were only given the information that the use case creators were given when they had to deal with this real-life example. That means we had to test all our new knowledge and try our best to think like a mainframe architect. My research project had me research and present to the whole company how mainframes and the Microsoft Azure cloud work together. The hard part is that cloud providers typically view mainframes as legacy systems. Most cloud providers want you to migrate off the mainframe into their cloud services. However, through my research I realized that these two technologies worked better together than competing technologies. A hybrid cloud that utilized the computing power of mainframes and the benefits of Microsoft cloud such as data replication and access to the Microsoft data science application like Power BI or Azure DevOps

means that mainframe users now have an effortless way to view and visualize their data. Kyndryl and Microsoft realized the power of the hybrid cloud and created data pipelines between Kyndryl mainframes and the Azure cloud. These data pipelines allow seamless transfers of data between the cloud and mainframe systems making it even easier to utilize the power of a hybrid cloud.

The main recommendations I have for students that get this internship is to have an open mind and put the most effort in to learn as much as you can. This company is very generous to its interns no matter what role you intern in. They encourage you to get certification while here and will cover the costs of most exams. For the architect role specifically, make sure you are taking the initiative when it comes to your learning. Many architects on the team will answer your question, look over your work, and give you shadowing opportunities if you take the initiative to contact them. They even found out ways to incorporate my cybersecurity major into our projects, assignments, and training. The people here really want you to succeed, and this is a great internship opportunity whether you are an Information Technology, Computer Science, or Cybersecurity major.

Conclusion

In conclusion, this internship has provided me with more insight and ideas for how to advance my cybersecurity career. I can take my skills into many distinct roles in the tech field. Cybersecurity is a versatile role and the architect experience I have been through at Kyndry has opened my mind for the future. I am a lot more optimistic about my college graduation and am less scared about the job hunt that comes after I am done with school. This internship has led me to be more of a well-rounded student and take classes other than cybersecurity classes to round out my education and give me the skills I need to be successful in my future career. The most important thing for me is that I learned to stop tunnel visioning on roles that include world security. I can take my security skillset to so many different roles. This internship has given me the push I needed to make my skillset more versatile which will help aid my success in the future.

Appendix A.

My first use case

In this use case, I designed a z16 mainframe with a mindset to make the mainframe secure, efficient, and cost effective.

Chase Seider Use Case 1 Documentation msb markup.docx

Appendix B.

My group presentation on the disruptive technology MainTegrity

File Integrity Monitoring is an internal control or process that validates the integrity of z/OS system files, application software, configuration parameters, and log files by comparing current files contents to a known desired baseline.

(I cannot upload this PowerPoint because it contains confidential information)

Appendix C.

My paper on Azure and the Mainframe

Instead of trying to figure out which computing technology is better than the other, we can compare what each technology is better at doing. Mainframes are the best of the best when it comes to running applications that require an extreme amount of I/O processing. Cloud cannot realistically handle the amount of processing power than mainframes have in their current state. However, not every application needs to be hosted on a mainframe. These applications can be run more efficiently and at a cheaper cost on cloud-based systems instead. Choosing the right platform for the right workload is a key idea of a hybrid cloud environment.

What if I told you the dinosaurs were not dead.docx

References

Our values. Kyndryl. (n.d.). https://www.kyndryl.com/us/en/about-us/values

What is RACF?. IBM. (n.d.). https://www.ibm.com/docs/en/zos-basic-skills?topic=zos-what-is-racf