Automating Security Checks Using Cloud Tools Through Additions to an API

Examining the Role of Security in the Widespread Adoption of Cloud Computing

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Jihong Min

November 1, 2021

Technical Team Members: Kyle Mikolajczyk

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Sean Ferguson, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

Daniel Graham, Department of Computer Science

James Cohoon, Department of Computer Science

Introduction

Viasat, a satellite internet company, tasked its cloud engineering team, VICE, with managing and providing cloud services for the company. The main mission of VICE is to build services and platforms to provide a variety of operational and development services to teams throughout the company, primarily using Amazon Web Services (AWS). Interning with VICE this past summer, one other intern and I made additions to the Viasat.io API in order to automate certain security checks with AWS accounts and audit AWS logs. These additions provided the engineers with more tools for managing their resources in the cloud, making it easier for them to manage the AWS accounts, and providing additional safeguards against fraudulent activity while reducing costs.

Utilizing cloud computing tools is becoming the norm, especially in IT. For businesses, the cloud has the potential to transform their operations in a way that makes it cheaper and more efficient. Offices running computer networks would no longer have to deal with software installation for each computer, as well as all the licenses. This relieves a huge burden on IT. However, as more and more organizations turn to the cloud, the security of it becomes more and more crucial. When organizations and users transition to the cloud, security is one of the most important aspects to consider. Over the years, cloud providers have done much work to meet compliance requirements and continue to build more security tools to give users the most secure experience.

Technical Topic

This past summer, VICE tasked two interns to make additions to the Viasat.io API, one of the main services of VICE, that would help improve security and management of all AWS accounts. These included automating security checks with AWS accounts, automating audits of AWS logs, finding accounts associated with problematic IP addresses, and finding a more efficient way to update user's email addresses. As it is also VICE's job to manage all of Viasat's AWS accounts, it is important that all these accounts are secure and being used properly. Due to this, it is crucial that there are security checks put in place so that the team can be notified if there is any suspicious activity that might be a threat to the security of the company. Our goal for the summer was to meet these needs in a usable and expandable manner, and deploy our changes to production by the end of the internship.

To make the API additions, we needed a deeper understanding of how the API works and figure out what AWS tools we needed to use. For automating security checks, AWS Config and Lambda were needed. Config data includes all the settings for every resource in an AWS account, while Lambda is a function that runs in the cloud. The Config data for all the AWS accounts was scraped into a Postgres database table, so we needed to design queries that would get us the information we needed. One of the main API calls we added was an account changes call. This would return any resource that was added, deleted, or modified in an account between two days. The main purpose of this call was to check for possible changes in the team's master AWS account, which should usually not have any changes. To automate this check, a Lambda function that would run the account changes call once a day was created. Once the function is runs, it would send an alert email to VICE if changes were detected, so they can inspect the changes in more detail.

The implementation of the remaining calls followed a similar pattern of first identifying what AWS tool was needed, understanding the data, then automating our call. Something very important was to make the calls expandable for the future. For example, in the account changes Lambda, VICE might later have another account they want to check for periodically. Keeping these additions in mind, the calls were all implemented in a way where only small things, like just adding an account ID to the code was the only change needed to be made. For some calls where there was an extensive setup process needed in AWS, we automated using CloudFormation, so that it didn't need to be done by hand in case it needed to be setup again. Finally, to make sure the additions were fully understood, we wrote detailed documentation in the team's wiki.

STS Topic

Cloud computing brings so much potential to businesses, education, and individuals. The cloud provides better data storage, data security, flexibility, and increased collaboration between employees. It can change the workflow of small businesses and large enterprises to help them make better decisions while also decreasing costs. With these benefits, it is clear that utilizing the cloud is a trend that is continuing to grow. It is predicted that 90% of organizations will be using cloud services by 2022 (Durcevic, 2019). As organizations and individuals continue to transition to the cloud, a big factor they must consider is security. Security was and still is one of the biggest challenges facing cloud computing. As more companies turn to using these cloud services, the location of our data becomes more uncertain. The fact that we do not know the exact location of where our data is stored or processed can be a worry for many people. Also, there are the occasional headlines highlighting data breaches, compromised credentials, and more that only add to that worry. Major cloud service providers like Amazon, Microsoft, and Google process personal data either of the cloud client, but also of third parties. The majority of the risks fall within the categories of lack of control and the absence of transparency, and these risks exist regardless of the actual cloud service model implemented. As a large technological system, the work done to improve cloud computing's security can be seen as a key component in allowing it to gain traction over the past decade. These can be seen through the legislative, organizational, and technical artifacts within cloud computing.

Legislative artifacts include various standards and laws put in place to address growing concerns for data security in the cloud. In 2014, the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) came together to establish standards regarding the security and privacy aspects of the cloud. The new standard, ISO/IEC 27018, addressed the transparency issues and pre-contractual concerns of the client (de Hert et al., 2015). As these standards are voluntary, they are not entirely non-binding. However, in the case that an ISO standard is expressly referred to in the relevant contracts, providers could face claims by their clients on the basis of contractual liability.

Apart from the ISO standards the European Union (EU) has the General Data Protection Regulation, which governs how personal data of individuals in the EU may be processed and transferred. In the United States, although there is no comprehensive federal law regarding generalized data privacy or security, there are various sectoral federal laws imposing regulation on data security for certain types of information, including information that is often stored in the cloud. Some of these include the Payment card Industry data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and more. To comply with these, cloud providers offer a broad set of policies, technologies, and controls that strengthen users' security posture overall, helping protect clients' data, apps, and infrastructure from potential threats (Farris et al., 2019). With more transparency of their policies and tools, cloud providers continue to their mission gain the trust of their users and remove any barriers holding people back from the cloud.

Through complying with the various legislations, cloud providers, the organizational artifacts, like Amazon's AWS, Microsoft's Azure, and Google's GCP manage the security of the cloud. However, it is responsibility of the users, whether if it is an organization or individual, to manage the security in the cloud. This means that users retain control of the security they choose to implement to protect their own content, platform, applications, systems, and networks no differently than they would in an on-site data center. To aid in this responsibility, cloud provides supply users with an extensive set of tools and detailed documentation that outlines best practices. More specifically, they provide security-specific tools and features across network security, configuration management, access control, and data encryption, making up the technical artifacts. (AWS, 2021). As most users may not be experts, they provide additional guidance through online resources, personnel, and partners.

Next Steps

For the technical report, I will complete by November 9, 2021, providing more details about my experience as an intern in the cloud engineering team of Viasat. This will include background and the purpose of my work, process of implementing the solution, and the end result and impact of the project. It will also include the things I learned from the experience and thoughts on how the CS curriculum helped in preparing me for this project.

For the STS report, I hope to produce a paper that will give an in-depth understanding of the importance of security in cloud computing becoming a ubiquitous technological system. This will be done by providing more details on the development of regulations and how cloud providers have worked to comply to them. This will involve further examining the plethora of security tools and solutions developed by the major cloud providers, and how it enables users to better manage their data.

References

Amazon Web Services. (2021). *Security and Compliance*. AWS Whitepaper. Retrieved from https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html.

de Hert, P., Papakonstantinou, V., & Kamara, I. (2015, December 24). *The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection*. Retrieved October 11, 2021, from https://doi.org/10.1016/j.clsr.2015.12.005.

Durcevic, S. (2019, January 10). *Cloud computing risks, challenges & problems businesses are facing*. datapine. Retrieved October 10, 2021, from https://www.datapine.com/blog/cloud-computing-risks-and-challenges/.

European Union - Data Privacy and Protection European Union - Data Privacy. European Union - Data Privacy and Protection | Privacy Shield. (n.d.). Retrieved October 12, 2021, from https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection

Farris, A., Rawat, M., & Mousley, M. C. (2019, March 21). *Cloud computing in the United States*. Lexology. Retrieved October 13, 2021, from https://www.lexology.com/library/detail.aspx?g=6c9daf49-3ab7-42e1-9d63-e24741609258.