Software Developer Internship at Amdocs

The Current State of Data Privacy

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
Christopher Nguyen

October 27, 2022

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

Professor Kent Wayland, Department of Engineering and Society
Brianna Morrison, Department of Computer Science

General Research Problem: Ensuring Data Privacy in Internet Systems

What is the current state of data privacy and how can it be improved?

The evolution of telecommunication has revolutionized the way society uses technology, connecting all users in a single global network. The complexities of telecommunication today requires a deep technical understanding of many concepts, beyond what is easily available to the public. This creates a divide between what is known by the users about how these systems work and how the user's interactions with the systems are accessible to others. Lackluster user education, lack of transparency from service providers, and unclear and imprecise government regulation have led to data privacy issues society faces today. Internet users have continued to integrate this technology while general knowledge lags behind, leading to the companies that provide these services taking advantage of its users and severe leaks in privacy.

Software Developer Internship at Amdocs

Creating Dashboards, Alerts, and Reports for C Spire

Amdocs provides multiple cloud based services such as internet of things (IoT) and catalog services for their customers, which include large telecommunications companies such as AT&T and T-Mobile. For my internship, I worked on a project for C Spire, a wireless solution company in the southeast United States. Amdocs had provided the 4G infrastructure for C Spire previously, and was now upgrading the existing infrastructure to 5G.

The cellular infrastructure is delivered on Kubernetes, a platform that allows the deployment of a cluster of machines, known as nodes, that each contribute work to the solution. Within the nodes are pods that are containers of processes; these pods share resources with other pods in the same node. The advantage of isolating processes from each other in pods is the failure of one process will not affect the entire solution globally, and that modification of a part of the solution does not require redeployment of the entire solution.

The 5G solution provided by Amdocs is made up of two different systems: Amdocs Openet Charging (AOC) and Amdocs Openet Policy (AOP). AOC handles how customers are charged when using data, while AOP handles how the data is distributed to the customers and how customers interact with the system. Within AOC is the Unified Monitoring System (UMS) pod, which gets statistics about all other pods and uses the Elastic Stack to create visualizations alarms. In my role, I was tasked with creating the dashboards to display the statistics on each pod such as how much CPU memory is currently being used or whether or not the pod is running. The dashboards contain tables and graphs that make it easy for the support team to pinpoint issues and resolve them quickly. I was also tasked with creating alarms that would alert the support team when a pod used too much memory, or when a pod went down. These alarms help the support team narrow down issues that arise, reducing down time for the solution.

In addition to the UMS, I also had to create user data plan and usage reports through the SBA Profile Manager (SBAPM) within AOP. The SBAPM contains large datasets where each customer has their own account. This data includes their name, address, phone number, data plan type, and available data. These reports are generated daily and monthly so that C Spire can monitor how their customers use their services and if any changes need to be made as demand changes.

The AOC and AOP are given to the software development team by the product team with default settings; it was our job to customize them to C Spire's needs. Kubernetes is deployed using helm charts that define every pod's behavior, files it has access to, and how it interacts with other pods. These helm charts use variables defined in values files; by having the values files separate from the helm charts, global variables can be modified in a single file rather than in every instance in the helm charts. To create the dashboards and alerts, I customized the values defining the dashboards and alerts using the Kibana API. When I installed my new values file onto the cluster, Kibana pulled the dashboards I created and displayed them and added the alerts to the alerts list.

Kubernetes supports scheduled scripts called CronJobs, which are added to individual pods and have access to the pod's data. The scripts I created run several SQL requests, and convert the output into spreadsheets.

The Current State of Data Privacy

How is user data currently regulated and how do companies interpret and incorporate these regulations?

The intricacies of AOP and AOC are not unique to C Spire; all telecommunication systems consist of just as many if not more complicated components. With multiple systems in play, the entire network becomes a blackbox, where no single person can point out the path data takes from end to end. Users are even more oblivious than the developers as being able to track data requires specific knowledge on the technology not available to them; almost all users do not know what data is being collected when they connect to the internet and how their data is used. It is impossible to hold those we trust with our data accountable if we cannot follow that they do with the data.

User and Corporate Responsibility

Before every aspect of life was interconnected with technology, the primary type of data collected from users were identity related, such as name, address, and phone number, as well as browsing history within applications. Today, technology has connected all systems, with companies collecting information on users, creating one very detailed profile for each user, expanding beyond identity. One example is companies such as Amazon, Facebook, and Google, entering the financial sector. They have built on top of their digital platforms in social media and e-commerce their own financial service, including “payments, money management, insurance, and lending.” These services require more sensitive information such as banking information, social security numbers, and credit history, which can be shared among other companies and added to a user’s global profile (Boissay, 2021). The sharing of this information must be consensual, which is impossible if the companies cannot be held accountable for their actions.

Evidence has shown that many users are either unaware of or feel a lack of control over how their personal information is being used. In a survey conducted by Pew Research Center, 81% of respondents stated they do not have control over their data and 59% said they do not understand how their data is collected or used (Auxier, 2020). The gap in understanding is both due to reluctance of users in understanding the complexities of telecommunications, and malpractice by providers through hiding information in user agreements and going against privacy agreements without consent.

Current State of Data Privacy

There are multiple instances of privacy violations by large corporations, and it has taken legislative and collective public action to expose and mitigate these issues. Facebook, along with many other large data companies, give access to user data to third parties such as Cambridge Analytica. In one case, it was discovered that Facebook gave Cambridge Analytica access to “personally identifiable information of more than 87 million users.” Facebook had violated a consent decree created in 2011, but Cambridge Analytica leveraged an “alliance” with Facebook that circumvented regulations (Jim, 2018). Because the amount of data is relatively unregulated, most users were unaware of what data was shared and Facebook could not be held responsible.

As more companies continue to adopt 5G, there are several existing infrastructure that do not meet the requirements of objectivity and transparency. An article the research primary security risks of telecommunication supplies found the following are related to reduced data privacy: a strong link between supplier and government of a third country, a third country's legislation, characteristics of the telecommunications supplier's ownership, and the ability of a third country to exercise pressure (Rogalski, 2021). Government intervention has taken a big part in regulating data; one example is a review done by the government of Australia on security risks involved in the telecommunications infrastructure. These reviews were decided to be held because of the rise in cybersecurity incidents, including officers of other countries colluding with the Australian government. In addition, the shift to new 5G in all government processes has increased the need for higher security measures.

Future Proofing

Telecommunication continues to innovate, creating new protocols and standards; 5G is anticipated to be replaced with 6G by 2028. In addition to the technological changes, there are several societal changes that have to be made. First is which groups will govern what aspects of the new technology. This includes the source code and user data. Second is how will the new technology be distributed between governments, including trade barriers and where the hardware is held. Lastly is how society will use 6G, such as how will the carbon footprint change and how will the public perceive 6G (Moussaoui, 2022).

While it is important to ensure user data is used ethically and securely for the existing systems, it is important to also prepare for changes in technology. The lack of preemptive planning when creating legislation has led to the existing gaps in data privacy, so preparing for future changes now will prevent the same issues repeating themselves.

Research

In order to determine the steps needed to improve data privacy, we must examine policies that have already been implemented and find where they do not provide adequate assurance of data privacy. I plan to examine government legislation regarding privacy, as well as major company privacy regulations to see if there are misinterpretations or holes that lead to malpractice. By finding where data privacy standards are violated, we can refine the legislation to provide a more comprehensive assurance of privacy.

Conclusion

The primary contributor to insufficient data privacy is gaps in user awareness. It has been shown that while many users either do not care for or are not aware of their own privacy, it is also the responsibility of the service providers to make users aware and clearly provide the resources that allow them to make more informed decisions. Complex systems and overly confusing terms have created issues regarding privacy, and it requires a combination of the users, providers, and government intervention to mitigate these issues.

My internship at Amdocs gave me a direct insight into the blackbox that is telecommunication. The knowledge I gained from the experience was very specific to one part of the entire solution; there was no single developer that had a grasp on the functionality of the entire product, supporting the claim that it requires multiple groups that interact with these systems to come together to create regulations that truly protect user data.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center: Internet, Science & Tech. Retrieved October 27, 2022, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Boissay, F., Ehlers, T., Gambacorta, L., & Shin, H. S. (2021). Big Techs in Finance: On the new Nexus Between Data Privacy and Competition. *The Palgrave Handbook of Technological Finance*, 855–875. https://doi.org/10.1007/978-3-030-65117-6_31

Botton, N., & Lee-Makiyama, H. (2018). *5G and national security after Australia's telecom sector security review*. Retrieved from European Centre for International Political Economy (ECIPE) website: http://hdl.handle.net/10419/202509

Isaak, J., & Hanna., M. (2018). *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*. in *Computer*, *51* (8), 56-59, https://doi.org/10.1109/MC.2018.3191268

Moussaoui, M., Bertin, E., & Crespi, N. (2022). Telecom Business Models for Beyond 5G and 6G \ networks: Towards Disaggregation?. *2022 1st International Conference on 6G Networking (6GNet)*, 1-8, https://doi.org/10.1109/6GNet54646.2022.9830514

Rogalski, M. (2021). Security assessment of suppliers of telecommunications infrastructure for the provision of services in 5G Technology. *Computer Law & Security Review*, *41*, 105556. https://doi.org/10.1016/j.clsr.2021.105556