Thesis Project Portfolio

Zero Trust Architecture: Different Technologies Used to Implement ZTA in a Commercial Environment

(Technical Report)

How have developments in network technologies changed the relationship between users and e-commerce companies

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Joseph Padraic Bannon

Spring, 2023

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Zero Trust Architecture: Different Technologies Used to Implement ZTA in a Commercial Environment

How have developments in network technologies changed the relationship between users and e-commerce companies

Prospectus

Sociotechnical Synthesis

Identity is an increasingly important aspect of how users interface with the internet. In this report, I delved into the technical and societal aspects involved in how the development of user identity has impacted how users authenticate their identity to access internet resources and how e-commerce companies have influenced network technology to generate control over user data. My capstone project covered the technical process of implementing a zero-trust architecture system. Zero-trust architecture is used to prove a user's identity in an environment where a traditional network perimeter can not maintain security when faced with a variety of remote access methods. My STS research focused on how development of a user identity combining data from multiple websites has been exploited by the e-commerce industry to profit from data collection. While the zero-trust architecture and e-commerce data collection are unrelated at an implementation level, they both deal with collecting user data, although in different contexts. What data users provide and how they choose to provide it will have to address both zero-trust architecture and e-commerce data collection as internet users identity continues to mature.

The largest security concern that many companies face is the increasing number of both devices and methods used to access corporate networks. The solution to this issue is removing traditional network security boundaries and implementing a zero-trust architecture model for all users. My technical report is based on my time working for a consulting firm to implement a zero-trust architecture-based identity and access management solution for a state government client. To design our solution, we communicated with the client to determine compliance, risk and user requirements. From this analysis, my team selected features such as multi-factor authentication and context-based authentication. For this project, we tailored our implementation choices towards the specific technology the client required. Communication with the client

throughout the design and implementation process was vital to the success of the project. As threats change over time, adapting to a changing attack surface becomes a crucial aspect of the zero-trust model.

In my STS research paper, I explored how the current system of data collection has developed through the lens of Actor Network Theory. First, I examined how e-commerce companies have influenced network technology to generate control over user data. Second, I looked at how e-commerce companies have influenced both users and other actors, such as governments, technology developers and commerce regulators to maintain control over user data. Finally, I studied how users have attempted to regain control of their data by adopting privacy technology and supporting privacy advocacy groups. Additionally, I choose Actor Network Theory because it can be applied to human and nonhuman actors in order to understand how relationships affect the entire network. Finally, my analysis consists of how the system of data collection described above negatively impacts both users and e-commerce companies. E-commerce companies' exploitation of users via cookie technology has resulted in a data collection system that reduces user willingness to participate in e-commerce business and incurs additional ethical costs to users in terms of violating data ethics, and monetary costs of investing in privacy technology.

Working on my STS research paper and technical report together granted me a unique perspective on the development of user identity on the internet. My STS research paper influenced my technical report by making me question how the ethics of data ownership affects zero-trust architecture. The tension between security, in terms of users providing data to organizations to authenticate their identity, and user privacy is a topic that I would not have influenced my research without performing my technical and societal research together. In

particular, the exploitation of users that is a central theme in my STS research paper can certainly be applied to my research on zero-trust architecture. In my technical research I found that technical features in zero-trust architecture are similar to those used in e-commerce data collection. Furthermore, I speculated that security concerns can be used as a justification for increased data collection by e-commerce companies as well as governments. In conclusion, combining these two projects by focusing on the ethical implications of data collection for security is an intriguing topic for future work and will inform how identity develops as the internet continues to evolve.