Improving Database Security through General Cybersecurity Principles

Effects of Rising Use of Interconnected Technologies on the Relationship Network of Government, Developers, and End Users

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

Anthony Tiancheng Sun

November 1, 2021

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

Introduction

Modern human society has become increasingly reliant on information technologies to function. Many aspects of an average person's life now exist solely within the digital realm. Bank statements and medical records are uploaded to online databases, while search habits and personal information are collected by social media websites. The widespread adoption of the Internet of Things (IoT) has further merged the digital and physical realms in daily life. Watches, home appliances, and vehicles have been getting 'smarter', and now rely on internet connections for their enhanced features. Like their citizens, the governments of nation-states have also become further reliant on information technologies. Infrastructure like pipeline and transportation apparatuses are controlled through an electronic network, while militaries are beginning to develop autonomous weapons and augmented reality goggles that are reliant on network connections to function.

Technologies that sport network connections are highly vulnerable to cyberattacks from bad actors, and as the societal role these technologies play grows so too does the damage of a successful cyberattack. As a result of this phenomenon, the social responsibility and power software development companies possess have begun to increase. Developers now must constantly consider cybersecurity when building applications, as negligence in security implementations could have disastrous consequences, while also finding themselves in possession of an increasing amount of power and control over society by having backend access to critical software and harvested

data. This project will investigate how to further enhance database security using general cybersecurity principles and discuss how the relationship between governmental bodies, IT companies, and end users have shifted as society has become increasingly dependent on interconnected technologies.

Technical Topic

Since the advent of the digital age, online databases have replaced paper storage and have been widely adopted by many organizations to store and manage large amounts of information, including sensitive user information. Banks, hospitals, and websites use databases to store a user's financial statements, medical records, and password hashes. As more aspects of human life has digitized, it has become all but guaranteed that an average end user has private information stored in an online database.

Due to the lucrative nature of the information stored in them, databases are one of the most popular targets for cyberattacks, with around 1,767 publicly reported data breaches in the first half of 2021 alone (Security Magazine, 2021). Data breaches can cause severe damage to a company's operations and reputation, while also proving devastating for users whose sensitive information was leaked through no fault of their own. In an effort to protect these victims from the consequences of a successful cyberattack, database designers have created best practices for security, including enforcing strict group-level access permissions for database users and ensuring their code is written in a way that shields the system from known attack vectors, like SQL injections.

However, not all data breaches are caused by the failure of specific database security measure, but instead on some outside factor. It is estimated that 28% of cybersecurity attacks are from social engineering attacks where bad actors target the humans behind the database instead of attempting to attack the system itself (Moustafa et al., 2021). No amount of sophisticated security engineering would have been able to prevent these attacks since the measures were not targets to begin with. Other vectors of attack that could similarly bypass the inbuilt database security measures include attacking the app which utilizes the database or the network which the database uses to function.

With this in mind, the goal of the technical research will be to investigate how cybersecurity principles can intersect with database security practices to create a more complete security apparatus that covers not only the database, but the end user, application, and network as well to better protect databases from cyberattacks. This will be accomplished by a technical report which takes ideas from two CS areas, database systems and cybersecurity, synthesizing ideas from both of these areas to devise and promote more secure development and usage methodologies for database applications. For example, while general database security principles revolve around the program itself and technical users, very little attention is given to non-technical users who still have backend access to the database. General cybersecurity knowledge posits that the most likely attack vector is the weakest link in a security apparatus, which often are non-technical users that can be tricked into giving away important credentials through social engineering schemes, like phishing. Using this knowledge, database security can be strengthened by investing in

security awareness training for database users and managers which informs them about the dangers of these types of attacks that target individuals with a relatively low amount of technical knowledge.

STS Topic

The increasing prevalence of Internet of Things technology has continued to digitize aspects of human life, interweaving electronic devices into everyday life. As individuals, organizations, and larger social structures begin to rely heavily on these digital technologies, the responsibilities and influence tech companies have to wider human society has shifted beyond a simple provider of IT solutions. Negligence on the software company's part to properly secure their applications opens up their application, and its users, to the disastrous effects of cyberattacks. In parallel with this, IT companies have found themselves possessing a greater amount of influence over society due to the control they have over these crucial software applications, encroaching upon the role of governmental bodies. These changes shift the power-dynamics within the actor-network of companies, end users, and government beyond their traditional roles of provider, consumer, and regulator.

One of the consequences of the widespread integration of Internet of Things technology with daily life is the increased responsibility IT companies have when it comes to cybersecurity. The potential impact of breaches in the security of digital applications have become so severe that experts in the field consider cyberattacks to be the next platform of modern warfare (Brujin & Janssen, 2017) with damage from cyberattacks

escalating from individual and organizational level harm to a wider, societal level harm. This was observed during the 2021 Colonial Pipeline hack, in which a cyberattack was able to disable a pipeline which provides half of the East Coast's fuel supply by targeting its electronic systems, spiking the price of gasoline across the United States and starting a nationwide fuel shortage. The hack was later reported to have been facilitated through the use of a leaked password, exemplifying how negligence within the cybersecurity field now has drastic societal consequences (Morrison, 2021). This threatens to strip the citizenry of their agency in these issues as they are now only able to hope that the work done by these service providers is sufficiently secure while also being forced to bear the brunt of the consequences of failures in the security design, illustrating the increased power technology providers have over end users.

Tech companies have also experienced an increase in the influence they possess over society as humanity has become increasingly reliant on their technologies. Tech giants now have an unprecedented ability to reach populations and control the information circulated through their applications, with Google and Facebook having been reported to reach more citizens in the UK than the state sponsored BBC media corporation (Swabey & Harracá, 2021) while also censoring political speech from Palestinians, historians, and war crimes investigators (Doctorow, 2021). Tech companies have also grown their economic influence greatly, with the five largest IT companies projected to account for one fifth of earnings within the S&P 500 by 2023 while 43% of European Union businesses describe themselves as significantly dependent on digital platforms (Swabey & Harracá, 2021). These

conditions have given tech companies the power to shape the future of society by dominating both the digital marketplace and the societal exchange of ideas, further increasing the power companies have over end-users while also threatening the position that governmental bodies have in this network.

The rising role of information technology companies has created friction between private sector IT companies and the governmental bodies of nation states. As tech companies find themselves outcompeting the governments they operate under for power and influence over society, government institutions have begun to take measures to counteract their growth. China fined internet giant Alibaba $2.8 billion for anticompetitive practices while the U.S. Federal Government has gathered trustbusters to look at breaking up Amazon, Facebook, and Google (Mozur et al., 2021). These actions can be seen as examples of a shift in the relationship between government and tech companies in a societal network towards a more hostile one as the two grapple for power and influence over the citizenry.

The evolving role of Internet of Things technologies has set the stage for fundamental shifts between the power dynamics and relationships of a network of actors made up of IT companies, end users, and governing institutions. Properly exploring the dynamics within this network requires an investigation into both their traditional relationship and the developing interaction between actors in relation to emergent network technologies.

Next Steps

Technical Topic

- I will be entering the CS 4991 course next semester where I will have access to additional guidance and information about my technical topic.
- In the meantime, I will be spending the rest of the Fall 2021 semester going over database security and cybersecurity, looking for areas in which they can work together to enhance a database application's security apparatus.

STS Topic

- Further research will be done on the STS topic for the rest of the Fall 2021 semester.
    - Some more research could be done on how intergovernmental relationships and geopolitics have changed with the widespread adoption of information technologies. In particular looking at state sponsored cyberattacks, i.e. Stuxnet virus and online bots, and how countries, especially those outside the West, deal with the fact that the largest technology companies are U.S. based.
    - There is research to be done on government usage of information technologies to further push their own power over the citizenry. This includes state surveillance programs and nationwide firewalls blocking their citizens from accessing certain sites

    - Further research could be done on the end user's response to how both the private and public sector have been increasing their power over them, in particular looking at the rise of distrust among end users for large tech companies and the rising use of VPNs and Tor networks for increased privacy among average internet users.
- My goal is to have research done by the start of the Spring 2022 semester, an initial draft of my research paper finished around halfway through the Spring semester, and then spend the rest of the Spring semester collecting teaching staff feedback to finalize my paper.

References

Bruijn, H. de, & Janssen, M. (2017, March 17). *Building Cybersecurity Awareness: The need for evidence-based framing strategies.* Government Information Quarterly. Retrieved October 18, 2021, from https://www.sciencedirect.com/science/article/pii/S0740624X17300540.

Doctorow, C. (2021, July 16). *Right or Left, You Should be Worried About Big Tech Censorship*. Electronic Frontier Foundation. Retrieved October 18, 2021, from https://www.eff.org/deeplinks/2021/07/right-or-left-you-should-be-worried-about-big-tech-censorship.

Morrison, S. (2021, May 10). *How a Major Oil Pipeline Got Held for Ransom*. Vox. Retrieved October 18, 2021, from https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021, June 18). *The role of user behaviour in improving cyber security management*. Frontiers. Retrieved October 18, 2021, from https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full.

Mozur, P., Kang, C., Satariano, A., & McCabe, D. (2021, April 20). *A global tipping point for reining in Tech has arrived*. The New York Times. Retrieved October 18, 2021, from https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

Security Magazine. (2021, August 4). *Data breaches in the first half of 2021 exposed 18.8 billion records*. Retrieved October 18, 2021, from https://www.securitymagazine.com/articles/95793-data-breaches-in-the-first-half-of-2021-exposed-188-billion-records.

Swabey, P., & Harracá, M. (2021, February 16). *Power of Tech Companies: How Big Tech Draws its Influence*. Tech Monitor. Retrieved October 18, 2021, from https://techmonitor.ai/boardroom/power-of-tech-companies.