Design of a Formal Verification Module and Security Analysis Components of A Moral-Distress Monitoring Application

Analysis of the Recall of the Medtronic MiniMed Insulin Pump in August 2018

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
Neha Krishnakumar

December 6, 2023

Technical Team Members:

Neha Krishnakumar

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

Benjamin Laugelli, Department of Engineering and Society
Kevin Sullivan, Department of Computer Science

Introduction

In an era plagued with both conventional wars and other security threats, cybersecurity has come to be considered a crucial part of digital operations in both the public and private sectors. As a matter of fact, Joe Biden, the President of the U.S., has expressed his concern that Russia could "conduct malicious cyber activity" against the United States ("Statement by President Biden on Our Nation's Cybersecurity", 2022). Not only did he warn about this in the press release associated with the above statement, but he also stressed the importance of both the public sector and the private sector to collaborate on cybersecurity measures.

It is onerous to implement security measures in software-based systems. Thus, it is necessary to reasonably and objectively find measures to ensure the security of these systems. Formal verification seeks to objectively verify security, though it is time-consuming and theoretical, while penetration testing or ethical hacking to discover common attack patterns, is incomplete. Both measures could benefit from being implemented together, however. Thus, I propose an approach that unites formal verification and penetration testing as two disparate forms of evidence - which makes the case that a system is secure. I propose that this approach be completed in a four-pronged style. First, I will focus on the development of an assurance argument with security as the primary property. Next, I will shift my attention to a security reconnaissance and investigation where I look into the different forms of security employed by Amazon Web Services, the primary technology used for the backend of this application. Next, I will integrate different security testing tools into the CI/CD pipeline, which will form some of the traditional coding portion of my approach. Finally, I will create a formal verification module with Dafny, an imperative, or non-functional, programming language for the purpose of formally verifying code to ensure it is technically correct, i.e. bug-free, and satisfies certain security properties. There is also the added benefit of an assurance argument being evolvable as technology continues to evolve.

Making a case that a system is secure is imperative to demonstrate responsibility toward users of the software-based system. This is especially crucial if the stakeholders are from marginalized populations because they continue to be more vulnerable to external threats such as hackers. However, not every group of developers has used an assurance argument, formal verification, or even adequate penetration testing for their software-based systems because of reasons such as lack of incentive in terms of profit, amount of time involved, and amount of research involved. Through their lack of fixing the vulnerability, providing for large-scale replacement, and assuring diabetic patients of their continuous safety, a recall associated with the Medtronic MiniMed Insulin Pump in August 2018 provides a case study of a company that further marginalized a group of diabetic patients. I will be applying Technological Politics to analyze this recall by analyzing the dynamic of the power relations between the company as well as its key technological user - the diabetic patient, but this will be specifically associated with the aftermath of the recall. Analyzing the dynamics of the power relationship between these two groups will inform my approach in developing my technical project because it will grant me sensitivity toward the users involved in the further detailed case-study application which I will be developing my formal verification module for and applying my security reconnaissance and analysis towards. Cybersecurity has always had a sociopolitical component to it, and an analysis of an existing failure and recall of a device involving cybersecurity will inspire one to develop secure devices with the hope that users will not be further burdened through the use of a software-based system.

Technical Project Proposal

Resistance to malicious attacks, or security, can be difficult to include in a system, even when the financial resources are present to do so. As a matter of fact, though 49 billion dollars were spent on cybersecurity in the United States ("Spending on Cybersecurity in the United States from 2010 to 2018", 2015), nearly 20 percent of Americans reported that their identities were stolen within that same year ("Most Americans Continue to Have Privacy and Security Concerns, NTIA Finds", n.d.). This number does not even count the amount of Americans employed federally, which featured 36 percent of households ("Most Americans Continue to Have Privacy and Security Concerns, NTIA Finds", n.d.). This group should arguably be the safest considering the employees' close proximity to the government and additional resources and training in cybersecurity.

Clearly, Americans must do more work to improve cybersecurity. There have been multiple manners by which security has been improved. For example, formal verification involves the use of math and logic, which construct an objective basis for security (Lee & West, 2020). Penetration testing is another method, in which attacks can be simulated and corrected to improve the overall security of the program, with a theory that prevention is the best cure (Editor, n.d.). However, formal verification only guarantees that a mathematical model of an application is bug-free, while penetration testing only guarantees the security of an application under already specified conditions. It is thus necessary to find a way to make a case or an argument to ensure that a system is reasonably secure to be used, especially considering the growing importance of software-based systems in all aspects of life, including healthcare. A case or an argument will promote the use of informal logic, which actively combines the theoretical benefits of formal verification with the actual benefits of penetration testing. This is especially necessary because private data is often involved in applications as part of authentication, entry into an application, and authorization, or access control.

It would be inordinately difficult to ensure that every single application in the United States is secure, which is why this technical project, which will be further detailed subsequently, will seek to formalize and assure the security of a case study. The case study in question is an application designed to record when nurses and other healthcare providers are experiencing moral distress. Because this application features sensitive data, it is a decent small-scale application to represent a modern-day privacy-involving application. This project will involve Neha Krishnakumar, solely, and will involve the creation of an assurance argument, featuring disparate pieces of evidence to assure security such as a formal verification module using the programming language Dafny as well as penetration testing and security reconnaissance and analysis with Wireshark, Nmap, Nikto, and Nessus, all of which are security tools. Not all of these tasks will be completed together; instead, they will be completed subsequently. First, I will develop the assurance argument in graphical form with GSN (Goal Structuring Notation). Next, I will conduct research into the security involved with the application through networking applications such as Wireshark and port scanning and vulnerability scanning applications such as Nmap, Nikto, and Nessus. Because I have been involved in research with Professor Kevin Sullivan in a long-term fashion, I was involved with the development of the case-study application, so I will use a combination of what I already know in terms of security as well as research through a grey-box approach, where security details may still be unknown. The next task will involve some development, particularly scripting, as I integrate static and dynamic analysis security testing tools into the existing CI/CD, or continuous integration and continuous deployment for the application. The application uses Github Actions, which is what I will use for the CI/CD pipelining work. Finally, the task that will require the most traditional software development will be the formal verification module, which will be made in Dafny, and will be done specifically to verify the cryptographic components of the case-study application that were not already part of the Amazon Web Services backend, i.e. the original code that was constructed by researchers.

STS Project Proposal

In August 2018, the Medtronic MiniMed Insulin Pump was recalled after the remote control pump was found to have been hacked to result in insulin levels that were too low or too high for patients (Zaldivar et. al, 2020). Medtronic only suggested people be careful of the alerts associated with using this, but it was later found that hackers could even disable these alerts to result in even higher or lower insulin levels (Zaldivar et. al, 2020). After the MiniMed Insulin Pump recall, new models continued to be developed coming into 2023, involving new features such as meal-time adjustments and other components (“Innovation Milestones”, 2023). However, while the vulnerability was found and detailed as a CVE (Common Vulnerabilities and Exposures) element online, it was never fully fixed, and it remains possible that this system is still being used by those who lack resources, and knowledge, and are vulnerable (Kovacs, 2023).

This technology functions as a remedy for those with diabetes, helping them face immediate relief. While this is true, the technology functions as a social statement as well, further marginalizing people who are already facing a disease through poor handling of the recall of the devices and a lack of truly fixing the problem, while not offering proper remuneration. If American society continues to hold the belief that the Medtronic MiniMed Insulin pump only benefits people with diabetes through consistent updates and developments such as the recall and mealtime adjustments, the society fails to consider the implications of a lack of resources associated with fixing the device when it faces a recall situation or a new software update. People will thus fail to consider the socioeconomic implications of further disadvantaging a group that has already been afflicted by a lifelong disease. Drawing on Langdon Winner's Technological Politics, I argue that this technology performs sociopolitical work by prioritizing the concerns of the Medtronic company while marginalizing diabetic patients. Technological politics involves the concern of power dynamics in design, and how people can benefit or be harmed through technology in the context of power relations (Winner, 1980). To undertake this analysis, I will utilize interviews with the Medtronic company regarding this recall, statements that have been given surrounding the recall, and statements and interviews from diabetic patients and the company over time.

Conclusion

The deliverable for this technical problem discussed in this paper will be a formal verification module and security analysis components of the case-study application, the Moral Distress monitoring application. The STS research paper will strive to investigate the technological politics associated with the Medtronic MiniMed Insulin Pump that, through improper handling and updating, failed to address the needs of a population it sought to uplift. This will be accomplished by applying the theory of Technological Politics, by analyzing the sociopolitics associated with diabetic patients in the wake of a cybersecurity disaster and the ramifications of the recall. The combined results of this technical report will serve to address the issue regarding the sociotechnical work associated with cybersecurity, highlighting the social and economic costs of improving cybersecurity for a software-based system and the ramifications of not updating such a device, and the assurance of a similar medical software-based system to ensure a similar disaster does not occur for nurses and healthcare providers.

Word Count: 1845

References

Editor, C. C. (n.d.). *Penetration testing*. CSRC Content Editor. https://csrc.nist.gov/glossary/term/penetration_testing

Innovation milestones. Medtronic Diabetes. (2023, April 26). https://www.medtronicdiabetes.com/about-medtronic-innovation/milestone-timeline

Kovacs, B. (2023, January 22). *Some medtronic insulin pumps vulnerable to hacker attacks*. SecurityWeek. https://www.securityweek.com/some-medtronic-insulin-pumps-vulnerable-hacker-attacks/

Lee, N. T., & West, D. M. (2020, July 16). *Formal methods as a path toward better cybersecurity*. Brookings. https://www.brookings.edu/articles/formal-methods-as-a-path-toward-better-cybersecurity/

Most Americans continue to have privacy and security concerns, NTIA survey finds. Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds | National Telecommunications and Information Administration. (n.d.). https://www.ntia.gov/blog/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

Published by Statista Research Department, & 1, A. (2015, April 1). *Spending on cybersecurity in the U.S. 2010-2018*. Statista. https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

The United States Government. (2022, March 21). *Statement by president Biden on our nation's cybersecurity*. The White House.

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121-136.

Zaldivar, D., Tawalbeh, L. A., & Muheidat, F. (2020). Investigating the security threats on Networked Medical Devices. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. https://doi.org/10.1109/ccwc47524.2020.9031212