A Synthesis of Core Ideas From CS 4630 and CS 4640: Sandboxing SQL Databases to Defend Against SQL Injection Attacks

An Actor Network Based Examination of the Cybersecurity Crisis Affecting Healthcare

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 Your Major

By

Gabriel Edwards

November 5, 2021

Technical Team Members:

Gabriel Edwards

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 G. Graham, Department of Computer Science

Introduction

The prevalence of cyber attacks on healthcare facilities has been steadily rising throughout the 2010's, and has only grown worse in more recent years. In 2020 alone, more than 600 facilities were affected by data breaches and ransomware attacks (Horowitz, 2021); this is up by 42% from the amount of attacks in 2019 (Culbertson, 2021). Many attacks like these are meant to steal patient financial data, as well as healthcare provider credentials (Coventry, Branley, 2018); one of these breaches can cost a single hospital up to seven million dollars (Jalali, Kaiser, 2018), which could be disastrous for small hospitals. Other attacks are even more sinister than these, however, like a 2019 ransomware attack which shut down an Alabama hospital for eight days (Poulsen, McMillan, Evens). As well, some attacks seek to damage medical devices and infrastructure, which directly harm patients (Perakslis, 2014). In the short term, these types of attacks can majorly disrupt hospitals ability to provide care, and can reduce the amount of resources that they have; with hospitals practically bursting at the seams due to the Covid-19 pandemic, this disruption could prove to be devastating to both individuals and communities. In the long term, as Coventry and Branley (2018) point out, there is the potential for foreign nation actors to disrupt healthcare across countries by attacking healthcare systems and shutting down medical devices. Existing accounts of nations launching cyber attacks on foreign infrustructures, such as in 2016 when Russian agents were responsible for causing nationwide blackouts in Ukraine (Department of Justice, 2020), lend credibility to this idea.

With the widespread and increasing prevalence of these cyber attacks on hospitals, and their potentially devastating impact both generally and in light of the Covid-19 pandemic, there is a greater need than ever to pay closer attention. As such, my STS research will focus on an examination of the beliefs and tactics employed by the various actors within and outside of hospital

networks to assess and mitigate the risk of cyber attacks. This is loosely coupled with my technical research topic, which will serve to synthesize the concepts of sandboxing software from CS 4630 and SQL databases from CS 4640, in order to mitigate the risk of SQL injection attacks. The goal of this synthesis will be to determine the efficiency and desirability of testing SQL queries on a separate copy of a given database, to prevent potential attacks from harming vulnerable systems. Though both will cover the topic of cyber security, SQL injection has not been shown to be overtly prevalent in typical hospital cyber attacks.

Technical Topic

The technical project will be in the form of a research paper, synthesizing concepts from two separate courses in the CS curriculum. The first concept to be examined is that of sandboxing software, taught in CS 4630. The idea of sandboxing is to completely separate and isolate a particular program from the rest of the machine it is running on. Doing so involves running the given program, along with every single other program, library, and system function that it requires, in a separate environment. This means that it has no physical way for the program to access any system resources outside of its scope, and can therefore not maliciously interact with the machine. The second concept is that of SQL databases from CS 4640. SQL is a computing language used to create databases and interact with them. It provides the user the ability to write queries, or statements that can select, insert, delete, or edit large sections of data within databases very quickly and easily. As such, SQL is very widely used in internet applications to store data.

The motivating factor behind the synthesis of these two ideas is a form of cyber-attack known as a SQL injection. According to security company Akamai, SQL injection attacks comprised two thirds of all attacks from 2017-2019 alone (Vijayan, 2019). As such, an efficient defense from them could save potentially billions from attacks (Vijayan, 2019). The idea of a SQL injection is that

when a website allows users to directly interact with a database, by providing input used to search the database, the user can instead provide an SQL query statement. This statement will then run as code instead, and potentially produce harmful results. For example, if a given website stores user account information in a SQL database, and searches for a user's account by matching a username and password input by the user, the user without an account could instead provide a query that tricks the server into believing that matching info was provided.

The actual technical topic will be to examine sandboxing SQL databases; that is, copying a database that is to be queried by some user input into a separate database, and comparing the isolated query results to a sample of expected results to verify that an injection leak will not occur. The goal of this examination is to determine primarily how effectively and efficiently this idea can be produced in a real web server environment. If this idea is infeasible, or impractical, then it has no application. Secondly, the goal is to determine the potential effects of doing this on both the runtime of the query, and the added space requirement. If sandboxing to test a query takes too long, then a user will not want to use the web service. As well, databases can become quite large, and storing more data on a server can become costly; if copying entire databases consumes too much storage, then server operators will not wish to adopt it.

STS Topic

The goal of the STS research will be to determine why hospitals are so easily attacked by cyber criminals, mainly through examining how hospitals assess their risk, and what they do to mitigate it. The responsibility for mitigating the risk of cyber attacks falls upon no single party, and in this case is split in many directions. As such, this examination is best served by the use of the actor network theory (or ANT), which emphasizes examining the roles of both human and non-human agents, and the relationships between them. Specifically, this research will be modeled

after a version of the framework proposed by Cavelty (2018), which examines the global effects of cyber attacks through their influence on national politics and practices related to cyber security. Unlike the model framework, this research will focus on the policies and practices of actors involved with hospitals, as opposed to the politics of nations.

A logical first step in conducting research using ANT is to determine the actors involved in the cyber-security of hospitals. To this end, a pertinent question to answer is how are cyber criminals attacking most hospitals, i.e. what are the attack vectors most commonly used by criminals to gain access to hospital networks. According to a 2020 survey of 168 US healthcare professionals conducted by the HIMSS non-profit, the most commonly exploited security vulnerability is phishing scams (HIMSS, 2020). The nature of a phishing scam is that malicious code is attached to an email, which is sent to an employee of some organization; opening the email releases the code into the organization's network. Falling victim to this sort of attack could be the responsibility of either the hospital staff, if they were negligent in vetting their emails, and/or of the hospital administration, if they failed to provide adequate training in defending against such attacks. According to the chief strategy officer of security company MediaPro, this potential for a lack of training is likely, especially due to the Covid-19 pandemic: security/technology budgets tend to be low, and with the necessity of purchasing technology to enable working from home, security training is often low priority (Henriquez, 2020).

Another contributing factor to cyber criminals' access to hospital networks is the large amount of medical devices attached to them. Technology and medical devices are increasingly able to provide more efficient methods of treating patients. As such, hospitals are continuously acquiring more and more varied devices for use in their networks, as well as to monitor patients outside of the hospital (Coventry, Branley, 2018). An IT security professional at one hospital, interviewed in a

study by Jalali and Kaiser (2018), reported that they alone are responsible for "8000 iPhones, 2000 Androids, 2000 iPads, and some Blackberries", as well as countless personal devices used by hospital staff (Jalali, Kaiser, 2018). With networks of tens of thousands of devices, it can be very easy for an attacker to obtain one and use it to breach a network (Coventry, Branley, 2018). In addition to the vastness in the amount of devices used, many hospitals employ legacy computer systems which are no longer supported, and are highly vulnerable to attack (Coventry, Branley, 2018). This heightened vulnerability also extends to the medical devices used to directly provide care in hospitals, like heart monitors or ultrasound machines. According to security professionals interviewed by Jalali and Kaiser (2018), many of these medical devices are not built with any thought to security, and as such can be easily compromisable, posing an inherent risk to hospital networks and patient health. Worsening this is that for some devices it can be highly impractical and challenging to factor security in, such as with Implantable medical devices like pacemakers and monitoring equipment, which are becoming increasingly electronically complex and connected (Rostami, Burleson, Juels, & Koushanfar, 2013). The limited resources available to them, along with a requirement for them to be readily accessible to and reprogrammable by healthcare providers, make it very difficult to apply security measures to them.

Another factor to consider with insecurity is the intervention of government agencies and legislation. For example, the FDA has begun to pass regulations and guidance in recent years for the manufacturers of medical devices to design them with a greater emphasis on security (U.S. Food and Drug Administration, 2021). Aside from this, organizations like HIPAA (Perakslis, 2014) and legislation like the Health Information Technology for Economic and Clinical Health Act (Jalali, Kaiser, 2018) offer regulations on cyber security practices. Many IT professionals, however, feel that these merely "create a floor of cyber capabilities" (Jalali, Kaiser, 2018), and are only so helpful.

From this examination of the landscape of healthcare cybersecurity, several important actors are identified. Firstly, hospital administrators are directly responsible for setting the cybersecurity budgets of facilities (Coventry, Branley, 2018), providing training for staff (HIMSS, 2020), and procuring the networks potentially vulnerable devices and securing/updating them (Jalali, Kaiser, 2018). Secondly, hospital staff are the ones primarily targeted in social engineering based cyber attacks (like phishing), and are responsible for interacting daily with the plethora of devices that require security protocols (which, according to IT professionals interviewed by Jalali and Kaiser (2018), are often bypassed in the name of patient care). Third, device manufacturers are responsible for building the medical devices in hospital networks with security measures (or in cases not doing so) (Jalali, Kaiser, 2018). Additionally, the devices themselves serve as an important actor to consider, given the vast amounts of them in hospital networks (Jalali, Kaiser, 2018) and the difficulty of providing security designed into some medical devices (Rostami, Burleson, Juels, & Koushanfar, 2013). Finally, the attackers and their cyber-attacks themselves play the most important role in this discussion, as their specific actions motivate the reactions taken by all of the other actors. In addition to providing different roles in the cybersecurity of hospitals, these actors influence each other in a myriad of different ways. These networks of influence, though not touched on here, are extremely important to the topics understanding, and require deep analysis.

Next Steps

The research at this point has primarily served to identify the actors present in this discussion, and identify their roles and some of their behaviors/responsibilities. Using the evidence cited in this paper, as well as additional research that will be done, these actors all require further investigation to completely understand the exact roles that they play, and exactly how they interact with cybersecurity systems. As well, more research is needed to examine the networks of influence

between these actors. Additionally, as the research to this point all has used secondary sources, as much primary research (interviews) as feasible should be conducted.

References

Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance. 6(2)*. 22-30 https://www.cogitatiopress.com/politicsandgovernance/article/view/1385/1385

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas. 113.* 48-52 https://www-clinicalkey-com.proxy01.its.virginia.edu/#!/content/journal/1-s2.0-S0378512218301658

Culbertson, N. (2021, June 7). *Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=60fc75985650

Henriquez, M. (2020, November 23). *Iowa City Hospital Suffers Phishing Attack*. Security. https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack

Horowitz, B. (2021, March 26). 2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry. *Fierce Healthcare.* https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers

Jalali, S., &, Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research. 20(5).* https://www.jmir.org/2018/5/e10059/

Office of Public Affairs. (2020). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.* U.S. Department of Justice. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Perakslis, E. (2014). Cybersecurity in Health Care. *The New England Journal of Medicine, 371(5),* 395 – 397. http://www.forpath.org/glem/minutes/140905/Glem_140905_Cybersecurity_in_Health_Care.pdf

Poulsen, K., McMillan, R., & Evans, M. (2021, September 30). *Distress: The Case of the First Alleged Ransomware Death*. The Wallstreet Journal. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

Rostami, M., Burleson, W., Juels, A., & Koushanfar, F. (2013). Balancing security and utility in medical devices? *DAC '13: Proceedings of the 50th Annual Design Automation Conference. 13*, 1-6. https://dl.acm.org/doi/abs/10.1145/2463209.2488750?casa_token=JBujwvM9dFUAAAAA:uk0SQpADbJdJSRQcyc8KvCRMhMGgrgXWprwazkRys_BiznuwhNwghFiewwJUquKDXAK79shxk612OA

U.S. Food and Drug Administration. (2021, November 4). *Cybersecurity.* https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Vijayan, J. (2019). *SQL Injection Attacks Represent Two-Third of All Web App Attacks.* Dark Reading. https://www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-two-third-of-all-web-app-attacks

(2020, November 16) HIMSS Healthcare Cybersecurity Survey. *HIMSS* https://www.himss.org/resources/himss-healthcare-cybersecurity-survey