Thesis Project Portfolio

Automating DOM-based Cross Site Scripting Protections on Chromium and Chromium-based browsers

(Technical Report)

Investigating barriers to pipelining food assistance to America's food insecure via web platforms

(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

Dale Scott Wilson

Spring, 2020

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

(Executive Summary)

Securing Chromium's client-side attack surfaces from DOMXSS through low-overhead run-time sanitization and browser engine updates

Billions of individuals, ranging from your everyday consumer to captains of industry and country presidents, interface with the world wide web via an internet browser every day. Both my STS and technical research topics concern the security of end-users who interact with web applications through a web browser. My technical report investigates a compatible, easy-to-implement defense for engineers who wish to develop and defend their web applications from DOMXSS attacks, a nefarious attack that can be impossible for web application developers to detect on their servers as the malicious attack information may never leave a web application end user's browser. My STS research report investigates the current roadblocks to participation in food assistance programs, how these roadblocks might be alleviated with a migration to web application based platforms for managing enrollment, and the drawbacks in security for proposed web migrations.

Analyzing the roadblocks of food assistance program adoption across distributed communities creates a better picture of the programs' inefficiencies. Actor-network theory explains why some barriers to entry exist; relationships between an individual who experiences food insecurity and aid programs as well as the current social climate helps define these barriers. The research I cite reveals why these barriers could exist and support the proposal that continued adoption of Internet Connected Technologies (ICT's) could help alleviate these

barriers. However, the conclusions of my STS research should also caution the careless adoption and reliance on ICT's for infrastructure's that can place the most needy at risk.

My technical research proposes a protection against an increasingly common web attack that targets the internet browser: DOM-based Cross Site Scripting (DOMXSS). The defense is implemented in two parts: an update to the browser engine of Chromium that fixes the behavior of functions intended for use by web developers and a JavaScript library served with web pages at runtime that enforces a policy restricting the source of runnable code to that allowed by the web developer. The benefit of this defense is the nature of its compatibility because both the changed behavior of the Chromium browser and JavaScript library can be applied at the will of a web developer. Furthermore, the overhead for this defense is lower than previously proposed solutions, some of which require more intensive computations in creating models of the attack surface on-the-fly to better detect malicious user input. This implementation of a DOMXSS defense operates entirely on the client (web browser) which further distances this kind of defense from others which may occur on a web server. The proposed update for Chromium and the JavaScript library are promising but actual adoption of the defense is uncertain; contribution to the open source community should be thoroughly prepared and the software industry moves at incredible pace. The idea of defending the attack vector (functions implemented by a web browser for use by a developer) by updating the behavior of these attack vectors (updating the aforementioned functions) is exciting and could be promising for other client-side vulnerabilities.

While trying to land on a topic for my STS research, I realized elements from my food sustainability group project in STS 4500 had great merit. The age of the internet will push governments and nonprofits to provide all kinds of aid, specifically that for food insecurity through online infrastructure. The kinds of web attacks that my technical research hopes to

defend against are nefarious; they have hidden themselves in unsuspecting entities ranging from URL's to PDF's opened with the 'wrong' browser extension to comments on a family member's facebook post. Online infrastructure created to help the most needy will most certainly have a target on its back, requiring end-users to sign-in and provide sensitive, valuable information that an attacker will steal. If an attacker understands a potential victim's urgency, weaponizing this need can be abused through deceptive promises: Is the link, email or advertisement you clicked hiding something? My STS and technical research come together in pointing out the certainty in online migrations for assistance programs and one of the many necessary cyber-protections for this ongoing change.