**Project report Matthew Jackson, Dimitrije Prosevski**

**Introduction**

For this project we decided to create a fully functional security extension, Promised LAN, for Google Chrome. This extension is intended to provide extra security to the user while using Google Chrome to access sites.

**Problem you are trying to solve/Background**

The problem we are trying to solve has to do with the security risks involved in visiting unknown sites within Google Chrome. There are many sites that attempt to harm your device and steal personal information. And protecting yourself from accessing sites that are known to do this can be beneficial.

The background of Google Chrome extensions involving security is decent. However, most extensions have to do with ads and less to do with harmful sites in general. Because of this, our goal was to create an extension to learn more about how to blacklist and whitelist sites.

**Implementation details**

Implementation of this project was done using JSON, JavaScript, CSS, and HTML with the added usage of the Chrome storage API. We have three main JavaScript files background.js, popup.js, and content.js. All logos, images, formatting, and code is original.

**Testing/Results**

Our results were good and we were able to implement most of the functionality that we wanted within the extension. We are able to disallow access to a site if it is stored as a blacklisted site by returning any tab visiting a blacklisted site back to Google.com. We were also able to disallow image loading of a site if it is stored as a whitelisted site. The functionality of our extension is separated into two sections. These sections include its automated and manual functionality.

Automated section: every time extension is installed on a device’s Chrome app it will pull the information from Amazon updated storage of harmful sites.

Manual section: user can manually add or remove sites from the blacklist and whitelist.

The rest of our testing and results had to do with fixing the output and the display of the extension. This was done mainly in the popup.js file. Some of the things we did involved allowing the user to see all of the blacklisted and whitelisted sites currently stored for the device, and giving them the functionality to remove the sites from these lists.

**Summary/Future work**

Looking back on what we accomplished, we learned a lot about how security measures can be taken within a browser extension. We gained an increased understanding of the Google Chrome storage API and how it can help sandbox permanent data for a user on Chrome.storage. We gained experience with how sites are accessed and how this can be limited. Including stopping certain features of a site, like displaying images, and accessing an updated file list for dangerous sites.

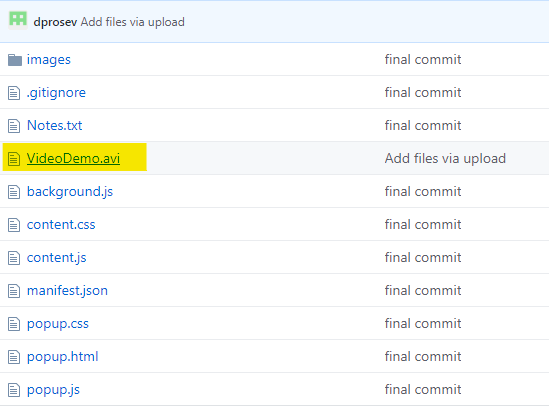
This extension, however, can definitely be improved in the future. We hope to add more functionality like, stopping downloads prompted by whitelisted sites, and creating our own sandboxed function to test a website's intent before giving it complete access. We are both excited to continue this work and apply our newfound knowledge.

**Demonstration**

Video (highlighted on the image below) demonstrating our extension is uploaded on the IU GitHub link.

<https://github.iu.edu/dprosev/SecurityExtension>

The repository is private and we added you as a collaborator using your email/username “smorr”. All the code is also uploaded there.



**References:**

YouTube video used as basis for our project:

<https://www.youtube.com/watch?v=wHZCYi1K664>

Assisted using various websites, mainly:

<https://stackoverflow.com/>

<https://www.w3schools.com/>