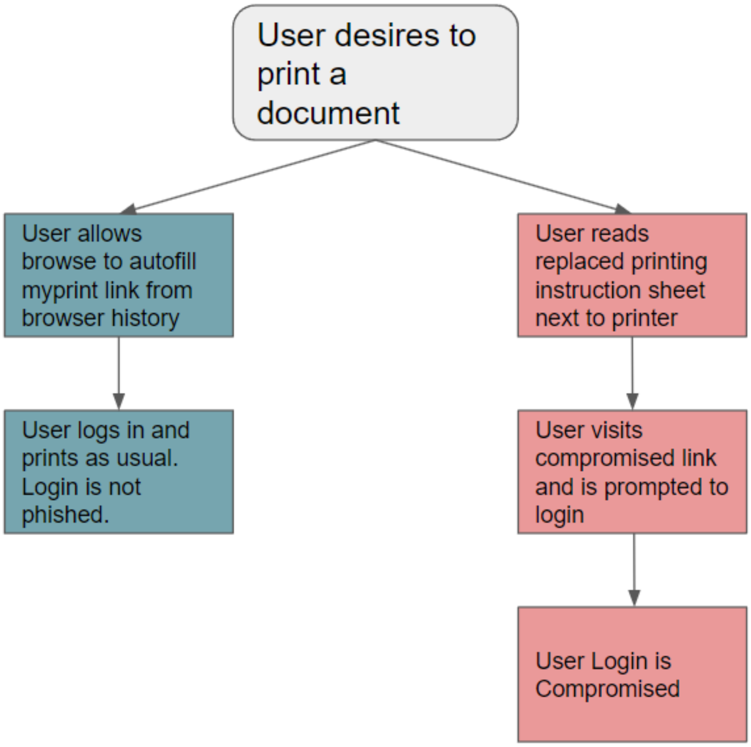
Myprint Phishing Report

Justin Bowers, Joseph Eaton, Andrew Hines, Zachary Perry

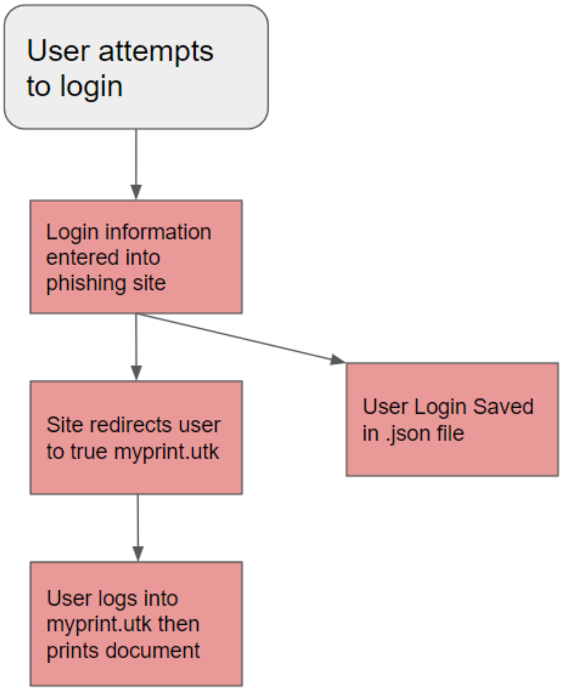
COSC 366 Spring 2023

Attacker-Oriented Threat Analysis

1. Our target is the University of Tennessee. If you are unfamiliar with this organization, it is a public postsecondary institution in the state of Tennessee that "serves the state by educating its citizens, enhancing its culture, and making a difference in people's lives through research and service."
2. Our phishing attack is aimed at gathering UTK logins (be that student, faculty, staff, etc) in a relatively discrete manner by replicating the myprint site. The most obvious value in stealing UTK login information is that each individual's account contains a plethora of personal information that can be used for malicious purposes. The secondary use of stolen login information is that there is a strong possibility that people reuse their password (or some simple variation of it) on other accounts, possibly opening the door for future attacks.
3. Phishing attack description
    a. The type of user we will be attacking will be people with UTK logins that use the campus printers. The easiest of which would be new students.
    b. In the library, there are instruction cards to inform users how to print. We can replace these with identical ones that instead instruct them to our site. When the user attempts to login, we store their login information and redirect them to the real myprint website.
    c. Workflow Diagram


User desires to print a document
User allows browse to autofill myprint link from browser history
User logs in and prints as usual. Login is not phished.
User reads replaced printing instruction sheet next to printer
User visits compromised link and is prompted to login
User Login is Compromised

d. Dataflow Diagram


User attempts to login
Login information entered into phishing site
Site redirects user to true myprint.utk
User Login Saved in .json file
User logs into myprint.utk then prints document

4. The main defense against UTK logins is two-factor authentication. A user can suspect something is wrong when there is no prompt for 2FA. However, the legitimate myprint service does not actually utilize 2FA which allows for a more discrete phishing attack. The 2FA would make using the stolen login information more difficult, but our attack is strictly to acquire the user's login information.

Phishing Website

The website is a replica of UTK's printing website (https://myprint.utk.edu/myprintcenter/). On the phishing site, the user will start at the login page just like the real website. Upon attempting to log in with their NedID and password, they will be redirected to the actual website. Their user information will have been stolen and stored in a JSON file, allowing an attacker to use their credentials to log into any of the user's UTK accounts.

To build the site, we borrowed the HTML and CSS from the actual UTK print center website. We were able to do this by going into the developer tools and copying the HTML and all of the corresponding CSS files. After removing some embedded Javascript within the HTML, we were left with an identical UI. Next, we set up an Express.js server. Doing so allowed us to run the site locally and control different HTTP methods. Whenever the user attempts to log in with their credentials, the app sends a POST request to the server. We were then able to control this post request and instead use it to store the user's credentials into a JSON file and reroute them to the real website. Next, we used LetsEncrypt and OpenSSL to generate a private key and self-signed certificate for our local host environment. To integrate this into the application, we modified our server to create an HTTPS server using the generated certificate and key. After trusting the certificate within the security tab in Chrome's developer tools, we then had a secure HTTPS connection.

Phishing Message

Our phishing message (print_phish.pdf) is an edited version of the printing instructions that can be found around the library or on OIT's website. Instead of directing users to the legitimate printing website, it directs them to utkprint.com (a potential domain name for our phishing site). These new instructions can then be printed and used to replace the real instructions found throughout the printing areas.