Blog Post 1

Due: 11:59 pm, Tuesday February 3rd

To post, visit the main blog page at [http://blogs.brown.edu/csci-1951e-s01/](http://blogs.brown.edu/csci-1951e-s01/). Clicking “Add Post” in the top left corner of the page will prompt you to log in with Shibboleth (use your Brown credentials, not your CS department credentials) and bring you to the Add Post page. You can save your post as a draft at any time and access it later via the Dashboard. Tag your post under Blog Post #1 and submit the final copy for review when you are ready to turn in the assignment.

The course staff reserves the right to modify postings, but we will try to do so rarely and will always make it clear that the post is modified. For example, if we notice an entry describing a zero-day exploit, then we may remove the discussion of that exploit first and then work with the articles author to revise the post.

Introduction

During this semester, we will be asking you to make a couple of blog posts relating to security in the real world. In this post, you are asked to perform a security review of a system that you choose, anywhere from handheld devices to municipal transportation. This review will require you to think beyond the standard or intended uses of these systems, and evaluate them holistically for potential security and privacy issues. These posts should be the result of some in-depth research as well as thinking outside the box as to how systems can be manipulated or misused.

And now a quick quiz: We asked you to perform a security review. Why?

A) We want you to be l337 h4x0rs
B) We want you to shoplift
C) We are forming an army of rebellious and destructful college hackers
D) We want you to embrace the attacker’s mindset

If you were curious, the answer is D.

Assignment

As a general rule, your review should include the following:

- Summary of the technology or system you are evaluating. List features/characteristics that are important to your analysis.
- The intended security and privacy objectives of the technology. What is important to get right?
- List of potential adversaries, threats, and weaknesses.
- List of defenses to the above, or things that should be changed to mitigate the issues.
• Evaluate the system holistically. How does this compare to similar systems? Are the risks inherent worth the services provided? Is this something that users should feel comfortable with, or does something need to change?

For more advice, Washington University has done a similar assignment from which we are borrowing: https://cubist.cs.washington.edu/Security/2007/11/23/what-to-contribute-winter-2008-cse-484/

**Inspiration**

To get you started, enjoy this anecdote from famed security expert Bruce Schneier\(^1\):

> Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail. I replied: “What’s really interesting is that these people will send a tube of live ants to anyone you tell them to.”

\(^1\)https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html