**Abstract:**

With well over 1 billion users combined, Chrome and Firefox internet browsers are among the most popular in the world. A contributing factor to that popularity is that users have the ability to install third-party browser extensions, usually to streamline a user’s experience with that browser. Unfortunately, black-hat hackers have exploited the fact that millions of these extensions are downloaded every day, and can easily build malicious extensions that can track browser usage, intercept cookie information, and even obtain logon credentials for web sites.

In this paper, I’ll examine how extensions are built and what extensions can be given access to, attempts that Google and Mozilla have made to secure their browsers, and demonstrate how an individual could create an extension to hijack a Facebook or Twitter account.

**Mentor:** Ming Chow