Ryan Ponstein

Dr. Walter Schilling

SE-4930 – Secure Software Development

11 January 2012

Article Review #2: How to Shop for Free Online

Web applications have gradually integrated third-party services which introduces new security challenges due to the complexity for an application to coordinated its internal states with those of the component services and the web client across the internet, This paper, "How to Shop for Free Online: Security Analysis of Cashier-as-a-Service Based Web Stores", was completed for the 2011 IEEE Symposium on Security and Privacy and studies security implications of this issue in regards to third-party cashiers (e.g., PayPal, Amazon Payments and Google Checkout), which are referred to as Cashier-as-a-Service (CaaS). This research, completed by Rui Wang and XiaoFeng Wang of Indiana University along with Shuo Chen and Shaz Qadeer from Microsoft Research, identified that leading merchant applications (e.g., NopCommerce and Interspire), popular online stores (e.g., Buy.com and JR.com) and a prestigious CaaS provider (Amazon Payments) all contained serious logic flaws that could be exploited to cause inconsistencies between the states of the CaaS and the merchant. Consequently, a malicious shopper could purchase an item at an arbitrarily low price, shop for free after paying for one item, or even avoid payment.

The research began with a systematic study of representative merchant software/websites that use the cashier services of PayPal, Amazon Payments, and Google Checkout. This revealed numerous security-related logic flaws in a variety of merchant systems. The attacker model simply called the web APIs exposed by the merchant and the CaaS website in an arbitrary order

with arbitrary argument values. By exploiting the logic flaws, a malicious shopper has the capability to purchase an item at an arbitrarily-set price, shop for free after paying for one item, or even avoid payment. The paper further states that real-world systems fail to answer these state challenges, indicating the urgent need to better examine the systematic solution to this problem. Their research found vulnerabilities in a variety of websites and revealed that these attacks can happen without disclosing the attacker's identity.

Through reading this article, I learned of the importance of discovering and combating logic flaws in a system. As the authors state, this study simply "takes the first step in the new security problem space that hybrid web applications bring to us." Clearly, the development of this new web programming model demands new research efforts on ensuring the security quality of the systems it produces.