CPEN442 Project Proposal

CPEN 442

October 27, 2015

Lauren Fung, Emil Maric, Koushik Peri, Kieren Wou
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada

I. What is the system that is going to be analyzed?

The system that we have chosen to analyze is an application called Bo, which is a freight management platform that allows shippers to find, track, and pay pre-verified truckers [1]. It was developed by a group of recently graduated UBC engineers as their startup, and it is currently in the beta phase. The platform allows shippers to transfer the method of payment to truck drivers and required paperwork into a digital process. The app also allows dispatchers to set up designated routes for the pickup and dropoff of freight loads, and assign truck drivers to work these routes.

II. Why is security analysis of this systems important?

When we examined the importance of security for this system, we identified several assets, their values, potential threats, and the corresponding risks. The assets that are at risk are the freight loads, the truck drivers, the accounts containing the information of the truck drivers and dispatchers, and financial information pertaining to payment from shippers to truck drivers. Threats to this system include theft of the freight loads, bribery or manipulation of the truck drivers, contraband smuggling, access to the truck drivers and dispatchers accounts, which can then be used to make false transactions, and access to certain financial information.

We identified freight load theft as being high risk especially for loads containing items with high value. Attackers who have access to a truck drivers or dispatchers account can see all the scheduled freight load routes, including their pickup and drop-off location, and could use this information to locate high-value shipments.

Attackers could also try to target the truck drivers themselves, and either manipulate, bribe, or assault them in order to gain information from them, or for their own personal vendettas. While we identified many potential threats against truck drivers, the value of the information or service gained from the realization of these threats are low. While organized gangs could use the truck drivers to smuggle contraband across the border, steal the freight loads, or gain insider information, there were more efficient ways of achieving these objectives.

Since shippers use this platform to make payments to the truck drivers, attackers with access to an account could view the compromised users financial information. There is also the possibility that attackers could redirect the payments from the shippers to their own personal accounts. We identified this as being a high risk as the attack leads to direct access to financial information, which is very valuable for attackers.

III. Who else did perform similar analysis or analyzed similar systems?

CyberKeel, a maritime cyber-security consultancy, performed a security analysis on 20 of the worlds largest carrier container companies in the world [3]. They concluded that 18 of the 20 companies were vulnerable to a form of internet fraud known as click-jacking.

In this attack, the attacker set up a mirrored version of the carrier container website, which was hosted under a very similar domain name. The attacker sent out a phishing e-mail containing a link to this fake website, where the goal is to get the victim, usually a shipper, to click the link. Given that the domain names are often very similar, and the layout and design of the webpage are setup to mimic the original website, it is fairly easy to trick the victim. Once the victim visits the fake page, they are prompted to enter their credentials to login, and then will be redirected to the actual website, unknowingly handing over their information to the attacker. The attacker can then use this information to target and steal shipments sent off by the shipper, or to charge the shippers account for their own personal shipments, in which case the shipper would get an invoice for shipments unknown to him/her. CyberKeel was also able to conclude that 37 of the 50 maritime web-pages they accessed were susceptible to relatively simple penetration attacks [3].

ClearSky Cyber Security, a cyber-security group that partnered with CyberKeel, also performed their own investigation into the cyber-security of maritime carrier container companies. They were able to uncover a large scale operation to impersonate a New Zealand shipping website, amongst other smaller shipping and banking websites [3].

IV. What is the methodology of your analysis?

The Company has provided us with a sandbox from which we will be conducting our analysis on Bos web application. The Company will also provide us with the beta build of Bos iOS application. With the web application, we will analyze the data being sent from the web client to the server by using WireShark, or other similar applications. We will verify that packets are being encrypted and that origin integrity is not compromised. We will also attempt to crack existing passwords stored on the system, through the web application, using automation. Moreover, the team will perform cross-site scripting and SQL injection attacks to verify the security of the system.

The iOS application will be analyzed to determine if packets being sent to the server are encrypted in the same way as the web application and if origin integrity is maintained. Moreover, data stored on the phone or tablet will be tested to ensure that saved data is confidential and that mechanisms exist to protect against memory corruption attacks.

Runtime analysis will be conducted using Cycript to check values of instance variables and to determine how values are set. Cycript can be used to call methods and manipulate the runtime of the application. The team will attempt to use this tool to expose a vulnerability [2].

V. Why will the world be a better place after our analysis?

The analysis is important as new iOS applications appear on the Apple App store every day with most having a web application counterpart. It is important that developers of these applications are aware of possible security risks during development so that they can take measures to reduce the risk of an attack before releasing their application to the public. Since there are an abundance of new iOS and web applications, our analysis is applicable to many developers who can use our findings to improve their own applications. This can only benefit society as it will improve the security of all users data.

VI. What is our plan for completing the project and submitting the report by the deadline?

From October 30th to November 3rd, the team will work on finalizing the Introduction, Related Work, and Methodology sections of the project report. From November 4th to November 25th, the team will work on finding vulnerabilities with the application. The team members will analyze both the web application and the iOS application in tandem. Video clips of any found vulnerabilities will be documented as they are discovered. The team is dedicated to making progress on finding exploits every week to ensure that a vulnerability is found. From November 25th to December 6th, the team will finalize the final report and prepare for the mini-conference.

Dates from Calendar:
November 4 - Finalized Introduction, Related Work, and Methodology sections of the term project report due
December 1 - Term project video clips should be handed to the instructor in the class
December 8 - Term project report due

References

[1] *Bo*. http://www.gogetbo.com/. 2015.

[2] Prateek Gianchandani. *iOS Application Security Part 5 Advanced Runtime Analysis and Manipulation Using Cycript (Yahoo Weather App)*. 2013. URL: http://highaltitudehacks.com/2013/07/02/ios-application-security-part-5-advanced-runtime-analysis-and-manipulation-using-cycript-yahoo-weather-app/.

[3] Gavin Van Marle. *Alert on cyber criminals that go phishing and then reel in shipping firm victims*. 2015. URL: http://theloadstar.co.uk/alert-on-cyber-criminals-that-go-phishing-and-then-reel-in-shipping-firm-victims/.