Niantong Dong

Dr. Osama Alshaykh

EC601 A1

September 13th, 2020

Project 1: overview and analysis

The project I want to get involved in the “cybersecurity WebRTC”. My area of interest is also cybersecurity and I want to develop my skills in cybersecurity. It is a great project for me to try as my first project in Master school and a good project to give me some real-world experience of cybersecurity.

Before I research WebRTC, Understanding the basic concept of cybersecurity is important. In my understanding, cybersecurity is a way to keep people's privacy safe on the internet. According to Dr. Gianluca Stringhini, who teaches the EC521 this semester, in the beginning, the internet was built to communicate, not for security. Also, internet protocols and computers were not for security at the beginning. The rise of cybersecurity began when some untrusted users use the weakness of the internet to attack others and steal people’s private information. One of the first computer worms, the Morris worm, infected thousands of computers and cost a large amount of money to fight the worm. The Morris worm is one of the reasons which let the public concern about the safety of the internet. I am a person who very cares about my privacy, especially when I use the internet. When cybersecurity comes to our life, there are three core elements we need to take care of. The people who are using the network, the processes which transfer the data, and the technology which we use to protect the whole processes are the three elements in cybersecurity. When we talk about cybersecurity, we cannot

stand our point without these three elements. For WebRTC, I believe we can focus on the process element and try to find out the weakness of this platform.

On the other hand, to be more specific, I find out that there are three categories of cybersecurity, Data security, network security, and application security. I believe the focus of this project is the process between users. Network security should be our primary focus. The weakness of WebRTC, in my opinion, is not about the data security on the receiver or the sender, which I believe the platform should have some technology to encrypt and decrypt the data. Also, application security is not our priority because this open-source platform is a tool to build an application. Each company should have its way to protect its application from malicious users. The network security, however, is the most common way for the attacker to hijack our communication because the most of protocol prefers to trust the user. One of the famous methods to attack the server is DoS. The DoS exploits the TCP and UDP packets to overload the target, which the protocols cannot do anything to prevent the DoS attack. Therefore, we may find the weakness of WebRTC if we learn and examine their communication standards and protocols to find out a way to hijack the communication between users.

To prepare this project, I need to know what exactly the WebRTC is. According to the official website, the WebRTC is an open-source project that enables real-time communication to the application. With WebRTC, we can call a voice or video chat with our friends and family in the browser. We can also hold a web conference and transfer data directly to our contact simply using our browser. The WebRTC enhances the capability of our browser. Also, in the last couple of years, the smart assistant comes to our life. Most of the family have a smart assistant such as Alexa or Google assistant. According to Allie Mellen, Amazon uses WebRTC for Alexa. One-way Conversational devices are one of the most common use cases of WebRTC in our life. The

other common use case is the IoT, Internet of things. The WebRTC supports the communication between machine. The self-driving automobiles, for example, use the WebRTC to implement real-time communications. Apparently, WebRTC has a lot of use cases in our life and it can grow faster and faster when those use cases are getting more and more important in our life. It has a lot of advantages and disadvantages. For this project, all I need to do is to focus on its disadvantages. On the other hand, to learn more about it, I find out that there are lots of applications using this platform. For example, Discord, Facebook messenger, and Google Meet are a great example to show the good side of WebRTC. I used Discord a lot and WebRTC shows its mighty power of real-time communication.

To examine the vulnerability of WebRTC, I propose some paths that are possible to do. First, the WebRTC itself is a good way to examine. Since WebRTC is still developing. The most current version is WebRTC 1.0 so that it should have some vulnerable point we can find out. However, this path may not be easy to analyze the vulnerability because even it is developing, it has been implemented to a lot of applications and run a ton of testing. So, it may not a good option for me, as a new graduate student, to find the vulnerable point. The second path is the protocol or the process. I learned that there is a protocol named SIP, the session initiation protocol. The idea of SIP is to initiate or terminate communication between devices. Since the SIP message is pure text format to send out, the attacker can hijack the message and modify the SIP message. This modification can direct all the messages from the sender to the attacker's destination. It should be an ideal path to examine. However, the way to hijack and modify the SIP message is a big problem for me and it should take time to learn it at the beginning. Furthermore, there is a lot of type of attack we can do for the process aspect, for example, the MiTM attack, replay attack, and session hijacking. In this case, we should have a lot of potential

options in this aspect. Above all, we have two approaches for this project, finding bugs in the code, and finding problems in the protocol. The code is easy to access since it is open-source, but the shortcoming is that it requires a very sufficient knowledge to find out the bug. The protocol, on the other hand, is easier to examine the vulnerability. My preference is to use the protocol to attack the users.

In conclusion, in this paper, I first learn about what cybersecurity is, the essence of cybersecurity, and the category of cybersecurity. Also, for the WebRTC, generally, I understand what the WebRTC is used for and some popular use cases. I also purpose some aspects to examine the vulnerability of WebRTC. The protocol aspect is my preference and there are several ways to perform the vulnerability test. Throughout this semester, I believe that I and my teammate should be able to perform the attack and hopefully, find out a solution for the issue.

Works Cited

Stringhini, Gianluca. *Lecture 1: Introduction*. EC521, 09/03/2020, Boston University. Zoom Lecutre.

"A Study of WebRTC Security." *A Study of WebRTC Security · A Study of WebRTC Security*, webrtc-security.github.io/.

Mellen, Allie. "8 Use Cases for Real-Time Communications with WebRTC." *No Jitter*, 1 Nov. 2018, www.nojitter.com/8-use-cases-real-time-communications-webrtc.