Effect of the Address Resolution Protocol (ARP) Spoofing Attacks on Web Real-Time Communication

AL Dhananjaya#, K Gunawardhana and RL Dangalla

Department of Computing & Information Systems. Faculty of Applied Sciences,
Sabaragamuwa University of Sri Lanka, Belihuloya
#aldhananjaya@std.appsc.sab.ac.lk

Web-RTC (Web Real-Time Communication) is a free, open-source project that gives web browsers and mobile applications with real-time communications via easy application programming interfaces (APIs). Web-RTC is being standardized through the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF). Previous findings include risk of Man-in the middleware (MITM) attacks for Web-RTC. This study tests ARP (Address Resolution Protocol) spoofing attacks with web-RTC that are part of MITM attacks. In this case, the objective was to test the security of web-RTC, which fails purposes of new security architecture and verifies the architecture. The study selected Google hangouts and Firefox hello as the major parts of web-RTC. Ettercap hacking tool and wire-shark data analysis tool are used to analyse the data packet. Threat model is created by using two machines and a Wi-Fi router for the testing purpose. The Ettercap tool included the victim's IP address and selected the ARP spoofing attack category, and also started to remotely attack the victim machine. Then Wireshark was used to capture all transmission packets between the attacker PC and the victim's PC. Those packets were analysed and filtered IP category, ARP category, IP and ARP category, Bad TCP category and RST TCP category. But the researcher failed to hack that system. The researcher confirmed web-RTC is secured from ARP spoofing attack. But it has more future carriers, the researcher will be able to do the testing for other attacks as well with web-RTC.

Keywords: Web-RTC, MITM Attacks, ARP Spoofing, Security