Issued 12/3/18

Wi-Fi Calling Services on AT&T, T-Mobile US, Verizon are Insecure

Experts from Michigan State University in the US and National Chiao Tung University in Taiwan have found that the Wi-Fi calling services offered by AT&T, T-Mobile US, and Verizon suffer from four security flaws that can be exploited to attack mobile phone users, leaking private information, harassing them, or interfering with service. In a research paper [link] distributed through preprint service ArXiv on Thursday, eight computer scientists – Tian Xie, Guan-Hua Tu, Bangjie Yin, Chi-Yu Li, Chunyi Peng, Mi Zhang, Hui Liu, and Xiaomin Liu – dismiss existing Wi-Fi calling security mechanisms. They say that defenses like storing private keys on SIM cards, 3GPP Authentication and Key Agreement, IPSec for call signaling and voice/text packets, and switching to cellular networks to defend against Wi-Fi denial of service attacks fall short. "Given these security mechanisms, which have been well studied in the VoLTE [Voice over LTE] and cellular networks for years, it seems that the Wi-Fi calling should be as secure as the VoLTE," the researchers state in their paper. "Unfortunately, it is not the case. We have identified several security threats in the Wi-Fi calling services deployed by T-Mobile, Verizon and AT&T in the US." They attribute the flaws to "design defects of Wi-Fi calling standards, implementation issues of Wi-Fi calling devices, and operational slips of cellular networks." And to underscore the need to improve the security of Wi-Fi calls, they point out that Wi-Fi calling is expected to surpass VoLTE and VoIP (e.g. Skype) services this year in terms of usage time. In the attack scenario described by the researchers, the victim is a mobile user who connects to a Wi-Fi access point with a device that has a Wi-Fi calling service. Specifically, the boffins tested eight smartphone models – Samsung Galaxy

S6/S7/S8/J7, Apple iPhone 6/7/8, and Google Nexus 6P – with Wi-Fi calling from AT&T, T-Mobile, and Verizon. The attacker can be anyone with a networked device on the same subnet as the victim. For their experiment, the researchers used a software-based Wi-Fi access point on a MacBook Pro 2014 laptop and an ASUS RT-AC1900 Wi-Fi access point on several university networks, including Michigan State University, New York University, University of California Berkeley, and Northeastern University.