Voice Hacking Extended:
Using Inaudible Voice Commands to Exploit Mobile Devices

Andre V. Gonzales, Bryson R. Payne
andrevgonz2066,bryson.payne@ung.edu

University of North Georgia
Dahlonega, GA 30597

Abstract Proposal

The purchase of mobile smart devices and intelligent assistants, such as Siri, Google Home, and Alexa Echo, continues to increase due to their simplicity and practicality. For this study, we will look explicitly at Apple and Android mobile devices. Most individuals feel their information is safe on their device if it is protected by a passcode or a wake word such as “Hey Siri” in a specific voice tone. However, many users are unaware of mobile devices’ privacy and security weaknesses.

Prior work [1, 4, 7] has shown that incompressible (obfuscated attacks) and inaudible (dolphin attacks) voice commands can be understood by voice-controlled systems and may be used to inject unnoticed security breaches. We hypothesize that without the person knowing their device is compromised, we can use a voice-enabled phone or other mobile device as an attack vector to scan for vulnerable laptops, desktops, or workstations on any wireless network that it may encounter. The scanning will identify the devices’ vulnerabilities that enable further hacking. Finally, the mobile device can be used to send malware to the victims, and damage or disable the systems.

Complying with ethical standards, we will use an experimental methodology and simulations with virtual machines in a controlled environment to test our hypothesis. We expect to find that the high-quality microphones in mobile devices will be susceptible to inaudible or unrecognizable voice commands attacks. These findings will be applied to investigate preventive measures and possible fixes to both dolphin and obfuscated attacks in order to protect consumers.

Keywords: Computer science, ethical hacking, intelligent assistants, mobile hacking, dolphin attacks, obfuscated attacks, malware, mobile device exploitation, vulnerability scan, prevent hacking.

References

[1] Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., Zhou, W. (2016). Hidden Voice Commands. In *Proceedings of the USENIX Security Symposium.*

[2] Daio, W., Liu, X., Zhou, Z., & Zhang, K. (2014). Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone.

[3] Fend, H., Fawaz, K., & Shin, K. G. (2017). Continuous Authentication for Voice Assistants.

[4] Mauran, L. I., Payne, B. R., & Abegaz, T. T. (2017). Voice Hacking Proof of Concept: Using Smartphones to Spread Ransomware to Traditional PCs.

[5] Roy, N., Hassanieh, H., & Choudhury, R. R. (2017). Backdoor: Making Microphones Hear Inaudible Sounds. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Application, and Services*. ACM, 2-14.

[6] Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., & Wang, X. (2011). Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *Proceedings of the Network and Distributed System Security Symposium (NDSS),* Vol. 11. 17-33.

[7] Zhang, G., Yan, C., Ji, X., Zhang, T., & Xu, W. (2017). DolphinAtack: Inaudible Voice Commands.