ENHANCING SECURITY AND PRIVACY FOR VOICE ASSISTANT SYSTEMS

Speaker:	Bang Q. Tran
Committee Members:	Prof. Xiaohui Liang (Chair), Prof. Dan Simovici, Prof. Marc Pomplun, Prof. Bo Sheng, Prof. Honggang Zhang, and Prof. Kenneth K. Fletcher
GPD:	Prof. Dan Simovici
Date & Time:	May 22nd, 2023 (Monday) at 10:00 AM
Zoom Link:	https://umassboston.zoom.us/j/98212843286
Passcode:	879160

ABSTRACT

The rapid proliferation of Voice Assistant (VA) devices such as Amazon's Alexa, Google Home, and Apple's Siri has transformed how we interact with technology in our daily lives. These devices provide users with hands-free access to various services, from weather forecasts and news updates to music streaming and home automation. However, the convenience and utility of VA devices come with a trade-off regarding privacy and security. Researchers have noted that voice assistant devices may be vulnerable to attacks by malicious actors, who could take control of the device or use it to access other devices on a user's network. Besides that, leaking the biophysical status of the users from voice signals and being profiled by Voice Service Providers (VSP) are recent concerns as the advances of Deep Learning techniques as well as Natural Language Processing (NLP).

This dissertation first presents a solution to enhance the security of VA devices. Our proposed defending system on the VA devices can against both voice replay and injection attacks without any additional devices or any extra user's effort. Specifically, we use both voice and wireless data to verify the correlation between the user's presence and voice commands, then finally detect the attacks.

Secondly, this dissertation proposes an anonymity scheme on VA devices to protecting users' voice data from being linked to their accounts by the VSP. Our proposed scheme aims to mix the queries from multiple VA users' devices, hiding the source of queries and hiding the relay's real queries. To achieve effective anonymity, the anonymizer is equipped with a proposed privacy-preserving pattern matching scheme, which is run with the help of a semi-trusted server and is used to find the most effective relay for the requester based on their pattern similarity.

Lastly, we introduce a framework VPASS, that supports managing personalized privacy requirements for VA systems. Specifically, we propose mechanisms to quantify two key aspects: the amount of information disclosure and the level of privacy sensitivity each voice command has. Our mechanisms employ deep learning techniques for natural language processing and can accurately detect privacy-sensitive commands based on an individual's prior history of VAS interaction. Finally, VPASS generates monthly reports or immediate privacy alerts based on the privacy policies pre-defined by users.