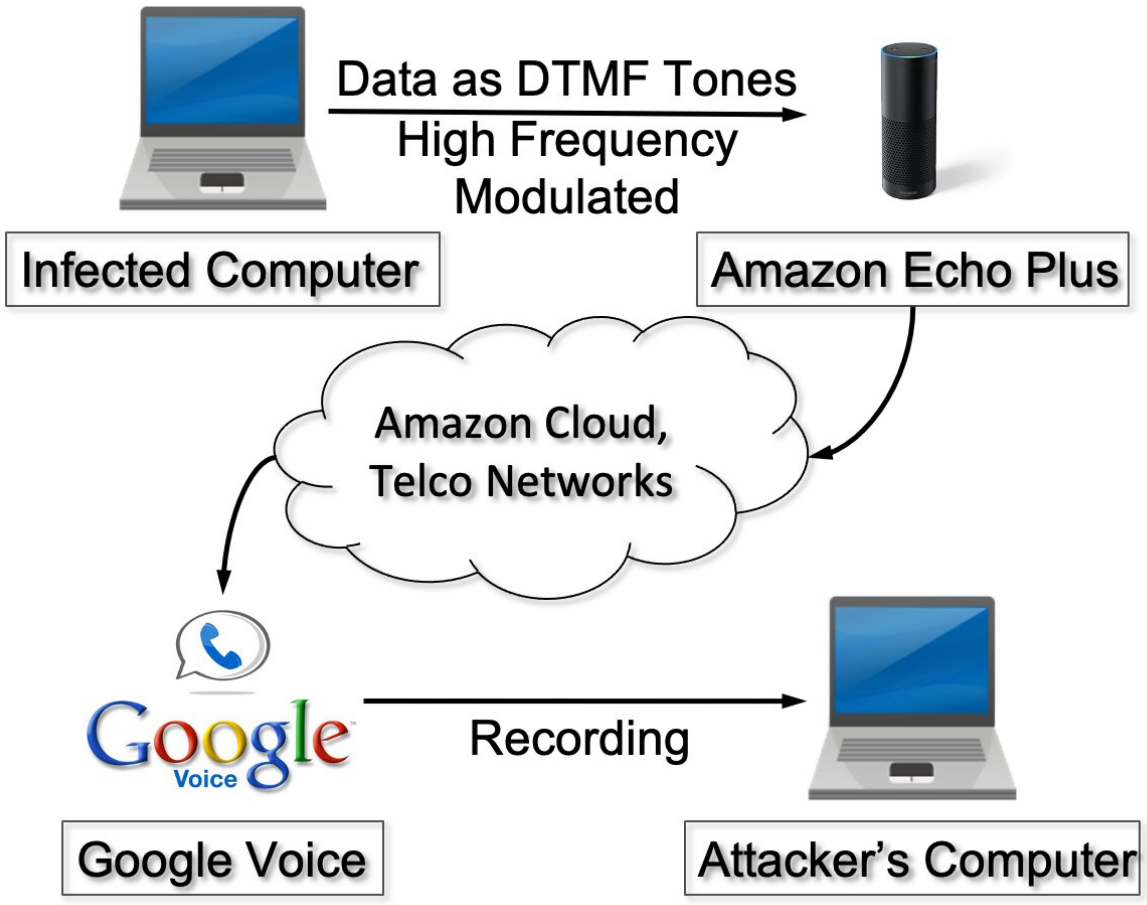
An attacker can steal sensitive user data over the phone using smart speakers

October 27 2020, by Ingrid Fadelli



Credit: He, Rajput & Ahamad.

In recent years, voice assistants such as Siri, Amazon Alexa, Google

Assistant and Cortana have become increasingly popular. People in many countries worldwide communicate with these artificial intelligence (AI) agents on a daily basis, asking them to search for information online, send emails or messages, play their favorite songs, and so on.

While voice assistants can greatly simplify the way in which we use our smartphones, PCs, tablets and other devices, they also raise a number of privacy and security-related concerns. In fact, these agents can also be used to collect data for targeted advertising and may even allow cyber-attackers to steal sensitive information from users or tamper with their devices.

Researchers at Georgia Institute of Technology recently showed that a simple attack could allow malicious users to gain access to people's personal information via voice assistants. Their findings, presented in a paper pre-published on arXiv, highlight a number of vulnerabilities and risks associated with the use of conversational agents.

"In recent years, there have been news stories about Amazon Echo accidentally recording and sending the conversations between people in its vicinity to a contact via a phone call," Zhengxian He, one of the researchers who carried out the study, told Tech Xplore. "Our research is motivated by new threats to sensitive information in these environments that arise due to the proximity of compromised computers and voice assistants. We are able to demonstrate that such threats could be real, and that data stored on computers could be stolen via voice assistants over a phone channel."

To unveil the vulnerabilities of voice assistants, He and his colleagues devised an attack that would extract sensitive data from users over the phone. Firstly, they converted data stored in a user's device into sound recordings and ensured that these recordings could be transferred over a simple phone call. They achieved this by transforming user data into dual-

tone multi-frequency (DTMF) tones, which are essentially signals that can be transferred over telephone lines.

"Another challenge we had to overcome was to make transmission of such sound from a computer stealthy, so that it does not alarm a person who may be nearby," He said. "We achieve this by modulating the tones onto very high frequency (16kHz in our work), or ultrasonic frequency, to make them inaudible to most people."

When the voices of users are recorded by an Amazon Echo device's in-built microphone, the original tones of these recordings are naturally demodulated, due to the microphone's intrinsic nonlinearity (i.e., its distortion of sounds/voices). The researchers showed that these tones can be transferred to a remote device controlled by an attacker, who may then reconstruct the sensitive data they contain.

"The attack we identified can be carried out without being noticed by a human, demonstrating the feasibility of stealthy data exfiltration from compromised computers with smart speakers," He said. "A modest amount of data (e.g., a kilobyte of data) can be transmitted with high accuracy by a call lasting less than 5 minutes in a realistic setting even when the smart speaker is several feet away from the computer where the data is stored."

The experiments carried out by He and his colleagues show that a user's personal data could easily be transmitted via smart speakers, such as Amazon Echo, to an attacker's device. The rate at which this data is transferred depends on a number of factors, including the distance between a user's computer and his/her smart speaker, background noise and the frequency of carrier waves (i.e., the waves through which the data is transferred).

This recent study identified vulnerabilities of voice assistants and smart

speakers that are not addressed by existing defenses and security measures against data theft. In their paper, the researchers discuss solutions that could help to mitigate these risks, which they plan to explore in their future research.

"In our next studies, we plan to devise strategies that improve the security and privacy of voice assistants," He said. "In addition, we plan to explore possible defenses against these kinds of attacks."

More information: Using inaudible audio and voice assistants to transmit sensitive data over telephony. arXiv:2009.10200 [cs.CR]. arxiv.org/abs/2009.10200