Keyboard acoustics could let hackers untangle typed text through Skype

COMPUTERS

Michael Irving
October 19th, 2016

A new study suggests that hackers may be able to untangle typed text just by studying the acoustics of key presses through voice chat software like Skype(Credit:perig76/Depositphotos)

Those worried about their personal information leaking over the internet may already fear keystroke logging software, but a new study cautions against typing while Skyping. By analyzing the acoustic signals of key presses, hackers may be able to untangle typed text through the clickety-clack of a keyboard itself, with an alarming accuracy of over 90 percent.

Anyone who uses a keyboard regularly knows that the sounds produced by typing differ by device brand and style, but to a tuned ear, individual keys on the same keyboard produce unique acoustic signals. With the help of some machine learning algorithms and an understanding of the user's typing style, these sounds can be enough for a hacker to recreate large sections of text, passwords and all.

"It's possible to build a profile of the acoustic emanation generated by each key on a given keyboard," says Gene Tsudik, co-author of the study. "For example, the T on a MacBook Pro 'sounds' different from the same letter on another manufacturer's product. It also sounds different from the R on the same keyboard, which is right next to T."

Historically, though, that kind of eavesdropping required the attacker to physically place a microphone within earshot of the victim's keyboard, rendering the method largely impractical. Now, the study suggests, voice-over-IP software like Skype or Google Hangouts potentially makes things much easier. If users on a voice call happen to type during the conversation, the keystroke acoustics can be recorded by other call participants for later analysis.

Those who use Skype to chat with friends or grandma from overseas might not be too worried, but that's not the only use of the application.

"The interesting thing is that people who talk on Skype are not always friends and do not always have mutual trust," says Tsudik. "Imagine a call between lawyers on opposite sides of a legal case, or business competitors or diplomats representing different countries."

Armed with knowledge of the victim's typing style and brand of keyboard, the study found a hacker could determine individual key presses with 91.7 percent accuracy. But perhaps more worrying is the finding that even when they don't have that information, keystrokes can still be figured out almost 42 percent of the time, thanks to the frequency distribution of letters in the English language.

Thankfully, only clunky physical and mechanical keyboards are at risk. Since they don't produce sound, touchscreen keyboards of mobile devices, and laser projection keyboards may be a safer option.

"Our work is yet another nail in the coffin of traditional physical keyboards that are common in modern laptop and desktop computers," says Tsudik. "It clearly shows previously unnoticed privacy dangers of using popular VoIP technologies in conjunction with such keyboards."

The research was published online at *ArXiv* (PDF).

Source: University of California, Irvine