Traditional keyboard sounds can be decoded, compromising privacy

October 19 2016

"People who talk on Skype are not always friends and do not always have mutual trust," says study co-author Gene Tsudik, Chancellor's Professor of computer science at UCI. "Imagine a call between lawyers on opposite sides of a legal case – or business competitors or diplomats representing different countries." Credit: Steve Zylius / UCI

If you type on your desktop or laptop computer's keyboard while participating in a Skype call, you could be vulnerable to electronic eavesdropping, according to researchers at the University of California, Irvine and in Italy.

In a new study published online at arXiv, they describe a security breach whereby keystroke sounds, or acoustic emanations, can be recorded during a Skype voice or video call and later reassembled as text.

"Skype is used by a huge number of people worldwide," said co-author Gene Tsudik, Chancellor's Professor of computer science at UCI. "We have shown that during a Skype video or audio conference, your keystrokes are subject to recording and analysis by your call partners. They can learn exactly what you type, including confidential information such as passwords and other very personal stuff."

He specified that such an attack is not possible with touch-screen or holographic keyboards and keypads. And since data transfer over Skype is encrypted, it's extremely difficult for someone who's not part of a call to pilfer keystrokes. However, he outlined scenarios in which this cybersecurity threat could be all too real.

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

Security experts have long known of attackers' ability to capture acoustic signals from typewriters and computer keyboards for nefarious purposes. Various brands of keyboards, from Apple to HP to Logitech, emit distinct sounds. That information combined with some knowledge of a user's typing style could be enough to allow a spy to re-create whole texts.

"It's possible to build a profile of the acoustic emanation generated by each key on a given keyboard," Tsudik said. "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."

He said that if the sound of someone typing is recorded, each keystroke can be analyzed and matched to a key using machine learning techniques.

The challenge in such attacks has been finding a way to place a recording device near a victim's computer keyboard. Now the recording can be done remotely if a person is typing while utilizing a voice-over-internet-protocol application, such as Skype, Google Hangouts or Vonage.

The study found that if attackers have some knowledge of the typist's style and information about the keyboard, they have a 91.7 percent rate of accuracy in guessing a key pressed by the victim. If snoops are oblivious to both the typing style and keyboard, they still have a 41.89 percent chance of identifying which keys are being struck, since the English language has a well-known frequency distribution of letters.

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

The touch-screen keyboards on many smaller devices, such as smartphones and tablets, are not susceptible to these attacks. Laser projection, or holographic, keyboards are also immune.

More information: Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP. arxiv.org/pdf/1609.09359.pdf