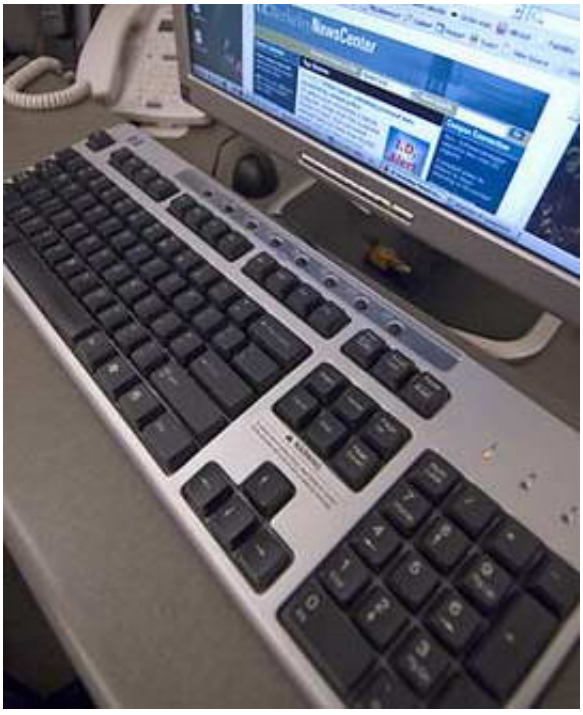
Researchers recover typed text using audio recording of keystrokes

September 15 2005



A new security threat revealed by computer scientists at the University of California, Berkeley, may be enough to drive some people away from their computer keyboards and back to pen and paper. The researchers show that a simple audio recording of those keyboard clicks can betray the text you just entered, from passwords to secret love notes.

Image: "Acoustical spying" using an audio recording of the sounds generated by typing on a computer keyboard is a potential security threat identified by UC Berkeley researchers.

The researchers were able to take several 10-minute sound recordings of users typing at a keyboard, feed the audio into a computer, and use an algorithm to recover up to 96 percent of the characters entered.

"It's a form of acoustical spying that should raise red flags among computer security and privacy experts," said Doug Tygar, UC Berkeley professor of computer science and information management and principal investigator of the study. "If we were able to figure this out, it's likely that people with less honorable intentions can - or have - as well."

The results of their findings will be presented Nov. 10 at the 12th Association for Computing Machinery Conference on Computer and Communications Security in Alexandria, Va.

What makes the technique feasible is that each keystroke makes a relatively distinct sound, however subtle, when hit. Typical users type about 300 characters per minute, leaving enough time for a computer to isolate the sounds of individual keystrokes and categorize the letters based upon the statistical characteristics of English text. For example, the letters "th" will occur together more frequently than "tj," and the word "yet" is far more common than "yrg."

"Using statistical learning theory, the computer can categorize the sounds of each key as it's struck and develop a good first guess with an accuracy of 60 percent for characters, and 20 percent for words," said Li Zhuang, a UC Berkeley Ph.D. student in computer science and lead author of the study. "We then use spelling and grammar checks to refine the results, which increased the character accuracy to 70 percent and the word accuracy to 50 percent. The text is somewhat readable at this point."

Acoustical spying

Here is an example of text recovered by UC Berkeley researchers using audio recordings of keystrokes.

Original Text *(Notice that the text contains two typos, underlined)*:

the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys gnnerals in states, who fear the file sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and dimished sales tax revenue.

Recovered Text Before Spell Check *(underlined words are wrong)*:

the big money fight has drawn the shoporo od dosens of companies in the entertainment industry as well as attorneys gnnerals on states, who fear the fild shading softwate will encourage illegal acyivitt, srem the grosth of small arrists and lead to lost cobs and dimished sales tas revenue.

Recovered Text After Spell Check and Decoding *(underlined words are wrong)*:

the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys generals in states, who fear the film sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and finished sales tax revenue.

But that's not the end. The recording is then played back repeatedly in a feedback loop to "train" the computer to increase its accuracy until no significant improvement is seen. In the UC Berkeley experiments, three

feedback cycles were often enough to obtain recovery rates of 88 percent for words and 96 percent for characters.

Once the system is trained, recovering the text became more straightforward, even if the text was a password and not an English word. After just 20 attempts, the researchers were able to retrieve 90 percent of five-character passwords, 77 percent of eight-character passwords and 69 percent of 10-character passwords.

There are limitations to the technique, however. The researchers pointed out that they did not use the Shift, Control, Backspace or Caps Lock keys for their experiments, but describe approaches for training a program to account for those keystrokes as well. The ability to account for use of a computer mouse will be more challenging, the researchers said.

Nevertheless, the findings highlight a security hole that could be exploited and should be investigated, the researchers said.

The new study builds upon prior work by IBM researchers Dmitri Asonov and Rakesh Agrawal in which 80 percent of text was recovered from keyboard recordings. One key difference is that the experiments by Asonov and Agrawal relied upon controlled conditions in which the same typist is using the same keyboard and the algorithm is trained with known text and corresponding sound samples.

In contrast, the computer algorithm in the UC Berkeley study can "learn" and adapt to different typing patterns. To show this, the researchers experimented with multiple users on different keyboards, including so-called "quiet" keyboards, and found that their algorithm was successfully able to predict data. Moreover, recordings were taken in a variety of conditions, such as environments in which music was playing or cell phones were ringing in the background.

"Background noise definitely made it harder to recover accurate text, but the differences became smaller after several rounds of feedback," said Tygar. "Given enough tries, the computer algorithm will eventually come up with a pretty good estimate of the text that was typed."

The researchers noted that sophisticated Karaoke systems already exist that can separate voice and music, so it may be possible to separate out music from the taps and clicks on a keyboard.

What was particularly striking about this study, the researchers said, was the ease with which the text could be recovered using off-the-shelf equipment. "We didn't need high-quality audio to accomplish this," said Feng Zhou, a UC Berkeley Ph.D. student in computer science and co-author of the study. "We just used a $10 microphone that can be easily purchased in almost any computer supply store."

Tygar warned that parabolic microphones allow people to record sounds in a room while standing outside the building, and presumably without the knowledge of the typist.

"The message from this study is that there is no easy escape from this acoustic snooping," said Tygar. "The type of keyboard you use doesn't matter, your typing proficiency doesn't matter, and the background noise can be overcome."

So what's a typist to do? Other than scanning one's surroundings for bugs or recording devices, and making sure a room is soundproof, the researchers suggest that we rethink the use of typed passwords or even long passphrases for security.

"There are different forms of authentication that could be used, including smart cards, one-time password tokens or biometrics," said Tygar. "That helps with passwords, but it doesn't help protect text

documents we would want to keep classified. I'm not sure what the solution is, but it's important that we're aware of this vulnerability."

The project is part of the UC Berkeley-led Team for Research in Ubiquitous Secure Technology (TRUST), a multi-institution center funded by the National Science Foundation to protect the nation's computer infrastructure from cyberattacks.

Source: UC Berkley