The Economist

Monitor

Loose clicks sink ships

Computer security: The sounds of individual keystrokes making it possible to eavesdrop on computer users

Jun 10th 2010

CLATTERING keyboards may seem the white noise of the modern age, but they betray more information than unwary typists realise. Simply by analysing audio recordings of keyboard clatter, computer scientists can now reconstruct an accurate transcript of what was typed—including passwords. And in contrast with many types of computer espionage, the process is simple, requiring only a cheap microphone and a desktop computer.

Such snooping is possible because each key produces a characteristic click, shaped by its position on the keyboard, the vigour and hand position of the typist, and the type of keyboard used. But past attempts to decipher keyboard sounds were only modestly successful, requiring a training session in which the computer matched a known transcript to an audio recording of each key being struck. Thus schooled, the software could still identify only 80% of the characters in a different transcript of the same typist on the same machine. Furthermore, each new typist or keyboard required a fresh transcript and training session, limiting the method's appeal to would-be hackers.

Now, in a blow to acoustic security, Doug Tygar and his colleagues Berkeley, have published details of an approach that reaches 96% labelled training transcript. The new approach employs methods de

software to group together all the similar-sounding keystrokes in a alphabet of clicks. The software tentatively assigns each click a lett then tests the message created by this assignment using statistical language. For example, certain letters or words are more likely to c keystroke follows a “t”, it is much more likely to be an “h” than an example” make likelier bedfellows than “fur example”. In a final ref employed a method many students would do well to deploy on tern spellchecking.

By repeatedly revising unlikely or incorrect letter assignments, Dr T from sonic chaos. That said, the method does have one limitation: model, at least five minutes of the recorded typing had to be in sta principle any systematic language or alphabet would work). But on met, the program can decode anything from epic prose to randomis

This sort of acoustic analysis might sound like the exclusive provinc according to Dr Tygar, such attacks are not as esoteric as you migh simple to find the instructions needed to build a parabolic or laser r You could just point one from outside towards an office window to r points out, would-be eavesdroppers might not even need their own laptop computers increasingly come equipped with built-in microph

To protect against these sonic incursions, Dr Tygar suggests a simp His computers were less successful at parsing recordings made in r though, more sophisticated recording gear could overcome even ba typed text vulnerable. Dr Tygar therefore recommends that typed p be replaced with biometric scans or multiple types of authorisation some form of silent verification (clicking on a pre-chosen picture in example). Loose lips may still sink ships, but his research demonst keystroke could do just as much damage.

Technology Quarterly