JitterBugs could turn your keyboard against you

August 7 2006

Researchers from the University of Pennsylvania School of Engineering and Applied Science warn against an entirely new threat to computer security: peripheral devices – such as keyboards, mice or microphones – which could be physically bugged in an attempt to steal data. Penn graduate student Gaurav Shah has identified a class of devices that could covertly transmit data across an existing network connection without the user's knowledge.

They are called JitterBugs, named by Shah's advisor, Penn Associate Professor Matthew Blaze, for both the way they transmit stolen data in "jittery" chunks by adding nearly imperceptible processing delays after a keystroke and for the "jitters" such a bug could inspire in anyone with secure data to safeguard.

Shah presented his findings Aug. 3 at the USENIX Security Conference in Vancouver, B.C., where it was designated the "Best Student Paper" by conference organizers. As proof of the concept, Shah and his colleagues built a functional keyboard JitterBug with little difficulty.

"This is spy stuff. Someone would need physical access to your keyboard to place a JitterBug device, but it could be quite easy to hide such a bug in plain sight among cables or even replace a keyboard with a bugged version," said Shah, a graduate student in Penn's Department of Computers and Information Science. "Although we do not have evidence that anyone has actually been using JitterBugs, our message is that if we were able to build one, so could other, less scrupulous people."

JitterBug devices are conceptually similar to keystroke loggers, such as the one famously used by the FBI to gather evidence against bookmaker Nicodemo Scarfo Jr. Unlike keystroke loggers, which would have to be physically installed into a subject's computer and then retrieved, a keyboard JitterBug only needs to be installed. The device itself sends the collected information through any interactive software application where there is a correlation between keyboard activity and network activity, such as instant messaging, SSH or remote desktop applications. The bug leaks the stolen data through short, virtually unnoticeable delays added every time the user presses a key.

Anytime the user surfs the web, sends an e-mail or instant messages someone, an implanted JitterBug could be timed to open a covert jitter channel to send stolen data. According to Shah, a JitterBug could not log and transmit every touch of the key due to limited storage space on the device, but it could be primed to record a keystroke with a particular trigger.

"For example, one could pre-program a JitterBug with the user name of the target as a trigger on the assumption that the following keystrokes would include the user's password," Shah said. "Triggers might also be more generic, perhaps programmed to detect certain typing patterns that indicate some sort of important information might follow."

JitterBugs are potentially worrisome to governments, universities or corporations with information meant to be kept confidential. One particular scenario is what Blaze refers to as a "Supply Chain Attack," in which the manufacture of computer peripherals could be compromised. Such an attack could, for example, result in a large number of such JitterBugged keyboards in the market. An attacker would only then need to wait until a target of interest acquires a bugged keyboard.

According to Shah, the channel through which the JitterBug transmits data is also the point where it could be most easily detected and countered.

While his presentation only discussed simple countermeasures to JitterBugs, Shah's initial results indicate that the use of cryptographic techniques to hide the use of encoded jitter channels might be a promising approach.

"We normally do not think of our keyboard and input devices as being something that needs be secured; however, our research shows that if people really wanted to secure a system, they would also need to make sure that these devices can be trusted," Shah said. "Unless they are particularly paranoid, however, the average person does not need to worry about spies breaking into their homes and installing JitterBugs."

Source: University of Pennsylvania

Citation: JitterBugs could turn your keyboard against you (2006, August 7) retrieved 23 April 2024 from https://phys.org/news/2006-08-jitterbugs-keyboard.html