Free Adeona service tracks stolen laptops

September 25 2008

Researchers (from left to right) Gabriel Maganis (UW), Thomas Ristenpart (UC San Diego), Tadayoshi Kohno (UW) and Arvind Krishnamurthy (UW), posing as laptop thieves, are caught in the act by the computer's internal camera. The Adeona laptop-tracking software securely sends these photos and Internet protocol addresses to a remote database, where the computer's owner can privately track the laptop's location.

(PhysOrg.com) -- As college students head back to school with gleaming new laptops, some will, unfortunately, see the last of their machine in a library, cafeteria or dorm room. And it's not just college campuses that are hot spots for computer theft, or just students who are the targets. Newspapers recently reported that airports in the United States record hundreds of thousands of laptop thefts annually. Such thefts are not only expensive, they also often mean losing sensitive data.

Researchers at the University of Washington and at the University of California, San Diego have created a new laptop theft-protection tool. The software not only provides a virtual watchdog on your precious machine -- reporting the laptop's location when it connects to the Internet -- but does so without letting anybody but you monitor your whereabouts.

The tool is named Adeona, after the Roman goddess of safe returns, and is posted at adeona.cs.washington.edu/ . It works by using the Internet as a homing beacon. Once Adeona is installed, the machine will occasionally send its Internet protocol address and related information to OpenDHT, a free online storage network. This information can be used to establish the computer's general location.

On a Macintosh computer, Adeona also uses the computer's internal camera to take a photo that it sends to the same server.

Adeona was initially released for free under an open source license in June, and further work will be presented at the ToorCon computer security conference in San Diego Sept. 28. The authors are Thomas Ristenpart, a doctoral student at UC San Diego, who was a UW visiting student in summer 2007; Gabriel Maganis, who recently received his UW undergraduate degree in computer engineering; Tadayoshi Kohno, a UW assistant professor of computer science and engineering; and Arvind Krishnamurthy, a UW research assistant professor of computer science and engineering.

Unlike commercial systems, in which users surrender their location information to a company, Adeona scrambles the information so it must be deciphered using a password known only by the person who set up the account. If the laptop is stolen, only the original owner can access the location data (and, for Macintosh users, a photo). The owner can then bring this information to the police to aid in tracking down the stolen machine. Even if the free OpenDHT storage network was hacked, the information would remain private.

"Adeona is free and easy to install, so anyone who owns a laptop, or even a small company, can use it to track their assets," Maganis said. "We're really hoping laptop users all over the world will install it on their machines."

The tool resulted from an experiment in privacy protection that began two years ago.

"We wanted to build a tool that allows you to track the location of your laptop but at the same time doesn't allow someone else to track you," Kohno said. "Typically when you create a forensics trail, you leave breadcrumbs that you can see, but so can everyone else. We've created a private forensics trail where only you can see those breadcrumbs."

More broadly, the research investigates ways to maintain privacy in a world where geographic tracking is becoming increasingly common.

"Platforms such as the iPhone enable development of more and more software programs that use geographic information in fun and useful ways. Many of these applications could benefit from mechanisms for preserving user location privacy," Ristenpart said.

Since Adeona's public release, more than 50,000 people have downloaded the software under the open source license. The current version works on desktop and laptop machines running Windows, Macintosh or Linux. Researchers say they have already received numerous requests for an iPhone version.

"People like it because it's open source," Maganis said. "That's what we're hearing."

Companies offer features that might justify paying a fee, but they too can learn from Adeona to ensure clients' privacy, Maganis said. "Companies can adapt our techniques to provide high levels of privacy for their own services."

Provided by University of Washington