Researchers show ATM theft by thermal imaging

September 1 2011, by Nancy Owano

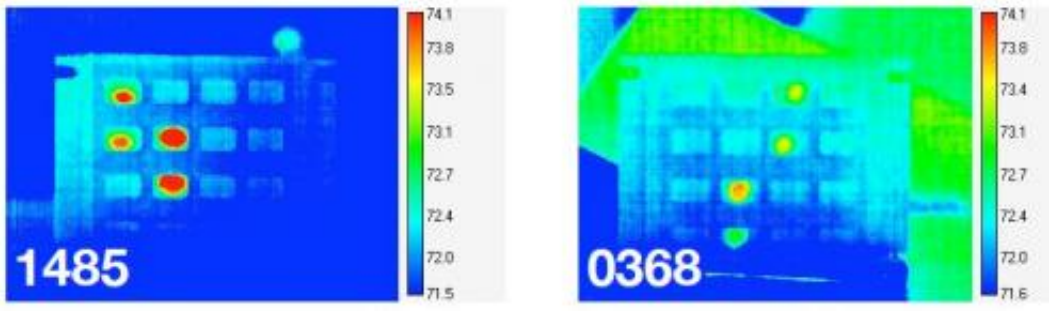

Image credit: Keaton Mowery

(PhysOrg.com) -- A paper presented at the August USENIX Security Symposium (USENIX Security '11) in San Francisco explains how PINs can be stolen using digital cameras capable of thermal imaging. The paper, "Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks," showed how an ATM customer's pressing down keys of a personal code number gives these cameras the ability to catch the numbers from residual heat left behind from the user's fingertips.

The research team from the University of California, San Diego, found that their cameras picked up a PIN entered on a keypad more than 80 percent of the time if used immediately. If used a minute later, it picked up the digits about half the time. After 90 seconds, the chance of extracting the digits dropped to about 20 percent. They tested the frequency using custom software that they wrote to automate their

analysis.

The noteworthy feature of thermal cameras is that the usual protective measure of shielding the keypad with the hand is ineffective. The PIN is captured regardless. Thermal cameras can bypass hand-shielding techniques.

For the study, 21 volunteers tried out 27 randomly selected PIN numbers in the form of four-digit codes on plastic pads and on brushed metal pads.

Keaton Mowery, a doctoral student in computer science at UCSD, Sarah Meiklejohn and professor Stefan Savage did the research, and they said that the surveillance ploy is possible but it is not an easy crime. Although thermal imaging can easily pick up PIN numbers when pressed, the method cannot easily determine in which order. Another hurdle for thieves would be metal keypads, nearly impossible. Because of their high conductivity, metal keys do not retain heat long enough for the ploy to work.

The study extends the conversation about keypad entry systems as a security mechanism in a range of applications, such as to access offices in buildings, secure safes, and operate ATMs. In 2005, security guru Michal Zalewski discussed the use of an infrared camera to detect codes punched into a safe with a keypad lock.

The most recent findings have elicited two viewpoints about personal ID thievery. One reaction to the findings is that while thermal imaging can capture the numbers, the effort is impractical and unlikely to represent a major headache for crime fighters. The numbers captured are not in order, metal keypads thwart efforts, and the high-end cameras required cost approximately $18,000. The other point of view is that thieves will in time get smarter and find ways to recover the exact code or “harvest”

PIN numbers with the help of the right software.

Consumer Reports recommends using a pen, plastic stylus or other object and not your fingers to press the keypad. The study's researchers said what could work is placing the hand over the entire keypad to warm all the keys.

More information: K. Mowery, S. Meiklejohn, and S. Savage "Heat of the Moment: Characterizing the Efficacy of Thermal-Camera Based Attacks" Proceedings of WOOT 2011. August 2011. www.usenix.org/events/woot11/t … nal_files/Mowery.pdf