Issued 7/7/18

How Hackers can Steal your Password with an Infrared Photo of your Keyboard

Researchers at University of California Irvine have demonstrated the ability to recover passwords from the thermal residue of computer keyboards, in a recently published paper. The attack type, called "Thermanator," was tested using a commodity-level FLIR SC620 infrared camera, and four standard PC keyboards. The researchers indicate that "entire sets of key-presses can be recovered by non-expert users as late as 30 seconds after initial password entry," while partial sets can still be viable to recover one minute after entry. As the cost of thermal cameras have become within reach of attackers of average means, this type of attack extends beyond deep-pocketed state-sponsored actors. Of particular interest, FLIR brand imaging devices are available at a variety of price points—the researchers highlight the X8500sc, which they claim to be available for about $100,000, as being at the high end of the market. Conversely, the FLIR One Pro is available for $400 and can attach to any Android smartphone, while the CAT S61 smartphone integrates a FLIR camera into the phone itself. In their research, the researchers attached the camera to a tripod, set 24 inches above the keyboard. Both secure and insecure passwords were used for the experiment. For "hunt and peck" typists, the participants guessing passwords from images were able to correctly guess "12341234" on average "45.25 seconds after entry." For comparison, the weakest result, "football" was recoverable after 25.5 seconds, on average. When using secure passwords, the researchers note that full recall was possible between 19.5 seconds and 31 seconds. For touch typists, the researchers indicate that the best (most secure) was "12341234," which

took 47.6 seconds on average, with "jordan23" at 17.8 seconds. The researchers indicate that full recall was only possible, on average, in the first 14.33 to 18.5 seconds, as images after this time were too indistinct. In terms of efficacy, the researchers note that so-called "hunt and peck" typists are particularly susceptible to having their passwords recovered through Thermanator-style attacks, as these typists use their forefingers to type, thereby using a larger fingerprint for a longer period of time for each keystroke than touch typists. Accordingly, touch typists generate a great deal of "thermal noise" by resting their fingers on the home row of keys on the keyboard, making it more difficult to analyze infrared images of keyboards. The researchers also note that typists with with long acrylic fingernails are "virtually immune" to Thermanator-style attacks, because users with those leave nearly no thermal reside when tapping keys with fingernail tips.