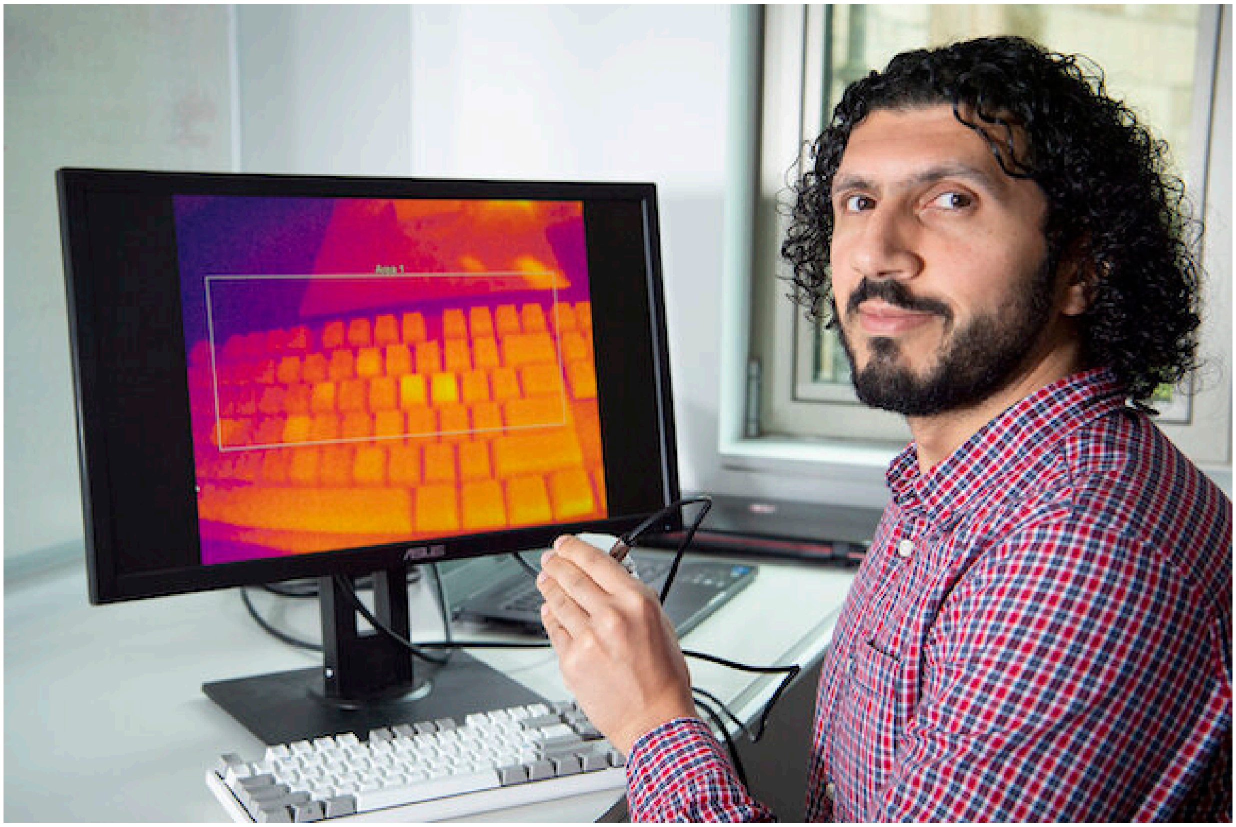
TechXplore

AI-driven 'thermal attack' system reveals computer and smartphone passwords in seconds

October 10 2022



Dr Mohamed Khamis of the School of Computing Science demonstrates using a thermal camera on a computer keyboard. Credit: University of Glasgow

Computer security experts have developed a system capable of guessing computer and smartphone users' passwords in seconds by analyzing the traces of heat their fingertips leave on keyboards and screens.

Researchers from the University of Glasgow developed the system, called ThermoSecure, to demonstrate how falling prices of thermal imaging cameras and rising access to machine learning are creating new risks for "thermal attacks."

Thermal attacks can occur after users type their passcode on a computer keyboard, smartphone screen or ATM keypad before leaving the device unguarded. A passerby equipped with a thermal camera can take a picture that reveals the heat signature of where their fingers have touched the device.

The brighter an area appears in the thermal image, the more recently it was touched. By measuring the relative intensity of the warmer areas, it is possible to determine the specific letters, numbers or symbols that make up the password and estimate the order in which they were used. From there, attackers can try different combinations to crack users' passwords.

Previous research by Dr. Mohamed Khamis, who led the development of ThermoSecure, has already demonstrated that non-experts can successfully guess passwords simply by looking carefully at thermal images taken between 30 and 60 seconds after surfaces were touched.

In a paper published in the journal *ACM Transactions on Privacy and Security*, Dr. Khamis and the authoring team, Ms. Norah Alotaibi and Dr. John Williamson, explain how they set out to harness machine learning to make the attack process more accurate. To do so, they took 1,500 thermal photos of recently-used QWERTY keyboards from different angles.

Then, they trained an artificial intelligence model to effectively read the images and make informed guesses about the passwords from the heat signature clues using a probabilistic model.

Through two user studies, they found that ThermoSecure was capable of revealing 86% of passwords when thermal images are taken within 20 seconds, and 76% when within 30 seconds, dropping to 62% after 60 seconds of entry.

They also found that within 20 seconds, ThermoSecure was capable of successfully attacking even long passwords of 16 characters, with a rate of up to 67% correct attempts. As passwords grew shorter, success rates increased—12-symbol passwords were guessed up to 82% of the time, eight-symbol passwords up to 93% of the time, and six-symbol passwords were successful in up to 100% of attempts.

Dr. Khamis, of the University of Glasgow's School of Computing Science, said, "They say you need to think like a thief to catch a thief. We developed ThermoSecure by thinking carefully about how malicious actors might exploit thermal images to break into computers and smartphones.

"Access to thermal imaging cameras is more affordable than ever—they can be found for less than £200—and machine learning is becoming increasingly accessible too. That makes it very likely that people around the world are developing systems along similar lines to ThermoSecure in order to steal passwords. It's important that computer security research keeps pace with these developments to find new ways to mitigate risk, and we will continue to develop our technology to try to stay one step ahead of attackers.

"We're also keen to highlight to policymakers the risks that these kind of thermal attacks pose for computer security. One potential risk-reduction pathway could be to make it illegal to sell thermal cameras without some kind of enhanced security included in their software. We are currently developing an AI-driven countermeasure system that could help address this issue."

The researchers also looked at additional variables which made it easier for ThermoSecure to guess passwords. One was the typing style of the keyboard users. "Hunt-and-peck" keyboard users who type slowly tend to leave their fingers on the keys for longer, creating heat signatures which last longer than faster touch-typists.

Images taken within 30 seconds of the keyboard being touched allowed ThermoSecure to successfully guess hunt-and-peck typists' passwords 92% of the time, but only 80% of the time for touch-typists.

Secondly, the type of material keyboards are made from can affect their ability to absorb heat, with implications for the effectiveness of thermal attacks. ThermoSecure could successfully guess passwords from the heat retained on keycaps made from ABS plastics around half of the time, but only 14% of the time on keys manufactured from PBT plastics.

The ThermoSecure team has a number of suggestions for computer and smartphone users to protect themselves from thermal attacks.

Dr. Khamis added, "Longer passwords are more difficult for ThermoSecure to guess accurately, so we would advise using long passphrases wherever possible. Longer passphrases take longer to type, which also makes it more difficult to get an accurate reading on a thermal camera, particularly if the user is a touch typist. Backlit keyboards also produce more heat, making accurate thermal readings more challenging, so a backlit keyboard with PBT plastics could be inherently more secure.

"Finally, users can help make their devices and keyboards more secure by adopting alternative authentication methods, like fingerprint or facial recognition, which mitigate many of the risks of thermal attack. In my team we have previously proposed authentication schemes that rely on eye movements for password entry; gaze-based authentication is resistant to thermal attacks by design."

The team's paper, titled "ThermoSecure: Investigating the effectiveness of AI-driven thermal attacks on commonly used computer keyboards," is published in *ACM Transactions on Privacy and Security.*

More information: Norah Alotaibi et al, ThermoSecure: Investigating the effectiveness of AI-driven thermal attacks on commonly used computer keyboards, *ACM Transactions on Privacy and Security* (2022). DOI: 10.1145/3563693

Provided by University of Glasgow

Citation: AI-driven 'thermal attack' system reveals computer and smartphone passwords in seconds (2022, October 10) retrieved 26 April 2024 from https://techxplore.com/news/2022-10-ai-driven-thermal-reveals-smartphone-passwords.html