TechXplore

Computer security experts offer advice to freeze out risk of thermal attacks

August 10 2023

Thermal camera. Credit: University of Glasgow

A team of computer security experts have developed a set of recommendations to help defend against "thermal attacks" which can steal personal information.

Thermal attacks use heat-sensitive cameras to read the traces of fingerprints left on surfaces like smartphone screens, computer keyboards and PIN pads.

Hackers can use the relative intensity of heat traces across recently-touched surfaces to reconstruct users' passwords.

Last year, Dr. Mohamed Khamis and colleagues from the University of Glasgow set out to demonstrate how easily thermal images could be used to crack passwords.

The team developed ThermoSecure, a system which used AI to scan heat-trace images and correctly guess passwords in seconds, alerting many to the threat of thermal attacks.

Now, Dr. Khamis and colleagues have put together the first comprehensive review of existing computer security strategies, and surveyed users on their preferences on how thermal attacks can be prevented at public payment devices like ATMs or transport ticket dispensers.

Their research, set to be presented as a paper at the USENIX Security Symposium conference in Anaheim, California, on Friday 11 August, also includes advice to manufacturers on how their devices could be made more secure. USENIX Security is widely recognized as one of the leading conferences in the fields of computer security and cybersecurity.

The team identified 15 different approaches described in previous papers on computer security which could reduce the risk of thermal attacks.

Those included ways to reduce the transfer of heat from users' hands, by wearing gloves or rubber thimbles, or changing the temperature of hands by touching something cold before typing.

Approaches suggested in the literature also included pressing hands against surfaces or breathing on them to obscure their fingerprint heat once they had finished typing.

Other suggestions for increased security focused on hardware and software. A heating element behind surfaces could erase traces of finger heat, or surfaces could be made from materials which dissipate heat more rapidly.

Security on public surfaces could be increased by introducing a physical shield which covers keys until heat has dissipated. Alternatively, eye-tracking inputs or biometric security could reduce the risk of successful thermal attacks.

After their research on existing security measures, the team conducted an online survey with 306 participants. The survey aimed to determine users' preferences among the strategies the team had identified, as well as asking their own thoughts about security measures they could adopt when using public devices like bank machines.

Dr. Mohamed Khamis, of the University of Glasgow's School of Computing Science, led the research. He said, "This is the first comprehensive literature review of security measures against thermal attacks, and our survey showed some interesting results. Intuitively, users suggested some strategies that weren't in the literature, like waiting to use an ATM until their surroundings seemed safest. They were also keen on strategies that were already familiar, like two-factor authentication, because they were aware of their effectiveness.

"We also saw that they considered issues like hygiene, which made the strategy of breathing on devices to mask heat traces very unpopular, and privacy, which some users considered when thinking about additional security measures like face or fingerprint recognition."

The paper concludes with recommendations for users on how they can defend themselves against thermal attacks in public, and for device manufacturers on how safety measures could be built into future generations of hardware and software.

Prof. Karola Marky, who was a postdoctoral researcher in Dr. Khamis' team at the University of Glasgow during this research, and is now a professor at the Ruhr-University Bochum in Germany, is the corresponding author of the paper. She said, "Users told us that they considered themselves at least partially responsible for their own security, so we advise that they pay close attention to their surroundings when entering sensitive data in public to make sure no-one is watching, or use a secure facility such as a bank. Where that's not possible, we suggest resting palms on devices to obscure traces of heat, or wearing gloves or finger protection if they can.

"We'd also advise using multi-factor authentication wherever users are able because it protects against a range of different attacks including thermal attacks, and safeguard all authentication factors as much as possible."

Paper co-author Dr. Shaun Macdonald, from the University of Glasgow's School of Computing Science is a member of Dr. Khamis' team. He said, "For manufacturers of devices used in public spaces, we suggest that thermal attacks are considered as early as possible in the design phase, so that devices could be augmented with physical screens to block the surfaces for a brief period, or privacy-enhancing keyboards that shuffle the layout of keys after use. Where devices are already in circulation, software updates could help remind users to be aware of their surroundings and take action to prevent observation with thermal cameras."

Dr. Khamis added, "Our final recommendation is to the manufacturers of thermal cameras, who could stop attacks by integrating new software locks to prevent thermal cameras from taking pictures of surfaces like PIN pads on bank machines.

"We're continuing to explore potential approaches to mitigating the risk of thermal attacks. Although we still don't know how widespread these attacks on personal information are at the moment, it's important that computer security researchers keep pace with the risks that thermal cameras could pose to users' personal information, particularly since they are now so cheap and widely available.

"Ultimately, our advice to the public would be to try to find one strategy that suits their own personal habits and behaviors and to remember to use it as often as possible in their lives. Any action they can take regularly to help guard against thermal attacks will make it harder for others to gain access to their personal data."

More information: In the Quest to Protect Users from Side-Channel Attacks—A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals. www.usenix.org/conference/usen … 3/presentation/marky

Provided by University of Glasgow

Citation: Computer security experts offer advice to freeze out risk of thermal attacks (2023, August 10) retrieved 8 May 2024 from https://techxplore.com/news/2023-08-experts-advice-thermal.html