جامعة جدة
University of Jeddah

Project Proposal

Thermal Imaging Attacks

CCCY 221: Cybersecurity Fundamentals

Dr. Rawan Baalous

31/12/2022

University of Jeddah

College of Computer Science and Engineering

Project partners:

- Raghad Lafe - 2111941
- Abrar Al-Madani- 2115118
- Deem Al-Suoilme - 2111423
- Joury Al-Shelwai - 2110772
- Sirin Al-khamisi - 2111517

Content Page

This video aims to spread awareness to the general population about thermal imaging attacks. Attacks that use thermal cameras to detect the heat trace on keyboard or touchscreen to reconstruct victim password. We want to increase the awareness of individuals in terms of reducing the possibility of stealing private passwords by 70% by thieves who use thermal imaging devices through ways that the individual does, which helps them to increase the difficulty for the thief to know the password. We are committed to spread awareness to the Saudi public about the threats of the thermal imaging attack and the protection methods they should take for defense. Most, if not all the time, we don't check our surroundings when entering a password into a device. Thermal imaging attacks are so simple that they can be done over the shoulder without notice. We will start by taking enough notes about people's awareness of the problem during the next week, and then in the following weeks, we will create an awareness video about thermal imaging attacks. We will finish after 5 weeks, which is before our deadline on 11 February.

At the beginning of the video

We will make an animation video to illustrate the danger of thermal imaging attacks. At first the video will explain this attack and how it happens. Then it will show a few examples of the attack. At the end it will teach the audience how to protect themselves from it.

Explain Different Types to Use Thermal Cameras

There are two ways to use thermal cameras, the first is by installing them at an angle that allows them to see the entire keyboard of a building's door, or another way is a portable camera where the attacker can walk and photograph the keyboard in a few.

Thermal Imaging on ATMs and Smartphones

On ATMs: The victim goes to an ATM, inserts his card, enters his PIN, takes his cash, and walks off. A few seconds later an attacker takes a picture of the same ATM's keyboard using a thermal imager. But this kind of attack is unlikely because the attacker should have stolen the victim's credit card. In addition, ATMs allow users to try entering the PIN only three times before it blocks the card.
On Smartphones: During a thermal attack, the thermal camera transfers heat traces from the user's hands to the touch screen, which attacks can be taken out after the user has left the device(This rarely happens) which is an advantage since the attacker no longer needs to watch the user when authenticating.

how to prevent yourself from it?

The method of creating a password is very similar to the method of creating a code for doors, but in addition to that raising the brightness of the device increases the temperature, and thus this helps to reduce the time during which thermal effects appear.

Thermal Imaging on Doors Code

attacks on keyboard building's doors and home house doors works the same way. But in this case the attack would be more effective and harmful. Because to enter a building the attacker would only need the password. And by a thermal camera he would have the key, the only thing left for him is to reconstruct the key.

This attack depends on several aspects such as one person differs from another in terms of the strength of his pressure on the buttons, whether light or strong. Also, people with warm blood produce more thermal energy than those with cold blood.

How to prevent it?

Using passwords that contain multiple overlaps, such as 7267423, as there are two repeated numbers, but one of the conditions for repeating the numbers is that the password is long because the short and repeated numbers make it easier for the attacker to guess the number easily, and also the length of the number helps to fade the effect of the entered numbers, so the beginning is simple, which complicates the attack.

Also, placing the full hand on all the buttons makes it difficult for the attacker to know the code, because the buttons have been smeared with random fingerprints.

Requirements:

- Proposal: we used Google Docs to share ideas with our partners and work together at the same time
- Video: we plan to use animation and graphic design programs to create our awareness video (Canva, etc.)
- Audio: we intend on using audio enhancers to have a professional audio result (inShot)

Implementation Plan:

Step1: Search and gather information

Step2: Writing proposal

Step3: Create video

Step4: Record audio

Step5: Editing

Step6: Publish video

In the end, thermal attacks are a real threat to devices and should be paid more attention to by both users and creators of authentication schemes. Because, as we mentioned earlier, devices contain confidential and sensitive information, such as personal photos and bank account information or even the code that opens your door. Based on our in-depth study, we also provide several thermal attack defense solutions.

Reference

K. Mowery, S. Meiklejohn, and S. Savage, “Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks.” [Online]. Available: https://cseweb.ucsd.edu/~kmowery/papers/thermal.pdf

“How to glean passwords using thermal imaging,” *www.kaspersky.com*. https://www.kaspersky.com/blog/thermal-imaging-attacks/46041/ (accessed Dec. 31, 2022).