IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 May 2024, accepted 5 June 2024, date of publication 12 June 2024, date of current version 21 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3413571

RESEARCH ARTICLE

LightTouch: Harnessing Laser-Based Signal Injection to Manipulate Optical Human–Computer Interfaces

TATSUKI TANAKA[1], SARA RAMPAZZI[2], (Member, IEEE), AND TAKESHI SUGAWARA[1], (Member, IEEE)

[1]Department of Informatics, The University of Electro-Communications, Tokyo 182-8585, Japan
[2]Department of Computer and Information Science and Engineering, University of Florida, Gainesville, FL 32611, USA

Corresponding author: Takeshi Sugawara (sugawara@uec.ac.jp)

This work was supported in part by the SECOM Science and Technology Foundation, in part by Japan Society for the Promotion of Science under KAKENHI Grant Number 22H00519, in part by Japan Science and Technology Agency under CREST Grant Number JPMJCR23M4, and in part by a gift from Meta.

ABSTRACT This paper studies the capability of light-based signal injection attacks to remotely inject fake inputs to modern optical sensor-based input devices. We demonstrate how an attacker can successfully inject malicious Character User Interface (CUI) commands on different laser-projection keyboards and generate fake mouse-cursor movements in bending mouses, using invisible to human eyes, infrared lasers. Our proof-of-concept evaluation shows how the attack achieves 100% success rate on injecting basic keyboard operations up to 7 meters away from the victim input device and through glass windows, without tampering with the victim computer system, or needing a network connection to pursue the attack. This vulnerability allows the attacker not only to type unauthorized commands but also to prevent the unlocked victim PC or workstation from automatically going to sleep mode, thereby extending the time window for locally committing malicious activities, i.e., lunchtime attacks. Within a wide viewing angle of 30°–45° from the victim input device location, the attacker can continuously inject false movements and press at least 24 consecutive keys without any failure up to 5 meters away. We also verify the attack feasibility in realistic office environments where the laser beam is partially occluded. Our analysis shows the potential security risks of invisible light injection attacks, including providing preventive defense measures to limit exposure of optical input interfaces to such a threat. This work aims to help manufacturers address the vulnerability and build reliable Human-Computer Interfaces.

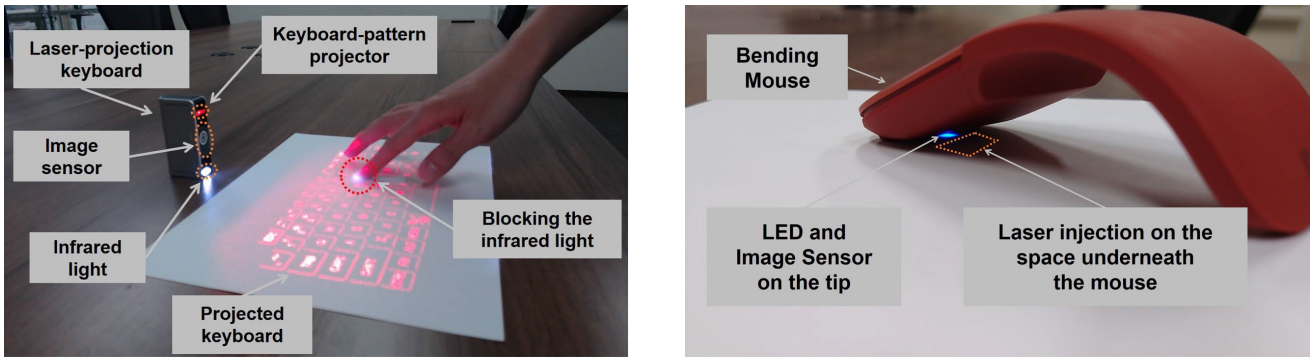
INDEX TERMS Signal-injection attack, human–computer interface, command-injection attack, optical interference, mouse, keyboard.

I. INTRODUCTION

The human-computer interface (HCI) plays a crucial role in computer systems, facilitating the interaction between humans and computers. In personal computers (PCs), mice and keyboards serve as the prevailing Human-Computer Interfaces (HCIs), while smartphones and other smart devices also incorporate advanced HCIs such as touch panels, voice commands, and, more recently, headsets [41].

However, despite the impressive variety of features offered by advanced HCIs, traditional input devices like keyboards and mouses remain widely spread for their established familiarity, versatility, and the tactile feedback they provide especially in the gaming industry [28], [41]. These devices provide an extremely fast and efficient way of interacting with computers and are still evolving to satisfy various needs. For instance, modern mouses and keyboards, such as projection keyboards and optical mouses (see Fig. 1), use the accuracy of reflected laser beams to interpret human hand and finger motions with greater accuracy. Such devices overcome the limitations of mechanical input units

The associate editor coordinating the review of this manuscript and approving it for publication was Patrizia Livreri.



(a) Laser-projection keyboards (b) Bending mouse

FIGURE 1. The target optical HCIs examined in this study. (a) Keyboards that draw keys on a desk surface with a laser projector. (b) Modern optical mouses with ergonomic shapes and bent forms that improve usability and portability.

and touchscreen sensitivity issues allowing optimization for a specific application while maintaining speed and simplicity.

Despite these technological advancements, the security of mouses and keyboards remains under exploration, as these input devices continue to serve as a common attack vector for malicious actors seeking unauthorized access to computer systems by capturing and/or maliciously mimicking user inputs and actions. Common attack vectors for these devices include eavesdropping radio communication, compromised cables or chargers, and malicious firmware reprogramming [3], [22], [26]. However, these threats need exploitable vulnerabilities in the digital systems or an untrusted USB device plugged to a victim PC. In addition to such attack vectors, researchers have discovered that physical side channels can be used to infer sensitive information from these input devices. For instance, an attacker can perform key eavesdropping by capturing the sound emitted from keyboards while typing [2], [6], [44], by observing thermal images and [48], electromagnetic emanation [14], [38], [45], or by exploiting electrical crosstalk in USB's physical communication layer [9].

Signal injection attacks are also widely recognized as a threat to computer systems. In particular, researchers have identified that physical phenomena, such as ultrasonic waves [25], [37], [39], [43], [49], electromagnetic waves [18], [21], [46], and light [4], [5], [27], [29], [36], [39], [40], [47], can interfere with sensors, enabling the attacker to control advanced systems by manipulating sensor reading arbitrarily. This work focuses on investigating the possibility of attackers remotely controlling optical input devices by exploiting the susceptibility of their optical sensors to injection attacks invisible to human eyes. More precisely, this work aims to tackle the following research questions:

- Can attackers leverage the presence of exposed optical sensors in input devices to achieve remote control?
- Which factors can limit the effectiveness of this type of remote injection over input devices such as projected keyboards and optical mouses?

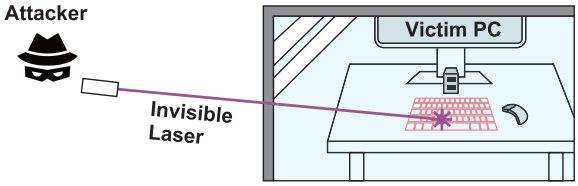


FIGURE 2. An example of attack scenario. The attacker from outside a building injects invisible keys into a keyboard connected to the victim PC through a closed glass window.

- How attackers can exploit this vulnerability to pursue other attacks such as command injection attacks or lunchtime attacks?

This paper begins to examine how an attacker can use laser light to attack commercial optical input devices remotely and effectively, and which malicious activities can be carried out with such attacks without the need to tamper with the victim input device or the victim computer system. More specifically, we start answering the above questions by experimentally evaluating the attack methodology on different commercial input devices by considering an attacker who remotely injects invisible, infrared (IR) lasers, as shown in Fig. 2. We also provide an evaluation in a realistic office setting to demonstrate the feasibility of our attack in partially occluded scenarios.

A. CONTRIBUTIONS

The proposed work separately investigates the adversarial capability of attacking optical keyboards (Section IV) and mouses (Section V) by providing the following main contributions. Videos showing the experimental verification are provided as supplementary material.

1) COMMAND INJECTION ON LASER-PROJECTION KEYBOARDS

We demonstrate our threat model by successfully injecting fake keys and commands on two different laser-projection keyboard models (see Fig. 1-(a)) by shooting an IR laser

on the keyboard's projected region. Once the access to the command shell is established, the attacker can inject any command as the end user, such as installing a malware, eavesdropping on sensitive data, or disrupting information.

Our proof-of-concept setup achieves 100% success rate in injecting basic keyboard operations up to 7 meters through a glass window, the maximum distance available in our experimental environment. In particular, our minimal setup allows an attacker to inject at least 24 consecutive key events without any failure up to 5 meters and two attack directions (front and back). We show that this is sufficient to effectively perform basic commands such as (i) reducing the volume for acoustic feedback, (ii) opening the Windows command prompt, and (iii) opening a target file with a specified software application. Furthermore, we show how the attacker can pursue a successful attack from a location partially occluded by a mesh (e.g., an office chair).

2) INVISIBLE MOUSE CURSOR MANIPULATION

We demonstrate how our threat model is applicable as well to optical mouses with exposed optical sensors by evaluating our attack on two popular bending mouses models. By shining a laser toward the space between the mouse and the desk (see Fig. 1-(b)) and moving the laser spots, an attacker can induce fake mouse-cursor movements in the victim PC. With such false movement, an attacker can prevent the victim PC or workstation from automatically going to sleep mode, thereby extending the time window available to pursue malicious activities such as lunchtime attacks [11], [17]. Within a laser injection angle of 30°– 45° from the front of the device and in line of sight to the optical sensor (see Fig. 10), we show how the attacker can successfully manipulate the victim mouse cursor up to 7 meters away, consistently preventing the victim PC from going to sleep mode, including partially occluded scenarios.

II. THREAT MODEL

Fig. 2 illustrates the attack scenario considered in this work. A victim uses a computer with optical input devices in regular home or office environments. The victim temporarily leaves the computer without locking it, creating room for an adversary to take advantage of the circumstances, as explored in previous work [11]. The attacker is motivated to take control of the victim PC by inducing fake inputs by remotely injecting invisible laser light toward the optical HCIs.

We assume the target HCI has an exposed optical sensor, such as in the case of laser-projection keyboards or bending mouses. The attacker might have a direct line of sight toward the optical sensor such as in previous work light-based attacks [4], [5], [27], [29], [36], [39], [40], [47], or also via indirect laser reflection as explored in previous works [33]. For instance, bending mouses make use of light reflected by a surface, e.g., a desk, to calculate the amount of movement and direction. In this case, we demonstrate that the line of sight to the point of reflection on the surface is sufficient for the attacker to pursue a successful injection.

We also assume the attacker knows the target input devices and can investigate the device's properties in advance, such as keyboard type, optical sensor location, and light wavelength used by the optical sensor. The attacker can retrieve this information by buying a similar device or leveraging publicly available information such as device manuals.

Our attack can be applied in different lunch-time attack scenarios. For example, we consider a private room closed by the victim user with a physical lock. The victim might assume their PC is secure since nobody has access to the room. The attacker from a nearby building/room/outside separated from the target room by a glass surface (e.g., windows, glass doors) can use laser injection to achieve control of the victim PC. Another attack scenario might happen in a shared office where the victim user goes out for lunch, assuming that the computer automatically goes to sleep with a short timeout. The attacker wants to physically operate on the unlocked computer, but the attempt might raise the attention of nearby people which might be present in the same room. The attacker can achieve this by keeping the computer awake with invisible laser injections until people leave.

Finally, for our end-to-end analysis, we consider the difficult scenario of a one-way (cf. adaptive) attack without feedback from the victim computer. If such feedback is available to the attacker, e.g., using a camera to look at the victim's computer monitor using the same line of sight as the injected signal, the attacker can use the feedback to adaptively adjust the light-based injection and maximize the attack success.

III. PREVIOUS WORKS

In this section we briefly summarize previous research that has a close relation to our work.

A. CONVENTIONAL ATTACKS ON MOUSE AND KEYBOARDS

There are several hardware attack vectors on mouses and keyboards which mainly target communication protocols [19], [26], [30]. For instance, BadUSB [26] demonstrates a dongle-like USB device that behaves as a USB keyboard and injects malicious sequence of text commands. Other attacks exploit weak radio communication in wireless mouses and keyboards. For example, MouseJack [3] remotely manipulates mouse operations by sending particular commands to the radio communication between a PC and a vulnerable mouse.

In another work done by Maskiewicz et al. [22], an attacker can overwrite the firmware on a target input device, which can be then used to deliver malware to the victim computer system. The above attack vectors assume either the user plugs the input systems into untrusted USB devices or the presence of device-specific vulnerabilities. In contrast, physical-layer exploitation is possible without such assumptions. For instance, researchers have discovered how to infer keys using sound [2], [6], [44], thermal images [48], and electromagnetic emanation [14], [38], [45]. However, these attacks suffer from

two main limitations: (1) the susceptibility to the noise level from the environment which substantially reduces the amount of information that can be retrieved, and (2) the proximity (typically in the order of centimeters) in which the attacker device should be located respect to the victim input system, which in turn limits the practicality of such attacks in realistic settings. Our work focuses on a different type of exploitation, using laser signal injection attacks to induce fake inputs.

B. SIGNAL INJECTION ATTACKS ON HCIs

Signal injection attacks consist of injecting specially crafted physical signals such as modulated electromagnetic interference, light, and sound, to manipulate or gain control over a victim system. Such attacks pose severe security risks since they cannot be easily detected or mitigated using conventional defense mechanisms such as software checking or network filtering. Researchers have investigated the security risks of such attacks in a wide range of input devices and sensors, including touch screens [21], [46], voice assistants [18], [39], [49], and motion sensors [25], [43]. For example, touch screens used in smartphones, tablets, and PCs detect human fingers using capacitive sensors. Researchers discovered that such capacitive sensors are susceptible to electromagnetic injection, allowing adversaries to inject false touches [21], [46]. Meanwhile, voice assistants (e.g., Amazon Alexa and Google Assistant) capture spoken language with microphones and recognize commands after natural language processing. In recent years, several works have shown how to inject false signals into microphones to mimic the human voice using electromagnetic waves [18], inaudible sound [49], and light [39]. In a similar way, motion sensors which are used to recognize human motions and gestures in VR systems and phones, use MEMS gyroscopes and/or accelerometers that have sensitivity to acoustic vibrations. Such vulnerability can be exploited by attackers to manipulate locations and perceived movements [25], [37], [43].

C. LASER-BASED INJECTION ATTACKS

The early laser-based injection attacks exploited the photoelectric effects to cause bit-flips and errors in digital circuits to bypass security mechanisms or cryptographic protection [10], [16]. More recently, laser light has been used to inject false data into sensors, including cameras [29], [33], [47], LiDARs [4], [5], [36], and drip sensors [27]. Malicious laser light can also affect non-optical sensors through the photoelectric and photoacoustic effects, such as microphones [39] and pressure sensors [40]. In contrast with other signal injection attacks based on sound and electromagnetic interference, laser-based injection exploits the unique characteristics of coherent light to allow attackers to pursue accurate long-range and invisible injection attacks on systems. In this work, we explore the attacker capability to use this unique advantage against optical keyboards and mouses.

TABLE 1. Target laser-projection keyboard models.

Identifier	Product Name	Manufacturer
K_1	Epic [7]	Celluon
K_2	TK-PBL042BK [12]	ELECOM

IV. COMMAND INJECTION ATTACK ON LASER-PROJECTION KEYBOARDS

A. TARGET KEYBOARDS AND ATTACK PRINCIPLE

We begin by evaluating laser-based injection attacks on laser-projection keyboards that use a built-in laser scanner to project keyboard keys on a surface (e.g., a desk or table) as shown in Fig. 1-(a). In this analysis, we mainly focus on two representative keyboard models [7], [12], namely K_1 and K_2, summarized in Table 1. Similar products based on the same principle are commercially available from several vendors worldwide [35].

Our target keyboards use both visible and invisible wavelengths. The visible red lasers around 630 nm are used to draw keys on the surface. When a user taps on the laser-projected keys with their fingers, they are recognized as key-pressing events. The keyboard uses a pair of an IR projector and an IR camera for detecting finger locations. When a user touches the desk, the finger blocks the projected light, as indicated in Fig. 1-(a). The keyboard captures the change in IR reflection by using the IR camera and detects the finger location after image processing. Our preliminary experiments using a spectrometer (Hamamatsu C13053MA) verifies that the IR light wavelength for finger detection is ~826 nm for both K_1 and K_2.

The above sensing principle suggests that when an attacker injects an IR laser, the keyboard can falsely recognize the injected light as a legitimate reflection from a finger, causing the keyboard to accept false inputs. By remotely pressing keys on the keyboard, the attacker can gain control over the victim's computer system connected to it by typing commands. In the following sections, we evaluate the feasibility and attacker capability to perform such command injection attacks on laser-projected keyboards.

B. SETUP

Our attack setup is composed mainly of the following components: a laser, optics, a tripod, and a laser driver. This constitutes the minimal setup necessary to conduct a successful key injection.

Laser sources with roughly 800–1000 nm wavelengths are desirable for a stealthy attack since they are invisible to human eyes while visible to CMOS image sensors without IR filter. We choose an invisible laser diode (ROHM Semiconductor RLD85PZJ4 [31]) with a wavelength (852 nm) similar to the measured IR projectors finger-detection (826 nm in K_1 and K_2). Furthermore, we empirically verified that the target keyboards are also sensitive to higher IR wavelengths, such as 940 nm.

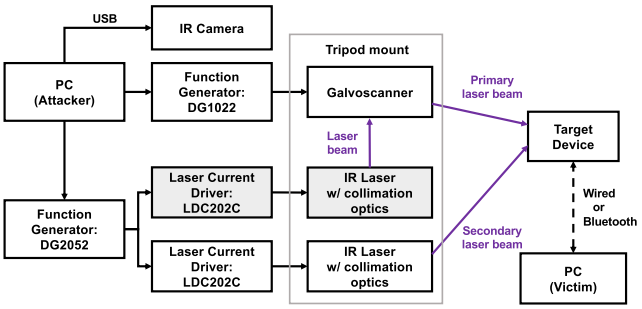


FIGURE 3. The complete experimental setup used in our evaluation. The gray boxes are the essential components: a laser with collimation optics mounted on a tripod and a laser driver. The full setup also includes (i) a galvoscanner for electrical laser scanning, (ii) a secondary laser for sophisticated attacks.

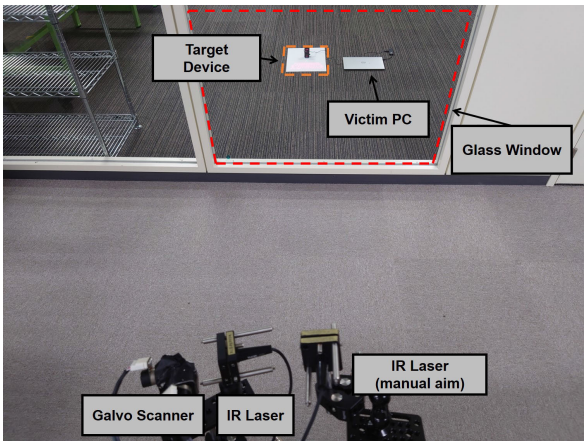


FIGURE 4. The laser and galvoscanner mounted on a tripod aimed at the target.

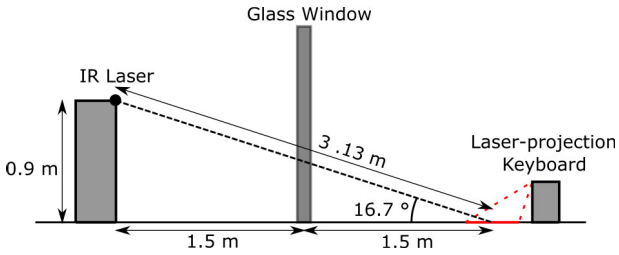


FIGURE 5. Side view of the experimental setup for the 3m case.

The diode laser has a collimation lens (Thorlabs C330TMD-A/C340TMD-A) to regulate the laser spot size on the projected keyboard by adjusting the distance between the laser diode and the lens. We also use a function generator (RIGOL DG2052) connected to the current driver to regulate the minimum laser power required by the adversary to pursue the attack.

Although the attacker can conduct the attack directly by aiming a fixed laser source manually at the target keyboard, in our capability evaluation, we use a more sophisticated setup (that we will refer to as "full" setup) for automatic reproducibility and accuracy evaluation. Our full setup deploys a galvoscanner [1] to allow automatic injection and a webcam as shown in Fig. 3. The webcam (ELP-USB4KHDR01-MFV) without an IR filter is placed next to the laser diode. We use the webcam image feedback to automatically aim the injection by checking the injected IR laser spots invisible to human eyes. By controlling the electrically controlled mirrors of the galvoscanner through a function generator (RIGOL DG1022), this full setup can systematically inject the light in programmed locations. In our end-to-end evaluation, we show how this automatism can be implemented by the attacker to quickly inject a command composed of a series of key events. We also show how an attacker can enhance the setup with a second laser source to execute advanced operations, such as decreasing the sound volume by pressing multiple keys simultaneously.

Finally, we connect our victim system, a Windows laptop, to the target laser-projection keyboards via either USB or Bluetooth. During the experiments, we use either a text editor or the command prompt running on the victim PC to monitor the keyboard activities and determine our attack success rate.

C. ATTACKER CAPABILITY: DISTANCE ANALYSIS

We evaluate the Attack Success Rate (ASR) on the two keyboard models (K_1 and K_2) at different distances and laser power, considering an attack from an adjacent room separated by a glass window. Both rooms are illuminated with fluorescent lights, and their illuminance level is 420 lx, which fits within the illumination range of a standard office environment (300–750 lx) [15]. Fig. 4 shows the experimental environment, wherein the laser is aimed at the target keyboard placed on the floor over a white paper. For each key, we activate the laser for 0.2 seconds. Fig. 5 shows the side view of the attack scenario when the laser and the keyboard is apart by 3 meters. The laser-glass distance is fixed to 1.5 m, and the glass-keyboard distance is gradually increased for our distance evaluation. Note that in our capability analysis, we project the keyboard on the floor and locate the adversarial laser source on a tripod at the maximum height of 90 cm to allow the line of sight of the keyboard at 3, 5, and 7 meters away from the attacker. This setup location is necessary for safety measures, to maintain the laser beam trajectory below eye level as shown in Fig. 4.

We evaluate both single-key and multiple-key injections. For the single-key injection, we examine four selected keys distributed along the QWERTY layout, namely the keys `Q`, `F`, `M`, and `Enter`. The success or failure of the injection is verified with a text editor running on the victim PC. Note that for this analysis we do not use the computer monitor visual feedback to adjust the attack, to simulate a realistic attack scenario. For the multiple-key injection, on the other hand, we test the correct continuous pressure of the `Function` and the `down-arrow` keys. This combination reduces the volume of a feedback beep from the keyboard, supposedly used by the attacker for a stealthy attack. Since this injection makes no visible event on the PC monitor, we verify the injection by hearing the feedback beep.

TABLE 2. Attack success rate (%) over 10 trials for each operation with the two keyboard models K_1 and K_2. Q, F, M, and Enter are the single-key injection of the corresponding keys. Mult. is multiple-key injection pressing the Function and down-arrow keys simultaneously, which reduces the volume of an audio feedback.

Distance	Laser Power	Keyboard K_1					Keyboard K_2				
[m]	[mW]	Q	F	M	Enter	Mult.	Q	F	M	Enter	Mult.
3	2.00	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
3	1.75	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
3	1.50	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
3	1.25	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
3	1.00	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%
3	0.75	100%	100%	100%	0%	100%	100%	100%	100%	0%	0%
3	0.50	0%	100%	100%	0%	0%	100%	100%	100%	0%	0%
3	0.25	0%	100%	100%	0%	0%	0%	100%	0%	0%	0%
5	2.00	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
5	1.75	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
5	1.50	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
5	1.25	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
5	1.00	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%
5	0.75	100%	100%	100%	0%	0%	100%	100%	100%	0%	0%
5	0.50	0%	100%	100%	0%	0%	0%	100%	100%	0%	0%
5	0.25	0%	100%	100%	0%	0%	0%	100%	0%	0%	0%
7	2.00	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
7	1.75	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
7	1.50	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
7	1.25	100%	100%	100%	0%	100%	100%	100%	100%	100%	100%
7	1.00	100%	100%	100%	0%	0%	100%	100%	100%	0%	100%
7	0.75	100%	100%	100%	0%	0%	0%	100%	100%	0%	0%
7	0.50	0%	100%	100%	0%	0%	0%	100%	100%	0%	0%
7	0.25	0%	100%	0%	0%	0%	0%	0%	0%	0%	0%

We conduct 10 consecutive trials for the two keyboard models at increasing distances (3, 5, and 7 meters), and eight laser powers (from 2.00 to 0.25 mW at 0.25 mW step). The laser power is measured at the output of the galvoscanner using a laser power meter (Thorlabs PM100D with the S121C sensing head). The maximum laser power (2 mW) is determined by the laser diode's maximum power rating and the loss at the galvoscanner. Note that the maximum laser power tested (2 mW) is lower than the power of popular commercial laser pointers used for presentations (∼5 mW).

Results and Observations: Table 2 shows the ASR under the different tested scenarios. The results show a binary behavior: If the attack succeeds once, it will succeed for all the following nine trials (100% ASR); if not, none of the trials will succeed. This behavior suggests that the target keyboards set a threshold in recognizing key-pressing events. We also notice that the detection threshold depends on keys. Enter, Q, F, and M succeed for 1.25, 0.75, 0.25, and 0.25 mW of laser power, respectively. The required laser power increases as the position of the key is apart from the keyboard center. We hypothesize that a more conservative threshold is used for the keys farther from the center of the projected keyboard because the camera images captured by the keyboard become less accurate at the edges due to aberration. The same behavior can be observed for the multiple-key injection (shown as *Mult.* in Table 2), where unsuccessful injection is primarily caused by the down-arrow key pressure failure.

Our evaluation also shows that the ASR decreases for longer distances, e.g., the 3 m and 7 m results for K_1. As distance increases, the injected laser spot becomes larger (limited by the diffraction limit), reducing the peak optical power measured by the keyboard's camera and thus not reaching the necessary threshold to trigger the pressure event.

D. END-TO-END EVALUATION

We leverage the basic operations examined in the previous section to pursuit an end-to-end attack in a realistic scenario, i.e., an automatic and stealthy command-injection attack on the two target keyboards through a glass window from an adjacent room. We inject the following sequence of steps to execute a complete attack:

1) Decrease the sound volume by pressing the down arrow key while holding down the function key.
2) Press the Windows key
3) Execute the command prompt: type cmd and press the Enter key
4) File execution: type notepad secret.txt and press the Enter key

The first step is intended to improve the attack's stealthiness since some projected keyboards might emit beep sounds as audio feedback to users when they recognize the input events. The attacker first reduces the volume of such beep sounds to prevent a user nearby from noticing the attack attempt. In this evaluation, we inject the volume-reducing command for five times to set it to the minimum volume.

The following steps 2–4 open a secret text file with a notepad with keyboard inputs through the Windows

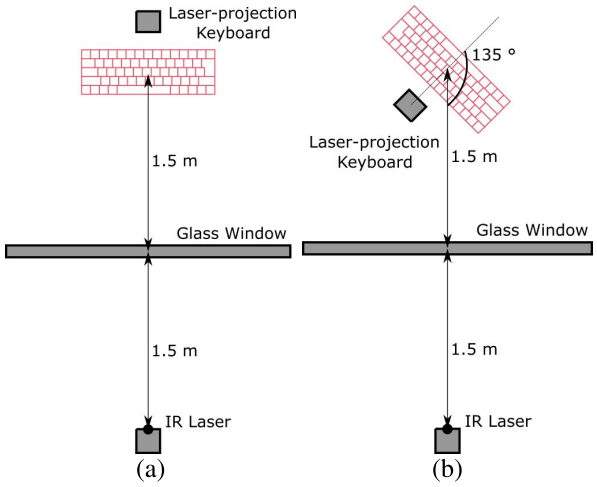


FIGURE 6. Top view of the evaluation scenario with the attacker located at 3 meter distance from the keyboard through a glass window. (a): "front" case with the attacker aiming at the front of the projected keyboard, i.e., the laser injection angle is 0°. (b): "back" case with the attacker aiming at the back of the projected keyboard with not occluded line of sight, wherein the laser injection angle is 135° from the device's center.

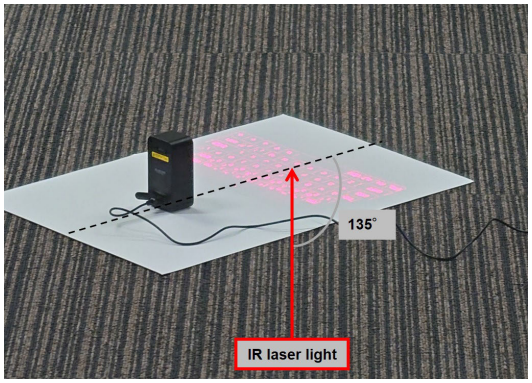


FIGURE 7. Injection in the "back" case, at 135° angle from the keyboard center. We consider the `G` key as the rotation center.

command prompt. The entire operation is composed of 24 consecutive keys, and we consider the attack successful if the file `secret.txt` is correctly opened on the PC monitor.

We program the galvoscanner and laser driver to achieve the injection quickly and automatically. With our full setup, the adversary is able to execute the entire sequence in 37 seconds, as each single-key and multi-key event takes 1.0 and 2.6 seconds, respectively.

We consider two corner cases to show the attack feasibility from different attacker locations, namely the attacker aiming at the front of the projected keyboard (we call this location "front"), and the backside (we call this location "back"). The first case considers an attacker located in front of the victim keyboard (the laser injection angle of 0°) as shown in Fig. 6-(a). In the second case, the attacker is located in the back of the projected keyboard (the laser injection angle of 135°) as shown in Fig. 6-(b) and Fig. 7. Note that 135° is the maximum attacker's view angle (on both left and right sides) from the keyboard center necessary for the attacker to maintain the line of sight of the entire keyboard.

TABLE 3. End-to-End ASR (%) over 10 trials for each operation with the two keyboard models K_1 and K_2. The experiment is conducted from the front (0°) and the back (135°) of the target keyboard, as shown in Figure 6. We set the laser-to-keyboard distance to 3, 5, and 7 meters.

Distance	Laser Power	Keyboard K_1		Keyboard K_2	
[m]	[mW]	0°	135°	0°	135°
3	2.00	100%	100%	100%	100%
3	1.75	100%	100%	100%	100%
3	1.50	100%	100%	100%	100%
3	1.25	100%	100%	100%	100%
3	1.00	0%	0%	100%	0%
3	0.75	0%	0%	0%	0%
3	0.50	0%	0%	0%	0%
3	0.25	0%	0%	0%	0%
5	2.00	100%	100%	100%	100%
5	1.75	100%	100%	100%	100%
5	1.50	100%	100%	100%	100%
5	1.25	100%	0%	100%	100%
5	1.00	0%	0%	100%	0%
5	0.75	0%	0%	0%	0%
5	0.50	0%	0%	0%	0%
5	0.25	0%	0%	0%	0%
7	2.00	0%	0%	0%	0%
7	1.75	0%	0%	0%	0%
7	1.50	0%	0%	0%	0%
7	1.25	0%	0%	0%	0%
7	1.00	0%	0%	0%	0%
7	0.75	0%	0%	0%	0%
7	0.50	0%	0%	0%	0%
7	0.25	0%	0%	0%	0%

Beyond this angle, the attack is still possible, however, some of the keys are occluded by the keyboard body.

Results and Observations: Table 3 summarizes the ASR obtained for K_1 and K_2 repeating the injection sequence 10 times at three increasing distances and eight different laser powers. We observe 100% ASR up to 5 m away from the target keyboard behind the glass window. The required laser power for the attack success at 3 m and 5 m is determined by the success of the `Enter` key pressure.

The ASR at 7 meters is zero even though pressing each key succeeds with high probability (see Table 2), which highlights the difficulty of pressing multiple keys in sequence without failure. There are two reasons for the performance degradation with the consecutive key inputs. First, a successful attack without visual feedback must successfully complete 24 injections without failure, increasing the probability of error. Second, the mechanical component of our setup (the galvo scanner) has limited precision. Small alignment errors are generated every time we move the mirrors, which do not happen in our single-key evaluation with fixed mirror positions. Moreover, the setup becomes more sensitive to natural vibration at longer distances, and the failure probability increases as the entire procedure takes longer, i.e., 37 seconds in this end-to-end evaluation. We discuss potential improvements to the attack in Section VII.

V. MOUSE CURSOR MANIPULATION

In this section, we demonstrate how our laser light injection can be used to take remote control over mouses with exposed optical sensors.

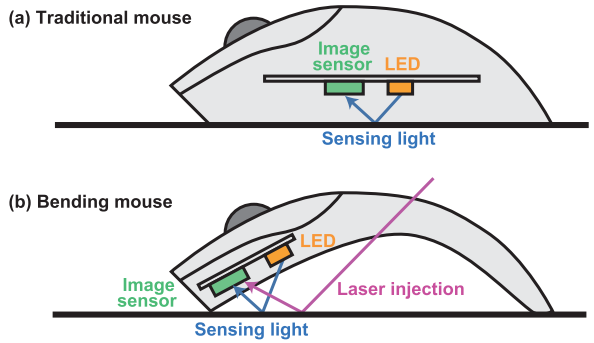


FIGURE 8. Functioning of traditional (top) and bending mouses (bottom).

TABLE 4. Details about the target bending mouses M_1 and M_2.

Identifier	Product Name	Light Source
M_1	Microsoft Surface Arc Mouse [24]	Blue
M_2	Lenovo ThinkPad X1 Presenter Mouse [20]	Infrared

A. TARGET MOUSES, ATTACK PRINCIPLE, AND SCENARIOS

Optical mouses use a pair of light emitters (LED or lasers) and an image sensor on the bottom to detect movement, as shown in Fig. 8. When the mouse is in operation, the image sensor continuously captures images of the bottom surface (e.g., a desk) illuminated by the light source. The image processing unit within the mouse compares the contiguous images to detect the direction and the amount of the mouse movement.

While traditional mouses have chassis that entirely covers the light source and image sensor (Fig. 8-(a)), modern ergonomic mouses come in various shapes and designs to provide a more comfortable and natural hand position while reducing strain and discomfort during prolonged computer use. For instance, widely available bending optical mouses [20], [23], [24], [32] follow the natural curvature of the hand to provide a relaxed grip and portability without sacrificing usability (see Fig. 1-(b)). These mouses have their light source and image sensors exposed, as shown in Fig. 1-(b). As for the keyboards, such mouses use similar functioning principles, thus our evaluation focuses on two representative bending mouse models described in Table 4.

As shown in Fig. 8-(b), bending optical mouses emits a beam of light, onto the surface below the mouse (e.g., a desk) within a certain angle to allow the capture by the image sensor. An attacker can leverage this knowledge to inject a laser beam into a specific spot on the desk surface with an intensity sufficient to overpower the legitimate light emitted by the mouse. If the attacker quickly changes the laser spot positions, the image processing unit in the mouse recognizes it as mouse movement, allowing the attacker to control the mouse cursor of the victim's PC. In this scenario, the attacker's control is limited to the mouse cursor, meaning the attacker cannot click the mouse buttons realized with mechanical switches. Despite this limitation, the attacker can use this methodology to pursue other attacks by preventing the victim computer from going into sleep mode.

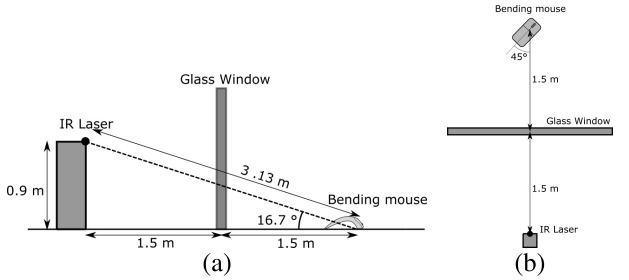


FIGURE 9. The setup of the 3 m bending mouse experiments. (a): the side view. (b): the top view where the laser injection angle is 45°.

For example, we consider a lunchtime attack where a malicious adversary temporarily gains access to a co-worker's workstation while the co-worker is away for lunch, as explored in previous works [11], [17]. A significant challenge for successfully executing a lunchtime attack is avoiding the computer system's automatic locking due to inactivity (e.g., a minimum of one minute in Windows 10). Companies often implement automatic screen lock features on workstations to provide an additional layer of security to protect sensitive information. When a user steps away from their workstation, the screen automatically locks, preventing unauthorized access to the system. If the attacker can keep the cursor moving by a laser injection, it prevents the victim's system from going to sleep mode after a timeout, which extends the time window for the lunchtime attack.

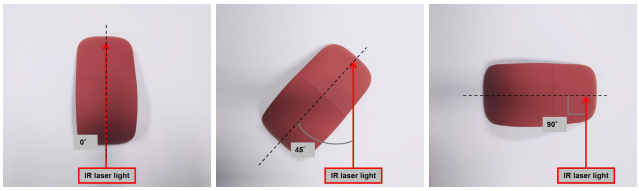
B. ATTACKER CAPABILITY: ANGLE ANALYSIS

We characterize the attacker capability by evaluating the ASR in terms of the relative position between the attacker and victim. Our evaluation consists of shooting a laser beam toward the target bending mouses from various angles (see Fig. 10) using the same setup used for the keyboard injection. We then define the maximum achievable distances to ensure the remote mouse control in Section V-C.

1) SETUP AND PROCEDURE

We use the same full setup of Section IV-B (Fig. 3) with a single IR laser scanned through the galvoscanner. Similar to the keyboard attack evaluation, the attacker setup and the targets are apart by 3 m through a glass window, as illustrated in Fig. 9. The target bending mouse models are M_1 and M_2 from different vendors, as summarized in Table 4. Both two models have the image sensor exposed, but different bending angles and shapes. M_1 and M_2 use blue and IR LEDs for light sources, respectively.

Our preliminary experiments show that the target mouses recognize a movement only when the laser spot moves over time, while they did not react to static and continuous laser illumination. Thus in our evaluation, to trigger the mouse event, we move a laser spot between two coordinates on the desk in the field of view of the mouse camera. We inject a laser underneath the target mouse and move the spot position by ∼1.8 cm over 1 second. Such injection generates a mouse cursor movement of 1–3 pixels.



(a) 0° (b) 45° (c) 90°

FIGURE 10. Laser injection toward the mouse's light sensor from different laser injection angles.

TABLE 5. Attack success rate (%) over 10 trials with seven angles, as shown in Figures 9 and 10. The laser injection angle is changed from 0° to 90° at 15° step.

Target	Laser Injection Angle						
	0°	15°	30°	45°	60°	75°	90°
Mouse M_1	0%	0%	48%	80%	0%	0%	0%
Mouse M_2	0%	0%	35%	57%	0%	0%	0%

We perform 100 trials and obtain the ASR for each mouse model at seven different laser injection angles in 0°–90° range with an increment of 15° from the mouse center, as shown in Fig. 10. We consider the attack successful if there is a difference in the mouse cursor position before and after the laser injection.

2) RESULTS AND OBSERVATIONS

Table 5 summarizes the ASR for each tested laser injection angle. Both M_1 and M_2 are activated by laser injection from 30° and 45°, and ASR is higher at 45°. We noticed that M_1 has sensitivity to IR despite the genuine light source being blue. This result suggests that the image sensor used by M_1 lacks a color filter which allows attackers to use different laser wavelengths to attack the input device.

Furthermore, we noticed that for both models, the ASR becomes greater than 35% once the attack succeeds for the first time, which is sufficient for preventing the system from going to sleep. A trial takes approximately 1 second, and the attacker can repeat the trials until the PC enters into sleep mode. For example, the attacker can execute 60 trials within 60 seconds, the minimum time period in Windows 10 to enter sleep mode. Note that a single success within the time slot is sufficient to keep the PC awake. The failure probability is thus $(1 - 0.35)^{60}$, which is extremely low.

C. ATTACKER CAPABILITY: DISTANCE ANALYSIS

We characterize the success rate at different distances between the bending mouse and attacker setup.

1) SETUP AND PROCEDURE

With the same setup used for the angle analysis, we first fix the laser injection angle to 45°, which is the optimal parameter found in the previous evaluation. The laser is injected through a glass window with the setup in Fig. 9. We increase the glass-mouse distance while keeping the laser-glass distance to 1.5 m. We then evaluate the ASR of M_1 and M_2 at three increasing distances (3, 5, and 7 m) and eight increasing laser power (2.00–0.25 mW with 0.25 mW step). For each distance and laser power, we evaluate the ASR for 100 trials.

TABLE 6. Attack success rate (%) over 100 trials with three distances (3, 5, and 7 m) and eight laser power (2.00–0.25 mW at 0.25 mW step) for the two mouse models M_1 and M_2.

Target	Laser Power	Distance		
	[mW]	3 m	5 m	7 m
Mouse M_1	2.00	80%	36%	37%
Mouse M_1	1.75	66%	25%	24%
Mouse M_1	1.50	75%	6%	32%
Mouse M_1	1.25	34%	4%	4%
Mouse M_1	1.00	2%	0%	0%
Mouse M_1	0.75	3%	0%	0%
Mouse M_1	0.50	0%	0%	0%
Mouse M_1	0.25	0%	0%	0%
Mouse M_2	2.00	57%	14%	11%
Mouse M_2	1.75	66%	16%	0%
Mouse M_2	1.50	54%	25%	0%
Mouse M_2	1.25	0%	0%	0%
Mouse M_2	1.00	0%	0%	0%
Mouse M_2	0.75	0%	0%	0%
Mouse M_2	0.50	0%	0%	0%
Mouse M_2	0.25	0%	0%	0%

2) RESULTS AND OBSERVATIONS

The laser injection successfully activates both M_1 and M_2 up to 7 meters away, as summarized in Table 6. As in the keyboard attack evaluation, the ASR depends on both laser power and distance. The laser power is the dominant factor, and the dropped ASR at longer distances can be compensated with increased laser power. This suggests that lower ASR at longer distances is mainly caused by the larger laser spot that reduces the peak power. As in the case of the keyboard attack, these results also suggest that longer-range attacks are possible with more precise aiming and a higher laser power.

VI. EVALUATION IN REALISTIC OFFICE ENVIRONMENTS

We verify the feasibility of our attack in a realistic office scenario when the victim and attacker devices are placed on working desks. We also evaluate the cases where a laser beam is occluded by a mesh chair.

A. SETUP

Fig. 11 shows the office environment where the victim and attacker's desks are separated by a glass window at 3 meter distance. The victim uses a regular office desk at 0.73 m in height. The attacker uses a standing desk at 1.06 m height to get a minimum angle of elevation to pursue the attack. We also evaluate the scenario where an office chair is located between the victim and the target. The mesh fabric on the chair is semitransparent as in typical office chairs (see Fig. 13). We use the same setup as in Section IV, except for the galvoscanner upgraded from a generic one [1] to Thorlabs

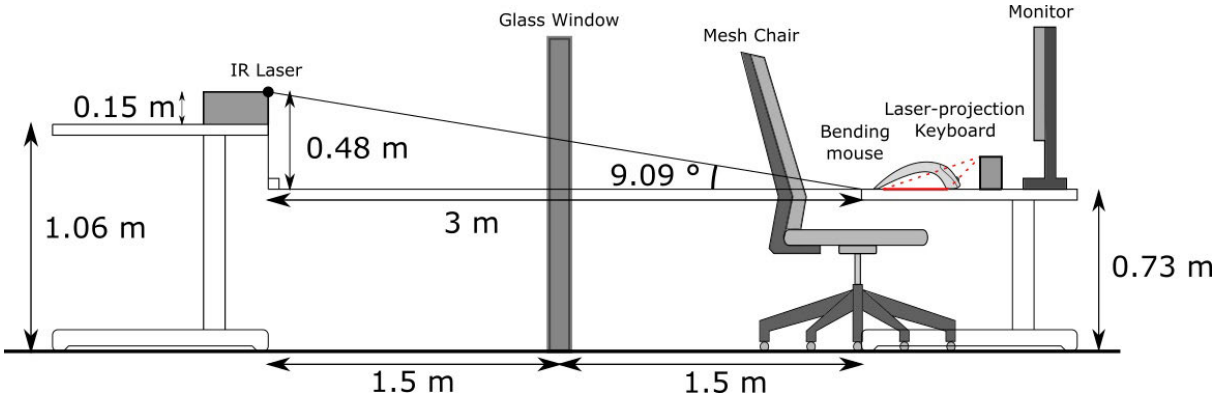


FIGURE 11. Setup for the office environment evaluation. The victim and attacker devices are placed on a regular and standing office desks 3 meters away from each other, across a window. We consider an office chair located between the glass window and the victim desk that partially occludes the injected laser beam.

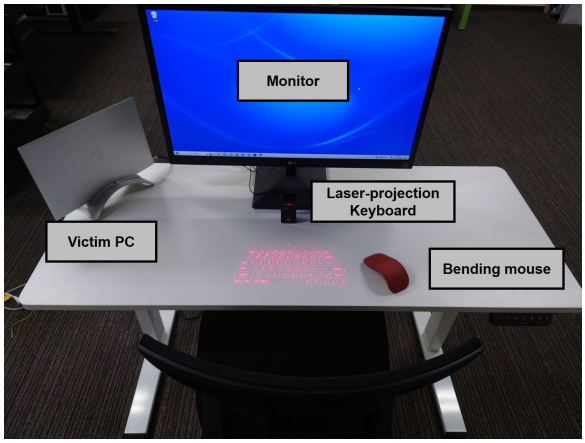


FIGURE 12. Victim's desktop. The victim PC is connected to the projection keyboard (K_2), the bending mouse (M_1), and a monitor.

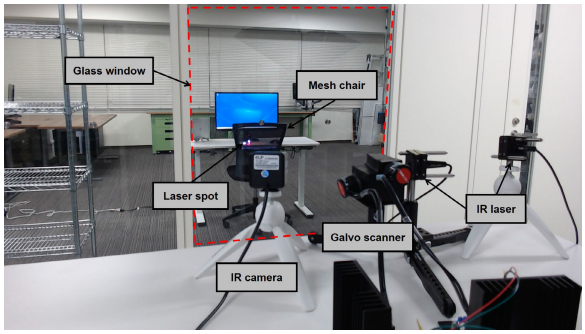


FIGURE 13. View from the attacker in the office environment scenario. The office chair between the victim and the attacker has a semitransparent mesh fabric. The laser spot is visible on the mesh because the scene is captured using an IR-sensitive camera.

GVS012 [42], which has a higher reflective index and can deliver a sufficient laser power over the mesh fabric.

B. PROCEDURE

To demonstrate the attack feasibility, we evaluate the more sensitive targets in the previous experiments, i.e., the keyboard K_2 and the mouse M_1. The keyboard and mouse evaluation follows the procedures described in Section IV-D and V, respectively. We examine increasing injection powers from 5 to 15 mW. We repeat the two sets of experiments with and without a mesh chair that occludes the laser beam. The ASR is evaluated with 10 and 100 trials with the keyboard and mouse injection, respectively.

TABLE 7. Attack Success Rate (ASR %) in our tested office environment scenario with different laser powers. The two sets of experiments are conducted with and without a mesh chair occluding the laser beam.

Target	Laser Power [mW]	w/o chair	w/ chair
Keyboard K_2	5	90%	0%
Keyboard K_2	10	0%†	50%
Keyboard K_2	15	0%†	60%
Mouse M_1	5	81%	0%
Mouse M_1	10	92%	78%
Mouse M_1	15	95%	84%

†ASR becomes low with too much laser power because it activates unwanted keys.

C. RESULTS

Table 7 summarizes the experimental results. First, we compare the cases without the office chair. The laser becomes more difficult to aim due to the sharper elevation angle (only 9.09° compared with 16.7° as shown in Figs. 5, 9, and 11). However, the keyboard injection achieves 90% ASR with 5 mW of power. The attack is unsuccessful at higher laser power (0% ASR with 10 and 15 mW) because nearby unwanted keys are simultaneously activated due to the aiming angle. This condition is nevertheless advantageous for the attacker as less laser power (equivalent to a laser pointer power used for slide presentations) is required to achieve successful consecutive key pressing without failure, despite the sharper elevation angle. On the other hand, the mouse injection reaches more than 80% ASR with all 5, 10, and 15 mW laser power tested.

The attack also succeeds in the presence of the office chair which attenuates and diffuses the laser beam. In the keyboard evaluation, the ASR drops from 90% to 0% at 5 mW power, but it achieves >50% ASR with higher laser power,

showing that the beam attenuation due to the mesh fabric can be compensated with higher laser power injection. The result is similar for the mouse evaluation: the ASR drops at 5mW but achieves up to 84% ASR with higher laser power.

VII. DISCUSSIONS

A. ANALYSIS AND OBSERVATIONS

1) ATTACK LIMITATIONS

In the majority of our tested cases, a stronger laser power is advantageous in improving the ASR and penetrating semitransparent obstacles. However, more power becomes disadvantageous in the case of a sharper elevation angle for aiming at the victim keyboards, since a strong laser can press unwanted keys. This shows that the attacker should choose the appropriate injection power based on the attack scenario.

Our evaluation also shows that a sufficient angle of elevation is necessary for a successful attack. We verified the minimum elevation angle as 9.09° in our realistic office environment scenario. To achieve the same angle of elevation in a long-distance attack, the attacker should perform the injection from a higher location.

Finally, although our keyboard attack can achieve 100% success rate at 5 m compared to previous work attacks, aiming and focusing becomes a bottleneck at longer distances. The large laser spot makes aiming more challenging, and the slight misalignment due to natural vibrations of the glass window also becomes critical at longer distances. One way to address this is to mount the setup on an anti-vibration base commonly used for optical experiments. The attacker can also approach the issue by reducing the laser spot size. The minimum aperture size determines the laser spot size by the diffraction limit, which is defined by the galvoscanner's mirrors (approximately 12 mm$\times$8 mm in the generic galvoscanner [1] and ϕ10 mm with GVS012 [42]) in our setup. This can be improved with larger mirrors [8] or by switching to motorized turrets.

2) ATTACKS WITH VISUAL FEEDBACK

Our end-to-end keyboard and mouse evaluation assumes the non-adaptive setting without any feedback from the victim computer monitor. This keyboard scenario cannot tolerate even a single failure in consecutive injections. With feedback from the victim computer instead (e.g., line of sight to the victim computer monitor, camera feedback), the ASR can substantially improve by adaptively correcting aiming errors.

We also observed that our laser-projection keyboard models might also have active trackpad capabilities. We empirically verified that we can control the mouse cursors and generate mouse clicks by remote laser injection on the keyboard. An attacker can further exploit this capability with the help of visual feedback.

3) ATTACK USING FLASH LIGHTS

We empirically verified that we can successfully inject fake inputs to both the mouses and keyboards also using a commercial IR flashlight (UniqueFire UF-1605), instead of a laser. Although the light emitted from flashlights quickly diverges, it is strong enough to activate input events from 10 meters away. Although the large spot size of the flashlight beam prohibits precise aiming at longer distances in the case of the keyboard attack, that is not a concern for the mouse attack scenario. In such a case, flashlights can be a better option for the attacker due to the easier aiming and high optical power which can reach several Watts [39].

B. DEFENSES

There are several approaches for preventing light-based injection attacks on HCIs. For instance, distinguishing genuine light from injected light is a promising approach. In particular, this is achievable by randomizing the IR emission pattern of the HCI device, as already deployed in some LiDARs [34].

An alternative methodology consists of leveraging a secondary sensor to check the user presence. For example, a proximity sensor to detect the user can prevent the attacks. Some commercial keyboards already deploy such sensors [13] which can be used also for attack prevention. Capacitive touch sensors already present in some mouses can also be used to check if the user is physically interacting with the keyboard or the mouse.

Another defense measure consists of restricting critical operations to non-optical input methods to limit the attacker's capability. In the case of a keyboard attack, for example, reducing the volume of the audio feedback is important for improving the attack stealthiness (as discussed in Section IV-D). Manufacturers can limit such control using dedicated hardware keys or a specific configuration software running on the computer system.

Finally, our attacks succeed if the victim computer system is left unlocked when the user is not present. User-awareness training is an effective administrative countermeasure that can be adopted to limit user bad practices.

VIII. RESPONSIBLE DISCLOSURE AND LASER SAFETY

We disclose the vulnerability to the tested laser-projection keyboard vendors (Celluon and ELECOM) and the mouse vendors (Microsoft and Lenovo). Unfortunately, Celluon was unreachable via either an email or web form. ELECOM did not schedule an update because the target product is after EOL. Lenovo did not update the design of the products considering the difficulty of eliminating interference and the low perceived risk level by their customers. Microsoft has no comments. Such responses show that addressing light injection attacks in HCIs remains an unsolved problem. With our work, we aim to raise awareness of such security risks and help manufacturers develop attack-resiliant HCI technology.

For laser safety, all experiments were conducted in an indoor controlled environment with appropriate laser safety measures.

IX. CONCLUSION

This paper studies the susceptibility of optical HCI devices, i.e., laser projection keyboards and bending mouses, to laser-based signal injection attacks. With our methodology, we successfully achieved 100% success rate attacking laser projection keyboards. We demonstrate how an attacker can inject several commands without failure up to 5 meters away from the victim keyboard and through a glass window using a laser or a flashlight beam invisible to human eyes.

With the bending mouses, on the other hand, an attacker can induce cursor-movement events up to 7 meters away which can prevent the victim computer system from going to sleep mode. Our goal in this work is to raise awareness of these potential threats and suggest effective countermeasures to secure optical HCI devices.

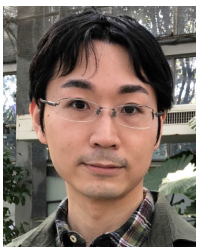
REFERENCES

[1] *20kpps Galvo Galvanometer Based Optical Scanner*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.amazon.com/dp/B01IZPMUPO
[2] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 3–11.
[3] B. Baxley. *Mousejack*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.mousejack.com/
[4] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: Physical removal attacks on LiDAR-based autonomous vehicles driving frameworks," in *Proc. USENIX Security*, 2023, pp. 2993–3010.
[5] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2267–2281.
[6] S. Cecconello, A. Compagno, M. Conti, D. Lain, and G. Tsudik, "Skype & type: Keyboard eavesdropping in voice-over-IP," *ACM Trans. Privacy Secur.*, vol. 22, no. 4, pp. 1–34, Nov. 2019.
[7] Celluon. *Epic*. Accessed: Jun. 26, 2023. [Online]. Available: https://celluon.com/epic/
[8] CITIZEN. *GM6*. Accessed: Jun. 15, 2024. [Online]. Available: https://ccj.citizen.co.jp/en/pdf/galvano_pdf.pdf
[9] R. Dumitru, D. Genkin, A. Wabnitz, and Y. Yarom, "The impostor among US (B): Off-path injection attacks on USB communications," in *Proc. USENIX Secur. Symp.*, 2023, pp. 5863–5880.
[10] J.-M. Dutertre, J. J. A. Fournier, A.-P. Mirbaha, D. Naccache, J.-B. Rigaud, B. Robisson, and A. Tria, "Review of fault injection mechanisms and consequences on countermeasures design," in *Proc. 6th Int. Conf. Design Technol. Integr. Syst. Nanosc. Era (DTIS)*, Apr. 2011, pp. 1–6.
[11] S. Eberz, K. Rasmussen, V. Lenders, and I. Martinovic, "Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics," in *Proc. NDSS*, 2015, pp. 1–13.
[12] ELECOM. *TK-PBL042BK*. Accessed: Jun. 15, 2024. [Online]. Available: https://www2.elecom.co.jp/peripheral/full-keyboard/tk-pbl042/
[13] EVGA. *Z20 Keyboard*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.evga.com/products/pdf/811-W1-20US-KR.pdf
[14] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, "A threat for tablet PCs in public space: Remote visualization of screen images using EM emanation," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 954–965.
[15] *Japanese Industrial Standards Committee*, Standard JIS Z9110, 2011.
[16] D. Karaklajic, J.-M. Schmidt, and I. Verbauwhede, "Hardware designer's guide to fault attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 12, pp. 2295–2306, Dec. 2013.
[17] P. Kasprowski and K. Harezlak, "Protecting from lunchtime attack using an uncalibrated eye tracker signal," in *Proc. ACM Symp. Eye Tracking Res. Appl.*, Jun. 2020, p. 6.
[18] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 145–159.
[19] K. Lee and K. Yim, "Vulnerability analysis and security assessment of secure keyboard software to prevent PS/2 interface keyboard sniffing," *Sensors*, vol. 23, no. 7, p. 3501, Mar. 2023.
[20] *Lenovo: ThinkPad X1 Presenter Mouse—Overview and Service Parts—Lenovo Support US*. Accessed: Jun. 15, 2024. [Online]. Available: https://support.lenovo.com/us/en/accessories/acc500115-thinkpad-x1-presenter-mouse-overview-and-service-parts
[21] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 620–637.
[22] J. Maskiewicz, B. Ellis, J. Mouradian, and H. Shacham, "Mouse Trap: Exploiting firmware updates in USB peripherals," in *Proc. 8th USENIX Workshop Offensive Technol.*, 2014, pp. 1–10.
[23] *Microsoft: Microsoft Arc Touch Wireless Mouse | Microsoft Accessories*. Accessed: Jan. 20, 2023. [Online]. Available: https://www.microsoft.com/en-my/accessories/products/mice/arc-touch-mouse?activetab=pivot:techspecstab#tab123079465-5695-4098-aebd-651cef584895
[24] *Microsoft: Microsoft Surface Arc Mouse (Light Gray, Bluetooth, Touch)—Microsoft Store*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.microsoft./en-us/d/surface-arc-mouse/8p5sv2rx3rn5?activetab=pivot:techspecstab#tab1f4a28f0b-1aff-4962-9f9a-6b96fc91078a
[25] S. Nashimoto, D. Suzuki, T. Sugawara, and K. Sakiyama, "Sensor CONfusion: Defeating Kalman filter in signal injection attack," in *Proc. Asia Conf. Comput. Commun. Secur.*, May 2018, pp. 511–524.
[26] K. Nohl, S. Krißle, and J. Lell. *BadUSB—On Accessories That Turn Evil*. Accessed: Jun. 15, 2024. [Online]. Available: https://assets-global.website-files.com/6098eeb4f4b0288367fbb639/62bc77c194c4e0fe8fc5e4b5_SRLabs-BadUSB-BlackHat-v1.pdf
[27] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This ain't your dose: Sensor spoofing attack on medical infusion pump," in *Proc. USENIX Workshop Offensive Technol.*, 2016, pp. 1–11.
[28] A. Petersmith. *Keyboard vs. Mouse vs. Touchscreen: Which Input Device Reigns Supreme?* Accessed: Jun. 15, 2024. [Online]. Available: https://www.vendr.com/blog/do-you-prefer-using-the-mouse-touchscreens-or-keyboard-shortcuts
[29] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," *Black Hat Eur.*, vol. 11, p. 995, Nov. 2015.
[30] A. D. Ramadhanty, A. Budiono, and A. Almaarif, "Implementation and analysis of keyboard injection attack using USB devices in windows operating system," in *Proc. 3rd Int. Conf. Comput. Informat. Eng. (ICIE)*, Sep. 2020, pp. 449–454.
[31] *Rohm Semiconductor: 850 nm Invisible Single Mode Laser Diode RLD85PZJ4*. Accessed: Jun. 15, 2024. [Online]. Available: https://fscdn.rohm.com/en/products/databook/datasheet/opto/laser_diode/infrared/rld85pzj400a007-e.pdf
[32] *Sanwa Supply: MA-BTIR116BKN*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.sanwa.co.jp/product/syohin?code=MA-BTIR116BKN
[33] T. Sato, S. H. V. Bhupathiraju, M. Clifford, T. Sugawara, Q. A. Chen, and S. Rampazzi, "WIP: Infrared laser reflection attack against traffic sign recognition systems," in *Proc. Inaugural Int. Symp. Vehicle Secur. Privacy*, 2023, pp. 1–5.
[34] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, "Revisiting LiDAR spoofing attack capabilities against object detection: Improvements, measurement, and new attack," 2023, *arXiv:2303.10555*.
[35] (2021). *Serafim: Serafim Keybo*. [Online]. Available: https://serafim-tech.com/wp-content/uploads/2021/08/serafim_keybo_user_manual_eng_20170712.pdf
[36] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against LiDARs for automotive applications," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 10529. Berlin, Germany: Springer, 2017, pp. 445–467.
[37] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. 24th USENIX Secur. Symp.*, 2015, pp. 881–896.
[38] Y. Su, D. Genkin, D. Ranasinghe, and Y. Yarom, "USB snooping made easy: Crosstalk leakage attacks on USB hubs," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1145–1161.
[39] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: Laser-based audio injection attacks on voice-controllable systems," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 2631–2648.

[40] T. Tanaka and T. Sugawara, "Laser-based signal-injection attack on piezoresistive MEMS pressure sensors," in *Proc. IEEE Sensors*, Oct. 2022, pp. 1–4.
[41] Z. Thomas. *After 50 Years of the Computer Mouse, What Does the Future Hold?* Accessed: Jun. 15, 2024. [Online]. Available: https://www.posturite.co.uk/blog/50-years-computer-mouse-future-hold
[42] *Thorlabs: Thorlabs Gvs012*. Accessed: Jun. 15, 2024. [Online]. Available: https://www.thorlabs.co.jp/drawings/4101d9ed94711bca-07B3A168-C548-B4C3-9DC8C4DBB086DA4B/GVS012_M-Manual.pdf
[43] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy*, Apr. 2017, pp. 3–18.
[44] Y. Tu, L. Shan, M. I. Hossen, S. Rampazzi, K. Butler, and X. Hei, "Auditory eyesight: Demystifying μs-precision keystroke tracking attacks on unconstrained keyboard inputs," in *Proc. 32nd USENIX Secur. Symp.*, 2023, pp. 175–192.
[45] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," in *Proc. USENIX Secur. Symp.*, 2009, pp. 1–16.
[46] K. Wang, R. Mitev, C. Yan, X. Ji, A. R. Sadeghi, and W. Xu, "GhostTouch: Targeted attacks on touchscreens without physical touch," in *Proc. USENIX Secur.*, 2022, pp. 1543–1559.
[47] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, "I can see the light: Attacks on autonomous vehicles using invisible lights," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2021, pp. 1930–1944.
[48] W. Wodo and L. Hanzlik, "Thermal imaging attacks on keypad security systems," in *Proc. 13th Int. Joint Conf. E-Business Telecommun.*, Lisbon, Portugal, 2016, pp. 458–464.
[49] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "DolphinAttack: Inaudible voice commands," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 103–117.

TATSUKI TANAKA received the bachelor's degree in engineering from The University of Electro-Communications, in 2022, where he is currently pursuing the master's degree with the Graduate School of Informatics and Engineering. He is studying laser-based signal injection attacks on sensors.

SARA RAMPAZZI (Member, IEEE) has been an Assistant Professor with the University of Florida, since 2021. She has made several key contributions to cyber-physical systems security, including transportation, the IoT, and healthcare systems. She leads the Cyber-Physical System Security Laboratory (CSPSec Lab), which investigates hardware vulnerabilities and defensive designs against threats to the physics of hardware and sensing, AI model security, and human factors. More details can be found at sararampazzi.com.



TAKESHI SUGAWARA (Member, IEEE) received the Ph.D. degree from Tohoku University, Sendai, in 2011. In 2011, he joined Mitsubishi Electric Corporation, involved in research and development of embedded systems security. He has been an Associate Professor with The University of Electro-Communications, Tokyo, since 2017. His research interests include hardware and embedded systems security, lightweight cryptography, and side-channel attack.