

# Technical Disclosure Commons

---

Defensive Publications Series

---

May 06, 2019

## Protecting against unintended inputs

Emmanuel Arriaga

Follow this and additional works at: [https://www.tdcommons.org/dpubs\\_series](https://www.tdcommons.org/dpubs_series)

---

### Recommended Citation

Arriaga, Emmanuel, "Protecting against unintended inputs", Technical Disclosure Commons, (May 06, 2019)  
[https://www.tdcommons.org/dpubs\\_series/2176](https://www.tdcommons.org/dpubs_series/2176)



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

## **Protecting against unintended inputs**

### **ABSTRACT**

Anomalous inputs to a computing device can occur in certain situations, e.g., when a pet walks across a keyboard, a baby slams their hand on keyboard or touches a trackpad, etc. For users that frequently experience this situation, e.g., parents of young kids, pet owners, etc., such input can result in having to take extra steps to undo the input. This disclosure describes techniques to automatically detect and ignore anomalous inputs to a device. When an anomalous input is detected, the received input is ignored and a temporary delay is enforced. Inputs received within the delay period are also ignored. Detection of anomalous inputs can be performed using machine learning techniques.

### **KEYWORDS**

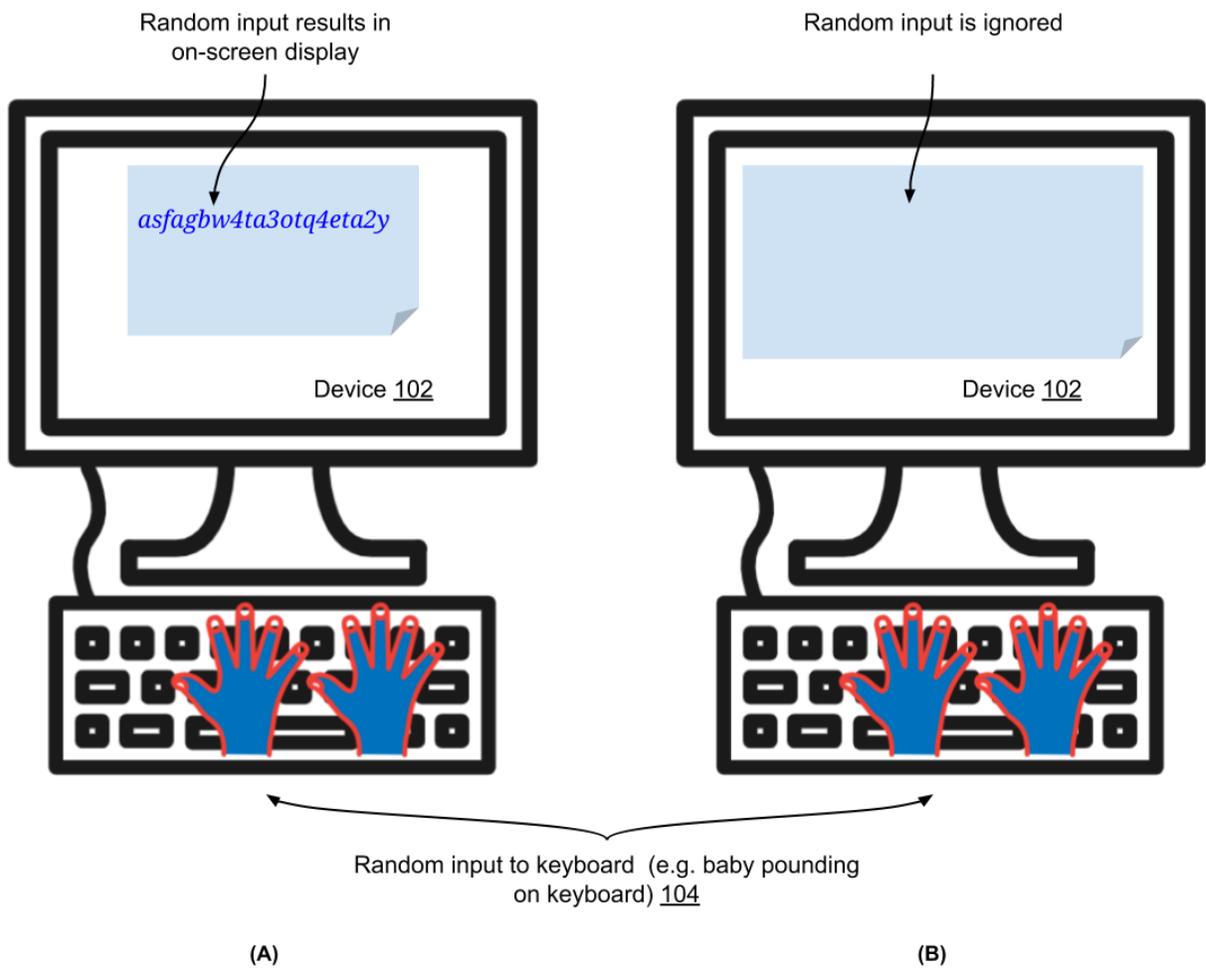
- Keyboard
- Trackpad
- Touchscreen
- Input device
- anomalous input
- Unintended input

### **BACKGROUND**

Anomalous inputs to a computing device can occur in certain situations, e.g., when a pet walks across a keyboard, a baby slams their hand on keyboard or touches a trackpad, etc. For users that frequently experience this situation, e.g., parents of young kids, pet owners, etc., such input can result in having to take extra steps to undo the input. For example, if such input occurs

when the user is composing a document, the user needs to use the undo command (possibly multiple times) to recover to a previous state of the document. In another example, if such input occurs when viewing a website or video, the user needs to take action to navigate back to the correct section of the website or video.

### DESCRIPTION



**Fig. 1: Protecting against unintended inputs**

Fig. 1(A) illustrates a device (102) that receives random input (104). For example, if the input is received while a word processing application is active, such input results in

corresponding characters being inserted into the document, e.g., “asfagbw4ta3otq4eta2y” as illustrated in Fig. 1(A).

Fig. 1(B) illustrates a device (102) that implements the techniques of this disclosure. Anomalous input (104) is detected and a delay is enforced during which inputs received from the input device, e.g., keyboard, touchpad, etc. are ignored. For example, the delay can be a short duration such as a few milliseconds to a second, corresponding to the time period during which anomalous inputs are received. The delay can be extended based on the context, e.g., if a pattern of anomalous inputs is detected, the delay can be extended to a few seconds. Thus, the document being edited does not show text corresponding to the input.

Machine learning techniques can be utilized to detect whether the input received from an input device such as a keyboard, trackpad, touchscreen, etc. is anomalous, e.g., caused by a baby pounding on the keyboard, a cat walking across the keyboard, etc. The techniques can be implemented in software or at the firmware level of the device. Firmware level implementation of anomalous input detection and delay enforcement can increase the responsiveness, since such inputs are ignored even before the inputs are processed by the operating system of the device. The detection techniques can be updated over time, e.g., with improved algorithms, to improve accuracy and responsiveness. While Fig. 1 shows inputs received via a keyboard, input received from other input devices such as a trackpad, mouse, gesture interface, gaming controller, etc. can be analyzed similarly to detect and mitigate anomalous input.

The techniques can be utilized in devices such as laptops, tablets, convertible devices, etc. Devices that implement the techniques can be especially helpful to users that work from home, with kids and/or pets around.

## CONCLUSION

This disclosure describes techniques to automatically detect and ignore anomalous inputs to a device. When an anomalous input is detected, the received input is ignored and a temporary delay is enforced. Inputs received within the delay period are also ignored. Detection of anomalous inputs can be performed using machine learning techniques.