NoisyKey: Tolerating Keyloggers via Keystrokes Hiding

Stefano Ortolani[1] **Bruno Crispo**[2]

August 7th, 2012
Bellevue, WA, USA

[1]Vrije Universiteit, Amsterdam, The Netherlands
[2]University of Trento, Trento, Italy

Yet Another Talk about Keyloggers

Keyloggers

- Provoke critical damage (steal user data).
- Pervasive (included in malware, worms, etc).
- Standard countermeasures: **detection** and **prevention**.

If only it was possible. . .

- Prevention may **not** be feasible (system dependent).
- Detection, instead, **works** on top of an existing system.
- Detection does not **aid** removal.

Stay foolish they said...

Provocative brainwashing

- Detection is not what we want.
- Prevention is not feasible.
- Assume the keylogger is just there.
- Assume we have to live with it.

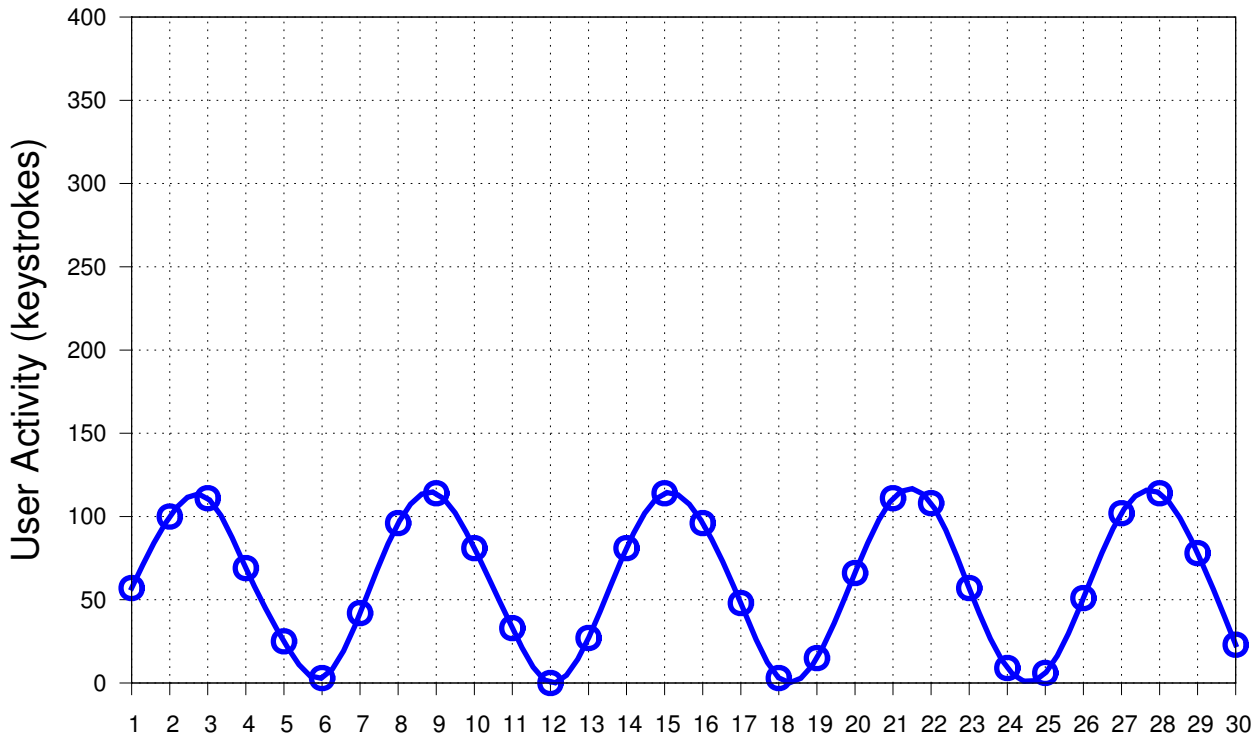
Living with a Keylogger

- Purportedly having a keylogger stealing keystrokes?
- How is that tolerating?

It will be fun they said...

How-to Tolerate (1/3)

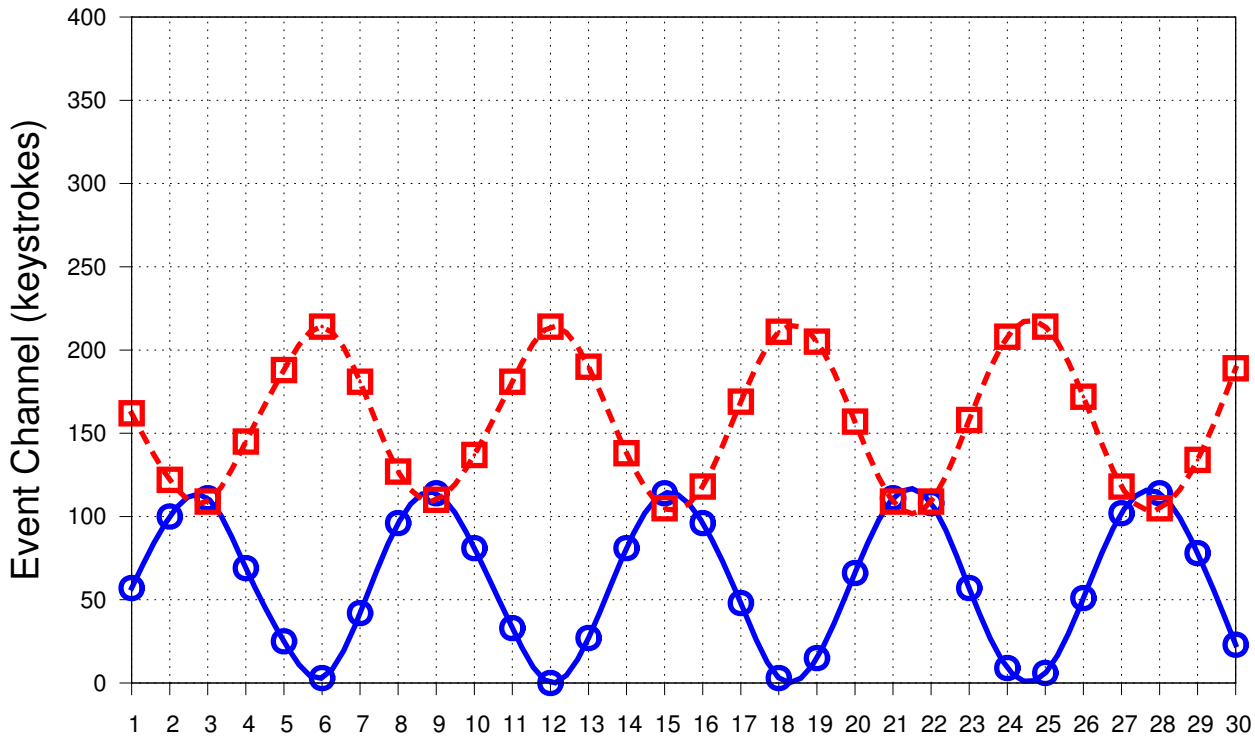
- The keylogger intercepts all the user keystrokes.
- Below an example of some keystroke activity.



The Main Idea

How-to Tolerate (2/3)

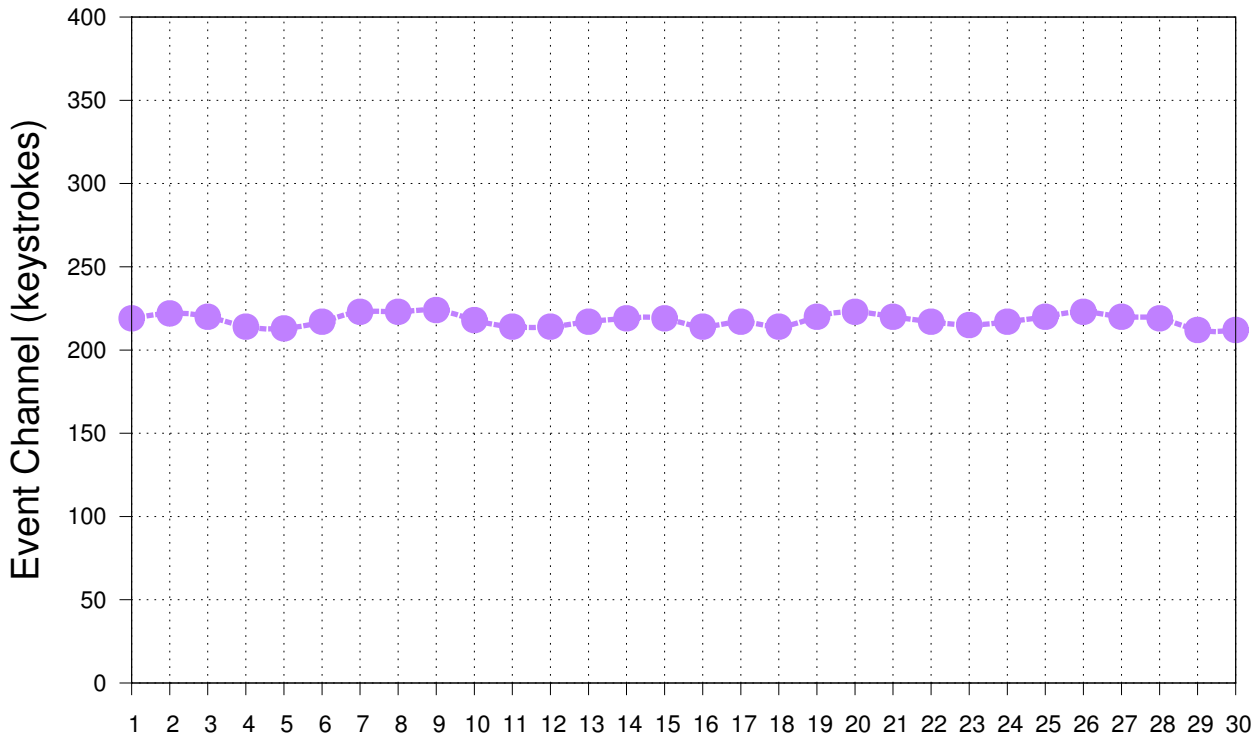
- The idea is to generate (and exfiltrate) bogus keystrokes.
- The keylogger sees two intermixed keystroke activities.



The Main Idea

How-to Tolerate (3/3)

- Result: "haystack" where the real keystrokes are safe-guarded.
- No information disclosed! (if done properly)



Challenges

Scientific Challenges

- What is **noise**? How the noise shall be modeled?
- User activity is not predictable. Several attacks possible.

Technical Challenges

- How shall the noise be generated and exfiltrated?
- In a compatible, robust, and efficient manner?

Addressing the Problem

Measurements defining keystroke dynamics

- Flight time: time between keystrokes.
- Dwell time: time a key pressed.
- **EXTRA** Scancode: the symbol which the key corresponds to.

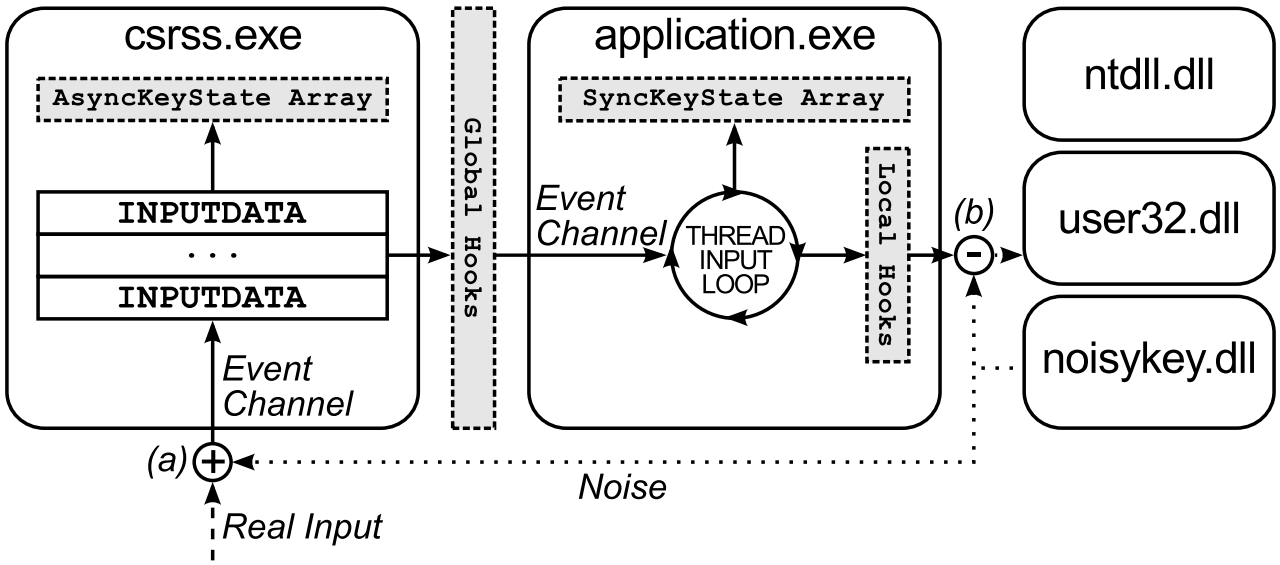
Our approach: NoisyKey

- We force the system to expose pre-set keystroke dynamics.
- Bogus keystrokes are adaptively generated.
- Example (flight time):
  - If no user input $\Rightarrow$ noise generations goes full throttle.
  - Lots of user input $\Rightarrow$ less bogus keystrokes.

Technical Challenges

Exfiltrating real keystrokes

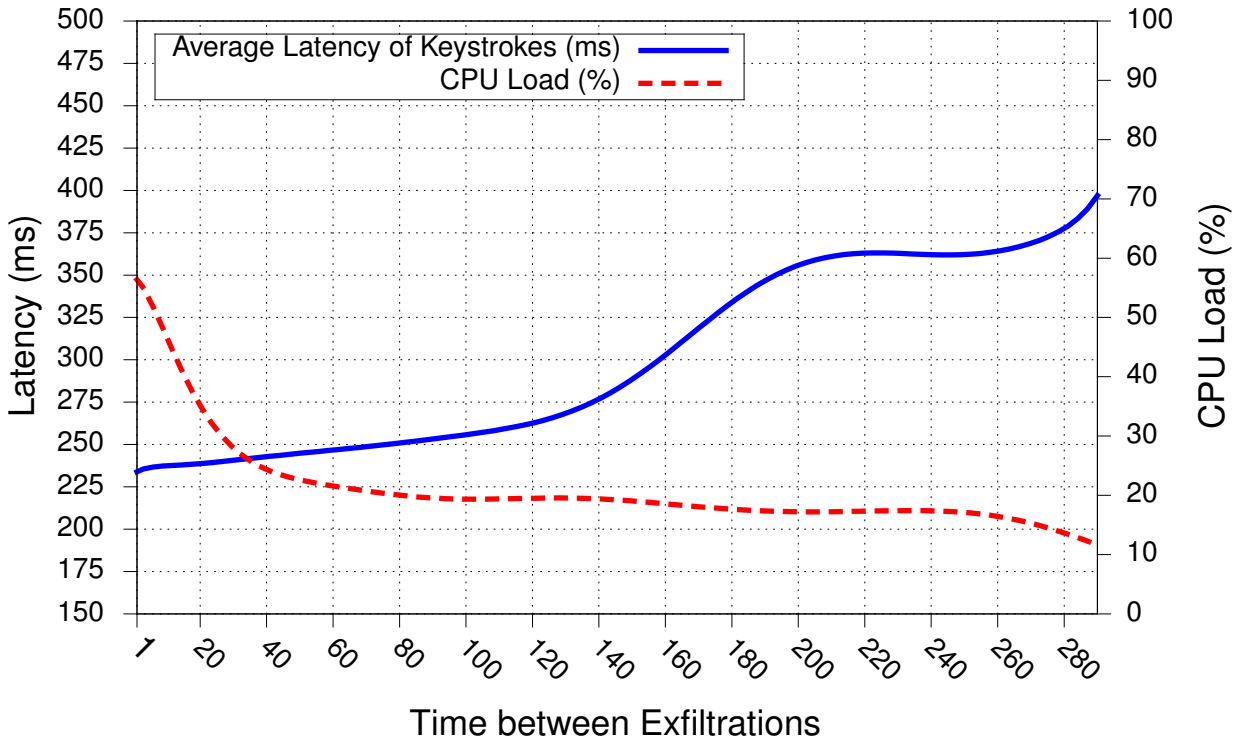
- Keyloggers sniff the event channel used to delivery keystrokes.
- We exfiltrate the keystrokes outside the event channel.



Performance Evaluation

A sliding-window approach exfiltrates the real keystrokes

- The **smaller** the sliding window, the **lower** the latency.
- The **bigger** the sliding window, the **lower** the CPU usage.



Conclusions

Full paper menu (check it out!)

- Correctness and performance evaluation.
- A novel privacy model for keystroke dynamics.
- Comprehensive evaluation against 51 test subjects.