What I need to worry about

Discover through Literature Survey
- AND, XOR, ADD, SUBTRACT – least inexpensive computation?
- Attack vectors
- Keylogger on Linux server

Speed of typing not hampered
Unauthorized access to key
Screenshots
My encryption occurs after keycode is generated. Can attacker access keyboard state at an earlier stage?
Keylogger decrypted text from window itself
Keylogger attaching itself to main window
People that use linux as servers, ssh to it. Host-side windowing system does not come into picture
Clipboard contents? Data in copy/paste?
How to work with modifier keys?

Literature Survey

Research paper	Methodology	Assumptions	Shortcomings	Checked?
Treat, D. G. (2002). Keyboard encryption. *IEEE Potentials*, *21*(3), 40-42.	Lists out the ways of encrypting communication between keyboard microcontroller and BIOS chip including stream cipher (PRNG XOR Keystroke)		No implementation, just idea presentation Does not talk about encrypting to hide from Software/OS level keyloggers	Y
Olzak, T. (2008). Keystroke logging (keylogging). *Adventures in Security*, *8*, 1-6.	Keylogging applications use hooking mechanism. It is packages as executable or DLL. Kernel-based (installed as rootkit, difficult to detect) keyloggers replace keyboard device drivers that interprets keystrokes. A hardware keylogger is a circuit located between the keyboard and the computer is invisible to anti-malware software.			Y
Croock, M. S. (2022). Keyboard Encryption Algorithm Based on Software Engineering Security. *International Journal of Computing and Digital Systems*, *11*(1), 1309-1317.	Focuses more on the proposed algorithm. ie. Random interleaving on bits of ASCII code, and XOR with itself using right circular shift. The same steps were adopted in the decryption process, in		Does not discuss where the keylogger fails because of this encryption. Does not implement it in real	Y

	which the same initial ASCII code is returned back. Is lightweight, computationally inexpensive and boasts speedy encryption/decryption time			
Ali, T. O., Awadelseed, O. S., & Eldewahi, A. E. (2016, February). Random multiple layouts: Keylogger prevention technique. In *2016 Conference of Basic Sciences and Engineering Studies (SGCAC)* (pp. 1-5). IEEE.	Prevents kernel, and user level keylogger. Using MSKLC, meaningless symbols have been assigned to each single key on the keyboard, except the control keys. The layouts are shuffled. When a user types, keylogger will see meaningless symbols wheras actual application window will get true characters		Does not talk about how decryption is taking place Does not mention cryptographic strength of the algorithm. Scancodes and keycodes vulnerable ie. does not cover keyboard drivers. Additional power required in creating layouts?	
David Cardoso, "ENCRYPTED KEYBOARD," U.S. Patent 20070143593, June 21, 2007.	Encrypts keycode, stores cipher key somewhere, sends it through secure channel, decrypts cipher before sending it to application.		No analysis of attack vectors prevented No implementation No technical depth No explanation of computation time Rolling key function. Perhaps key has to be successively generated? No certain encryption algo used. Just mentioned x can be used.	Y

Existing Products

1. Zemana AntiLogger
   No in depth detail of how it works.
   - Protects every application on your computer, and not just your web browser
   - Stops keyloggers by scrambling every key that you type instantly, quietly, effective, in the background

2. GuardedID - Currently available only for internet explorer browser, and it does not work with pop-up boxes that do not contain HTML forms
   Prevents browser from intercepting keystrokes

3. KeyScrambler
   https://www.techrepublic.com/article/keyscrambler-how-keystroke-encryption-works-to-thwart-keylogging-threats/

Does everything my idea is supposed to do but in windows

- Takes analogy of SSL/TSL.
- Intercepts keystrokes at lowest level possible
- Encrypts it into a different character
- Sends it to active application window
- Decrypts right before application window receives it
- Encrypts your Windows Logons

Methodology

- Implements both standard symmetric-key encryption (Blowfish 128-bit) and asymmetric-key encryption (RSA 1024-bit) for strong protection.
- Encryption happens in low level kernel driver
- Decryption only occurs inside protected applications

Shortcomings discovered -

- Does not prevent keyloggers from reading HTML forms
- No screenlogger defense
- Supposed to work with 70+ and all major apps (about 400+) ie. it is not general enough to work with all apps
  Encrypts only predefined list of applications
- For Windows

4. SpyShelter Anti-Keylogger

Methodology

- Encrypts keystrokes of all applications, regardless of the operating system language.
- Every Keystroke is encrypted on Windows Kernel level and sent via safe tunnel only to this application, on which your keyboard is focused.
- It locks out other applications from capturing those encrypted keystrokes. Once encrypted keystrokes reach the target window, they are being decrypted.
- No noticable input lag.
- Also stops suspicious applications from taking screenshots

Shortcomings

- For Windows

5. NextGen AntiKeylogger

Methodology

- Intercepts keystrokes at the lowest possible level
- Encrypts them and sends via its own protected path directly into the protected application.

Shortcomings

- Encrypts only predefined list of applications
- For Windows

Irrelevant Papers

Research paper	Methodology	Assumptions	Shortcomings
Rai, S., Choubey, V., & Garg, P. (2022, July). A Systematic Review of Encryption and Keylogging for Computer System Security. In *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 157-163). IEEE.	A simple survey on keylogger and encryption as individual components.		
Whiskerd, N., Körtge, N., Jürgens, K., Lamshöft, K., Ezennaya-Gomez, S., Vielhauer, C., ... & Hildebrandt, M. (2020). Keystroke biometrics in the encrypted domain: a first study on search suggestion functions of web search engines. *EURASIP Journal on Information Security*, *2020*(1), 1-16.	Interesting but unrelated to area of research. Privacy problems on Search Suggestion Functions		
Newlin, M. (2016). MouseJack, KeySniffer and Beyond: Keystroke Sniffing and Injection Vulnerabilities in 2.4 GHz Wireless Mice and Keyboards. *DEFCON*.	A survey on vendor side wireless peripheral vulnerabilities		
Srivastava, M., Kumari, A., Dwivedi, K. K., Jain, S., & Saxena, V. (2021, October). Analysis and Implementation of Novel Keylogger Technique. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.	Simply does white space encoding of log file. Keylogger Categories • Software-based • Hypervisor-based • Kernel-based • Memory Injection based: substitute memory tables linked with application functions. Place memory tables or push it directly in the memory eg. Trojans like Zeus, SpyEye Traditional keyloggers store only the keystrokes. Newer keyloggers also captures the running application, mac address, ip address etc.		
Norman, K. R. (2006). *Encryption of Computer Peripheral Devices*. Brigham Young University.	Inaccessible		