

VMM-based Approach to Detecting Stealthy Keyloggers

Kenji KONO
Keio Univ.

- Keyloggers are a real threat to security
 - Malicious software that steals keystrokes
 - ◆ A kind of spyware; spreading out private information
 - ◆ Stores keystrokes on disk or send them out to the Internet
 - ◆ May steal sensitive information such as passwords and credit card numbers
 - ◆ Potential to cause serious security incidents
 - Hide their presence from the users
 - ◆ Very stealthy
 - ◆ Often exists in the OS layer
 - ◆ User- or OS-level defense against keyloggers are useless

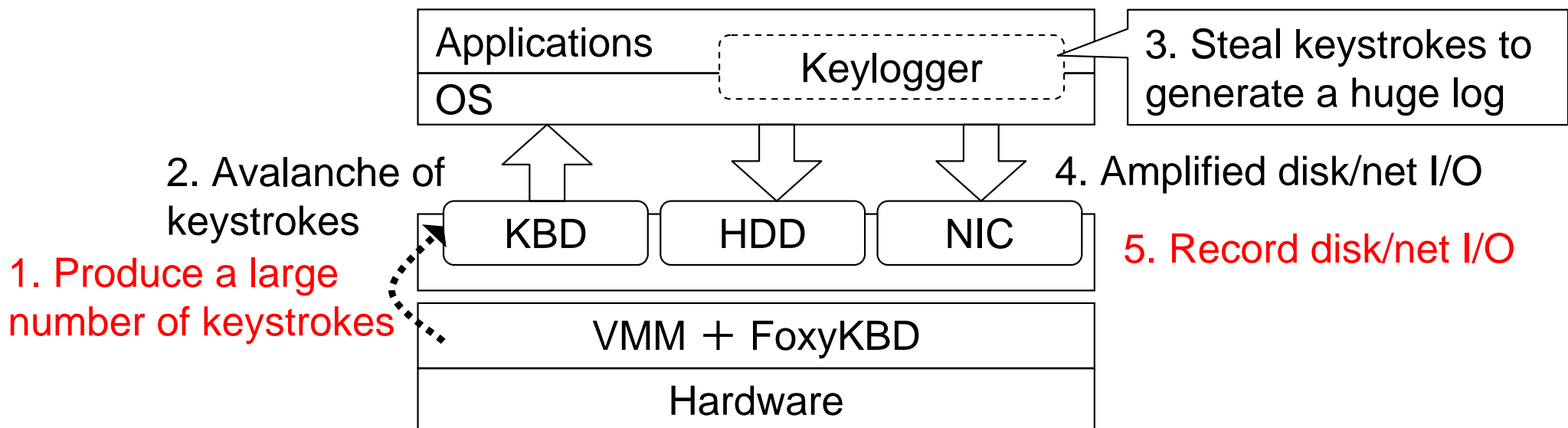
- Signature-based detection
 - Searches for binary image matching with signatures
 - ◆ Signature is a byte sequence that characterizes keyloggers
 - ◆ Signatures are crafted from existing sample keyloggers
 - ◆ Same methodology as viruses checkers
 - Shortcomings of signature-based detection
 - ◆ Can't detect unknown keyloggers
 - It's very easy to produce a variant of existing keyloggers that evades signature-based detection
 - ◆ Easy to evade signature-based detection
 - Obfuscation
 - Rootkits

Our Technique: FoxyKBD



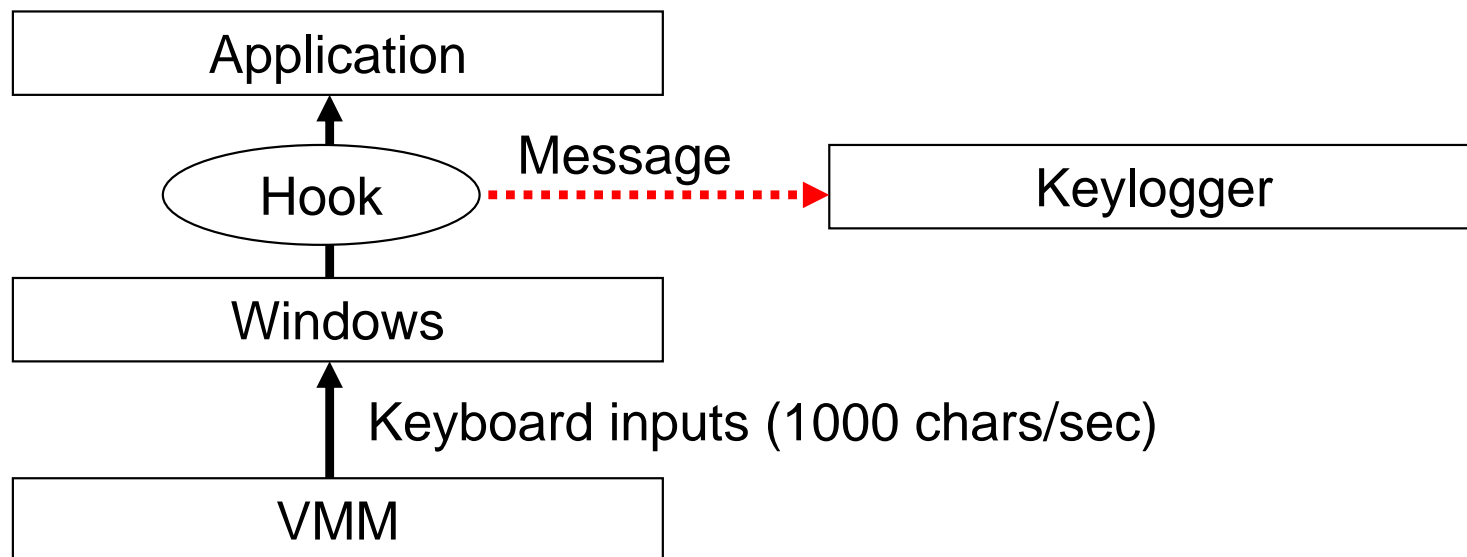
- VMM-based technique to detect keyloggers
 - Detects behaviors specific to keyloggers
 - ◆ No signatures
 - ◆ Can detect unknown keyloggers
 - Hinders hiding keyloggers
 - ◆ Can't evade FoxyKBD even if the guest OS is hijacked
 - ◆ This is because FoxyKBD runs in the VMM layer

- Amplifies the behavior of keyloggers by producing a huge number of keystrokes
 - Runs in the VMM layer
 - Generates a large number of KBD interrupts
 - Analyze the behavior of virtual disk/net I/O devices
 - ◆ Keyloggers, if installed, output a huge log on virtual devices
 - ◆ FoxyKBD judges keyloggers are installed if the output is dramatically increased



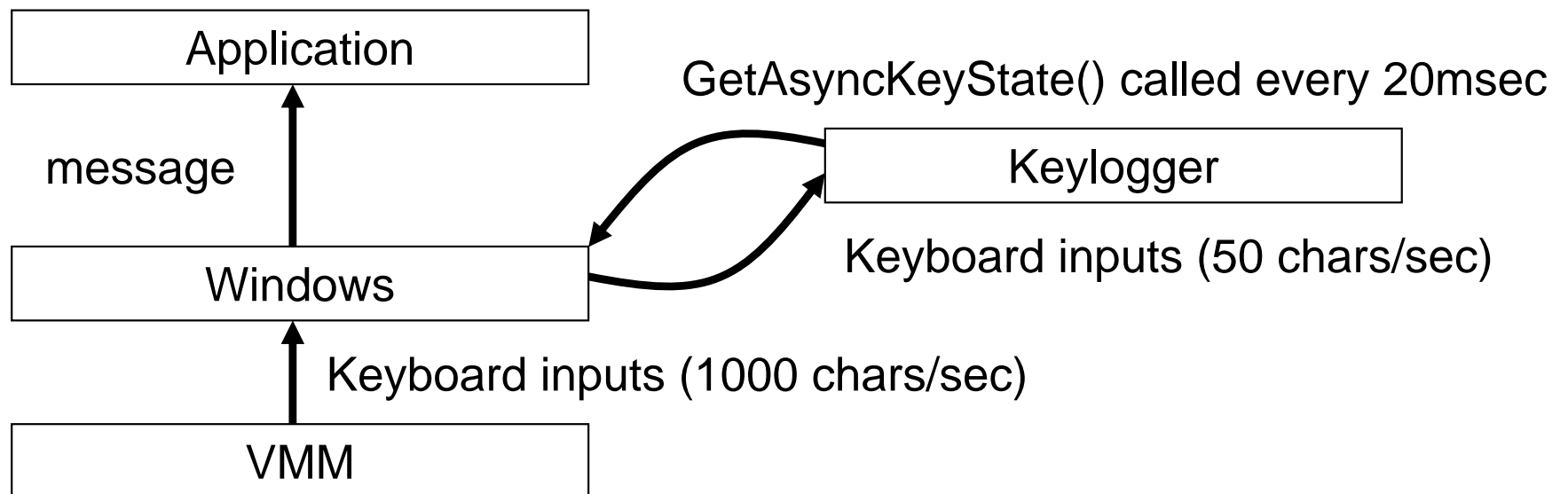
Keyloggers easily detected by FoxyKBD

- Steal keystrokes by hook functions
 - Implemented by SetWindowsHookEx() or filter drivers
 - Steal all keystrokes generated by FoxyKBD
 - Easy to feed a huge number of keystrokes
 - Examples : Family KGB Keylogger Ver. 1.8
All In-One Spy Ver. 2.0, Spy Agent 6.01,
Active Key Logger Ver. 3.7.3



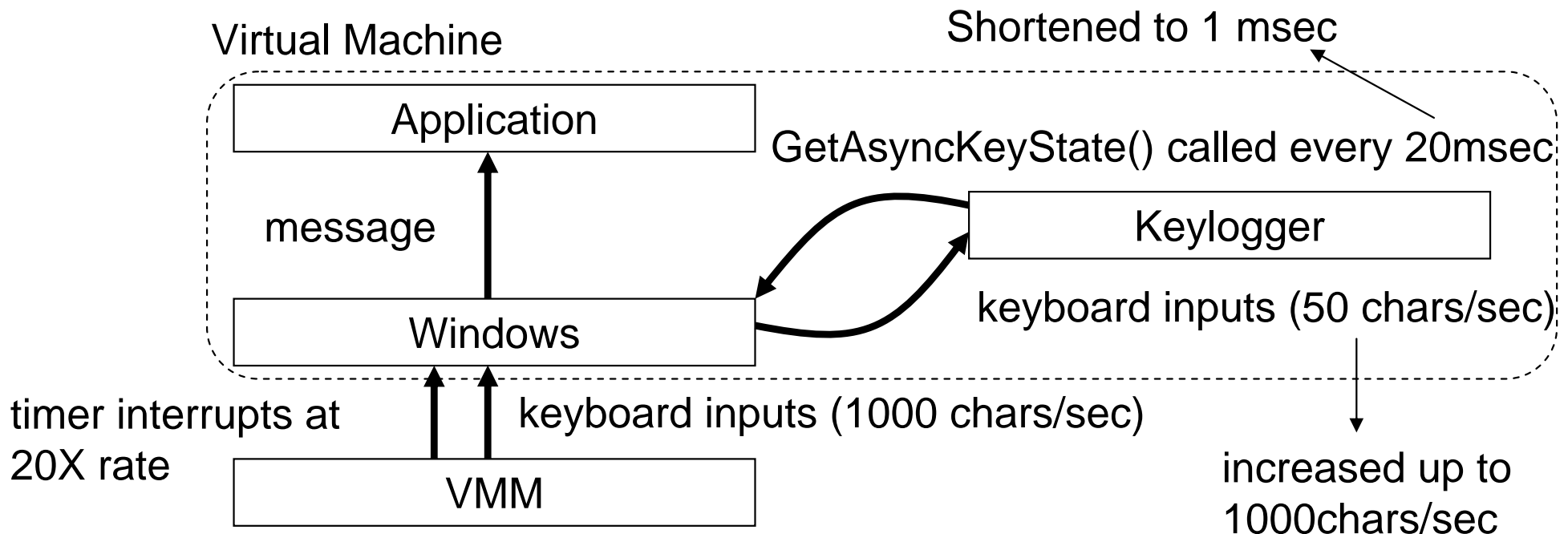
Keyloggers difficult to detect by FoxyKBD

- Periodically get keyboard status
 - Implemented by GetAsyncKeyState()
 - ◆ GetAsyncKeyState() returns true if specified key is pressed when it called
 - ◆ Keylogger calls it periodically
 - # of keystrokes is limited by # of calls on GetAsyncKeyState()
 - ◆ FoxyKBD can't feed keystrokes when the function is not called
 - FoxyKBD can't amplify the
 - Examples: All In One Keylogger Ver. 2.8, LoggerA, Keylogger Ver. 1.5.0



Our Solution

- Accelerates time flow in guest OS
 - Shortens the interval of timer interrupts in VM
 - As a result, the interval between func. calls is shorten
 - ◆ Keystrokes fed by FoxyKBD are virtually increased



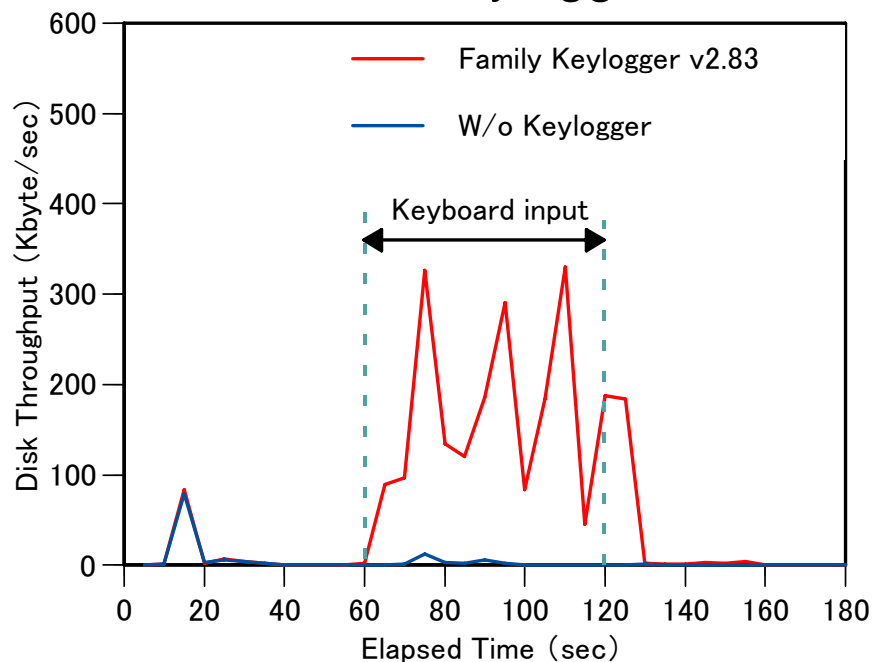
- Evaluate the accuracy of detection
 - Tested on 56 real keyloggers and 8 innocent keyboard utilities
 - ◆ All utilities get keystrokes
 - FoxyKBD feeds 30,000 chars during 60 seconds

- Experimental environment
 - CPU Core2Duo 1.8GHz
 - Physical mem. 2GB
 - Host OS Linux 2.6.19
 - Guest OS Windows XP
 - Guest mem. 128MB
 - VMM VirtualBox (sorry not Xen)

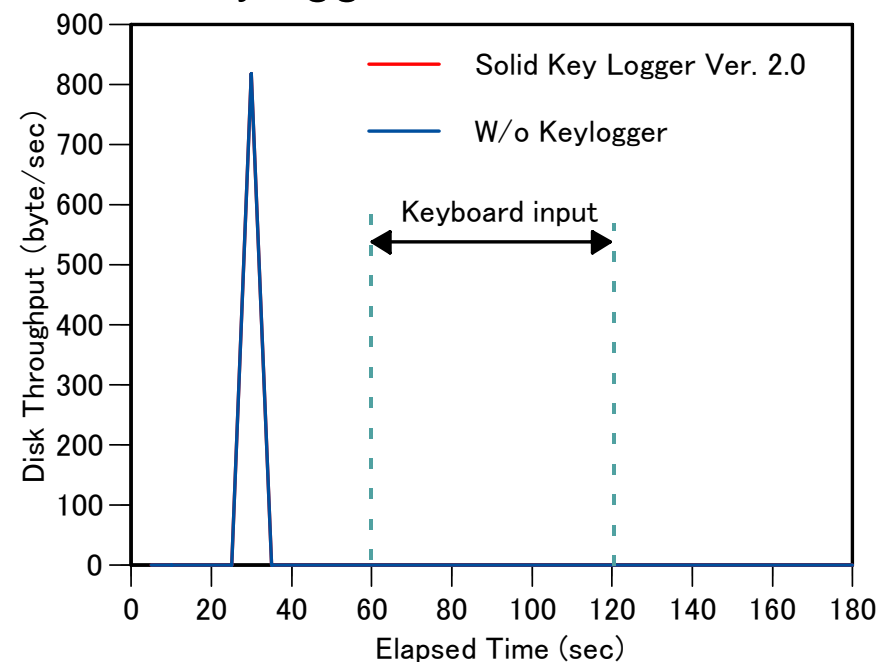
Experimental Results

- Detected 55 keyloggers
 - Can't detect the keylogger that does NOT store the log on files
- No false positives
 - Keyboard utilities do not access disk/net virtual devices
- No network access was detected
 - No keyloggers send out the stolen keystrokes immediately to Internet

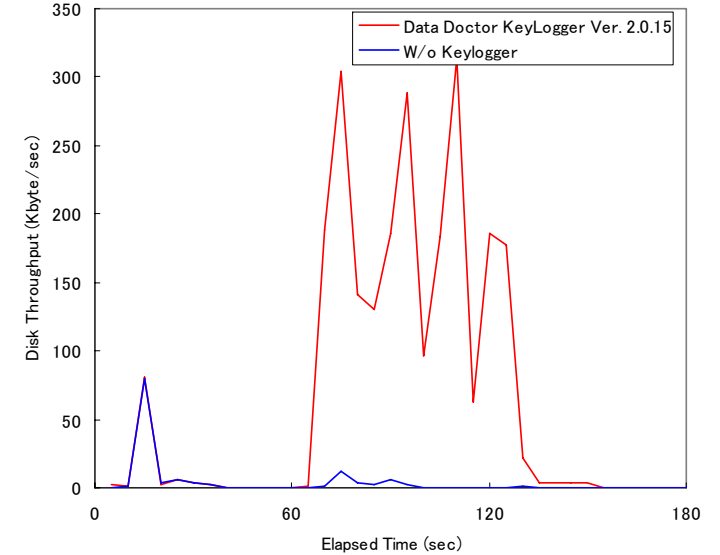
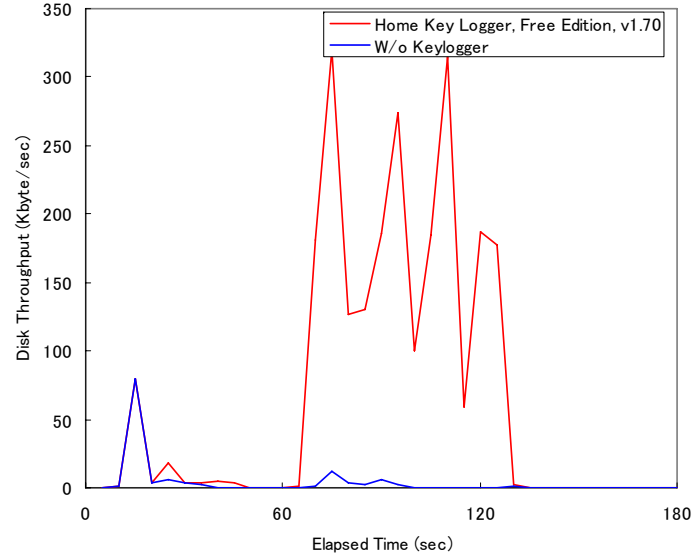
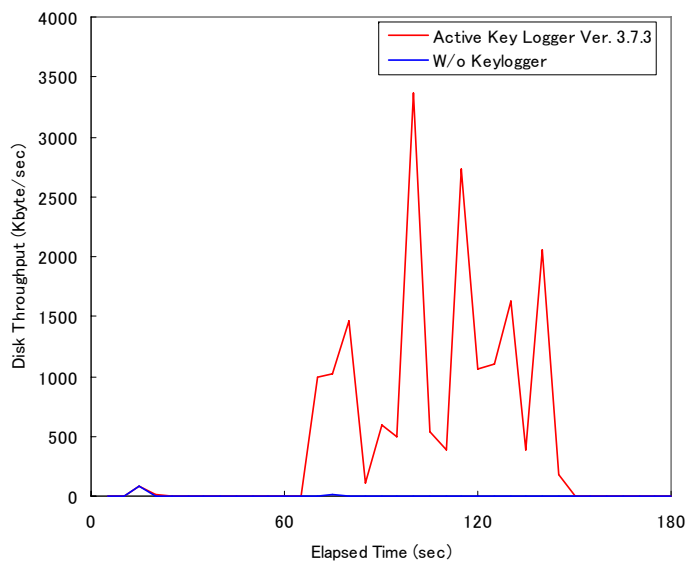
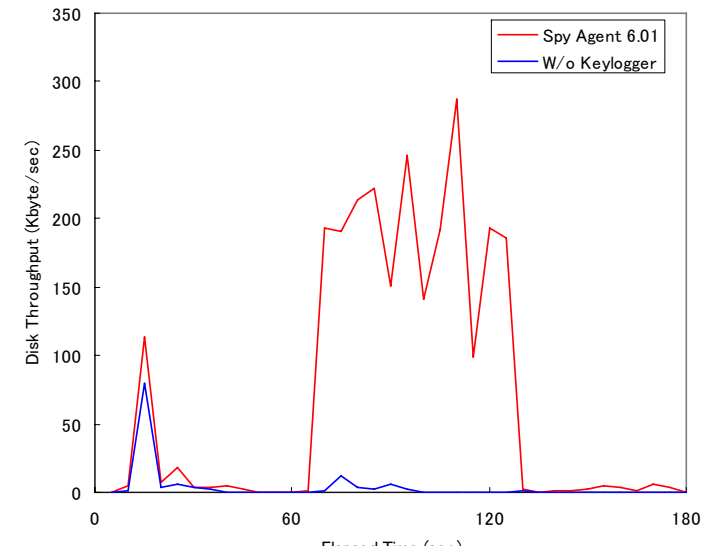
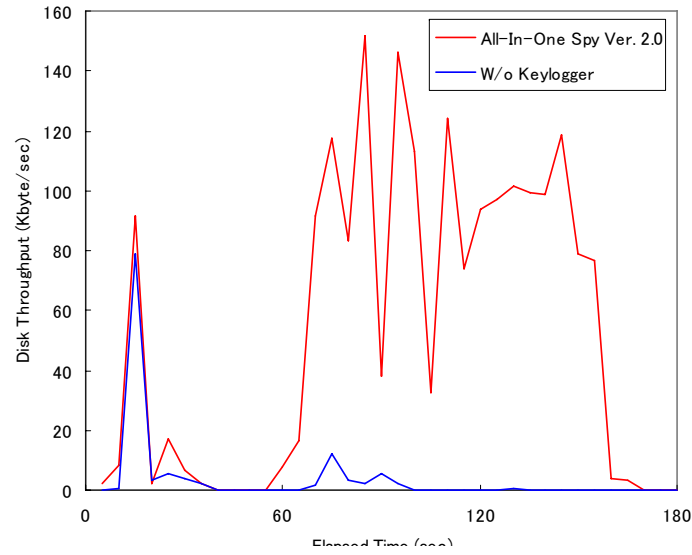
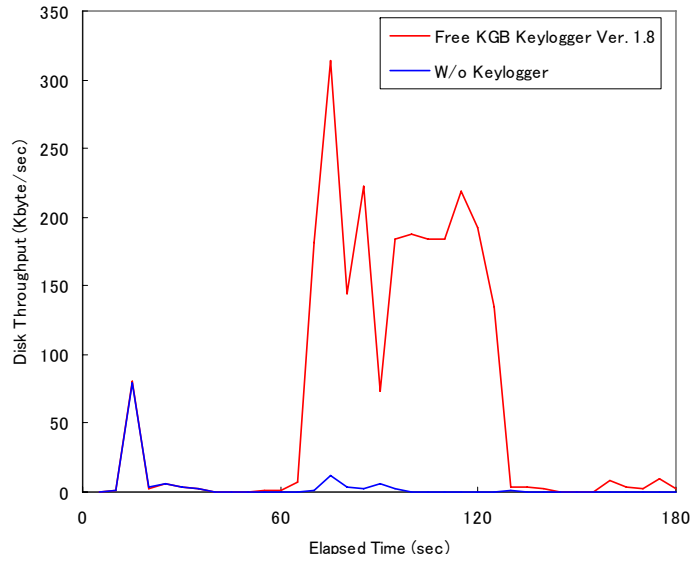
Detected keylogger



Keylogger not detected



Examples of detected keyloggers



- Proposed FoxyKBD, a VMM-based approach to detecting keyloggers
 - Amplifies the behavior of keyloggers
 - ◆ Feeds a huge number of keystrokes
 - ◆ Monitors behavior of virtual devices
 - Resilient to stealthy keyloggers
 - Detected 55 real keyloggers out of 56
 - No false positives