

仮想機械技術を利用した キーロガー検知システム

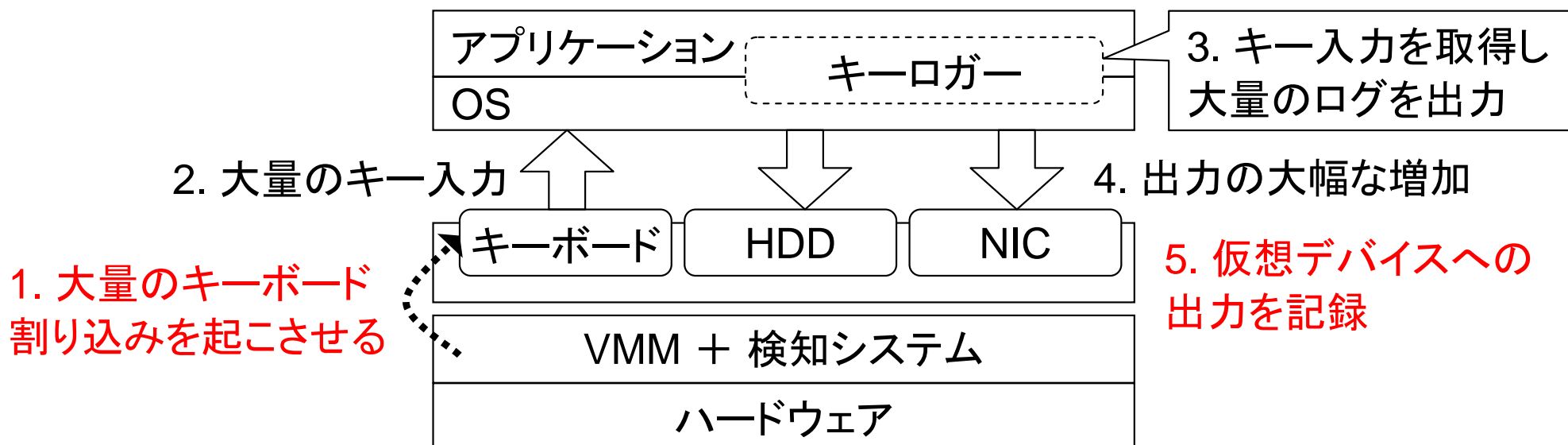
慶應義塾大学
河野健二

- キーロガーがセキュリティ上の脅威となっている
 - キー入力の記録を目的とした悪意あるプログラム
 - ◆ 情報漏洩を目的としたスパイウェアの一種
 - ◆ ログをディスクに保存したり, ネットワークに送信する機能を持つ
 - ◆ パスワードやクレジットカード番号などを漏洩させる
 - ◆ 多大な被害を与える可能性がある
 - 自身の存在を隠蔽する
 - ◆ ユーザに気づかれずに動作する
 - ◆ カーネルレベルに存在することで OS をのっとる
 - ◆ キーロガー検知システムを不能にする

- シグネチャマッチングによる検知
 - シグネチャに合致するバイナリイメージを検知
 - ◆ シグネチャとはキーロガーを特徴づけるバイト列
 - ◆ 既知のキーロガーからシグネチャを生成する
 - ◆ 多くのウィルス対策ソフトの方式と同じ
 - シグネチャマッチングの欠点
 - ◆ 未知のキーロガーは検知できない
 - シグネチャの対応しない亜種の生成は容易
 - ◆ 簡単に検知システムを回避できる
 - Obfuscation
 - ルートキット技術

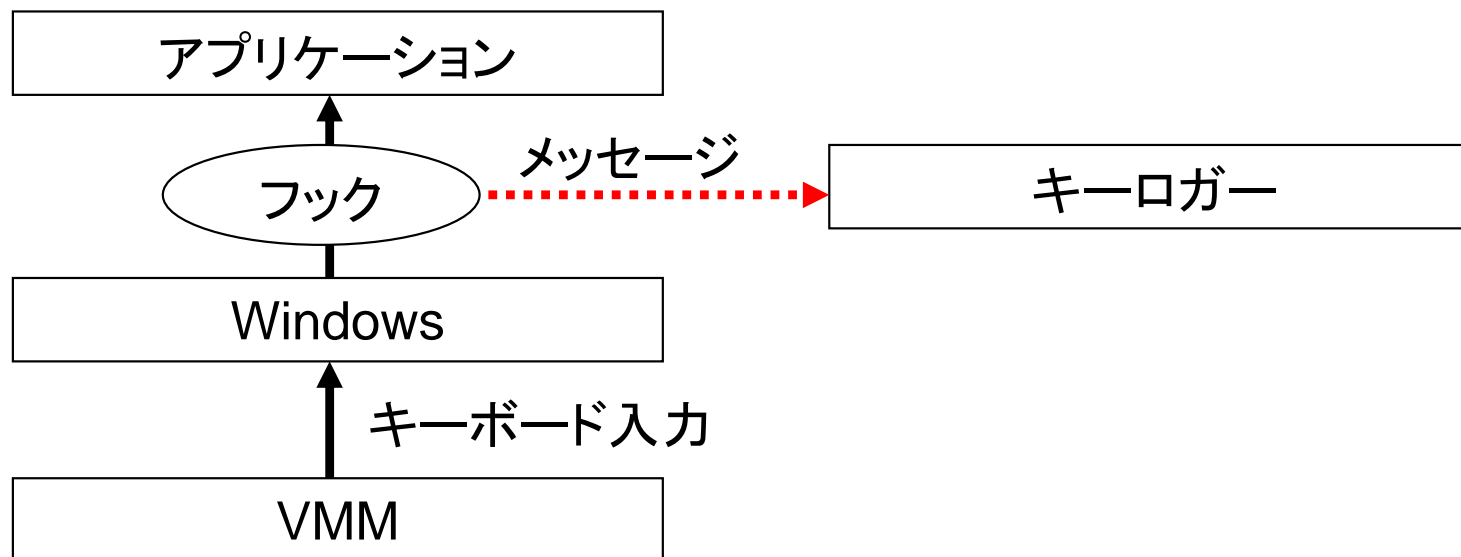
- 仮想機械技術を利用したキーロガー検知システム
 - キーロガー特有のふるまいから検知を行う
 - ◆ シグネチャを用いない
 - ◆ 未知のキーロガーも検知できる
 - キーロガーの隠蔽を困難にする
 - ◆ 検知システムを回避させない
 - ◆ OS をのっもられても検知できる

- 手動では不可能なほど大量のキー入力を与える
 - VM 上で検証対象システムを動作させる
 - VMM は VM に大量のキーボード割り込みを起こす
 - 仮想デバイスの出力量の変化を解析する
 - ◆ キーロガーが存在する場合大量のログが仮想デバイスに出力される
 - ◆ 出力が大幅に増加した場合キーロガーが存在すると判断する



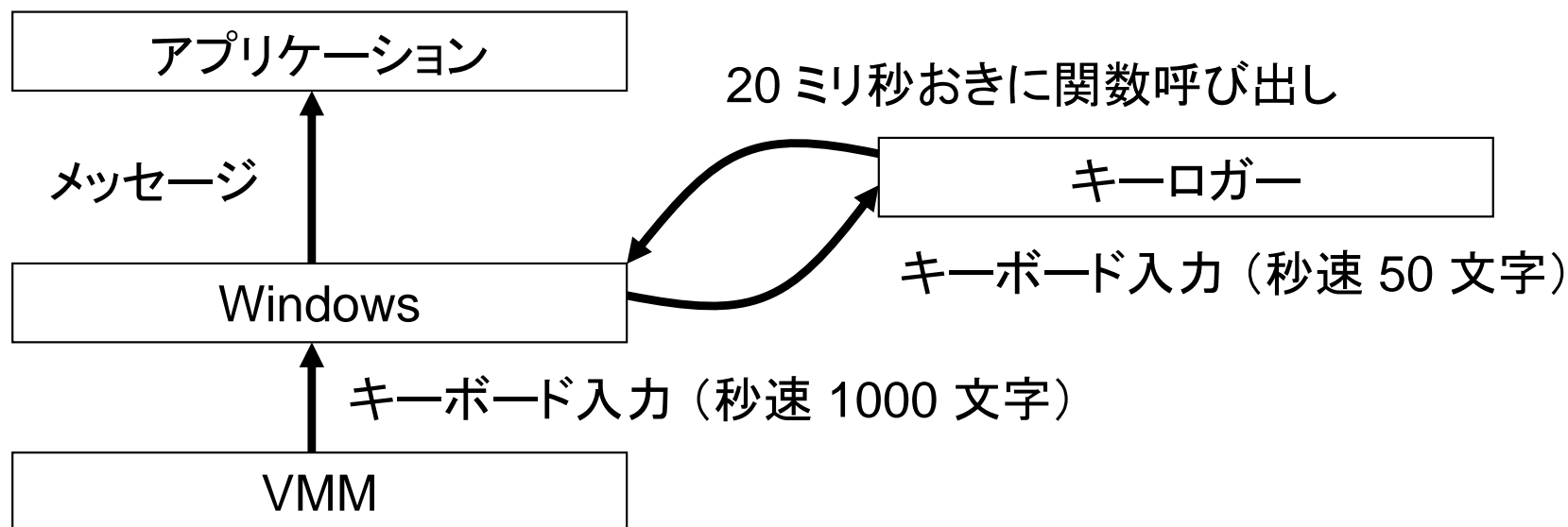
検知が容易なキーロガーのタイプ

- フックを利用してキーボード入力を取得するタイプ
 - SetWindowsHookEx(), フィルタドライバを利用して実装
 - VMMが与えたキーボード入力を全て取得する
 - 大量のキーボード入力を与えられる
 - 例: Family KGB Keylogger Ver. 1.8
All In-One Spy Ver. 2.0, Spy Agent 6.01,
Active Key Logger Ver. 3.7.3

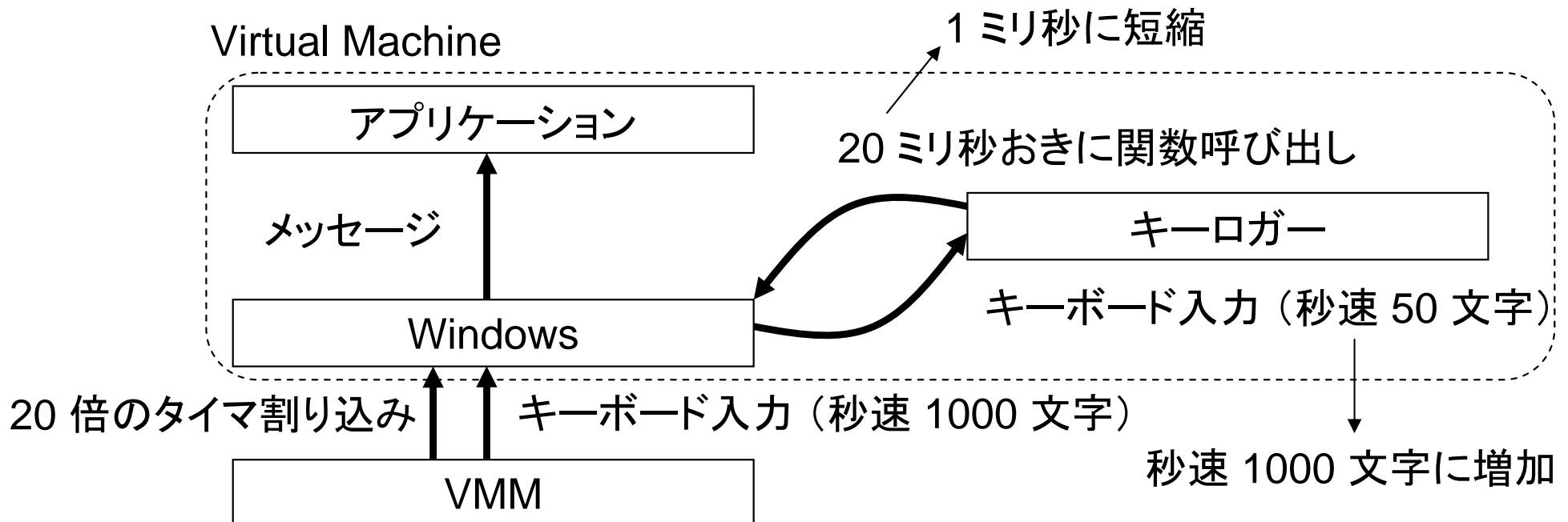


検知が難しいキーロガーのタイプ

- 反復的にキーボード状態を取得するタイプ
 - GetAsyncKeyState() を利用して実装
 - ◆ 関数呼び出し時に指定したキーが押されているかがわかる
 - ◆ 一定時間おきに関数呼び出しを行う
 - 関数の呼び出し回数がキーボード入力の取得数の上限
 - ◆ 関数呼び出しされた瞬間以外の入力は取得されない
 - 検知に十分な入力を与えられない可能性がある
 - 例: All In One Keylogger Ver. 2.8,
LoggerA, キーロガー Ver. 1.5.0



- ゲスト OS の内部時刻を加速する
 - VM のタイマ割り込み間隔を短縮する
 - 関数呼び出し間隔が短縮される
 - ◆ 単位時間あたりのキーボード入力の取得数が増える
 - ◆ VM の外側から見たとき、取得数と出力の増加が期待できる



■ 検知精度の評価

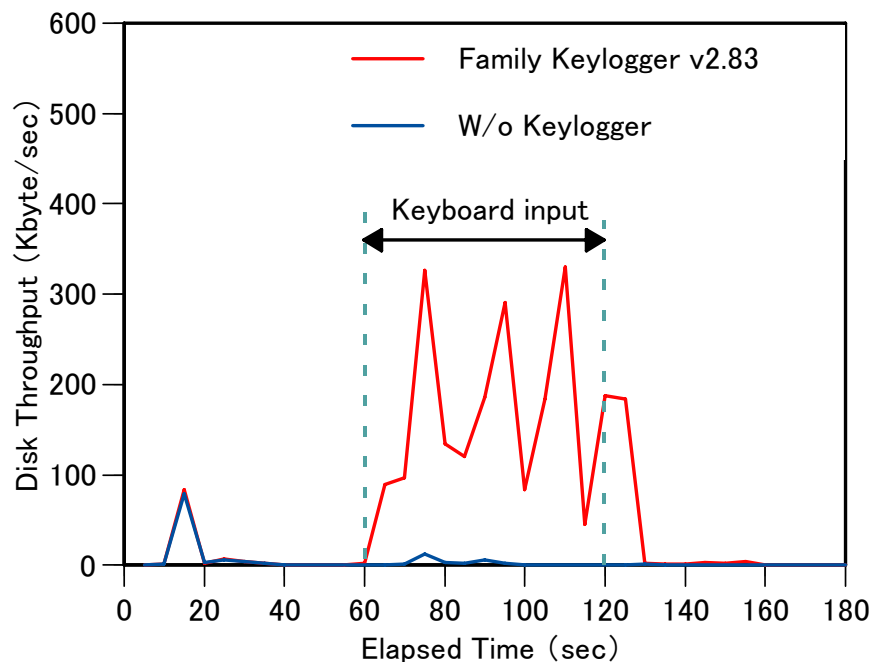
- 56 種類の実際のキーロガーと8 種類のキーボードユーティリティに対して実験
 - ◆ 全て常駐してキーボード入力を取得する機能を持つ
- 提案システムを用いて 60 秒間に約 3 万文字を入力

■ 実験環境

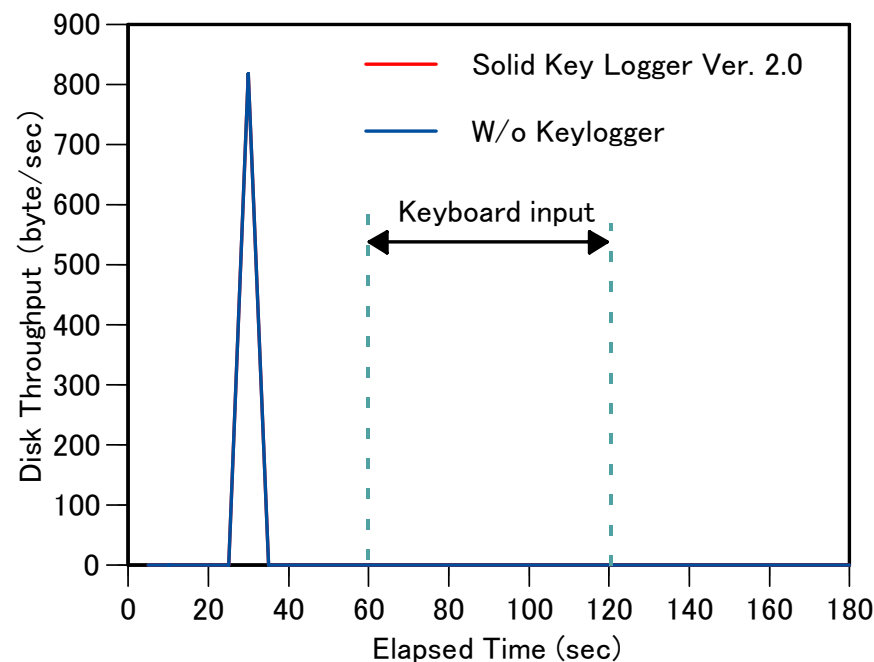
- CPU Core2Duo 1.8GHz
- 物理メモリ 2GB
- ホストOS Linux 2.6.19
- ゲストOS Windows XP
- ゲストメモリ 128MB

- 55 種類のキーロガーを検知した
 - ファイルにログを保存しないキーロガーを検知できなかった
- False positive 無し
 - キーボードユーティリティはほとんど出力しないため誤検知されなかった
- ネットワーク出力は計測されなかった
 - 取得した情報を直ちにネットワークに送信する仕様ではないため

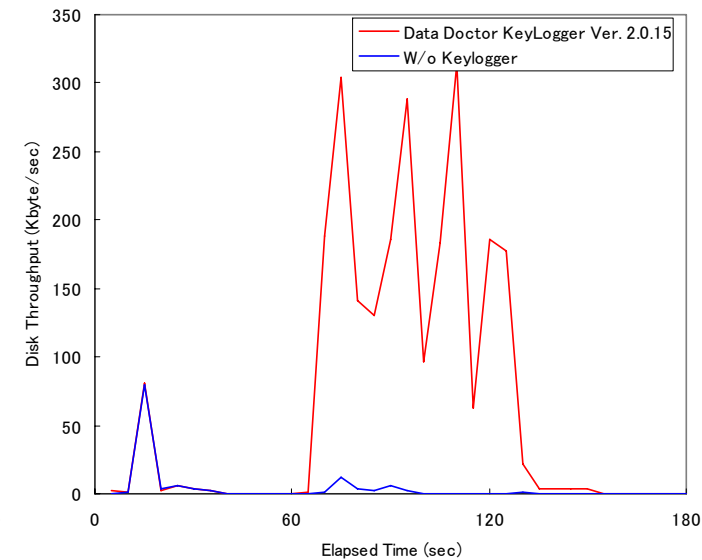
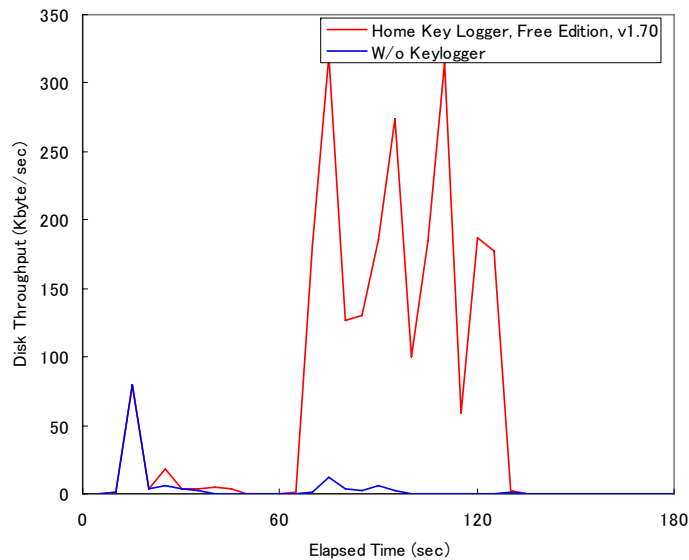
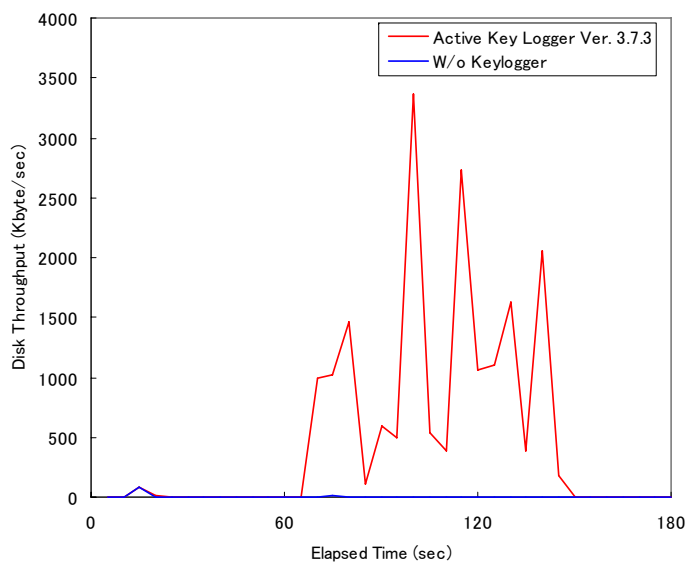
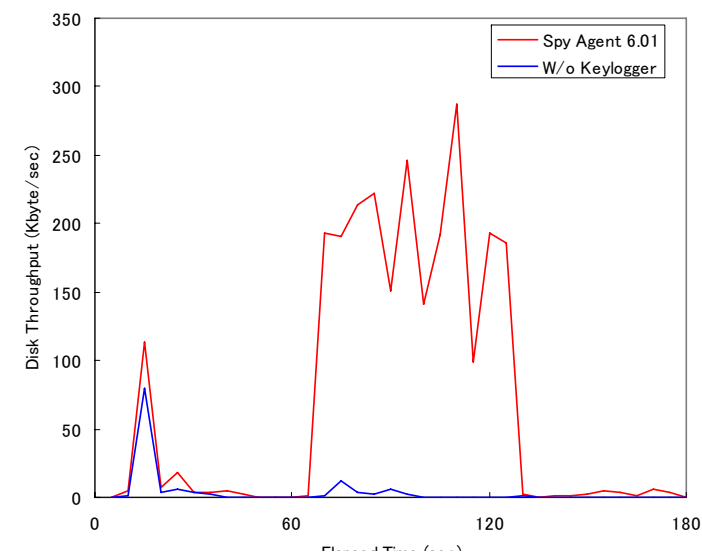
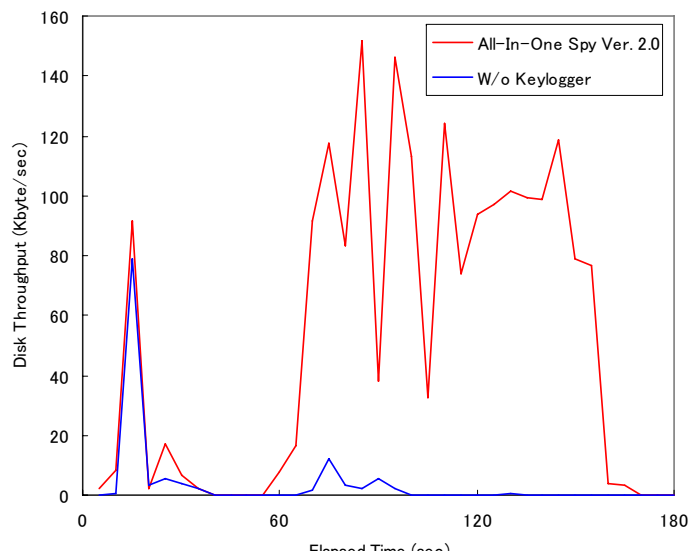
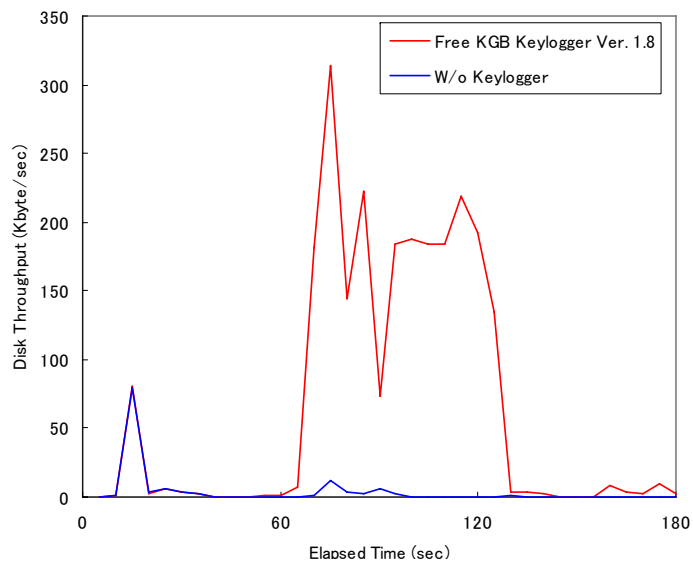
検知できたキーロガー



検知できなかったキーロガー



検知できたキーロガーの例



- 仮想機械技術を利用したキーロガー検知システムを提案した
 - キーロガーのふるまいを増幅して検知する
 - ◆ 仮想機械技術による大量のキーボード入力と出力の監視
 - キーロガーの隠蔽機能に対する耐性を持つ
 - 56 種類のキーロガーのうち 55 種類を検知した
 - False positive 無し
- 今後の予定
 - 提案システムの回避手法とその対策に関する考察