

ПРОГРАМНИЙ ЗАСІБ ДЛЯ АНАЛІЗУ КОНТЕНТНОГО ВВЕДЕННЯ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

В роботі розглядається додаток для перехоплення та аналізу натиснутих клавіш на клавіатурі, який дає можливість прихованого стеження та не є вірусним програмним забезпеченням. Розроблено алгоритм перехоплення та аналізу натиснутих клавіш на клавіатурі у операційній системі Windows.

Ключові слова: кейлоггер, контентне введення інформації, циклічне перехоплення.

Abstract

The paper considers an application for interception and analysis of keystrokes on the keyboard, which allows covert surveillance and is not a virus software. An algorithm for intercepting and analyzing keystrokes on the keyboard in the Windows operating system has been developed.

Keywords: keylogger, content input, cyclic interception.

У перекладі з англійської Keylogger (Keyboard Logger) позначає «клавіатурний реєстратор». Однак насправді кейлоггер є програмою-шпигуном, що відстежує всі дії, що відбуваються з клавіатурою. Встановлення кейлоггерів дає можливість визначити спроби передачі важливої інформації третім особам або набору паролів доступу, а також дослідити інциденти, пов'язані з комп'ютером [1]. Отже, актуальність розробки обумовлена потребами користувачів у прихованому стеженні за діями які відбуваються за їхніми комп'ютерами за умови відсутності.

Загальний принцип роботи програм для аналізу контентного інформації – втрутитися в процес проходження сигналу від натискання клавіші до появи символу на екрані [2].

Для програмного додатку «Key Logger» було створено діаграму «сутність-зв'язок», яка описує концептуальні схеми за допомогою узагальнених конструкцій блоків та виділяє найсуттєвіші елементи (вузли, блоки) моделі і встановлює зв'язки між ними (рисунок 1) [3].

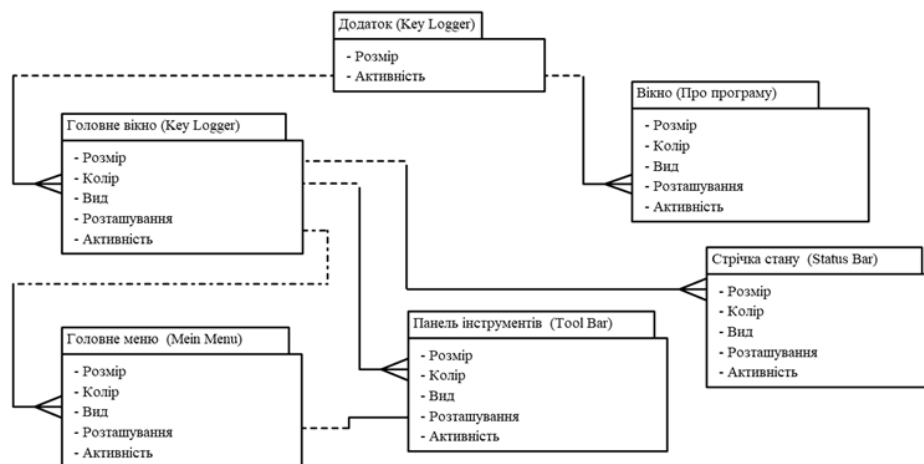


Рис.1 Діаграма «сутність-зв'язок» програмного додатку

Розроблено метод циклічного опитування стану натиснутої клавіші:

- спрацьовує таймер який починає циклічне опитування клавіатури;
- спрацьовує функція яка визначає розкладку клавіатури;
- при натисненні або відпусканні клавіші вона записується в масив даних;

- при копіюванні інформації у буфер обміну вона також додається у масив даних;
- масив даних передається в об'єкт текстового поля метою;
- заданий масив обробляється та виводиться у вигляді описаної текстової інформації про натиснуті клавіші та вміст буферу обміну.

Для перехоплення стану клавіш в системі встановлюється хук перехоплення. Далі активізується таймер, який розпочинає процес перехоплення натискання клавіш. Отже, загальна модель роботи додатку виглядає наступним чином: ініціація перехоплення; циклічне перехоплення (опитування) клавіш; аналіз, обробка та логування отриманої інформації; запис логу до файлу; представлення логу у зручному вигляді у вікні програми (рисунок 2).



Рис. 2 Діаграма послідовностей розробленого додатку

Розроблений додаток дає можливість прихованого стеження за діями клавіатури, а саме перехоплення та аналізу натиснутих клавіш, та не являється вірусним програмним забезпеченням. Додаток був розроблений мовою C++ в інтерактивному середовищі розробки Embarcadero RAD (Rapid Application Development) Studio (C++ Builder 10 Seattle).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кормен Т. Алгоритмы: построение и анализ, 2-е издание.: Пер. с англ./Т. Кормен – М.: Издательский дом «Вильямс», 2005. – 1296 с.: ил.
2. MacDonald M. Pro .NET 2.0 Windows Forms and Custom Controls in C#. - Springer-Verlag New York, Inc./ M. MacDonald, 2006. – 1081 p.
3. Графічний інтерфейс користувача [Електронний ресурс]: Режим доступу: URL: http://uk.wikipedia.org/wiki/Графічний_інтерфейс. - Назва з екрану.

Черноволик Галина Олександрівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: lina2433@gmail.com.

Кириляшук Світлана Анатоліївна – кандидат педагогічних наук, декан факультету інформаційних технологій та комп'ютерної інженерії, доцент кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: ksa07750@gmail.com.

Харкевич Кирило Андрійович – студент групи 2ПІ-19м, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: kirill98402@gmail.com.

Galyna Chernovolyk – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lina2433@gmail.com.

Svitlana Kyrylashchuk – Ph.D., dean of the Information Technology and Computer Engineering Department, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, e-mail: ksa07750@gmail.com.

Kirilo Harkevich – student of 2PI-19m, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kirill98402@gmail.com.