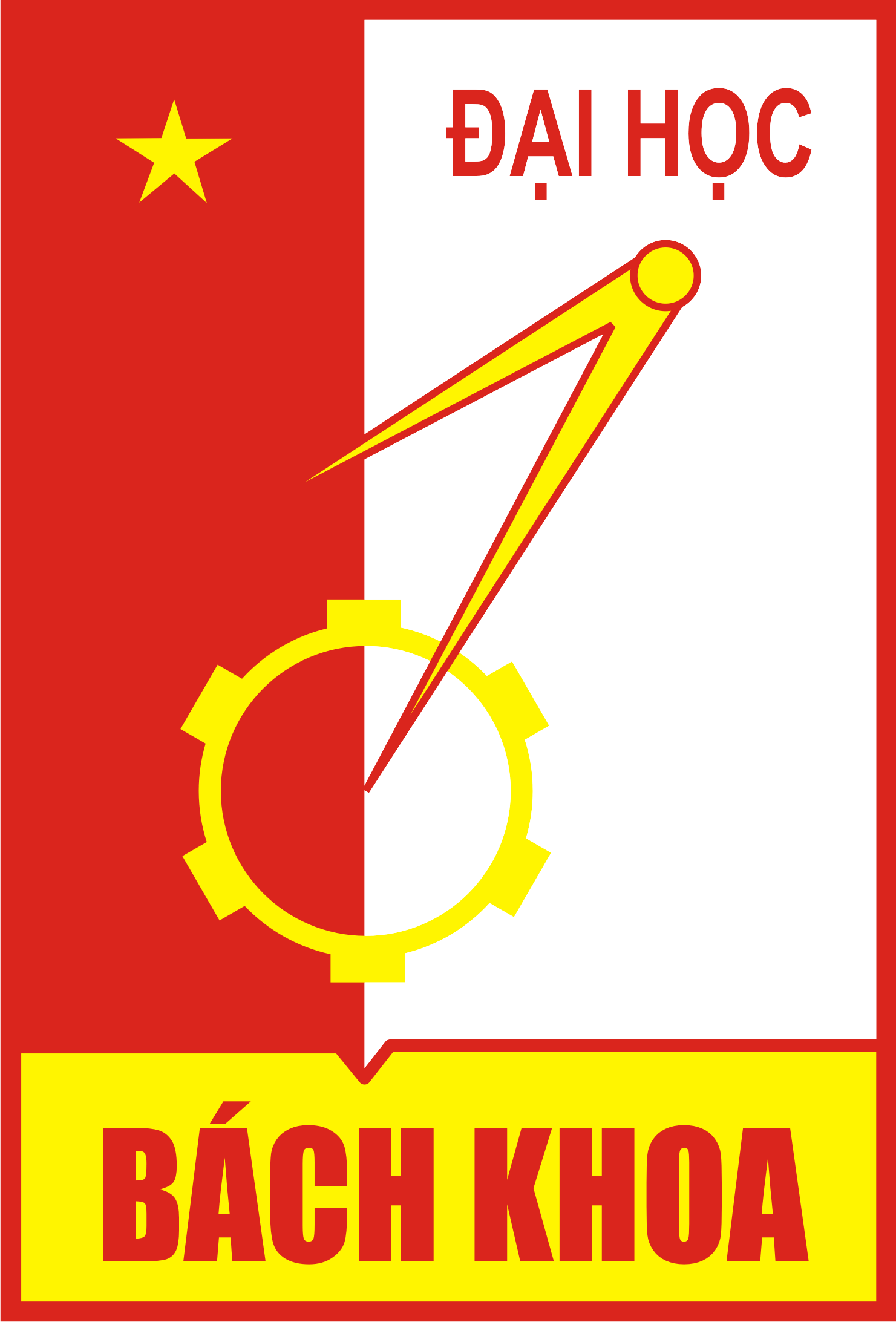
**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN ĐIỆN TỬ -VIỄN THÔNG**

****

**BÁO CÁO BÀI TẬP LỚN**

**MÔN KĨ THUẬT LẬP TRÌNH C/C++**

**Xây dựng lõi trình theo dõi thao tác bàn phím**

**(KEYLOGGER) dựa trên C++**

**Giảng viên hướng dẫn: ThS. Hoàng Quang Huy**

**Sinh viên thực hiện: Nguyễn Minh Tuấn 20213737**

**Mạc Quang Huy 20213709**

**Nhóm: 24 – Bánh mì bà Béo**

**MỤC LỤC**

**A-BẢNG PHÂN CÔNG CÔNG VIỆC CHO CÁC THÀNH VIÊN**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 01 | Mạc Quang Huy | 20213709 | Huy.mq213709@sis.hust.edu.vn |
| 02 | Nguyễn Minh Tuấn | 201213737 | Tuan.nm213737@sis.hust.edu.vn |

|  |  |  |
| --- | --- | --- |
| STT | Phân công công việc | Mức độ hoàn thành |
| 01 | -Thu thập tài liệu  -Viết báo cáo  -Chạy thử, kiểm tra chương trình | -100% |
| 02 | -Đưa ra ý tưởng  -Phát triển chương trình chính  -Cải tiến, nghiên cứu phương án phòng chống | -100% |

**B-NỘI DUNG BÁO CÁO**

**I- Giới thiệu bài toán**

* + Đề tài: Trong cuộc sống hiện đại ngày nay, việc đảm bảo tính bảo mật trên không gian mạng là vô cùng quan trọng. Các thiết bị công nghệ cao, đặc biệt là các máy tính cá nhân (PC) đang trở thành mục tiêu mới với nhiều hình thức tấn công và khai thác khác nhau, gây ra hậu quả khôn lường.
  + Theo ghi nhận của Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (A05), trong 6 tháng đầu năm 2022, Bộ Công an đã phát hiện và xử lý 840 chuyên án, vụ việc liên quan đến lừa đảo, chiếm đoạt tài sản qua mạng. “Các vụ việc đã tăng 42% so với 6 tháng cuối năm 2021. Đây là con số đáng báo động.” – Đại tá Nguyễn Ngọc Cương.
  + Vì vậy, việc tham gia nghiên cứu, hiểu biết và phòng chống các hình thức lừa đảo, gián điệp, theo dõi trên không gian mạng là điều vô cùng cần thiết trong kỉ nguyên Chuyển đổi số như hiện nay.

**II-Phân tích bài toán, mô tả hoạt động và phân tích dữ liệu**

**1.Phân tích bài toán**

**-** Keylogger là một phần mềm gián điệp sử dụng để theo dõi những phím bấm trên máy tính, dẫn tới nguy cơ lộ, lọt các thông tin nhạy cảm khi thực hiện các thao tác hàng ngày.

- Dùng để phục vụ cho mục đích nghiên cứu và phòng chống.

- Phát triển thành các phần mềm gián điệp phức tạp hơn.

- Phương án cụ thể:

Sử dụng ngôn ngữ lập trình C++ tạo ra các file header chứa các hàm LOG() (sử dụng để ghi lại các input), CapsLock\_isOn() (sử dụng để kiểm tra phím CapsLock đang bật/tắt), Shift\_isOn() (sử dụng để kiểm tra phím Shift đang bật/tắt), NumberKeyShift() (sử dụng để ghi lại các kí tự đặc biệt tương ứng với các phím số), MiscKeyShift() (sử dụng để ghi lại các phím kí tự đặc biệt khi có phím Shift), SpecialKeys() (sử dụng để ghi lại các phím điều khiển). Sau đó file Core.cpp sẽ bao gồm tất cả các hàm này và dựa trên thuật toán để hoàn thành chương trình.

**2.Mô tả hoạt động**

Khi chạy, chương trình sẽ sử dụng hàm GetAsyncKeyState() (một hàm trong thư viện Windows.h, API của hệ điều hành Windows) để thu thập thông tin xem phím nào đang được bấm. Sau đó, phím bấm sẽ được chạy qua hàm int() để đổi sang mã Ascii. Tới đây sẽ có 3 trường hợp xảy ra:

1, Nếu mã Ascii có giá trị từ 65 tới 90: đây là các chữ cái từ A-Z trong bảng chữ cái tiếng Anh. Phần mềm sẽ thực hiện kiểm tra xem 2 phím Shift và CapsLock có đang được bật hay không thông qua hàm Shift\_isOn và CapsLock\_isOn. Sau đó, sử dụng toán tử XOR (^) để kiểm tra xem 2 phím này có đang được cùng bật hoặc cùng tắt. Nếu toán tử XOR có giá trị là 0 (tức là chữ thường) thì phần mềm sẽ cộng thêm 32 đơn vị vào giá trị Ascii trả về, sau đó thông qua hàm char() để đổi về kí tự chữ và ghi vào file log.txt.

2, Nếu mã Ascii có giá trị từ 48 tới 57: đây là các số từ 0-9. Phần mềm sẽ thông qua hàm CheckShift xem phím Shift có đang được bật hay không. Nếu có thì sẽ thông qua hàm NumberKeyShift để ghi lại các kí tự đặc biệt. Nếu không, các chữ số sẽ được ghi vào file log.txt.

3, Nếu mã Ascii thuộc trường hợp khác: Đây là các kí tự đặc biệt, tuỳ vào từng phím sẽ có mã Ascii riêng và được ghi vào file log.txt thông qua hàm MiscKeyShift().

**3.Phân tích dữ liệu**

-Dựa vào yêu cầu bài toán, ta xây dựng các chức năng chính của hệ thống Ghi lại phím bấm thông thường

Ghi lại các phím bấm đặc biệt và phím chức năng

Phân biệt chữ hoa, chữ thường

**III-TRIỂN KHAI HỆ THỐNG**

**Ảnh có chứa ảnh chụp màn hình, văn bản, phần mềm, thiết kế

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động**

**IV-TỰ ĐÁNH GIÁ, HẠN CHẾ**

1. Tự đánh giá

* Dự án được triển khai thành công với kết quả khả quan.
* Dự án có thể được mở rộng và phát triển thêm trong tương lai.
* Phục vụ tốt cho mục đích giảng dạy và nghiên cứu về An toàn Thông tin trong nhà trường và trong thực tế.

1. Hạn chế

* Vẫn còn những bug nhỏ liên quan tới các kí tự đặc biệt khi mã Ascii sai lệch và nằm ngoài dự kiến.

1. Phương án phòng chống

* Cần liên tục kiểm tra máy tính và cài đặt các phần mềm quét/diệt virus uy tín.
* Không tải các file lạ hay bấm vào các đường link lạ trên mạng
* Các công ty, nhà phát hành các phần mềm diệt virus cần liên tục cập nhật để đảm bảo tính an toàn và hữu ích của phần mềm, ngăn chặn các mối nguy mới.