|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA CÔNG NGHỆ THÔNG TIN**  Logo HvKTMM  BÁO CÁO MÔN HỌC  **AN TOÀN HỆ ĐIỀU HÀNH**  **Đề tài:**  **TÌM HIỂU VỀ INTEGRITY FLAWS**   |  |  | | --- | --- | | **Sinh viên thực hiện:** | **Trần Cao Minh Bách – AT150204**  **Vũ Thị Ánh - AT150504**  **Bạch Trường An – AT150201**  **Phạm Đỗ Thuỳ Linh**  **Nguyễn Đình Hùng** | | **Giảng viên hướng dẫn:** | **Đồng Thị Thuỳ Linh** |   Hà Nội, 11-2021 |

**LỜI NÓI ĐẦU**

Tài liệu này được Khoa Công nghệ thông tin, học viện Kỹ thuật Mật mã soạn thảo và ban hành nhằm mục đích hướng dẫn sinh viên trình bày đồ án báo cáo thực tập cơ sở một cách khoa học và thống nhất. Bản thân tài liệu này được biên soạn phù hợp với các quy định về trình bày một đồ án tốt nghiệp, đồ án môn học. Vì vậy, sinh viên có thể sử dụng trực tiếp mẫu này như một template khi viết quyển đồ án của mình. Sinh viên cũng được khuyến khích tham khảo hoặc sử dụng mẫu này khi viết báo cáo thực tập, báo cáo kết quả nghiên cứu, và các đồ án môn học khác.

Chi tiết về nội dung của phần Lời nói đầu được trình bày trong Mục 1.3.3.

**LỜI CAM ĐOAN**

Lời cam đoan được viết tại đây. Xem cách viết lời cam đoan tại Mục 1.3.4.

**MỤC LỤC**

[DANH MỤC HÌNH VẼ i](#_Toc88481038)

[DANH MỤC BẢNG BIỂU ii](#_Toc88481039)

[TÓM TẮT ĐỒ ÁN iii](#_Toc88481040)

[CHƯƠNG 1. KHÁI NIỆM CHUNG VỀ INTEGRITY FLAWS 1](#_Toc88481041)

[1.1 Quy định chung về định dạng văn bản 1](#_Toc88481042)

[1.2 Quy định về đánh số thứ tự 2](#_Toc88481043)

[1.2.1 Đánh số trang 2](#_Toc88481044)

[1.2.2 Đánh số chương mục 3](#_Toc88481045)

[1.2.3 Đánh số hình vẽ và bảng biểu 3](#_Toc88481046)

[1.2.4 Đánh số phương trình 4](#_Toc88481047)

[1.2.5 Đánh số định nghĩa, định lý, và hệ quả 4](#_Toc88481048)

[1.3 Thứ tự các phần của đồ án 4](#_Toc88481049)

[1.3.1 Bìa quyển đồ án 4](#_Toc88481050)

[1.3.2 Mẫu nhận xét 4](#_Toc88481051)

[1.3.3 Lời nói đầu 5](#_Toc88481052)

[1.3.4 Lời cam đoan 5](#_Toc88481053)

[1.3.5 Mục lục 6](#_Toc88481054)

[1.3.6 Danh mục ký hiệu và chữ viết tắt 6](#_Toc88481055)

[1.3.7 Danh mục hình vẽ 6](#_Toc88481056)

[1.3.8 Danh mục bảng biểu 7](#_Toc88481057)

[1.3.9 Tóm tắt đồ án 7](#_Toc88481058)

[1.3.10 Phần mở đầu 7](#_Toc88481059)

[1.3.11 Nội dung chính 7](#_Toc88481060)

[1.3.12 Kết luận 7](#_Toc88481061)

[1.3.13 Tài liệu tham khảo 8](#_Toc88481062)

[1.3.14 Phụ lục 8](#_Toc88481063)

[1.4 Một số điều cần lưu ý trong trình bày 8](#_Toc88481064)

[1.4.1 Lưu ý về dấu câu 8](#_Toc88481065)

[1.4.2 Lưu ý về hình vẽ và bảng biểu 11](#_Toc88481066)

[CHƯƠNG 2. CÁC ĐỐI TƯỢNG - PHƯƠNG THỨC VÀ ẢNH HƯỞNG GÂY RA TRÊN CÁC ĐỐI TƯỢNG 13](#_Toc88481067)

[2.1 Liệt kê tài liệu tham khảo 13](#_Toc88481068)

[2.1.1 Cách liệt kê 13](#_Toc88481069)

[2.1.2 Các loại tài liệu tham khảo 13](#_Toc88481070)

[2.2 Trích dẫn tài liệu tham khảo 15](#_Toc88481071)

[2.3 Nộp đồ án 16](#_Toc88481072)

[2.3.1 Nộp bản cứng 16](#_Toc88481073)

[2.3.2 Nộp bản mềm 16](#_Toc88481074)

[2.4 Bản quyền kết quả nghiên cứu 16](#_Toc88481075)

[CHƯƠNG 3. CÁC HÌNH THỨC KHAI THÁC LỖ HỔNG 18](#_Toc88481076)

[3.1 Xác thực không đầy đủ 18](#_Toc88481077)

[3.2 Xác thực không đồng nhất 19](#_Toc88481078)

[3.3 Chia sẻ ngầm dữ liệu quan trọng 20](#_Toc88481079)

[3.4 Xác thực bất đồng bộ 21](#_Toc88481080)

[3.5 Nhận dạng/ Xác thực/ Uỷ quyền không đầy đủ 24](#_Toc88481081)

[3.6 Vi phạm giới hạn 25](#_Toc88481082)

[3.7 Lỗi logic 26](#_Toc88481083)

[KẾT LUẬN 28](#_Toc88481084)

[Kết luận chung 28](#_Toc88481085)

[Hướng phát triển 28](#_Toc88481086)

[Kiến nghị và đề xuất 28](#_Toc88481087)

[TÀI LIỆU THAM KHẢO 29](#_Toc88481088)

[PHỤ LỤC 30](#_Toc88481089)

[Phụ lục 1. Mẫu trang bìa chính của đồ án 30](#_Toc88481090)

[Phụ lục 2. Mẫu trang bìa phụ của đồ án 32](#_Toc88481091)

[Phụ lục 3. Mẫu nhận xét đồ án 34](#_Toc88481092)

# DANH MỤC HÌNH VẼ

[Hình 1.1 Sơ đồ khối của hệ thống 3](#_Toc9951164)

(Xem thêm Mục 1.3.7)

# DANH MỤC BẢNG BIỂU

[Bảng 1.1 Kết quả thí nghiệm 3](#_Toc9951165)

(Xem thêm Mục 1.3.8)

# TÓM TẮT ĐỒ ÁN

Tóm tắt đồ án, có độ dài 1-2 trang, được trình bày tại đây. Chi tiết xem Mục 1.3.9.

# KHÁI NIỆM CHUNG VỀ INTEGRITY FLAWS

Nội dung chương đề cập tới khái niệm chung của intergrity flaws, nhằm đưa cái nhìn khách quan nhất về dạng lỗ hổng này.

## Quy định chung về định dạng văn bản

Đồ án TTCS có thể được soạn thảo bằng Microsoft Word, Latex, hoặc các phần mềm soạn thảo tương đương khác nhưng quyển đồ án của sinh viên cần tuân theo các quy định sau:

* Cỡ giấy: A4, in 1 mặt hoặc **in 2 mặt** nhằm tiết kiệm không gian lưu trữ.
* Số trang: khoảng 50-150 trang, không kể phần phụ lục.
* Đóng bìa: bìa mềm có bóng kính.
* Căn lề:
  + Lề trên: 2,0 cm.
  + Lề dưới: 2,5 cm (số trang nằm ở footer).
  + Lề trong: 3,0 cm (để đóng gáy).
  + Lề ngoài: 2,0 cm.
* Các kiểu chữ (style) cơ bản:
  + Normal: kiểu chữ thường; sử dụng cỡ 13, font Times New Roman (unicode), giãn dòng (line spacing) multiple 1.2, giãn trước (spacing before) 6 pt, giãn sau (spacing after) 6 pt.
  + Heading 1: dùng cho tên chương; sử dụng cỡ 16, chữ hoa toàn bộ, in đậm, căn lề giữa, giãn trước 0 pt, giãn sau 30 pt (còn lại như Normal).
  + Heading 2: dùng cho các mục lớn trong chương; sử dụng cỡ 14, chữ in đậm, căn lề hai bên, giãn trước 10 pt, giãn sau 0 pt (còn lại như Normal).
  + Heading 3: dùng cho các mục nhỏ hơn Heading 2; sử dụng cỡ 13, chữ in nghiêng và đậm, căn lề hai bên, giãn trước 10 pt, giãn sau 0 pt (còn lại như Normal).
  + Heading 4: dùng cho các mục nhỏ hơn Heading 3; sử dụng cỡ 13, chữ in nghiêng, căn lề hai bên, giãn trước 10 pt, giãn sau 0 pt (còn lại như Normal).
  + Caption: dùng cho chú thích hình và bảng; sử dụng cỡ 12, chữ in đậm, căn lề giữa, giãn dòng single.
* Các quy định khác:
  + Chữ trong bảng: sử dụng cỡ 12 hoặc nhỏ hơn, tùy theo lượng thông tin. Nên để giãn dòng single, giãn trước 0 pt, giãn sau 0 pt. Tiêu đề các dòng và cột nên dùng chữ đậm, như trong Bảng 1.1.
  + Chữ trong mục lục, danh mục hình vẽ, và danh mục bảng biểu: tham khảo trực tiếp các phần tương ứng trong template này. Nên điều chỉnh giãn dòng và giãn đoạn để giảm độ dài trong trường hợp trang cuối của mục lục hoặc các danh mục chỉ có 1-2 dòng.
  + Mã nguồn chương trình (nếu có) được đưa vào Phụ lục. Sử dụng font Courier New, cỡ 10, giãn dòng single, giãn trước 0 pt, giãn sau 0 pt.

|  |
| --- |
| Ví dụ:  /\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/  #ifndef \_AVR\_HUNGET\_H\_  #define \_AVR\_HUNGET\_H\_ 1  static inline void DELAY\_4CK(unsigned int hunget\_delay\_us) \_\_attribute\_\_((always\_inline));  // Ham tre 4 \* n xung nhip he thong (CK). Goi ham mat 7 CK  void DELAY\_4CK(unsigned int hunget\_delay\_4ck)  {  \_\_asm\_\_ volatile  (  "1: sbiw %0,1" "\n\t"  "brne 1b"  : "=w" (hunget\_delay\_4ck)  : "0" (hunget\_delay\_4ck)  );  }  #endif  /\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Copyright (c) 2008 Hunget \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ |

## Quy định về đánh số thứ tự

### Đánh số trang

Việc đánh số trang cần tuân thủ các quy định sau:

* Không đánh số: bìa đồ án, phần nhận xét, lời nói đầu, lời cam đoan, mục lục.
* Đánh bằng số La Mã (i, ii, iii, iv, …): ba danh mục và tóm tắt đồ án.
* Đánh bằng số thường (1, 2, 3, 4, …): các chương mục còn lại.

### Đánh số chương mục

Các chương được đánh số theo thứ tự 1, 2, 3, v.v. Các mục nhỏ trong một chương được đánh số theo chương và các mức trên nó. Ví dụ: mục đầu tiên của chương 3 sẽ được đánh số 3.1, các mục tiếp theo là 3.2, 3.3; các mục nhỏ hơn trong mục 3.1 sẽ được đánh số 3.1.1, 3.1.2, v.v.

### Đánh số hình vẽ và bảng biểu

Hình vẽ và bảng biểu phải được căn lề giữa và đánh thứ tự theo chương. Ví dụ: hình 1 của chương 2 sẽ được đánh thứ tự là Hình 2.1. Chú thích của hình vẽ (tên hình) được đặt ngay dưới hình vẽ. Chú thích của bảng biểu (tên bảng) được đặt ở trên bảng biểu. Ví dụ minh họa xem Hình 1.1 và Bảng 1.1 dưới đây. Tuyệt đối tránh việc hình (hoặc bảng) và tên tương ứng nằm ở hai trang khác nhau.



Hình 1.1 Sơ đồ khối của hệ thống

Tất cả các hình vẽ và bảng biểu phải được đề cập đến trong phần nội dung và phải được phân tích hay bình luận. Khi hình vẽ hay bảng biểu được nhắc đến trong phần nội dung, phải viết hoa chữ H và chữ B.

Bảng 1.1 Kết quả thí nghiệm

|  |  |  |  |
| --- | --- | --- | --- |
| **Lần thí nghiệm** | **Điện áp đo được**  **(mV)** | **Điện áp tham chiếu**  **(mV)** | **Sai lệch**  **(%)** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| … |  |  |  |

### Đánh số phương trình

Phương trình được đánh số theo số của chương, như hình vẽ và bảng biểu.

### Đánh số định nghĩa, định lý, và hệ quả

Các định nghĩa, định lý, hệ quả sẽ được đánh số theo số của chương và được sử dụng chung một chỉ số (không tách riêng). Ví dụ trong Chương 6, các định nghĩa, định lý, và hệ quả liên tiếp sẽ được đánh số theo thứ tự như sau: Định nghĩa 6.1, Định nghĩa 6.2, Định lý 6.3, Hệ quả 6.4, Định lý 6.5 v.v.

## Thứ tự các phần của đồ án

### Bìa quyển đồ án

#### Bìa chính

Bìa chính được in 1 mặt, bao gồm các thông tin sau (xem mẫu trong Phụ lục 1):

* Trường Học viện Kỹ thuật Mật mã (kèm theo logo chuẩn của trường)
* Khoa Công nghệ thông tin
* Đồ án thực tập cơ sở
* Tên đề tài
* Tên sinh viên, tên lớp và khoá
* Tên các giảng viên hướng dẫn (ghi đầy đủ học hàm và học vị)
* Tháng và năm viết đồ án

#### Bìa phụ

xem mẫu trong Phụ lục 2.

### Mẫu nhận xét

#### Nhận xét của giảng viên hướng dẫn

Biểu mẫu này dành cho giảng viên hướng dẫn nhận xét và chấm điểm (xem mẫu trong Phụ lục 3). Sinh viên có thể in 1 mặt hoặc 2 mặt của cùng 1 tờ giấy.

### Lời nói đầu

Phần này trình bày một cách rất khái quát (khoảng 1-2 trang) về bối cảnh hình thành và mục đích của đồ án. Lời cảm ơn đối với những tổ chức và cá nhân đã góp phần trong việc hoàn thiện đồ án (nếu có) nên đặt ở cuối mục này.

### Lời cam đoan

Hiện nay, theo quy định, sinh viên làm đồ án TTCS theo nhóm (tối đa 3 người). Đề tài nghiên cứu có thể là một ý tưởng do sinh viên tự đề xuất hoặc là một phần trong các dự án nghiên cứu lớn hơn, của giảng viên hướng dẫn. Do đó, tùy theo đặc thù của từng đồ án và đóng góp của bản thân, tác giả cần viết lời cam đoan cho phù hợp. Lời cam đoan thường là một đoạn văn liền mạch, dài không quá một nửa trang, bao gồm các thông tin sau:

* Họ tên, mã số, lớp, khóa của sinh viên
* Tên người hướng dẫn
* Tên đồ án
* Lời khẳng định về: nguồn gốc của nghiên cứu được công bố trong đồ án, tính trung thực của các kết quả và số liệu, tính rõ ràng trong việc việc trích dẫn, v.v.
* Cam kết về trách nhiệm
* Địa điểm và thời gian lập bản cam đoan
* Chữ ký kèm họ tên đầy đủ của người cam đoan

Sinh viên phải ký vào bản cam đoan này trước khi nộp quyển đồ án. Sau đây là một ví dụ về lời cam đoan:

|  |  |  |
| --- | --- | --- |
| Tôi là Lê Lung Linh, mã số sinh viên YYY, sinh viên lớp ZZZ, khóa TTT. Người hướng dẫn là TS. Nguyễn Văn A. Tôi xin cam đoan toàn bộ nội dung được trình bày trong đồ án *Áp dụng mô hình học sâu trong bài toán phân loại ảnh* là kết quả quá trình tìm hiểu và nghiên cứu của tôi. Các dữ liệu được nêu trong đồ án là hoàn toàn trung thực, phản ánh đúng kết quả đo đạc thực tế. Mọi thông tin trích dẫn đều tuân thủ các quy định về sở hữu trí tuệ; các tài liệu tham khảo được liệt kê rõ ràng. Tôi xin chịu hoàn toàn trách nhiệm với những nội dung được viết trong đồ án này.   |  |  | | --- | --- | |  | Hà nội, ngày 20 tháng 10 năm 2021  **Người cam đoan**  **Lê Lung Linh** | |

### Mục lục

Phần mục lục liệt kê tên và trang tương ứng của các chương (Heading 1), các mục lớn trong chương (Heading 2), và các mục nhỏ trong các mục lớn (Heading 3). Các mục nhỏ hơn nữa (Heading 4 trở lên) không nên liệt kê trong Mục lục.

Nếu soạn thảo bằng Microsoft Word, có thể sử dụng chức năng tự động tạo mục lục (References 🡪 Table of Contents). Chú ý để có thể sử dụng chức năng này, tiêu đề của chương và của các mục trong chương phải được định dạng đúng theo kiểu Heading như trên.

### Danh mục ký hiệu và chữ viết tắt

Một đồ án TTCS ngành kỹ thuật thường chứa nhiều ký hiệu và cụm từ quen thuộc (thường được viết tắt). Để đảm bảo tính tường minh và tiện lợi khi diễn đạt, sinh viên cần thực hiện như sau:

* Tại vị trí ký hiệu xuất hiện lần đầu tiên, phải giải thích ý nghĩa và thứ nguyên (đơn vị) ngay tại vị trí đó.
* Chỉ viết tắt các từ hoặc cụm từ được lặp đi lặp lại với tần suất cao (trong quyển đồ án) hoặc vẫn thường được viết tắt (trong kỹ thuật nói chung). Khi cần viết tắt, chỉ viết tắt kể từ lần thứ hai trở đi; trong lần thứ nhất, phải viết dạng đầy đủ kèm chữ viết tắt để trong ngoặc đơn.
* Để thuận tiện cho người đọc khi gặp lại ký hiệu hoặc chữ viết tắt ở vị trí khác, phải đưa ký hiệu hoặc chữ viết tắt vào Danh mục tương ứng ở phần đầu đồ án.

### Danh mục hình vẽ

Danh mục hình vẽ liệt kê tên và trang tương ứng của các hình vẽ trong đồ án. Nếu soạn thảo bằng Microsoft Word, có thể sử dụng chức năng tự động tạo danh mục hình vẽ (References 🡪 Insert Table of Figures, với Caption label là “Hình” đã được định nghĩa trong template này).

Chú ý: để đảm bảo khả năng cập nhật và đánh số hình tự động, phải sử dụng chức năng References 🡪 Insert Caption (với label là “Hình”) mỗi khi thêm chú thích bên dưới hình vẽ.

### Danh mục bảng biểu

Danh mục bảng biểu liệt kê tên và trang tương ứng của các bảng biểu trong đồ án (nếu có). Nếu soạn thảo bằng Microsoft Word, có thể sử dụng chức năng tự động tạo danh sách các bảng biểu (References 🡪 Insert Table of Figures, với Caption label là “Bảng” đã được định nghĩa trong template này).

Chú ý: để đảm bảo khả năng cập nhật và đánh số bảng tự động, phải sử dụng chức năng References 🡪 Insert Caption (với label là “Bảng”) mỗi khi thêm chú thích bên trên bảng biểu.

### Tóm tắt đồ án

Phần này trình bày những mục đích và các kết luận quan trọng nhất của đồ án (khoảng 1 trang).

### Phần mở đầu

Phần mở đầu giới thiệu vấn đề mà đồ án cần giải quyết, mô tả được các phương pháp hiện có để giải quyết vấn để, trình bày mục đích của đồ án song song với việc giới hạn phạm vi của vấn đề mà đồ án sẽ tâp trung giải quyết. Phần này cũng sẽ giới thiệu tóm tắt cấu trúc đồ án và nội dung tương ứng của các phần sẽ lần lượt được trình bày ở các chương tiếp theo.

### Nội dung chính

Thường được chia thành nhiều chương. Mỗi chương sẽ bắt đầu bằng một đoạn giới thiệu các phần chính được trình bày trong chương đó và kết thúc bằng một đoạn tóm tắt các kết luận chính của chương. Chú ý phân bố chiều dài mỗi chương cho cân đối và hợp lý.

Về cơ bản, nội dung đồ án thường chia thành hai phần: (1) các chương đầu là phần cơ sở lý thuyết; (2) các chương sau là phần sinh viên tự phát triển như: xây dựng thuật toán, xây dựng chương trình, mô phỏng, tính toán, thiết kế, chạy thử kết quả v.v.

### Kết luận

Kết luận chung cho các chương trong đồ án. Mục này cần nhấn mạnh những vấn đề đã giải quyết và vấn đề chưa được giải quyết để đưa ra các đánh giá về mức độ hoàn thành công việc. Đánh giá này thường bao gồm việc so sánh kết quả thu được với mục tiêu đề ra ban đầu. Sinh viên có thể bàn luận thêm về các hạn chế của nghiên cứu và nguyên nhân, vấn đề nảy sinh, v.v. để đưa ra các kiến nghị và đề xuất.

### Tài liệu tham khảo

Phần này liệt kê danh sách các tài liệu đã được dùng để tham khảo trong quá trình làm đồ án. Chi tiết về cách liệt kê tài liệu tham khảo và cách trích dẫn tài liệu tham khảo sẽ được trình bày trong Chương 2.

### Phụ lục

Phụ lục (nếu có) chứa các thông tin quan trọng có liên quan đến đồ án nhưng nếu để trong phần chính sẽ gây rườm rà. Thông thường các chi tiết sau thường được để trong phần phụ lục: kết quả thô (chưa qua xử lý), mã nguồn phần mềm, thông số kỹ thuật chi tiết của linh kiện, hình ảnh minh họa thêm, v.v.

## Một số điều cần lưu ý trong trình bày

### Lưu ý về dấu câu

#### Dấu chấm “.”

Dấu chấm được sử dụng để đánh dấu việc kết thúc một câu hoàn chỉnh khi câu đó không phải là câu hỏi và câu cảm thán. Dấu chấm được đặt ngay sát từ phía trước và theo sau nó là một dấu cách. Chữ cái đầu tiên sau dấu chấm phải được viết hoa.

|  |
| --- |
| Ví dụ:  Cách viết sai: Đây là đồ án TTCS của tôi.Anh có thể tìm thấy nhiều kiến thức bổ ích trong đó.  Cách viết sai: Đây là đồ án TTCS của tôi .Anh có thể tìm thấy nhiều kiến thức bổ ích trong đó.  Cách viết sai: Đây là đồ án TTCS của tôi . Anh có thể tìm thấy nhiều kiến thức bổ ích trong đó.  Cách viết sai: Đây là đồ án TTCS của tôi. anh có thể tìm thấy nhiều kiến thức bổ ích trong đó.  Cách viết đúng: Đây là đồ án TTCS của tôi. Anh có thể tìm thấy nhiều kiến thức bổ ích trong đó. |

Không sử dụng dấu chấm ở cuối tiêu đề các chương mục. Không nên sử dụng dấu chấm ở cuối các cụm từ, chuỗi từ, chú thích đứng đơn lẻ, khi chúng không tạo nên một câu hoàn chỉnh.

|  |
| --- |
| Ví dụ tiêu đề chương:  Cách viết sai: Chương 2. Hướng dẫn trình bày đồ án.  Cách viết đúng: Chương 2. Hướng dẫn trình bày đồ án |

#### Dấu phẩy “,”

Dấu phảy thường được sử dụng để ngăn cách các thành phần khi liệt kê danh sách. Dấu phảy được đặt ngay sát từ phía trước và theo sau nó là một dấu cách.

|  |
| --- |
| Ví dụ:  Năm chữ cái đầu tiên trong bảng chữ cái là a, b, c, d, và e. |

Dấu phảy cũng được sử dụng để ngăn cách trạng ngữ với các thành phần khác của câu khi trạng ngữ nằm ở đầu câu.

|  |
| --- |
| Ví dụ:  Trong chương này, tác giả trình bày các cơ sở lý thuyết quan trọng nhất của đề tài. |

Khi sử dụng trạng từ ở giữa câu, chúng được ngăn cách với các thành phần khác của câu bởi một cặp dấu phẩy, ở trước và sau trạng từ đó.

|  |
| --- |
| Ví dụ:  Công suất của động cơ này rất lớn, tuy nhiên, nó vẫn chưa được khai thác tối đa. |

Dấu phẩy cũng được sử dụng khi cần bổ sung các thông tin phụ. Các thông tin này có thể bỏ đi mà không ảnh hưởng đến nghĩa chính của câu.

|  |
| --- |
| Ví dụ:  Vi điều khiển AVR, được sản xuất bởi hãng Atmel, là một họ vi điều khiển có hiệu năng khá cao. |

#### Dấu hai chấm “:”

Dấu hai chấm thường được dùng khi liệt kê một danh sách. Nếu danh sách nằm ngay sau dấu hai chấm và không xuống dòng, dấu hai chấm được đặt ngay sát từ phía trước và theo sau nó là một dấu cách. Từ theo sau dấu hai chấm không viết hoa (trừ trường hợp bản thân từ đó cần viết hoa).

|  |
| --- |
| Ví dụ:  Các loại linh kiện có sẵn trong phòng thí nghiệm này gồm: điện trở, tụ điện, cuộn cảm, và diode. |

Nếu danh sách liệt kê được tách thành các dòng riêng biệt, có khá nhiều quy tắc khác nhau có thể áp dụng. Về cơ bản, ở mỗi dòng liệt kê, chữ cái đầu không nhất thiết phải được viết hoa và cuối dòng không nhất thiết phải có dấu câu. Nếu dấu phảy hoặc dấu chấm phẩy được sử dụng ở cuối mỗi dòng liệt kê, cần sử dụng dấu chấm khi kết thúc mục liệt kê cuối cùng.

|  |
| --- |
| Ví dụ 1:  Phần mềm này có những chức năng sau:   * đọc ảnh * sửa ảnh * lưu ảnh * trình chiếu   Ví dụ 2:  Sinh viên sẽ được cộng điểm khi:   * đi học đầy đủ, * tích cực phát biển, * làm bài tập lớn và bảo vệ tốt trước lớp.   Ví dụ 3:  Nội dung của chương này gồm:   * vật liệu bán dẫn và sự pha tạp * cấu tạo và nguyên lý làm việc của diode bán dẫn; * đặc tuyến và các tham số chính của diode bán dẫn; * sơ đồ tương đương của diode và một số ứng dụng điển hình.   Ví dụ 4:  Nội dung chính của một đồ án TTCS thường bao gồm:   * Phần mở đầu giới thiệu về đề tài. * Một chương giới thiệu về cơ sở lý thuyết. * Một hoặc nhiều chương trình bày các vấn đề về tính toán và thiết kế. * Một chương mô tả các thí nghiệm và kết quả thu được. |

Dấu hai chấm cũng có thể được sử dụng để trình bày phần giải thích cho một ý nằm trước nó.

|  |
| --- |
| Ví dụ:  Chiếc điện thoại này có một nhược điểm lớn: không sử dụng được wifi mỗi khi pin yếu. |

#### Dấu chấm phẩy “;”

Có thể hiểu một cách gần đúng rằng dấu chấm phảy “mạnh” hơn dấu phảy nhưng “yếu” hơn dấu chấm, xét về khả năng tách ý. Do đó, dấu chấm phảy có thể được sử dụng để tách hai mệnh đề độc lập về cấu trúc nhưng có mối liên hệ nhất định với nhau về ngữ nghĩa hoặc logic. Từ ngay sau dấu chấm phẩy không viết hoa (trừ trường hợp bản thân từ đó cần viết hoa).

|  |
| --- |
| Ví dụ:  Kết quả này có độ tin cậy chưa cao; tác giả sẽ thực hiện lại các thí nghiệm trong thời gian tới.  BJT điều khiển dòng điện bằng dòng điện; FET điều khiển dòng điện bằng điện áp. |

Dấu chấm phẩy có thể được sử dụng giữa hai vế câu độc lập được nối với nhau bởi các liên từ hoặc trạng từ quan hệ. Khi đó, dấu chấm phẩy được đặt ngay trước liên từ.

|  |
| --- |
| Ví dụ:  Quyến sách này rất hay và hiếm; do đó, nhiều người sẵn sàng mua nó với giá cao. |

Khi liệt kê nhiều đối tượng ở các nhóm khác nhau, dấu chấm phẩy được sử dụng để ngăn cách giữa các nhóm.

|  |
| --- |
| Ví dụ:  Mạch điện này cần khá nhiều linh kiện như: điện trở 1 kΩ, 10 kΩ, 100 kΩ; tụ điện 1 μF, 10 μF, 100 μF; transistor 2SC828, 2SA564, 2SC2383, 2SA1013. |

Chú ý: không sử dụng dấu chấm phẩy thay cho dấu phẩy trong câu ghép nhân quả.

|  |
| --- |
| Ví dụ:  Cách viết sai: Vì cáp quang ngầm bị đứt; tốc độ truy cập internet bị giảm đáng kể.  Cách viết đúng: Vì cáp quang ngầm bị đứt, tốc độ truy cập internet bị giảm đáng kể. |

### Lưu ý về hình vẽ và bảng biểu

Khi trình bày đồ án TTCS, sinh viên thường mắc các lỗi sau:

* Co kéo ảnh (thay đổi tỷ lệ dài/rộng) để tiện điền đầy các khoảng trống trong văn bản. Việc này tuy không ảnh hưởng nhiều đến nội dung minh họa nhưng có thể gây khó chịu cho người đọc, đặc biệt là khi các hình tròn bị kéo thành hình elip.
* Giữ đúng tỷ lệ nhưng để ảnh quá lớn so với tổng thể, gây mất cân đối. Cỡ ảnh được coi là hợp lý khi các chi tiết nhỏ trong ảnh có kích thước tương đương (nếu có thể) với chữ trong văn bản. Đặc biệt, khi trong ảnh có chữ, cỡ chữ trong ảnh và cỡ chữ trong văn bản nên tương đương nhau.
* Sử dụng hình ảnh chất lượng thấp để minh họa. Cách khắc phục: sinh viên được khuyến khích sử dụng ảnh có độ phân giải phù hợp khi insert ảnh từ ổ cứng hoặc sử dụng chế độ paste ảnh vector (thay vì bitmap) khi copy từ các phần mềm khác như Visio, Altium, v.v. Để paste ảnh vector (sau khi copy) có thể ấn tổ hợp phím Ctrl-Alt-V rồi chọn Enhanced Metafile hoặc vào Home > Paste > Paste Special > Enhanced Metafile.
* Sử dụng ảnh chụp của bảng thay cho bảng số liệu thật. Lỗi này không nghiêm trọng nhưng gây khó khăn khi cần điều chỉnh và có thể không sắc nét khi in.
* Sử dụng bảng khi không thực sự cần thiết. Trong nhiều trường hợp, một bảng số liệu cỡ 2 × 2 có hiệu quả kém hơn việc diễn đạt trực tiếp bằng lời.
* Các lỗi nên tránh khác: sử dụng hình minh họa không điển hình, sử dụng các ảnh có ngôn ngữ khác nhau, vẽ hình và tạo bảng có hình thức thiếu cân đối, v.v.

# CÁC ĐỐI TƯỢNG - PHƯƠNG THỨC VÀ ẢNH HƯỞNG GÂY RA TRÊN CÁC ĐỐI TƯỢNG

Loại lỗ hổng này xảy ra trên tất cả các thành phần của hệ thống thông tin. Chỉ cần sơ xuất trong quá trình cấu hình, cài đặt hệ thống, các đầu mối nhỏ trong cả một chuỗi cũng có thể gây ra lỗ hổng theo tính dây chuyền, khiến việc ngăn chặn lỗi hết sức muộn màng và gây nên nhiều tác hại nặng nề. Chương 2 sẽ đề cập tới các đối tượng đặc trưng có thể bị ảnh hưởng trong hệ thống. Bên cạnh đó là các ảnh hưởng này sẽ gây ra các tác động gì trên các đối tượng này.

## Liệt kê tài liệu tham khảo

### Cách liệt kê

Có nhiều cách khác nhau để liệt kê tài liệu tham khảo. Trong mẫu đồ án TTCS này, cách liệt kê tài liệu tham khảo theo quy định của IEEE sẽ được áp dụng. Theo đó, tài liệu tham khảo được đánh số thứ tự trong ngoặc vuông, ví dụ [1], [2], hay [3]-[6]. Thứ tự liệt kê là thứ tự xuất hiện của tài liệu được trích dẫn trong đồ án. Tài liệu tham khảo đã liệt kê bắt buộc phải được trích dẫn trong phần nội dung của đồ án. Về nguyên tắc, không phải dịch ra tiếng Việt tiêu đề cũng như nguồn gốc của tài liệu tham khảo có nguồn gốc tiếng nước ngoài. Tài liệu tham khảo cần có nguồn gốc rõ ràng và phải từ nguồn đáng tin cậy. Hạn chế trích dẫn tài liệu tham khảo từ các website, từ Wikipedia.

### Các loại tài liệu tham khảo

Các nguồn tài liệu tham khảo chính là sách, bài báo trong các tạp chí, bài báo trong các hội nghị khoa học, và các tài liệu tham khảo khác trên Internet. Sau đây là các quy định về cách liệt kê thông tin của các loại tài liệu tham khảo này. Các thông tin này phải đầy đủ để giúp cho người đọc có thể dễ dàng tìm lại được các tài liệu gốc khi cần. Chú ý cách trình bày các tài liệu tham khảo phải nhất quán và theo một format chung. Ví dụ: nếu tên các tác giả có phần tên riêng được viết tắt thì không nên viết đầy đủ tên riêng của bất cứ một tác giả nào, trong tài liệu đó và trong các tài liệu khác.

#### Sách

Thông tin về sách được sắp xếp theo thứ tự sau: tên các tác giả, *tên sách* (chữ nghiêng). Tên nhà xuất bản, và năm xuất bản. Ví dụ:

|  |
| --- |
| T. H. Cormen, C. E. Leiserson, and R. L. Rivet, *Introduction to Algorithm*. MIT Press, McGraw-Hill, 1990. |

#### Bài báo hoặc chương trong sách

Thông tin được sắp xếp theo thứ tự sau: tên các tác giả bài báo, “tên bài báo hoặc chương,” *tên sách* (chữ nghiêng), tên người soạn sách. Tên nhà xuất bản, năm xuất bản, số thứ tự trang của bài báo. Ví dụ:

|  |
| --- |
| J. W. DuBois, S. Schuetze-Coburn, S. Cumming, and D. Paolino, “Outline of discourse transcription,” in *Talking Data: Transcription and Coding in Discourse Research*, J. A. Edwards and M. D. Lampert, Ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1993, pp. 45-89.  G. O. Young, “Synthetic structure of industrial plastics,” in *Plastics*, vol. 3, *Polymers of Hexadromicon*, J. Peters, Ed., 2nd ed. New York: McGraw-Hill, 1964, pp. 15-64. |

#### Bài báo trong các tạp chí

Các thông tin về bài báo trong các tạp chí được sắp xếp theo thứ tự sau: tên tác giả, “tên bài báo,” *tên tạp chí* (chữ nghiêng), volume, số, số thứ tự trang của bài báo trong tạp chí, tháng và năm xuất bản. Ví dụ:

|  |
| --- |
| J. M. Airey, J. H. Rohfl, F. Brooks Jr., “Towards Image Realism with Interactive Update Rates in Complex Virtual Building Environments,” *Comptuer Graphics*, Vol. 24, No. 2, pp. 41-50, 1990.  R. E. Kalman, “New results in linear filtering and prediction theory,” *Journal of Basic Engineering*, ser. D, vol. 83, pp. 95-108, Mar. 1961.  E. H. Miller, “A note on reflector arrays,” *IEEE Transactions on Antennas and Propagation*, to be published. |

#### Bài báo trong các hội nghị có xuất bản

Các thông tin về bài báo trong các hội nghị có xuất bản kỷ yếu được sắp xếp theo thứ tự sau: tên tác giả, “tên bài báo,” *tên hội nghị* (chữ nghiêng), địa điểm và thời gian tổ chức hội nghị, số thứ tự trang trong kỷ yếu của hội nghị. Ví dụ:

|  |
| --- |
| S. Brandt, G. Nutt, T. Berk, M. Humphrey, “Soft Real time Application Execution with Dynamic Quality of Service Assurance,” in *Proceedings of the Sixth IEEE/IFIP International Workshop on Quality of Service*, Hawaii, USA, May 1998, pp. 154-163. |

#### Bài báo trong các hội nghị không xuất bản

Các thông tin về bài báo trong các hội nghị không xuất bản kỷ yếu được sắp xếp theo thứ tự sau: tên tác giả, “tên bài báo,” tên hội nghị, địa điểm và thời gian tổ chức hội nghị. Ví dụ:

|  |
| --- |
| K. Riley, “Language theory: Applications versus practice,” presented at the Conf. of the Modern Language Association, Boston, MA, December 27-30, 1990. |

#### Tài liệu trực tuyến

* Sách và bài báo trực tuyến:

|  |
| --- |
| J. Jones. (1991). *Networks* (2nd ed.) [Online]. Available: http://www.atm.com.  R. J. Vidmar. (1994). *On the use of atmospheric plasmas as electromagnetic reflectors* [Online]. Available FTP:atmnext.usc.edu Directory: pub/etext/1994 File: atmosplasma.txt |

* Nếu tham khảo tài liệu trên Internet, sinh viên phải ghi rõ URL của trang web và ghi ngày truy cập cuối cùng mà trang web đó vẫn còn có hiệu lực. Ví dụ:

|  |
| --- |
| http://www.dvb.org/, truy nhập cuối cùng ngày 10/1/2005. |

## Trích dẫn tài liệu tham khảo

Các nguyên tắc chung:

* Thông tin được trích dẫn nguyên văn phải được đặt trong dấu ngoặc kép.
* Số thứ tự của tài liệu được trích dẫn có thể được đặt ngay sau thông tin được trích dẫn hoặc đặt trước thông tin được trích dẫn. Ví dụ: Trong một bài viết có đoạn thông tin như sau:

|  |
| --- |
| Dân số Việt nam cho đến năm 2010 sẽ là 90 triệu người [15]. |

Cách viết như trên cho thấy, số liệu về dân số đã được tác giả tham khảo ở tài liệu tham khảo số 15 (báo cáo của uỷ ban dân số quốc gia). Cũng có thể trích dẫn thông tin trên như sau:

|  |
| --- |
| Theo báo cáo của uỷ ban dân số quốc gia [15], dân số Việt nam cho đến năm 2010 sẽ là 90 triệu người. |

* Một hình vẽ nếu được copy 100% thì phải ghi rõ nguồn gốc của hình vẽ đó ở phần chú thích của hình. Ví dụ:

|  |
| --- |
| Hình 3.1 Biểu đồ dân số các vùng của Việt nam [15] |

## Nộp đồ án

### Nộp bản cứng

Sinh viên (hoặc nhóm sinh viên với tối đa 3 thành viên làm chung một đề tài) nộp 01 quyển đồ án TTCS tại văn phòng khoa CNTT trước ngày bảo vệ ít nhất 03 ngày. Mỗi quyển đồ án phải có các đặc điểm sau:

* Được in một mặt hoặc hai mặt nhằm tiết kiệm không gian lưu trữ.
* Được đóng bìa mềm và có bìa bóng kính. Lưu ý: không dùng bìa cứng.
* Quyển phải có chữ ký của sinh viên sau Lời cam đoan và của giảng viên hướng dẫn.

### Nộp bản mềm

Sinh viên nộp bản mềm đồ án TTCS theo Giảng viên hướng dẫn. Mỗi sinh viên hoặc nhóm sinh viên phải nộp đủ toàn bộ các nội dung được làm trong đồ án TTCS (quyển file mềm dạng .docx và .pdf; project bao gồm cả mã nguồn và hướng dẫn cài đặt). Tất cả đặt trong cùng 1 thư mục và được đặt tên theo: manhom\_tendetai\_tengvhd\_nam.rar. Sinh viên hoặc nhóm sinh viên nộp cho GVHD dưới dạng link tới file đã gửi lên cloud (google, microsoft, v.v.) hoặc copy cho GVHD.

## Bản quyền kết quả nghiên cứu

Đồ án TTCS của sinh viên thường thuộc một trong hai kiểu sau đây:

* Thực hiện một nhiệm vụ nào đó để hoàn thành quá trình học tập. Sinh viên tự tìm điều kiện làm việc để hoàn thành đồ án. Do đó, sinh viên có quyền khai thác và sử dụng đồ án của mình vào những việc khác. Đồng thời, **Khoa Công nghệ thông tin có toàn quyền sử dụng các kết quả của đồ án và cam kết chia sẻ các kết quả trong bản đồ án cho tất cả những ai quan tâm và có yêu cầu**.
* Thực hiện một đề tài, một nhiệm vụ trong ý đồ chiến lược, trong chương trình khoa học và lao động sản xuất của giảng viên hướng dẫn, của cơ sở đào tạo (trung tâm, viện nghiên cứu, các công ty, v.v.), của cơ sở đào tạo cung cấp các phương tiện và điều kiện làm việc khác (máy móc, sách vở, điện thoại, truy cập internet, máy in, dụng cụ thiết bị thí nghiệm, kinh phí, v.v.). **Trong trường hợp này, toàn bộ bản quyền của đồ án không thuộc về sinh viên**. Sinh viên chỉ là một người tham gia thực hiện nên không được tuỳ tiện sử dụng ở những nơi khác với mục đích khác. Khi sinh viên thực hiện một đề tài theo hình thức này, vai trò của giảng viên hướng dẫn là định hướng, cung cấp các tài liệu tham khảo (nếu có), tạo điều kiện cơ sở vật chất (chỗ ngồi, máy tính, máy in, vật tư tiêu hao, phương tiện thông tin liên lạc, internet v.v.) để hoàn thành công việc.

# CÁC HÌNH THỨC KHAI THÁC LỖ HỔNG

Ở chương này sẽ đề cập tới những lỗi bảo mật từ đó thấy được tầm quan trọng của việc đảm bảo sự toàn vẹn của hệ thống nói chung và sự toàn vẹn của hệ điều hành nói riêng. Từng mục cũng sẽ có những ví dụ cụ thể, giúp cho ta có cái nhìn khái quát nhất từng lỗi.

## Xác thực không đầy đủ

Ở mức độ hoàn thiện nhất định, một chương trình với những câu lệnh có đặc quyền này gồm các yêu cầu các dịch vụ từ bước thứ 2, với một tập các câu lệnh có đặc quyền khác. Việc bảo vệ tính toàn vẹn cho hệ thống đòi hỏi việc xác thực phải kĩ lưỡng. Đối với hầu hết các hệ điều hành hiện nay, ranh giới giúp bảo toàn tính toàn vẹn hệ thống là ranh giới giữa chương trình điều khiển với chương trình người dùng. Khi đó, chương trình người dùng sẽ có những hạn chế nhất định, giúp cho hệ thống an toàn hơn. Bên cạnh đó, việc tách biệt này khiến cho các thành phần của hệ thống hoạt động độc lập, không làm gián đoạn quá trình hoạt động.

Các chương trình người dùng muốn sử dụng thì hệ thống sẽ gọi các chương trình con và nạp vào nhiều tham số. Và để gọi được thì người dùng cần thông qua chương trình điều khiển, lúc ấy, các dịch vụ được yêu cầu mới có thể thực thi. Việc tạp ra sự tách biệt này giữa các chương trình nhằm hạn chế được việc người dùng nào đó cố ý hay vô tình làm ảnh hưởng đến hoạt động của chương trình điều khiển, kéo theo ảnh hưởng dây chuyền các dịch vụ đang cung cấp cho người dùng khác. Nếu cơ chế kiểm tra các tham số đầu vào này không được chặt chẽ, việc kẻ tấn công có thể lợi dụng và đánh lừa chương trình điều khiển thực hiện được một yêu cầu vượt quá quyền hạn, từ đó gây ra sự mất an toàn cho toàn hệ thống. Và các trường cần phải xem xét cũng như kiểm tra kĩ như:

* Các kiểu và định dạng dữ liệu.
* Số lượng và thứ tự
* Phạm vi của giá trị
* Quyền truy cập vào các vị trí lưu trữ
* Tính nhất quán giữ các tham số (vị trí lữu trữ, …)

Từ những tham số trên, lỗ hổng này có thể có kịch bản nguy hiểm xảy ra nếu người dùng thành công trong việc nạp tham số không hợp lệ vào chương trình điều khiển. Việc chấp nhận một tham số bao gồm một địa chỉ bên ngoài không gian bộ nhớ được cấp phát cho người dùng đó có thể khiến:

* Chương trình có thể lấy được dữ liệu trái phép cho người dùng đó.
* Một tập hợp các điều kiện có thể được tạo ra gây ra sự cố cho hệ thống.
* Có thể thực thi được dòng lệnh nhằm điều khiển hệ thống.

Với một kịch bản có sẵn như sau có thể khiến cho hệ thống ảnh hưởng nghiêm trọng:

* Một lệnh, khi được thực thi, sẽ chuyển quyền điều khiển đến một điểm xác định trước trong chương trình của người dùng được nạp vào một thanh ghi.
* Một lệnh hệ thống sau đó được thực hiện làm cho các thanh ghi được lưu bằng chương trình điều khiển trong Vùng lưu đăng ký.
* Sau khi trả lại quyền kiểm soát cho người dùng, một lệnh gọi hệ thống khác sẽ được thực hiện. Trong số các tham số cho lệnh gọi hệ thống này, là một con trỏ (địa chỉ) phải trỏ đến một vị trí trong chương trình điều khiển. Địa chỉ này sẽ được sử dụng để chuyển quyền kiểm soát sang quy trình dịch vụ chương trình khác thích hợp. Đương nhiên, địa chỉ được cung cấp là vị trí trong Vùng lưu đăng ký nơi chuyển trở lại chương trình của người dùng đã được thực hiện bởi lệnh gọi hệ thống trước đó.
* Trong khi thực hiện lệnh gọi hệ thống thứ hai, quyền điều khiển được trả lại ở trạng thái điều khiển/giám sát cho người dùng, cho phép người dùng kiểm soát hệ thống.

## Xác thực không đồng nhất

Việc có nhiều định nghĩa của cùng một cấu trúc trong một hệ điều hành, thì sẽ có khả năng xảy ra mâu thuẫn giữa các định nghĩa này, việc đó sẽ tạo ra một lỗ hổng bảo mật. Lỗi này vượt ra ngoài lỗi xác thực thông số không đầy đủ. Một trường hợp có thể tồn tại trong đó mỗi quy trình của một số chương trình điều khiển sẽ kiểm tra hoàn toàn các điều kiện mà nó cho là hợp lệ; tuy nhiên, nhiều bộ tiêu chí không hoàn toàn nhất quán với nhau.

Một ví dụ về loại lỗ hổng này:

Hệ điều hành duy trì các thư mục (ví dụ: danh mục) của các tệp dữ liệu được sử dụng bởi hệ thống và người dùng. Nội dung của các thư mục này thường được truy cập bởi nhiều chương trình. Mỗi chương trình này quy chuẩn riêng về cách tạo thành một điều kiện hợp lệ trong hệ thống tệp.

Hãy xem xét điều gì đó cơ bản như các ký tự trong các tham số đại diện cho (các) tên của người dùng được cấp quyền truy cập tệp. Quy trình tạo mục nhập chỉ mục-tệp-chính có thể chấp nhận một ký tự (chẳng hạn như một ô trống được nhúng) là hợp lệ trong một tên quyền cụ thể; trong khi tất cả các chương trình giao diện khác sửa đổi/xóa các mục nhập chính tệp chỉ mục giả định các khoảng trống sẽ không bao giờ hợp lệ và do đó không chấp nhận chúng. Trong các điều kiện như vậy, các quyền đối với tệp cụ thể có thể được tạo (chẳng hạn như quyền truy cập được chia sẻ vào tệp) mà sau đó không thể bị xóa.

## Chia sẻ ngầm dữ liệu quan trọng

Để đảm bảo tính toàn vẹn, hệ điều hành phải có khả năng cô lập từng người dùng với tất cả những người khác và với chương trình điều khiển. Sự cô lập này liên quan đến các luồng điều khiển và thông tin. Bất cứ khi nào việc cô lập các thông tin không hoàn thiện, hệ thống có thể cho phép người dùng có đặc quyền cao hơn truy cập thông tin có đặc quyền thấp hơn hoặc có thể cho phép một người dùng truy cập thông tin của người dùng khác theo mong muốn của người dùng đó.

Trong nhiều hệ điều hành, phần điều khiển/chương trình của hệ điều hành chia sẻ không gian bộ nhớ với các chương trình người dùng, dưới dạng không gian làm việc hoặc là nơi thuận tiện để đưa thông tin liên quan đến chương trình người dùng đó. Đây là một chính sách thiết kế có chủ ý nhằm tạo điều kiện cho người dùng cá nhân hoá cho các tài nguyên mà họ sử dụng. Nếu người dùng yêu cầu hoạt động tệp hoặc các loại tài nguyên hệ thống khác, hệ thống sẽ duy trì thông tin và không gian làm việc cho yêu cầu của người dùng trong một khu vực. Bởi vì không gian làm việc được chia sẻ, nhưng ở một chế độ không có sẵn cho người dùng, những người triển khai hệ điều hành thường bất cẩn đối với trạng thái mà không gian làm việc còn lại sau khi nhận được yêu cầu của người dùng.

Ví dụ: chương trình điều khiển có thể sử dụng không gian làm việc như vậy để đọc trong chỉ mục chính của tệp người dùng cùng với mật khẩu được liên kết của họ như một phần của tìm kiếm dữ liệu do một người dùng nhất định yêu cầu. Chức năng này là cần thiết để hệ thống xác định rằng yêu cầu được hình thành đúng cách và được cấp quyền cho người dùng thực hiện yêu cầu. Nếu chương trình điều khiển thấy rằng yêu cầu không đúng, nó sẽ trả lại quyền điều khiển cho chương trình người dùng bắt nguồn yêu cầu, với dấu hiệu của lỗi trong yêu cầu. Tuy nhiên, trong ví dụ này, chương trình điều khiển không làm gì với thông tin còn lại trong không gian làm việc được chia sẻ. Do đó, người dùng giờ đây có thể truy cập không gian làm việc và lấy từ đó các mã định danh và mật khẩu mà sau đó có thể sử dụng để giả mạo vào hệ thống. Như được hiển thị bên dưới, ngay cả khi hệ thống xóa thông tin trước khi trả lại quyền kiểm soát cho chương trình của người dùng, người dùng có thể lấy thông tin thông qua một số hình thức xử lý đồng thời, chẳng hạn như thao tác I/O độc lập đọc từ không gian làm việc được đề cập. Có những biến thể khác của lỗ hổng này. Đôi khi các tệp công việc và không gian làm việc không bị xóa khi người dùng giải phóng chúng và người dùng khác có thể quét "bảng đen chưa được xóa" này khi không gian tệp hoặc không gian tạm thời chưa thể xóa được chỉ định tiếp theo.

Đôi khi các tác động đầy đủ của thông tin cung cấp cho người dùng không được các nhà thiết kế của hệ thống nhận ra. Ví dụ: các chương trình điều khiển thường xuyên xác nhận việc xử lý các yêu cầu dịch vụ của người dùng bằng cách đặt mã báo cáo lại/cờ trạng thái. Các điều kiện trả lại khác nhau (chẳng hạn như: "illegal parameter", "segment error", "password OK", v.v.) và các hình thức giao tiếp giữa các quá trình khác (ví dụ: xác nhận GỬI/NHẬN) có thể biểu thị thông báo cho phép người dùng bảo mật chặt chẽ.

## Xác thực bất đồng bộ

Tính toàn vẹn của hệ thống yêu cầu duy trì tính toàn vẹn của thông tin được truyền giữa các quá trình hợp tác hoặc trình tự chương trình điều khiển. Nếu tuần tự hóa không được thực thi trong cửa sổ thời gian giữa việc lưu trữ giá trị dữ liệu và tham chiếu của nó (hoặc giữa hai tham chiếu tuần tự), thì tính nhất quán của giá trị dữ liệu đó có thể bị phá hủy bởi một quy trình không đồng bộ.

Thông tin kiểm soát đặc biệt dễ bị sửa đổi bất cứ khi nào nó được đặt trong bộ nhớ mà quy trình cấp dưới có thể truy cập được. Đây đôi khi được gọi là vấn đề "kiểm tra thời gian sử dụng". Như được mô tả trong phần ngụ ý chia sẻ lỗ hổng dữ liệu đặc quyền, một hệ điều hành có thể thường xuyên chia sẻ không gian bộ nhớ với các chương trình người dùng. Không gian này có thể không chỉ được sử dụng để lưu trữ thông tin một cách thụ động mà còn có thể chứa các thông số hệ thống hoặc người dùng đại diện cho dữ liệu mà các hành động trong tương lai sẽ dựa trên đó. Bất cứ khi nào có "cửa sổ thời gian" giữa thời gian chương trình điều khiển xác minh một tham số và thời gian nó truy xuất tham số từ bộ nhớ dùng chung để sử dụng, một lỗ hổng bảo mật tiềm ẩn sẽ được tạo ra. Điều này là do các hệ điều hành hiện đại cho phép người dùng có hai hoặc nhiều hoạt động (quy trình) thực thi đồng thời và chia sẻ phân bổ bộ nhớ của người dùng đó. Ví dụ: người dùng có thể bắt đầu thao tác I/O và sau đó tiếp tục thực hiện chương trình của mình trong khi thao tác I/O hoàn tất.

Trong một ví dụ khác, người dùng chia sẻ thời gian có thể tạm thời tạm dừng một hoạt động bằng cách nhấn phím "chú ý" hoặc xác nhận tiêu cực (NAK) trên thiết bị đầu cuối của họ, thực hiện thao tác thứ hai, sau đó trả lại quyền điều khiển cho thao tác đầu tiên để hoàn thành. Một số hệ thống cho phép "đa nhiệm", trong đó hai hoặc nhiều chương trình đang chia sẻ bộ nhớ được chỉ định của một người dùng (không gian a-ddress) và đang thực thi đồng thời —có thể mỗi chương trình được thực thi đồng thời bởi CPU riêng biệt của một hệ thống máy tính đa xử lý.

Dưới đây là kịch bản một ví dụ về việc xác thực bất đồng bộ:

* Trong khung thời gian 1, người dùng đưa ra yêu cầu I/O cho chương trình điều khiển. Chương trình điều khiển xác nhận tất cả các tham số I/O (bao gồm cả con trỏ địa chỉ tới bộ đệm hợp lệ trong bộ nhớ được gán hợp pháp cho người dùng), xếp hàng yêu cầu I/O [phải đợi cho đến khi thiết bị thích hợp không còn bận), và sau đó trả lại quyền kiểm soát cho người dùng.
* Trong khung thời gian 2, người dùng thay thế con trỏ địa chỉ hợp lệ tới bộ đệm của mình bằng một địa chỉ trỏ đến một vị trí trong chương trình điều khiển.
* Khi I/O đang thực hiện trong khung thời gian 3, dữ liệu mà người dùng yêu cầu sẽ được đọc vào (hoặc ra khỏi) chương trình điều khiển thay vì bộ đệm hợp lệ của anh ta. Do đó, các hướng dẫn trong chương trình điều khiển có thể được phủ lên với các hướng dẫn do người dùng cung cấp hoặc thông tin về chương trình điều khiển đặc quyền có thể được đọc ra tệp của người dùng.

Trong một số hệ thống, chương trình điều khiển có thể sử dụng vùng lưu thanh ghi tràn, nằm trong vùng lưu trữ có thể truy cập của người dùng, bất cứ khi nào vùng lưu chính của chương trình điều khiển được lấp đầy. Thông tin đã lưu này thường chứa trạng thái chương trình và thông tin điều khiển.

Tình huống này có thể làm phát sinh một biến thể khác của lỗi xác thực không đồng bộ, nếu người dùng có thể sửa đổi thông tin điều khiển đó. Một ví dụ về nỗ lực thâm nhập như vậy như sau:

* Người dùng tạo một bản ghi I/O chỉ chứa một địa chỉ trỏ đến một vị trí mong muốn trong một trong các chương trình của người dùng.
* Sau đó, nhiều bản sao của bản ghi này sẽ được xuất ra dưới dạng tệp.
* Người dùng tiếp theo bắt đầu thao tác I/O để đọc các bản ghi này lặp đi lặp lại vào khu vực bộ nhớ của người dùng được chương trình điều khiển sử dụng làm bộ nhớ tràn cho các thanh ghi.
* Sau đó, người dùng đưa ra một yêu cầu dịch vụ hệ thống khiến chương trình điều khiển thực hiện một số lệnh gọi nội bộ màn hình lồng nhau, do đó làm tràn vùng lưu chính của nó. [Việc phát hành lặp lại các yêu cầu dịch vụ nhất định cũng có thể đạt được mục đích này.)
* Các thanh ghi được lưu bởi chương trình điều khiển trong vùng lưu tràn sẽ được phủ lên bởi các bản ghi đầu vào có chứa địa chỉ trỏ đến mã của người dùng. (Người dùng có thể cần một số điều chỉnh về thời gian để thực hiện điều này.)
* Khi chương trình điều khiển cuối cùng khôi phục các thanh ghi và trạng thái từ vùng tràn, nó sẽ chuyển quyền điều khiển sang chương trình của người dùng ở trạng thái giám sát/điều khiển - do đó cho phép người dùng toàn quyền kiểm soát hệ điều hành.

Hệ điều hành có thể lưu trữ thông tin trong một khoảng thời gian trong bộ nhớ phụ dùng chung cũng như trong bộ nhớ chính. Ví dụ: một hệ điều hành có thể có cung cấp điểm kiểm tra/khởi động lại để ghi lại trạng thái của một chương trình đang chạy tại các điểm khởi động lại thuận tiện dưới dạng kết xuất "điểm kiểm tra". Các kết xuất điểm kiểm tra này chứa cả dữ liệu người dùng và thông tin điều khiển chỉ định trạng thái điều khiển sẽ được chỉ định nếu chương trình được khởi động lại. Các kết xuất điểm kiểm tra được người dùng ghi lại trong một tệp được chỉ định cho hệ thống và người dùng đó có thể truy cập để thao tác. Thông qua thao tác như vậy, người dùng có thể khiến chương trình của mình được khởi động lại với thông tin trạng thái đã sửa đổi mang lại cho chương trình của anh ta các đặc quyền lớn hơn so với quy định ban đầu. Ví dụ, điều này có thể dẫn đến việc người dùng giành được quyền kiểm soát/giám sát trạng thái.

## Nhận dạng/ Xác thực/ Uỷ quyền không đầy đủ

Nhận dạng, ủy quyền và xác thực là các thành phần thiết yếu của khái niệm truy cập có kiểm soát. Sự ủy quyền — bản quyền truy cập được kiểm soát — đa phần dựa trên nhận dạng duy nhất, được xác thực của các cá nhân và tài nguyên. Một hệ điều hành về cơ bản là một trình quản lý tài nguyên. Do đó, một hệ điều hành phải đối mặt với các vấn đề về tính toàn vẹn bất cứ khi nào 1) nó không yêu cầu ủy quyền cho một cá nhân hoặc quy trình để truy cập vào bất kỳ dữ liệu nào hoặc sử dụng bất kỳ tài nguyên nào không phải có sẵn cho tất cả, hoặc 2) nó không xác định duy nhất các tài nguyên mà nó đang giải quyết.

Một lỗ hổng được tạo ra bất cứ khi nào hệ thống cho phép người dùng sở hữu một tập hợp các đặc quyền/khả năng bỏ qua hợp pháp các cơ chế bảo mật (truy cập có kiểm soát) và thực hiện một hành động chỉ được phép đối với những người dùng có các đặc quyền/khả năng khác nhau hoặc bất cứ khi nào nó cho phép tất cả người dùng thực hiện một hành động chỉ nên bị hạn chế đối với những người dùng có đặc quyền lớn hơn.

Một lỗ hổng nhận dạng/cách ly không đầy đủ có thể được tạo ra bất cứ khi nào một quy trình hệ thống dựa vào các cơ chế (được thực hiện ở nơi khác trong hệ thống) để đảm bảo sự cô lập của các tài nguyên hệ thống và do đó, tính đầy đủ của việc nhận dạng chúng. Đây có thể là một chính sách tồi nếu trên thực tế, các cơ chế không phù hợp.

Ví dụ, để được xác định duy nhất một chương trình phải được xác định bằng cả tên chương trình và tên của thư viện mà từ đó nó được tải. Nếu không, người dùng rất dễ tải trước một chương trình giả mạo có tên giống với một số quy trình chương trình điều khiển (phải được tải động khi cần thiết) và quy trình giả mạo này được chương trình điều khiển sử dụng thay cho quy trình xác thực .

Để thực hiện điều này, người dùng tạo một hoạt động dẫn đến chương trình điều khiển yêu cầu lại quy trình này. Trình tải sẽ thấy rằng quy trình được đặt tên (giả mạo) đã được tải (hợp pháp) và sẽ thiết lập chương trình kiểm soát để sử dụng chương trình giả mạo.

Ví dụ khác, cơ chế kiểm tra mật khẩu hoặc ID người dùng có thể bị phá vỡ nếu nó không giới hạn hiệu quả số lần người dùng có thể cố gắng đăng nhập vào hệ thống hoặc nếu nó không giới hạn thời gian đã trôi qua được phép hoàn tất đăng nhập. Trong những trường hợp như vậy, người dùng có thể sử dụng một máy tính khác để liệt kê đầy đủ tất cả các tổ hợp bit mật khẩu và do đó phá vỡ tính bảo mật của mật khẩu.

Một số hệ thống có tính năng kiểm tra ủy quyền mở rộng được liên kết với hầu hết, nhưng không phải tất cả, các phương thức truy cập tệp và không hạn chế việc sử dụng các phương thức truy cập không thực hiện kiểm tra ủy quyền. Bất kỳ người dùng nào có được tài liệu cho các phương pháp truy cập sau này (khả năng không cần thiết) chỉ cần sử dụng chúng để truy cập vào bất kỳ tệp nào trong hệ thống. Đây là một ví dụ về việc bỏ qua các cơ chế truy cập được kiểm soát.

Bảng 3-6 tóm tắt các danh mục và trình bày các ngoại lệ bổ sung của lỗ hổng nhận dạng, ủy quyền và xác thực không đầy đủ.

## Vi phạm giới hạn

Hệ điều hành được mô tả bằng cả cách thể hiện của nó trong hướng dẫn máy tính và bằng tài liệu bên ngoài của nó. Bất cứ khi nào hai mô tả này khác nhau, một lỗ hổng toàn vẹn có thể tồn tại. Một lỗ hổng bảo mật được tạo ra bất cứ khi nào giới hạn hệ điều hành được lập thành văn bản hoặc quy trình cấm theo quy trình không được thực thi.

Ví dụ: những người triển khai hệ điều hành không được xử lý tình huống đạt đến giới hạn trên về kích thước của bảng hoặc bộ đệm hoặc khi không gian hàng đợi trở nên bão hòa. Tài liệu có thể chỉ định chính xác các giới hạn trên và cấm vượt quá giới hạn, nhưng nếu người dùng cố tình hoặc vô tình gây ra tràn hoặc quá tải, thì các kết quả khác nhau có thể xảy ra - đôi khi có thể xảy ra sự cố hệ thống, đôi khi hoạt động của hệ thống bị suy giảm dữ liệu nhạy cảm có thể bị mất và trong một số trường hợp, dữ liệu đó có thể bị xâm phạm.

## Lỗi logic

Trong bất kỳ hệ điều hành chính nào, đều có - tại bất kỳ thời điểm nào - một số "lỗi" hoặc lỗi logic. Nhiều lỗi trong số này phụ thuộc vào các tình huống thời gian không thể thống kê được và không nằm trong tầm kiểm soát của bất kỳ người dùng cá nhân nào. Tuy nhiên, một số lỗi logic này có thể bị người dùng cố ý khai thác để làm tổn hại đến tính toàn vẹn của hệ thống.

Một ví dụ liên quan đến việc xử lý lỗi không chính xác. Ví dụ, hệ thống có thể thực hiện một hành động bất hợp pháp trước khi báo hiệu một điều kiện lỗi. Ví dụ, hãy xem xét rằng một người dùng yêu cầu một loạt các sửa đổi được thực hiện đối với mục nhập thư mục tệp của một người dùng khác, mà người dùng đầu tiên có quyền chỉ đọc. Nếu hệ thống thực hiện các hành động được yêu cầu và sau đó xác định rằng các hành động vượt quá sự cho phép của người dùng yêu cầu, thì tính bảo mật của hệ thống đã bị xâm phạm thông qua một lỗi logic. Điều này cũng có thể xảy ra nếu một dịch vụ hệ thống như kết xuất bộ nhớ được khởi tạo đồng thời với việc kiểm tra ủy quyền của người dùng để yêu cầu dịch vụ được chỉ định cho các khu vực lưu trữ được chỉ định. Vào thời điểm lỗi được phát hiện, các khu vực cấm có thể đã được liệt kê.

Ở mức độ tinh tế hơn, người dùng có thể phát hiện ra rằng các hướng dẫn số học nửa từ được sử dụng để xử lý không đúng tham số địa chỉ trả lại nửa từ. Nếu số nửa từ lớn nhất có thể được sử dụng làm địa chỉ, có thể xảy ra hiện tượng tràn không lường trước được, dẫn đến địa chỉ trỏ đến vị trí 0001 trong bộ nhớ chương trình điều khiển, điều này có thể gây ra sự cố hệ thống.

Trong một tình huống khác, bằng cách nhấn vào nút ngắt "chú ý" (hoặc NAK) trên thiết bị đầu cuối của anh ấy trong quá trình in thông báo lỗi đăng nhập, người dùng có thể khiến hệ thống chấp nhận sai một nỗ lực đăng nhập mới mà không tiến bộ đếm được đặt thành ghi lại số lần đăng nhập trước đó. Lỗi hệ thống này cho phép tự động hóa việc liệt kê đầy đủ các mật khẩu, không có dấu hiệu cho người vận hành hệ thống biết rằng điều này đang diễn ra.

Trong một ví dụ cuối cùng về xử lý lỗi không chính xác, đôi khi xảy ra trường hợp cơ chế bảo vệ bị vô hiệu hóa hoặc sửa đổi do lỗi người dùng (cố ý) và không thể đặt lại khi chương trình điều khiển sau đó trả lại quyền điều khiển cho người dùng. Điều này có thể dẫn đến việc người dùng nhận được các đặc quyền trái phép.

Có thêm hai loại lỗi logic có thể khai thác. Những điều này được liệt kê ở đây cho đầy đủ và không có ví dụ:

* Bắt đầu hoặc kết thúc quá trình/chức năng không chính xác.
* Bẫy lỗi phần mềm trạng thái kiểm soát.

# KẾT LUẬN

## Kết luận chung

Xem Mục 1.3.12

## Hướng phát triển

(Nếu có)

## Kiến nghị và đề xuất

(Nếu có)

# TÀI LIỆU THAM KHẢO

1. T. H. Cormen, C. E. Leiserson, and R. L. Rivet, *Introduction to Algorithm*. MIT Press, McGraw-Hill, 1990.
2. J. W. DuBois, S. Schuetze-Coburn, S. Cumming, and D. Paolino, “Outline of discourse transcription,” in *Talking Data: Transcription and Coding in Discourse Research*, J. A. Edwards and M. D. Lampert, Ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1993, pp. 45-89.
3. J. M. Airey, J. H. Rohfl, F. Brooks Jr., “Towards Image Realism with Interactive Update Rates in Complex Virtual Building Environments,” *Comptuer Graphics*, Vol. 24, No. 2, pp. 41-50, 1990.
4. S. Brandt, G. Nutt, T. Berk, M. Humphrey, “Soft Real time Application Execution with Dynamic Quality of Service Assurance,” in *Proceedings of the Sixth IEEE/IFIP International Workshop on Quality of Service*, Hawaii, USA, May 1998, pp. 154-163.
5. K. Riley, “Language theory: Applications versus practice,” presented at the Conf. of the Modern Language Association, Boston, MA, December 27-30, 1990.
6. J. Jones. (1991). *Networks* (2nd ed.) [Online]. Available: http://www.atm.com.

# PHỤ LỤC

## Phụ lục 1. Mẫu trang bìa chính của đồ án

(Xem trang sau)

|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA CÔNG NGHỆ THÔNG TIN**  Logo HvKTMM  ĐỒ ÁN MÔN HỌC  **THỰC TẬP CƠ SỞ**  **Đề tài:**  **ÁP DỤNG MÔ HÌNH HỌC SÂU TRONG BÀI TOÁN PHÂN LOẠI ẢNH**  Sinh viên thực hiện: LÊ LUNG LINH AT150302  NGUYỄN VĂN NAM AT150033  TRẦN THU HÀ AT150345  Nhóm 68  Giảng viên hướng dẫn: ThS. LÊ ĐỨC THUẬN  Hà Nội, 10-2021 |

## Phụ lục 2. Mẫu trang bìa phụ của đồ án

(Xem trang sau)

|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA CÔNG NGHỆ THÔNG TIN**  Logo HvKTMM  ĐỒ ÁN MÔN HỌC  **THỰC TẬP CƠ SỞ**  **Đề tài:**  **ÁP DỤNG MÔ HÌNH HỌC SÂU TRONG BÀI TOÁN PHÂN LOẠI ẢNH**  Sinh viên thực hiện: LÊ LUNG LINH AT150302  NGUYỄN VĂN NAM AT150033  TRẦN THU HÀ AT150345  Nhóm 68  Giảng viên hướng dẫn: ThS. LÊ ĐỨC THUẬN    Hà Nội, 10-2021 |

## Phụ lục 3. Mẫu nhận xét đồ án

(Xem trang sau)

**ĐÁNH GIÁ QUYỂN ĐỒ ÁN THỰC TẬP CƠ SỞ**

(Dùng cho giảng viên hướng dẫn)

Tên giảng viên đánh giá:

Họ và tên Sinh viên: MSSV:

Tên đồ án:

**Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:**

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Có sự kết hợp giữa lý thuyết và thực hành (20)** | | | | | | |
| 1 | Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đồ án | 1 | 2 | 3 | 4 | 5 |
| 2 | Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế) | 1 | 2 | 3 | 4 | 5 |
| 3 | Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề | 1 | 2 | 3 | 4 | 5 |
| 4 | Có kết quả mô phỏng/thưc nghiệm và trình bày rõ ràng kết quả đạt được | 1 | 2 | 3 | 4 | 5 |
| **Có khả năng phân tích và đánh giá kết quả (15)** | | | | | | |
| 5 | Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống | 1 | 2 | 3 | 4 | 5 |
| 6 | Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng. | 1 | 2 | 3 | 4 | 5 |
| 7 | Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai. | 1 | 2 | 3 | 4 | 5 |
| **Kỹ năng viết quyển đồ án (10)** | | | | | | |
| 8 | Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định | 1 | 2 | 3 | 4 | 5 |
| 9 | Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.) | 1 | 2 | 3 | 4 | 5 |
| **Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)** | | | | | | |
| 10a | Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế | 5 | | | | |
| 10b | Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest. | 2 | | | | |
| 10c | Không có thành tích về nghiên cứu khoa học | 0 | | | | |
| **Điểm tổng** | | **/50** | | | | |
| **Điểm tổng quy đổi về thang 10** | |  | | | | |

***Nhận xét khác*** *(về thái độ và tinh thần làm việc của sinh viên)*

|  |  |
| --- | --- |
|  | Ngày: …/…/20…  **Người nhận xét**  (Ký và ghi rõ họ tên) |