

Sự bảo vệ



Bài tập thực hành

- 14.1** Sự khác biệt chính giữa danh sách khả năng và danh sách truy cập là gì? **Trả lời:** Danh sách truy cập là danh sách cho từng đối tượng bao gồm các miền có tập hợp quyền truy cập không có gì cho đối tượng đó. Danh sách khả năng là danh sách các đối tượng và các hoạt động được phép trên các đối tượng đó cho mỗi miền.
- 14.2** Tập MCP Burroughs B7000 / B6000 có thể được gắn thẻ là dữ liệu nhạy cảm. Khi một tệp như vậy bị xóa, vùng lưu trữ của nó sẽ bị ghi đè bởi một số bit ngẫu nhiên. Vì mục đích gì mà một chương trình như vậy sẽ hữu ích?
Trả lời: Điều này sẽ hữu ích như một biện pháp bảo mật bổ sung để không thể truy cập nội dung cũ của bộ nhớ bởi một chương trình khác, dù cố ý hay ngẫu nhiên, bởi một chương trình khác. Điều này đặc biệt hữu ích cho bất kỳ thông tin được phân loại cao.
- 14.3** Trong hệ thống bảo vệ vòng, cấp 0 có quyền truy cập lớn nhất vào các đối tượng và cấp n (lớn hơn 0) có ít quyền truy cập hơn. Quyền truy cập của một chương trình ở một mức cụ thể trong cấu trúc vòng được coi là một tập hợp các khả năng. Mỗi quan hệ giữa các khả năng của một miền ở cấp độ là gì và một miền ở cấp độ t đến một đối tượng (cho $t > 0$)? **Trả lời:** D_t là một tập hợp con của D_{t-1} .
- 14.4** Hệ thống RC 4000 (và các hệ thống khác) đã định nghĩa một cây quy trình (được gọi là cây quy trình) sao cho tất cả các con của một quy trình chỉ được cấp tài nguyên (đối tượng) và quyền truy cập bởi tổ tiên của chúng. Vì vậy, một người con cháu không bao giờ có thể có khả năng làm bất cứ điều gì mà tổ tiên của nó không thể làm được. Gốc của cây là hệ điều hành, có khả năng làm bất cứ điều gì. Giả sử tập hợp các quyền truy cập được biểu diễn bằng một ma trận truy cập, $MOT(x, y)$ xác định quyền truy cập của quy trình x đến

vật y . Nếu x là hậu duệ của z , mối quan hệ giữa $MỘT(x, y)$ và $MỘT(z, y)$ cho một đối tượng tùy ý? **Trả lời:** $MỘT(x, y)$ là một tập hợp con của $MỘT(z, y)$.

14,5 Những vấn đề bảo vệ nào có thể phát sinh nếu một ngăn xếp được chia sẻ được sử dụng để truyền tham số?

Trả lời: Nội dung của ngăn xếp có thể bị xâm phạm bởi (các) quy trình khác chia sẻ ngăn xếp.

14,6 Hãy xem xét một môi trường máy tính trong đó một số duy nhất được liên kết với từng quy trình và từng đối tượng trong hệ thống. Giả sử rằng chúng tôi cho phép một quy trình với số n để truy cập một đối tượng có số m chỉ nếu $n > m$. Chúng ta có loại cấu trúc bảo vệ nào? **Trả lời:** Cấu trúc thứ bậc.

14,7 Hãy xem xét một môi trường máy tính trong đó một quy trình được cấp đặc quyền chỉ truy cập vào một đối tượng n lần. Đề xuất phương án thực hiện chính sách này.

Trả lời: Thêm một bộ đếm số nguyên với khả năng.

14,8 Nếu tất cả các quyền truy cập đối với một đối tượng bị xóa, đối tượng đó không thể truy cập được nữa. Tại thời điểm này, đối tượng cũng sẽ bị xóa và không gian mà nó chiếm sẽ được trả lại cho hệ thống. Đề nghị thực hiện hiệu quả chương trình này.

Trả lời: Số lượng tham chiếu.

14,9 Tại sao lại khó bảo vệ một hệ thống trong đó người dùng được phép thực hiện I / O của riêng họ?

Trả lời: Trong các chương trước, chúng ta đã xác định sự khác biệt giữa chế độ nhân và chế độ người dùng, trong đó chế độ hạt nhân được sử dụng để thực hiện các hoạt động đặc quyền như I / O. Một lý do tại sao I / O phải được thực hiện trong chế độ hạt nhân là I / O yêu cầu truy cập phần cứng và quyền truy cập thích hợp vào phần cứng là cần thiết cho tính toàn vẹn của hệ thống. Nếu chúng tôi cho phép người dùng thực hiện I / O của riêng họ, chúng tôi không thể đảm bảo tính toàn vẹn của hệ thống.

14,10 Danh sách khả năng thường được giữ trong không gian địa chỉ của người dùng. Làm thế nào để hệ thống đảm bảo rằng người dùng không thể sửa đổi nội dung của danh sách?

Trả lời: Danh sách khả năng được coi là "đối tượng được bảo vệ" và chỉ được truy cập gián tiếp bởi người dùng. Hệ điều hành đảm bảo người dùng không thể truy cập trực tiếp vào danh sách khả năng.