HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Các yêu cầu hệ điều hành an toàn

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

Nội dung

- Các yêu cầu an toàn

Các yêu cầu

- Hệ điều hành an toàn là hệ điều hành mà việc thực thi truy nhập thỏa mãn các yêu cầu của giám sát tham chiếu
- Bộ giám sát tham chiếu xác định các thuộc tính cần và đủ của bất kỳ hệ thống nào để thực thi hệ thống bảo vệ một cách an toàn

Các thuộc tính của bộ giám sát truy nhập

1. *Ngăn chặn hoàn toàn (complete mediation)*: hệ thống đảm bảo cơ chế thực thi truy nhập ngăn chặn toàn bộ các thao tác nhạy cảm với an ninh
2. *Chống xâm nhập (Tamper-proof)*: hệ thống đảm bảo có chế thực thi truy nhập, kể cả hệ thống bảo vệ, không thể bị sửa đổi bởi các tiến trình (chương trình) không tin cậy
3. *Thẩm tra được (verifiable):* Cơ chế thực thi truy nhập, kể cả hệ thống bảo vệ, phải đủ nhỏ để có thể kiểm tra và phân tích, tính đúng đắn của nó có thể được đảm bảo. Nói cách khác, phải có khả năng chứng minh hệ thống thực thi các mục tiêu an toàn một cách đúng đắn

Giới thiệu kiến trúc an toàn

- Xây dựng hệ thống máy tính cần phải cân đối rất nhiều các yêu cầu như tính năng, độ linh hoạt, hiệu năng, tính dễ dùng và chi phí.
- An toàn đơn giản là một dạng yêu cầu khác và nếu có xung đột các tính năng an toàn phải cân đối với các tính năng khác tùy theo mức độ quan trọng với hệ thống

Giới thiệu kiến trúc an toàn

- Kiến trúc an toàn là mô tả chi tiết toàn bộ các khía cạnh của hệ thống liên quan đến vấn đề an toàn cùng với các nguyên tắc thiết kế
  - Kiến trúc an toàn tốt giống như thiết kế tổng thể mô tả ở mức khái quát quan hệ giữa các bộ phận then chốt theo cách mà chúng phải thỏa mãn các yêu cầu về an toàn.
  - Kiến trúc an toàn cần mô tả các chi tiết của quá trình xây dựng hệ thống mà qua đó các yêu cầu an toàn được đảm bảo

Một số nguyên tắc kiến trúc an toàn

1. Xem xét vấn đề an toàn ngay từ đầu
2. Lường trước các yêu cầu về an toàn
3. Giảm thiểu và cách ly các biện pháp an toàn
4. Thực hiện quyền tối thiểu
5. Giữ các tính năng an ninh thân thiện
6. An toàn không dựa trên bí mật

Xem xét vấn đề an toàn ngay từ đầu

- Coi trọng vấn đề an toàn ngang bằng như các tính năng vận hành của hệ thống và phải được tích hợp đầy đủ vào hệ thống
- Việc thiếu quan tâm đến vấn đề an toàn sẽ dễ dẫn đến việc không kiểm soát được các phí tổn để bổ sung các tính năng an toàn

Lường trước các yêu cầu về an toàn

- Kiến trúc an toàn cần có tầm nhìn xa đề cập tới các tính năng an toàn tiềm năng thậm chí chưa có kế hoạch sử dụng ngay lập tức. Việc này làm tăng chi phí một chút cho việc nâng cao tính an toàn.
- Điểm then chốt cho việc gắn kết hợp lý các tính năng an toàn tương lai là việc hiểu rõ các yêu cầu về an toàn của hệ thống máy tính. Hơn thế cần phải mô tả một cách tường minh nhất các yêu cầu trong tương ai này trong kiến trúc an toàn.
- Lường trước các yêu cầu an toàn không chỉ ảnh hưởng đến mức độ cần thiết làm hệ thống an toàn hơn trong tương lai mà còn giúp xác định liệu tính an toàn của hệ thống có thể được nâng cao hay không.
- Vấn đề khác là chính sách an toàn. Thay đổi trong chính sách an toàn có thể dẫn đến hậu quả tai hại với các ứng dụng đang hoạt động tốt mà nay xung đột với chính sách mới.

Giảm thiểu và cách ly các biện pháp an toàn

- Để đạt được độ tin cậy cao về an toàn của hệ thống, người thiết kế cần giảm thiểu kích cỡ và độ phức tạp của các phần liên quan tới an toàn của thiết kế. Lý do chính hệ điều hành không an toàn là kích cỡ quá lớn của chúng làm cho khó nắm bắt tổng thể hệ thống. Vì vậy, ngay cả với hệ thống phức tạp, cần giữa phần cốt lõi (liên quan đến an toàn) nhỏ và định nghĩa rõ ràng.

Giảm thiểu và cách ly các biện pháp an toàn

- Điểm then chốt để giảm thiểu các bộ phận liên quan tới an toàn của hệ điều hành là chỉ dùng số ít các cơ chế thực thi an toàn. Như vậy, bắt buộc các hành động liên quan tới an toàn được giữ trong một số ít phần cách ly. Thực tế với hệ điều hành rất khó đặt được điều này. Vấn đề an toàn liên quan tới rất nhiều chức năng khác nhau của hệ thống như quản lý file hệ thống, quản lý bộ nhớ ...
  - Ví dụ như xử lý truy nhập file bằng mật khẩu, quyền truy nhập,...

Giảm thiểu và cách ly các biện pháp an toàn

- Khi các cơ chế an toàn đơn giản, dễ nhận biết và cách ly thì dễ dàng triển khai các cơ chế bảo vệ bổ sung để tránh các thiệt hại do lỗi tại các phần khác của hệ thống.
  - Các đoạn mã liên quan đến an toàn có thể bảo vệ chống ghi

Thực hiện quyền tối thiểu

- Các chủ thể (người dùng hay chương trình) cần được cấp quyền không hơn mức cần thiết để thực hiện công việc. Như vậy, thiệt hại do lỗi hay phần mềm xấu được giới hạn.
- Quyền thể hiện ở các cơ chế phần cứng hạn chế việc sử dụng các câu lệnh đặc biệt (lệnh vào ra) và truy nhập tới các vùng ô nhớ.
- Quyền thể hiện ở các cơ chế phần mềm, như trong hệ điều hành, cho phép chương trình người dùng qua các biện pháp kiểm soát truy nhập hay thực thi các chức năng hệ thống.

Thực hiện quyền tối thiểu

- Quyền tối thiểu còn thể hiện trong nguyên tắc phát triển hệ thống. Như bằng việc đặt ra các tiêu chuẩn lập trình hạn chế các truy nhập tới các dữ liệu toàn cục (global data), như vậy giảm khả năng lỗi từ vùng này tác động tới vùng khác
- Quyền tối thiểu thể hiện trong việc quản trị người dùng và hệ thống. Người dùng và người quản trị không nên được cấp truy nhập nhiều hơn với công việc của họ.

Giữ các tính năng an ninh thân thiện

- Các cơ chế an toàn không được ảnh hưởng tới người dùng tuân thủ quy định
  - Cơ chế an toàn phải trong suốt với người dùng bình thường. Việc can thiệp vào công việc hàng ngày làm giảm năng suất và khiến người dùng tìm cách bỏ qua các cơ chế an toàn.
- Thuận tiện cho người dùng để cấp quyền truy nhập truy nhập
  - Người dùng cần được đảm bảo cung cấp đủ truy nhập khi cần thiết và tránh các thủ tục rườm rà và phức tạp.
- Thuận tiện cho người dùng để hạn chế truy nhập
  - Đảm bảo khả năng bảo vệ thông tin người dùng khi cần thiết

An toàn không dựa trên bí mật

- Ngoại trừ việc quản lý mật khẩu, đích chính của kiến trúc an toàn tránh phụ thuộc vào tính bí mật để đảm bảo an toàn.
  - Việc giả định người dùng không thể bẻ khóa hệ thống vì không biết mã nguồn hay tài liệu về hệ thống không an toàn chút nào.
  - Việc công khai mã nguồn hệ thống có khả năng cải thiện tính an toàn nhờ có khối lượng người dùng lớn hơn giúp phát hiện và sửa chữa các khiếm khuyết