



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0023341

(51)⁷ G06F 21/30

(13) B

(21) 1-2013-03191

(22) 29/11/2012

(86) PCT/CN2012/085579 29/11/2012

(87) WO2013/079010A1 06/06/2013

(30) 201110387409.X 29/11/2011 CN

(45) 27/04/2020 385

(43) 27/10/2014 319A

(73) Tencent Technology (Shenzhen) Company Limited (CN)

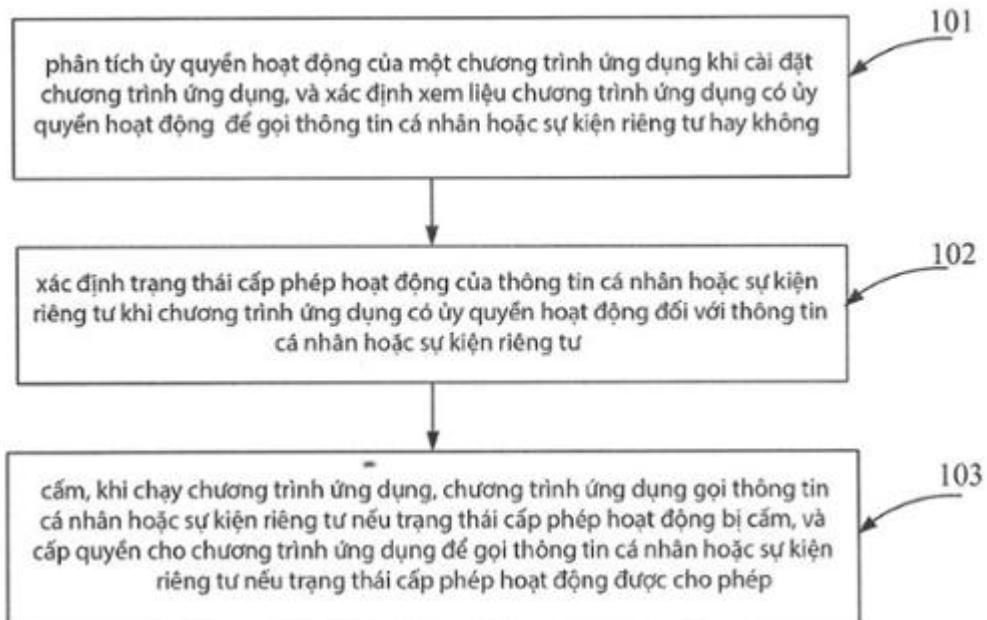
Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen City,
Guangdong 518044 China

(72) LU, Zhaohua (CN)

(74) Công ty TNHH Sở hữu trí tuệ ALNGUYEN (ALNGUYEN IP CO.,LTD.)

(54) PHƯƠNG PHÁP NGĂN CHẶN CÁC CHƯƠNG TRÌNH ỨNG DỤNG XÂM
PHẠM QUYỀN RIÊNG TƯ VÀ THIẾT BỊ DI ĐỘNG

(57) Sáng chế đề cập đến phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư và thiết bị di động, thuộc lĩnh vực bảo mật thông tin. Phương pháp này bao gồm phân tích ủy quyền hoạt động của một chương trình ứng dụng khi cài đặt chương trình ứng dụng, và xác định xem liệu chương trình ứng dụng có ủy quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không; xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi chương trình ứng dụng có ủy quyền hoạt động đối với thông tin cá nhân hoặc sự kiện riêng tư; cấm, khi chạy chương trình ứng dụng, chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động bị cấm, và cấp quyền cho chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép. Giải pháp kỹ thuật của sáng chế có thể xác định được trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi cài đặt chương trình ứng dụng. Phương pháp xác định là gọn và hoàn hảo. Người dùng không bắt buộc phải có trình độ chuyên môn nhất định, nhờ vậy giảm khó khăn thao tác cho người dùng.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực bảo mật thông tin, và cụ thể hơn là đề cập đến phương pháp ngăn chặn các chương trình ứng dụng xâm phạm quyền riêng tư và đề cập đến thiết bị di động.

Tình trạng kỹ thuật của sáng chế

Với việc phát triển nhanh chóng của các công nghệ máy tính, ngày càng nhiều các chương trình ứng dụng được phát triển và cài đặt trên các thiết bị di động, làm phong phú thêm cho cuộc sống khi cung cấp cho con người thêm nhiều tiện lợi. Tuy nhiên, việc phát triển nhanh chóng các công nghệ máy tính cũng tạo ra rất nhiều virus và Trojan (chương trình gián điệp). Các virus và Trojan này được cấy vào các chương trình ứng dụng. Khi cài đặt các chương trình ứng dụng có các virus và Trojan độc được cấy vào các thiết bị di động, các virus và Trojan được cấy vào này có thể đánh cắp thông tin cá nhân của người dùng. Điều này sẽ khiến người dùng bị thiệt hại về kinh tế và tinh thần ở một mức độ nhất định.

Hiện nay, các phương pháp chống xâm nhập của các phần mềm độc thường được sử dụng là đề phòng bằng cách quét trước. Cụ thể là, trước tiên mẫu của các chương trình độc xâm phạm quyền riêng tư được xác định, và sau đó các đặc điểm của các chương trình này được trích xuất để bổ sung vào cơ sở dữ liệu các chương trình độc. Khi cài đặt hoặc chạy các chương trình ứng dụng, các công nghệ quét có các công cụ chống virus được sử dụng để quét các chương trình ứng dụng này. Khi các chương trình ứng dụng được thấy là khớp với các đặc tính trong cơ sở dữ liệu chương trình độc, thì các chương trình ứng dụng này sẽ được xác định là các virus. Khi đó, đề xuất phát hiện và loại bỏ virus sẽ được đưa ra

cho người dùng, ví dụ, thông qua việc gỡ cài đặt hoặc buộc gỡ cài đặt các chương trình ứng dụng này.

Dựa trên những mô tả trên đây, có thể thấy rằng cần phải có các mẫu và sau đó trích xuất các đặc tính của các mẫu này để xác định một cách định tính một chương trình độc xâm phạm quyền riêng tư. Đối với các mẫu mà các đặc tính của nó không được lưu trong cơ sở dữ liệu thì có thể không xác định được liệu các chương trình ứng dụng đó có phải là các chương trình ứng dụng độc không. Ngoài ra, cũng có thể bỏ sót một số chương trình ứng dụng độc xâm phạm quyền riêng tư thực sự do những hạn chế của các tiêu chuẩn của các công nghệ quét có công cụ chống virus.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư và thiết bị di động. Giải pháp kỹ thuật của sáng chế được mô tả như sau:

Phương pháp ngăn chặn một chương trình ứng dụng xâm phạm quyền riêng tư, bao gồm các bước:

phân tích uỷ quyền hoạt động của một chương trình ứng dụng khi cài đặt chương trình ứng dụng này, và xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư;

xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi chương trình ứng dụng có uỷ quyền hoạt động đối với thông tin cá nhân hoặc sự kiện riêng tư;

cấm, khi chạy chương trình ứng dụng, chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động

bị cấm, và cấp quyền cho chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép.

Việc phân tích uỷ quyền hoạt động của một chương trình ứng dụng và xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không, bao gồm các bước:

thu được bảng uỷ quyền hoạt động của chương trình ứng dụng;

phân tích bảng uỷ quyền hoạt động của chương trình ứng dụng, và xác định rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư khi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư tồn tại trong bảng uỷ quyền hoạt động.

Việc xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư bao gồm các bước:

cung cấp cho người dùng chế độ cài đặt chống xâm phạm quyền riêng tư mà chế độ này cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư cho người dùng để lựa chọn trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư;

nhận và lưu trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư đã chọn do người dùng cung cấp.

Trước khi chạy chương trình ứng dụng, phương pháp theo sáng chế còn bao gồm bước:

sửa đổi trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư.

Sự kiện riêng tư bao gồm một hoặc nhiều sự kiện sau: gọi máy ảnh, gọi mô đun GPS (Global Positioning System – hệ thống định vị toàn cầu), gọi chức năng định vị người dùng của trạm gốc, bắt cuộc gọi ba

chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS (short message service – dịch vụ tin nhắn ngắn), chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, kết nối Internet tự động để truyền dữ liệu và tự động bật điện thoại;

Thông tin cá nhân bao gồm một hoặc nhiều thông tin để liên lạc, nội dung liên lạc, thông tin ảnh và thông tin video.

Thiết bị di động, bao gồm mô đun phân tích, mô đun xác định thứ nhất và mô đun xác định thứ hai;

mô đun phân tích được tạo cấu hình để phân tích uỷ quyền hoạt động của một chương trình ứng dụng khi cài đặt chương trình ứng dụng, và xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư;

mô đun xác định thứ nhất được tạo cấu hình để xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi chương trình ứng dụng có uỷ quyền hoạt động đối với thông tin cá nhân hoặc sự kiện riêng tư;

mô đun xác định thứ hai được tạo cấu hình để cấm, khi chạy chương trình ứng dụng, chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động bị cấm, và cấp phép cho chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép.

Mô đun xác định thứ nhất bao gồm:

bộ phận thu được tạo cấu hình để thu được bảng uỷ quyền hoạt động của chương trình ứng dụng;

bộ phận phân tích được tạo cấu hình để phân tích bảng uỷ quyền hoạt động của chương trình ứng dụng, và xác định rằng chương trình ứng

dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư khi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư tồn tại trong bảng uỷ quyền hoạt động.

Mô đun xác định thứ hai bao gồm:

bộ phận cung cấp chế độ cài đặt được tạo cấu hình để cung cấp cho người dùng chế độ cài đặt chống xâm phạm quyền riêng tư mà cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư cho người dùng để lựa chọn trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư;

bộ phận lưu được tạo cấu hình để nhận và lưu trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư đã được chọn do người dùng cung cấp.

Thiết bị này còn bao gồm:

Mô đun sửa đổi được tạo cấu hình để sửa đổi trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư.

Sự kiện riêng tư bao gồm một hoặc nhiều sự kiện sau: gọi máy ảnh, gọi mô đun GPS, gọi chức năng định vị người dùng của trạm gốc, bật cuộc gọi ba chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS, chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, kết nối Internet tự động để truyền dữ liệu và tự động bật điện thoại;

Thông tin cá nhân bao gồm một hoặc nhiều thông tin để liên lạc, nội dung liên lạc, thông tin ảnh và thông tin video. Khi cài đặt chương trình ứng dụng, uỷ quyền hoạt động của chương trình ứng dụng được phân tích để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không. Khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân

hoặc sự kiện riêng tư, các sơ đồ kết hợp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định. Khi chạy chương trình ứng dụng này, việc cấp phép chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư được xác định dựa vào trạng thái cấp phép hoạt động, tự động ngăn chặn hành động xâm phạm quyền riêng tư bởi chương trình ứng dụng và khắc phục được nhược điểm của phương pháp ngăn chặn bằng cách quét khi chương trình độc xâm phạm quyền riêng tư không được phát hiện. Ngoài ra, giải pháp kỹ thuật này có thể xác định được trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi cài đặt chương trình ứng dụng. Phương pháp xác định này gọn và dễ. Người sử dụng không bắt buộc phải có trình độ chuyên môn nhất định, giảm mức độ khó thao tác cho người sử dụng.

Mô tả vắn tắt các hình vẽ

Để minh họa rõ giải pháp kỹ thuật được đưa ra trong các phương án của sáng chế, các hình vẽ cần thiết đi kèm các phần mô tả các phương án này được giới thiệu vắn tắt như sau. Hiển nhiên là, các hình vẽ kèm theo này chỉ là các phương án của sáng chế. Người có trình độ trung bình trong lĩnh vực này đều có thể suy ra các bản vẽ khác dựa vào các bản vẽ kèm theo này mà không cần có bất kỳ nỗ lực sáng tạo nào.

FIG. 1 là lưu đồ về phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư được đề xuất trong Phương án 1 của sáng chế;

FIG. 2 là lưu đồ về phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư được đề xuất trong Phương án 2 của sáng chế;

FIG. 3 là sơ đồ thể hiện thiết bị di động được đề xuất trong Phương án 3 của sáng chế;

FIG. 4 là sơ đồ thể hiện thiết bị di động được đề xuất trong Phương án 3 của sáng chế.

Mô tả chi tiết các phương án được ưu tiên

Để các mục đích, giải pháp kỹ thuật, và các điểm ưu việt của sáng chế trở nên rõ ràng hơn, các phương án của sáng chế được mô tả chi tiết hơn dưới đây kết, kết hợp với việc tham khảo các hình vẽ kèm theo.

Phương án 1

Tham khảo FIG. 1, phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư được đề xuất. Thiết bị hoạt động trong phương pháp này có thể là thiết bị di động, và cụ thể thiết bị di động này có thể là điện thoại di động, máy tính bảng, và các thiết bị tương tự. Phương pháp này cụ thể bao gồm các bước sau:

Trong Bước 101, uỷ quyền hoạt động của một chương trình ứng dụng được phân tích khi cài đặt chương trình ứng dụng, và xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư được xác định hay không;

Trong Bước 102, trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định khi chương trình ứng dụng có uỷ quyền hoạt động đối với thông tin cá nhân hoặc sự kiện riêng tư;

Trong Bước 103, khi chạy chương trình ứng dụng, chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư bị cấm nếu trạng thái cấp phép hoạt động bị cấm, và chương trình ứng dụng được cho phép để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép.

Khi cài đặt chương trình ứng dụng, uỷ quyền hoạt động của chương trình ứng dụng được phân tích để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư. Khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, các sơ đồ kết hợp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định. Khi chạy chương trình ứng dụng, việc cấp phép chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư được xác định dựa vào trạng thái cấp phép hoạt động, tự động ngăn chặn hành động xâm phạm quyền riêng tư bởi chương trình ứng dụng và khắc phục được nhược điểm của công nghệ phòng thủ bằng cách quét khi chương trình độc xâm phạm quyền riêng tư không được phát hiện. Ngoài ra, giải pháp kỹ thuật có thể xác định được trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi cài đặt chương trình ứng dụng. Phương pháp xác định là gọn và hoàn hảo. Người dùng không bắt buộc phải có trình độ chuyên môn nhất định, nhờ vậy giảm độ khó thao tác cho người dùng.

Phương án 2

Tham khảo FIG. 2, phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư được đề xuất. Thiết bị hoạt động chính trong phương pháp có thể là thiết bị di động, và cụ thể thiết bị di động này có thể là điện thoại di động, máy tính bảng, và các thiết bị tương tự. Phương pháp này cụ thể bao gồm các bước sau:

Trong Bước 201, khi cài đặt chương trình ứng dụng, chương trình ứng dụng được xử lý trước. Việc xử lý trước ở đây bao gồm, nhưng không bị giới hạn ở, quét chương trình ứng dụng tìm virus.

Cụ thể là, quy trình quét chương trình ứng dụng tìm virus bao gồm:

khớp chương trình ứng dụng với các đặc tính đã được lưu trong cơ sở dữ liệu chương trình độc;

khi chương trình ứng dụng khớp với các đặc tính trong cơ sở dữ liệu chương trình độc, chương trình ứng dụng được thông báo là chương trình độc và người dùng được cảnh báo để ngăn cài đặt chương trình ứng dụng, dừng cài đặt chương trình ứng dụng và kết thúc thao tác;

khi chương trình ứng dụng không khớp với các đặc tính trong cơ sở dữ liệu chương trình độc, Bước 202 được thực hiện.

Trong Bước 202, uỷ quyền hoạt động của chương trình ứng dụng được phân tích, để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không.

khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, Bước 203 được thực hiện;

khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, cài đặt của chương trình ứng dụng được tiếp tục cho đến khi cài đặt của chương trình ứng dụng kết thúc;

Cụ thể là, việc phân tích uỷ quyền hoạt động của chương trình ứng dụng để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư bao gồm các bước:

thu được bảng uỷ quyền hoạt động của chương trình ứng dụng;

phân tích bảng uỷ quyền hoạt động của chương trình ứng dụng, và xác định rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư khi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư tồn tại trong bảng uỷ quyền hoạt động.

Các hoạt động của sự kiện riêng tư được mô tả trong các phương án của sáng chế bao gồm một hoặc nhiều các bước được mô tả sau về

chắc năng hoặc hoạt động mà có thể thực hiện, ghi hoặc truyền thông tin cá nhân: gọi máy ảnh, gọi mô đun GPS, gọi chức năng định vị người dùng của trạm gốc, bật cuộc gọi ba chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS, chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, kết nối Internet tự động để truyền dữ liệu và tự động bật điện thoại.

Thông tin cá nhân bao gồm một hoặc nhiều thông tin để liên lạc, nội dung liên lạc, thông tin ảnh và thông tin video.

Bước 203, trạng thái cấp phép hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư trong chương trình ứng dụng được xác định. Trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư bị cấm hoặc được cho phép.

Cụ thể là, xác định trạng thái cấp phép hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư trong chương trình ứng dụng bao gồm:

cung cấp chế độ cài đặt chống xâm phạm quyền riêng tư mà chế độ này cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư cho người dùng để lựa chọn trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư;

nhận và lưu trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được lựa chọn bởi người dùng cung cấp.

Quy trình vận hành các bước cụ thể được thực hiện như sau:

Ủy quyền hoạt động của chương trình ứng dụng được phân tích. Khi chương trình ứng dụng được thấy là có ủy quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, thông báo yêu cầu được gửi đến người dùng. Thông báo yêu cầu là để thông báo với người dùng rằng chương trình ứng dụng có ủy quyền hoạt động để gọi thông tin cá nhân

hoặc sự kiện riêng tư và hỏi người dùng xem liệu có muốn sửa uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không.

Đồng thời, chế độ cài đặt chống xâm phạm quyền riêng tư của trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được đề xuất cho người dùng và chế độ cài đặt chống xâm phạm quyền riêng tư được đặt chế độ “bị cấm” làm trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư mặc định.

Người dùng có thể huỷ một phần hoặc huỷ toàn bộ trạng thái bị cấm của thông tin cá nhân hoặc sự kiện riêng tư, trong đó trạng thái cấp phép hoạt động được cung cấp bởi chế độ cài đặt chống xâm phạm quyền riêng tư bị cấm, do đó trạng thái cấp phép hoạt động ban đầu bị cấm đối với thông tin cá nhân hoặc sự kiện riêng tư được đổi thành “được cho phép”;

Trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được lựa chọn do người dùng cung cấp được nhận và được lưu. Việc cài đặt chương trình ứng dụng được tiếp tục cho tới khi việc cài đặt của chương trình ứng dụng kết thúc.

Trong Bước 204, khi chạy chương trình ứng dụng, xác định xem liệu có cho phép chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư hay không dựa vào trạng thái cấp phép hoạt động của chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư.

Nếu trạng thái cấp phép hoạt động bị cấm, dừng chương trình ứng dụng khỏi việc gọi thông tin cá nhân hoặc sự kiện riêng tư.

Nếu trạng thái cấp phép hoạt động được cho phép, cấp phép chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư được cho phép.

Ngoài ra, cần lưu ý rằng trong các phương án của sáng chế, trạng thái cấp phép hoạt động của chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư đã được lưu cũng có thể được sửa đổi.

Khi cài đặt chương trình ứng dụng, uỷ quyền hoạt động của chương trình ứng dụng được phân tích để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không. Khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định. Khi chạy chương trình ứng dụng, việc cấp phép chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư được xác định dựa vào trạng thái cấp phép hoạt động hoặc người dùng cuối, việc ngăn chặn hành động xâm phạm quyền riêng tư bởi chương trình ứng dụng là tự động, vì thế mà khắc phục được nhược điểm của công nghệ phòng thủ bằng cách quét khi chương trình độc xâm phạm quyền riêng tư không được phát hiện. Ngoài ra, giải pháp kỹ thuật có thể xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi cài đặt chương trình ứng dụng. Phương pháp xác định là gọn và hoàn hảo. Người dùng không bắt buộc phải có trình độ chuyên môn nhất định, giảm độ khó thao tác cho người dùng.

Phương án 3

Tham khảo FIG. 3, thiết bị di động được đề xuất. Cụ thể là, thiết bị di động giống các thiết bị di động được mô tả trong phương pháp phương án 2. Ví dụ, thiết bị di động có thể là điện thoại di động, máy tính bảng, và các thiết bị tương tự. Thiết bị cụ thể bao gồm mô đun phân tích 301, mô đun xác định thứ nhất 302 và mô đun xác định thứ hai 303.

Mô đun phân tích 301 được tạo cấu hình để phân tích uỷ quyền hoạt động của một chương trình ứng dụng khi cài đặt chương trình ứng

dụng, và xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không.

Mô đun xác định thứ nhất 302 được tạo cấu hình để xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định khi chương trình ứng dụng có uỷ quyền hoạt động đối với thông tin cá nhân hoặc sự kiện riêng tư;

Mô đun xác định thứ hai 303 được tạo cấu hình để cấm, khi chạy chương trình ứng dụng, chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư bị cấm nếu trạng thái cấp phép hoạt động bị cấm, và cấp phép cho chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép.

Theo các phương án của sáng chế, thiết bị di động còn bao gồm:

mô đun khớp được tạo cấu hình để khớp chương trình ứng dụng với các đặc tính đã được lưu trong cơ sở dữ liệu chương trình độc;

mô đun thông báo được tạo cấu hình để thông báo, khi chương trình ứng dụng khớp các đặc tính trong cơ sở dữ liệu chương trình độc, rằng chương trình ứng dụng là chương trình độc, và cảnh báo người dùng để cấm cài đặt chương trình ứng dụng.

Cụ thể là, theo phương án của sáng chế, tham khảo FIG. 4, mô đun xác định thứ nhất 302 bao gồm:

bộ phận thu 3021 được tạo cấu hình để thu được bảng uỷ quyền hoạt động của chương trình ứng dụng;

bộ phận phân tích 3022 được tạo cấu hình để phân tích bảng uỷ quyền hoạt động của chương trình ứng dụng, và xác định rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư khi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư tồn tại trong bảng uỷ quyền hoạt động.

Mô đun xác định thứ hai 303 bao gồm:

bộ phận cung cấp chế độ cài đặt 3031 được tạo cấu hình để cung cấp chế độ cài đặt chống xâm phạm quyền riêng tư mà chế độ này cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư cho người dùng để lựa chọn trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư;

bộ phận lưu 3032 được tạo cấu hình để nhận và lưu trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được chọn bởi người dùng cung cấp.

Theo các phương án của sáng chế, thiết bị di động còn bao gồm:

mô đun sửa đổi được tạo cấu hình để sửa đổi trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư đã được lưu, và trạng thái cấp phép hoạt động bị cấm hoặc được cho phép.

Các hoạt động của sự kiện riêng tư được mô tả trong các phương án của sáng chế bao gồm một hoặc nhiều các hoạt động sau được hướng đến các chức năng hoặc các hoạt động mà có thể thực hiện, ghi hoặc truyền thông tin cá nhân: gọi máy ảnh, gọi mô đun GPS, gọi chức năng định vị người dùng của trạm gốc, bật cuộc gọi ba chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS, chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, kết nối Internet tự động để truyền dữ liệu hoặc tự động bật điện thoại.

Theo các phương án của sáng chế, thông tin cá nhân bao gồm một hoặc nhiều thông tin ảnh, nội dung liên lạc và thông tin video.

Khi cài đặt chương trình ứng dụng, uỷ quyền hoạt động của chương trình ứng dụng được phân tích để xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện

riêng tư hay không. Khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư được xác định. Khi chạy chương trình ứng dụng, việc cấp phép chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư được xác định dựa vào trạng thái cấp phép hoạt động hoặc người dùng cuối, tự động ngăn chặn hành động xâm phạm quyền riêng tư bởi chương trình ứng dụng và khắc phục được nhược điểm của công nghệ phòng thủ bằng cách quét khi chương trình độc xâm phạm quyền riêng tư không được phát hiện. Ngoài ra, giải pháp kỹ thuật có thể xác định trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư khi cài đặt chương trình ứng dụng. Phương pháp xác định là gọn và hoàn hảo. Người dùng không bắt buộc phải có trình độ chuyên môn nhất định, giảm độ khó thao tác cho người dùng.

Người có trình độ trung bình trong lĩnh vực này có thể hiểu rằng tất cả hoặc một phần của các bước của các phương án này đều có thể được thực hiện bởi phần cứng và cũng có thể được thực hiện bởi một phần cứng được điều khiển bởi phần mềm. Các bước này có thể được lưu trữ trong một phương tiện lưu trữ của máy tính và có thể đọc được trên máy tính, và phương tiện lưu trữ này có thể là phương tiện lưu trữ chỉ đọc, ổ đĩa từ hoặc ổ đĩa quang.

Như được mô tả ở trên, sáng chế đã được mô tả cùng với các phương án được ưu tiên, và cần được hiểu là bất kỳ sự thay đổi, thay thế tương đương và cải tiến nào đều có thể nằm trong phạm vi và nguyên lý của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp ngăn chặn chương trình ứng dụng xâm phạm quyền riêng tư, được đặc trưng ở chỗ phương pháp này bao gồm các bước:

khớp chương trình ứng dụng với các đặc tính đã được lưu trong cơ sở dữ liệu chương trình độc khi cài đặt chương trình ứng dụng;

thông báo, khi chương trình ứng dụng khớp với các đặc tính trong cơ sở dữ liệu chương trình độc, rằng chương trình ứng dụng là chương trình độc, và cảnh báo người dùng để cấm cài đặt chương trình ứng dụng và dùng cài đặt chương trình ứng dụng, và kết thúc cài đặt;

thu được, khi chương trình ứng dụng không khớp các đặc tính trong cơ sở dữ liệu chương trình độc, bảng uỷ quyền hoạt động của chương trình ứng dụng, phân tích bảng uỷ quyền hoạt động của chương trình ứng dụng, và xác định rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư khi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư tồn tại trong bảng uỷ quyền hoạt động;

gửi, khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, thông báo yêu cầu đến người dùng, và cung cấp cho người dùng chế độ cài đặt chống xâm phạm quyền riêng tư cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư, trong đó thông báo yêu cầu là để thông báo người dùng rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư và hỏi người dùng xem liệu có sửa đổi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không; trạng thái mặc định cấp phép hoạt động của chế độ cài đặt chống xâm phạm quyền riêng tư đối với thông tin cá nhân hoặc sự kiện riêng tư bị cấm do vậy người dùng huỷ một phần hoặc toàn bộ trạng thái bị cấm của

thông tin cá nhân hoặc sự kiện riêng tư, trong đó trạng thái cấp phép hoạt động được cung cấp bởi chế độ cài đặt chống xâm phạm quyền riêng tư bị cấm, do đó trạng thái cấp phép hoạt động ban đầu là bị cấm đối với thông tin cá nhân hoặc sự kiện riêng tư được chuyển thành được cho phép; trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư đã được chọn do người dùng cung cấp được nhận và được lưu, sau đó, tiếp tục cài đặt chương trình ứng dụng cho tới khi cài đặt của chương trình ứng dụng kết thúc;

khi chạy chương trình ứng dụng, cấm chương trình ứng dụng gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động bị cấm, và cấp quyền cho chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép.

2. Phương pháp theo điểm 1, được đặc trưng ở chỗ trước khi chạy chương trình ứng dụng, phương pháp còn bao gồm bước:

sửa đổi trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư.

3. Phương pháp theo điểm 1 hoặc 2, được đặc trưng ở chỗ sự kiện riêng tư bao gồm một hoặc nhiều sự kiện như gọi máy ảnh, gọi mô đun GPS (Global Positioning System – hệ thống định vị toàn cầu), gọi chức năng định vị người dùng của trạm gốc, bật cuộc gọi ba chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS (short message service – dịch vụ tin nhắn ngắn), chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, tự động truyền dữ liệu kết nối Internet và tự động bật điện thoại; và

thông tin cá nhân bao gồm một hoặc nhiều thông tin liên lạc, nội dung liên lạc, thông tin ảnh và thông tin video.

4. Thiết bị di động, được đặc trưng ở chỗ thiết bị này bao gồm mô đun phân tích, mô đun xác định thứ nhất và mô đun xác định thứ hai;

mô đun phân tích được tạo cấu hình để phân tích uỷ quyền hoạt động của một chương trình ứng dụng khi cài đặt chương trình ứng dụng, và xác định xem liệu chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không;

mô đun xác định thứ nhất được tạo cấu hình để gửi, khi chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư, thông báo yêu cầu đến người dùng, và cung cấp cho người dùng chế độ cài đặt chống xâm phạm quyền riêng tư cung cấp trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư, trong đó thông báo yêu cầu là để thông báo người dùng rằng chương trình ứng dụng có uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư và hỏi người dùng liệu có sửa đổi uỷ quyền hoạt động để gọi thông tin cá nhân hoặc sự kiện riêng tư hay không; trạng thái mặc định cấp phép hoạt động của chế độ cài đặt chống xâm phạm quyền riêng tư đối với thông tin cá nhân hoặc sự kiện riêng tư bị cấm do đó người dùng có thể huỷ một phần hoặc toàn bộ trạng thái bị cấm của thông tin cá nhân hoặc sự kiện riêng tư, mà trong đó trạng thái cấp phép hoạt động được cung cấp bởi chế độ cài đặt chống xâm phạm quyền riêng tư bị cấm, do đó trạng thái cấp phép hoạt động mà ban đầu là bị cấm đối với thông tin cá nhân hoặc sự kiện riêng tư được chuyển thành được cho phép; trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư đã chọn do người dùng cung cấp được nhận và được lưu, sau đó, tiếp tục cài đặt của chương trình ứng dụng cho tới khi cài đặt của chương trình ứng dụng kết thúc;

mô đun xác định thứ hai được tạo cấu hình để cấm, khi chạy chương trình ứng dụng, chương trình ứng dụng để gọi thông tin cá nhân

hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động bị cấm, và cấp quyền cho chương trình ứng dụng để gọi thông tin cá nhân hoặc sự kiện riêng tư nếu trạng thái cấp phép hoạt động được cho phép,

trong đó thiết bị còn được tạo cấu hình để khớp chương trình ứng dụng với các đặc tính đã được lưu trong cơ sở dữ liệu chương trình độc khi cài đặt chương trình ứng dụng, thông báo, khi chương trình ứng dụng khớp các đặc tính trong cơ sở dữ liệu chương trình độc, rằng chương trình ứng dụng là chương trình độc, và cảnh báo người dùng để cấm cài đặt chương trình ứng dụng và dừng cài đặt chương trình ứng dụng, và kết thúc cài đặt, và tiến hành thao tác phân tích uỷ quyền hoạt động của chương trình ứng dụng khi chương trình ứng dụng không khớp với các đặc tính trong cơ sở dữ liệu chương trình độc.

5. Thiết bị này theo điểm 4, được đặc trưng ở chỗ thiết bị này còn bao gồm:

mô đun sửa đổi được tạo cấu hình để sửa đổi trạng thái cấp phép hoạt động của thông tin cá nhân hoặc sự kiện riêng tư.

6. Thiết bị theo điểm 4 hoặc 5, được đặc trưng ở chỗ sự kiện riêng tư bao gồm một hoặc nhiều sự kiện như gọi máy ảnh, gọi mô đun GPS, gọi chức năng định vị người dùng của trạm gốc, bật cuộc gọi ba chiều, gọi điện thoại, nhận cuộc gọi điện thoại, bật ghi âm điện thoại, truy cập danh bạ điện thoại, truy cập lịch sử cuộc gọi, truy cập lịch sử tin nhắn SMS, chặn tin nhắn SMS, cài đặt bí mật các chương trình khác, tự động bật và truyền dữ liệu kết nối; và

thông tin cá nhân bao gồm một hoặc nhiều thông tin liên lạc, nội dung liên lạc, thông tin ảnh và thông tin video.

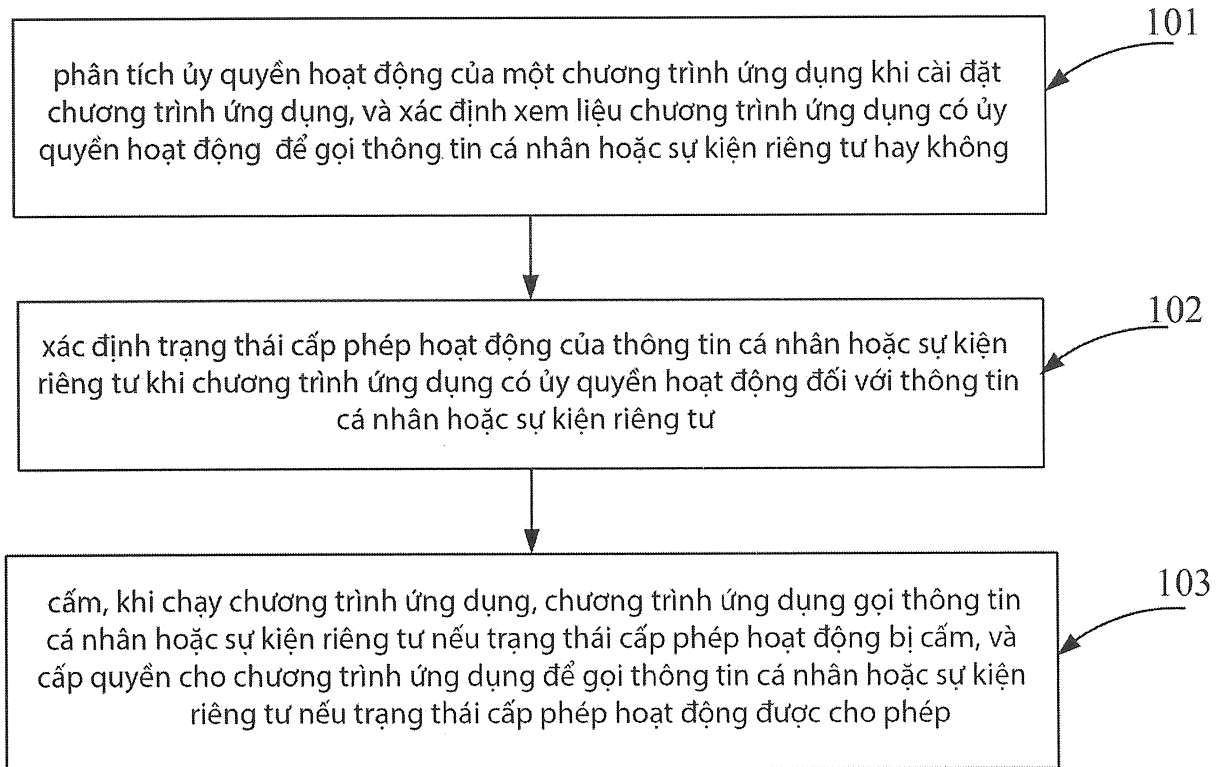


FIG. 1

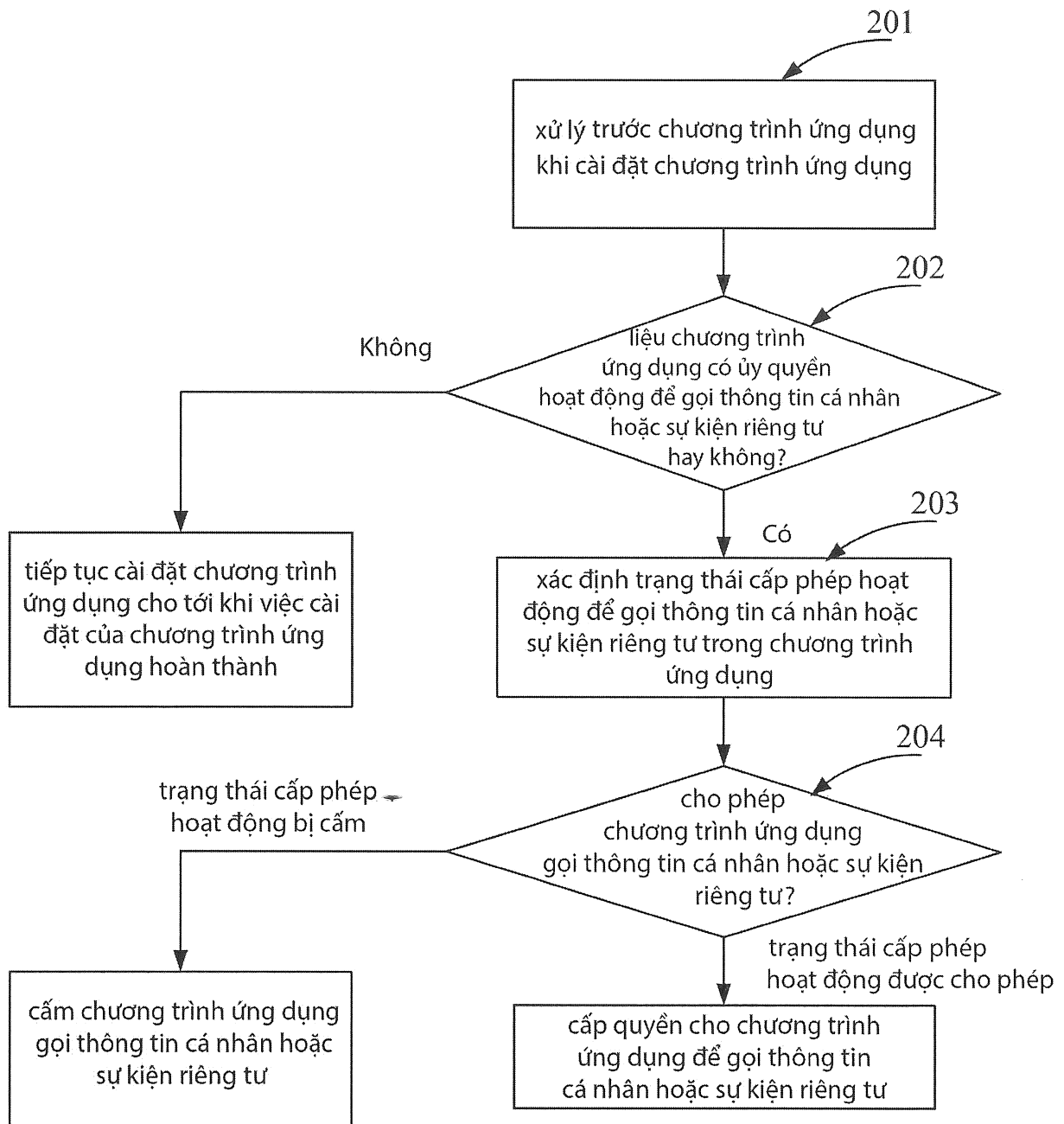


FIG. 2

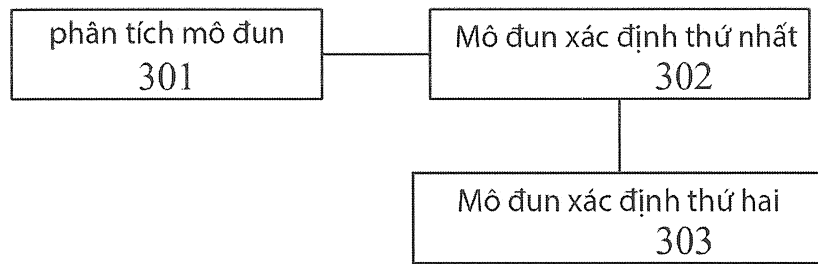


FIG. 3

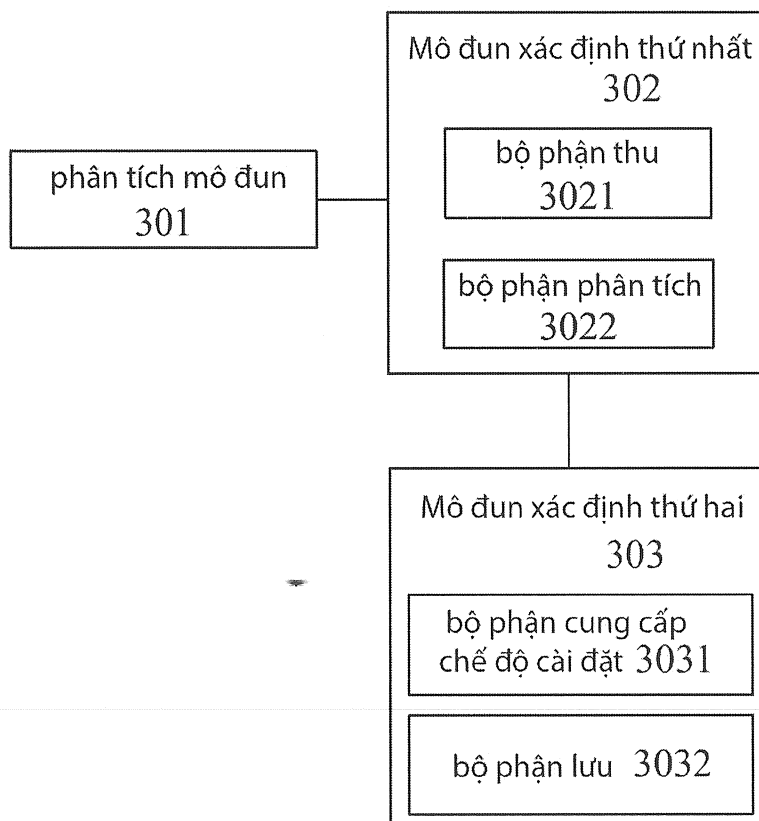


FIG. 4