(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) **1-0022343**

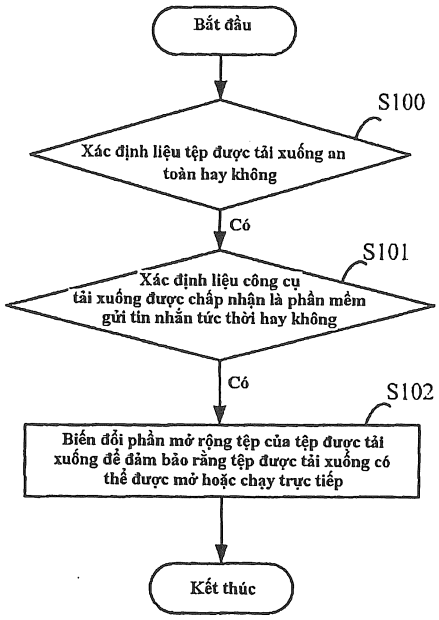
(51)[7] **H04L 29/06**

(13) **B**

(21) 1-2014-02389
(22) 19.08.2013
(86) PCT/CN2013/081785 19.08.2013
(87) WO2014/032533A1 06.03.2014
(30) 201210313865.4 30.08.2012 CN
(45) 25.11.2019 380
(43) 27.10.2014 319
(73) TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED (CN)
Room 403, East Block 2, SEG Park, Zhenxing Road, Futian Shenzhen, Guangdong 518044, China
(72) CHEN, Qiru (CN), LIU, Yang (CN), LI, He (CN), LU, Fei (CN)
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG THỰC HIỆN GIÁM SÁT AN NINH KHI TẢI XUỐNG TỆP

(57) Sáng chế đề cập đến phương pháp và hệ thống để thực hiện việc giám sát an ninh khi tải xuống tệp, và vật ghi đọc được bằng máy tính có lưu trữ các chỉ dẫn để thực hiện việc kiểm soát an ninh khi tải xuống tệp. Phương pháp bao gồm các bước khi phát hiện thao tác tải xuống tệp, thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn; nếu tệp được tải xuống an toàn, xác định xem liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm gửi tin nhắn tức thời (IM); và nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực an ninh mạng, và cụ thể là sáng chế đề cập đến phương pháp và hệ thống thực hiện giám sát an ninh khi tải xuống tệp và vật ghi đọc được bằng máy tính lưu trữ các chỉ dẫn để thực hiện giám sát an ninh khi tải xuống tệp.

Tình trạng kỹ thuật của sáng chế

Việc chuyển các tệp là kênh thông thường mà qua đó virus máy tính, như Trojan, xâm nhập máy tính người dùng. Hiện nay, hệ thống giám sát an ninh và phương pháp giám sát được tạo cấu hình để thực hiện phát hiện an ninh trên tệp được tải xuống đến thiết bị đầu cuối khách, để ngăn không cho virus máy tính từ thiết bị nguồn xâm nhập vào máy tính người dùng.

Tính đến độ an toàn của việc chuyển tệp, khi chuyển tệp, phần mềm gửi tin nhắn tức thời (IM) đã biết có thể đổi tên tệp được chuyển để ngăn các virus máy tính, như Trojan, không tự động chạy. Hiện nay, khi thực hiện việc phát hiện an ninh trên tệp được chuyển bằng phần mềm IM, hệ thống giám sát an ninh và phương pháp giám sát chỉ phát hiện an ninh của tệp được chuyển, và thông báo cho người dùng kết quả phát hiện an ninh. Tuy nhiên, đối với tệp an toàn, người dùng không được thông báo cách sử dụng tệp này, điều này gây bất tiện cho người dùng trong việc sử dụng, do đó không tạo ra hoạt động người dùng mong muốn.

Vì vậy, có một nhu cầu chưa được giải quyết tồn tại trong lĩnh vực kỹ thuật để giải quyết các nhược điểm và thiếu sót nêu trên.

Bản chất kỹ thuật của sáng chế

Một trong các mục đích của sáng chế là đề xuất phương pháp và hệ thống để thực hiện việc giám sát an ninh khi tải xuống tệp, và vật ghi đọc được bằng máy tính không chuyển tiếp mà lưu các chỉ dẫn để thực hiện việc giám sát an ninh khi tải xuống tệp, để giải quyết vấn đề tồn tại trong kỹ thuật an ninh mạng hiện thời.

Theo một khía cạnh của sáng chế, phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế bao gồm các bước: khi phát hiện thao tác tải xuống tệp, thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống là an toàn hay không; nếu tệp được tải xuống an toàn, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không; và nếu công cụ tải xuống được chấp nhận là phần mềm IM, thì biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp.

Theo khía cạnh khác của sáng chế, hệ thống thực hiện việc kiểm soát an ninh khi tải xuống tệp theo sáng chế bao gồm môđun phát hiện và môđun xác định. Môđun phát hiện được tạo cấu hình để, khi phát hiện thao tác tải xuống tệp, thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống là an toàn hay không. Môđun xác định được tạo cấu hình để, nếu tệp được tải xuống là an toàn, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không, và nếu công cụ tải xuống được chấp nhận là phần mềm IM, thì biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp.

Theo phương án nữa của sáng chế, vật ghi đọc được bằng máy tính không chuyển tiếp lưu trữ các chỉ dẫn mà, khi được thực hiện bởi một hoặc nhiều bộ xử lý, khiến cho hệ thống nêu trên thực hiện phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp nêu trên.

Có thể thấy từ các phương án nêu trên là, sáng chế thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống là an toàn hay không; nếu tệp được tải xuống an toàn, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM; nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp, sao cho an ninh trong quy trình chuyển tệp được đảm bảo, và trên cơ sở là người dùng được thông báo về an ninh, người dùng có thể mở hoặc chạy trực tiếp tệp, để không làm ảnh hưởng đến việc sử dụng bởi người dùng, do đó khiến hoạt động của người dùng dễ dàng hơn.

Phần mô tả ở trên chỉ là tóm tắt về các giải pháp kỹ thuật của sáng chế. Để cho phương tiện kỹ thuật của sáng chế được hiểu rõ hơn, phần triển khai có thể được thực hiện theo các nội dung của phần mô tả. Để khiến các mục đích nêu trên và các mục đích khác, và các ưu điểm của sáng chế dễ hiểu hơn, phần mô tả chi tiết được thể hiện dưới đây qua phương án ưu tiên có dựa vào các hình vẽ kèm theo.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo minh họa một hoặc nhiều phương án của sáng chế và, cùng với phần mô tả, để giải thích các nguyên lý của sáng chế. Các số tham chiếu giống nhau được sử dụng trên các hình vẽ đề cập đến các phần tử giống nhau hoặc phần tử tương tự của sáng chế. Các hình vẽ không giới hạn sáng chế ở các phương án cụ thể được bộc lộ và được mô tả ở đây. Các hình vẽ không cần phải có cùng tỷ lệ, nhấn mạnh thay vì được đặt vào việc minh họa rõ các nguyên lý của sáng chế.

Fig.1 là lưu đồ phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế.

Fig.2 là hình vẽ sơ lược hiển thị kết quả phát hiện an ninh của tệp được tải

xuống tại thiết bị đầu cuối khách theo phương án của sáng chế.

Fig.3 là lưu đồ phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án khác của sáng chế.

Fig.4 là sơ đồ khối về cấu tạo chính của hệ thống thực hiện việc kiểm soát an ninh khi tải xuống tệp theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần mô tả dưới đây chỉ là minh họa bản chất và không nhằm mục đích giới hạn sáng chế, các ứng dụng hoặc sử dụng nó. Các kiến thức về sáng chế này có thể được triển khai đa dạng. Vì vậy, mặc dù sáng chế có các ví dụ cụ thể, nhưng phạm vi của sáng chế sẽ không bị giới hạn vì các cải biến khác sẽ trở nên rõ ràng khi nghiên cứu các hình vẽ, phần mô tả, và yêu cầu bảo hộ dưới đây. Để cho rõ, các số tham chiếu giống nhau sẽ được sử dụng trên các hình vẽ để chỉ các phần tử tương tự.

Thuật ngữ được sử dụng trong phần mô tả này nói chung là có các nghĩa thông thường của chúng trong lĩnh vực, trong ngữ cảnh của sáng chế, và trong ngữ cảnh cụ thể mà mỗi thuật ngữ được sử dụng. Các thuật ngữ nhất định để mô tả sáng chế được thảo luận dưới đây, hoặc ở những phần khác trong phần mô tả, để cung cấp hướng dẫn thêm cho người thực hành liên quan đến phần mô tả của sáng chế. Việc sử dụng các ví dụ trong phần mô tả này, bao gồm các ví dụ về các thuật ngữ bất kỳ được thảo luận, chỉ để minh họa, và không giới hạn phạm vi và ý nghĩa của sáng chế hoặc của thuật ngữ được làm mẫu bất kỳ. Tương tự như vậy, sáng chế không bị giới hạn vào các phương án khác nhau được đưa ra trong phần mô tả này.

Như được sử dụng trong phần mô tả và xuyên suốt yêu cầu bảo hộ, nghĩa của "a", "an", và "the" bao gồm tham chiếu số nhiều trừ khi ngữ cảnh chỉ dẫn rõ ràng khác. Ngoài ra, như được sử dụng trong phần mô tả và xuyên suốt yêu cầu

bảo hộ, nghĩa của "trong" bao gồm "trong" và "trên" trừ khi ngữ cảnh chỉ dẫn rõ ràng khác.

Như được sử dụng trong phần mô tả, các thuật ngữ "bao gồm", "gồm có", "có", "chứa", "gồm", và tương tự sẽ được hiểu là nghĩa mở, tức là, nghĩa là gồm có nhưng không bị giới hạn.

Như được sử dụng trong phần mô tả, cụm từ "ít nhất một trong số A, B, và C" nên được hiểu theo nghĩa logic (A hoặc B hoặc C), sử dụng logic OR không loại trừ. Cần hiểu rằng một hoặc nhiều bước trong phương pháp có thể được thực hiện theo thứ tự khác nhau (hoặc đồng thời) mà không thay đổi bản chất của sáng chế.

Như được sử dụng trong phần mô tả, thuật ngữ "môđun" có thể đề cập đến, là một phần của, hoặc bao gồm mạch tích hợp chuyên dụng (Application Specific Integrated Circuit – ASIC); mạch điện tử; mạch logic tổ hợp; mảng cổng khả lập trình trường (field programmable gate array – FPGA); bộ xử lý (được dùng chung, chuyên dụng, hoặc nhóm) mà thực hiện mã hóa; các thành phần phần cứng thích hợp khác mà cung cấp các chức năng được mô tả; hoặc kết hợp của một số hoặc tất cả các phần tử ở trên, như trong hệ thống trên một chip. Thuật ngữ môđun có thể bao gồm bộ nhớ (được dùng chung, dành riêng, hoặc nhóm) mà lưu trữ mã được thực hiện bởi bộ xử lý.

Thuật ngữ "mã", được sử dụng trong phần mô tả, có thể bao gồm phần mềm, phần sụn, và/hoặc vi mã, và có thể đề cập đến các chương trình, các chương trình con, các chức năng, các lớp, và/hoặc các đối tượng. Thuật ngữ "được dùng chung", như được sử dụng trong tài liệu này, nghĩa là một số hoặc tất cả mã từ đa môđun có thể được thực hiện sử dụng một bộ xử lý (được dùng chung). Ngoài ra, một số hoặc tất cả mã từ đa môđun có thể được lưu trữ bởi một bộ nhớ (được dùng chung). Thuật ngữ "nhóm", được sử dụng trong tài liệu này, nghĩa là một số hoặc tất cả mã từ một môđun có thể được thực hiện nhờ sử dụng

nhóm các bộ xử lý. Ngoài ra, một số hoặc tất cả mã từ một môđun có thể được lưu trữ nhờ sử dụng một nhóm các bộ nhớ.

Các hệ thống và các phương pháp được mô tả trong tài liệu này có thể được triển khai bởi một hoặc nhiều chương trình máy tính được thực hiện bởi một hoặc nhiều bộ xử lý. Các chương trình máy tính bao gồm các chỉ dẫn thực hiện được bởi bộ xử lý mà được lưu trữ trên vật ghi đọc được bằng máy tính hữu hình không chuyển tiếp. Các chương trình máy tính còn bao gồm dữ liệu được lưu trữ. Các ví dụ không giới hạn về vật ghi đọc được bằng máy tính hữu hình không chuyển tiếp là bộ nhớ bất khả biến, bộ nhớ từ, và bộ nhớ quang.

Phần mô tả sẽ được thực hiện liên quan đến các phương án của sáng chế kết hợp với các hình vẽ từ FIG.1 đến Fig.4. Cần hiểu rằng các phương án cụ thể trong tài liệu này chỉ nhằm mục đích giải thích sáng chế, mà không nhằm mục đích giới hạn sáng chế. Theo các mục đích của sáng chế, như được thể hiện và được mô tả rộng trong tài liệu này, theo một khía cạnh, sáng chế đề cập đến phương pháp và hệ thống để thực hiện việc giám sát an ninh khi tải xuống tệp, và vật ghi đọc được bằng máy tính lưu trữ các chỉ dẫn mà, khi được thực hiện bởi một hoặc nhiều bộ xử lý, khiến cho hệ thống thực hiện phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp.

Để minh họa thêm phương tiện kỹ thuật được chấp nhận bởi sáng chế để đạt được mục đích định trước của sáng chế và các hiệu quả, phương pháp và hệ thống thực hiện việc giám sát an ninh khi tải xuống tệp theo sáng chế, và các phương án, các kết cấu, các đặc điểm, và các hiệu quả của nó được minh họa chi tiết dưới đây có dựa vào các hình vẽ kèm theo và các phương án ưu tiên.

Các nội dung, đặc điểm và hiệu quả nêu trên của sáng chế và các nội dung kỹ thuật, đặc điểm và các hiệu quả khác của sáng chế được thể hiện rõ trong phần minh họa chi tiết các phương án ưu tiên dưới đây có dựa vào các hình vẽ tham chiếu. Thông qua việc minh họa các phương án, phương tiện kỹ thuật được

chấp nhận bởi sáng chế để đạt được mục đích định trước và các hiệu quả sẽ được hiểu rõ và cụ thể hơn. Tuy nhiên, các hình vẽ kèm theo chỉ để tham khảo và minh họa, mà không nhằm mục đích giới hạn sáng chế.

Fig.1 là lưu đồ phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế. Dựa vào Fig.1, phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế có thể bao gồm các bước từ S100-S102.

Tại bước S100: khi phát hiện thao tác tải xuống tệp, thì thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định xem liệu tệp được tải xuống an toàn hay không, và nếu tệp được tải xuống an toàn, thực hiện bước S101.

Trong bước này, chẳng hạn, khi người dùng nhấp điều khiển để tải xuống tệp trên mạng hoặc thực hiện hoạt động tải xuống tệp theo cách khác, thì bước này phát hiện thao tác tải xuống tệp. Khi việc phát hiện an ninh được thực hiện trên tệp được tải xuống, thì có thể phát hiện liệu tệp được tải xuống mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus hay không, để phát hiện liệu tệp được tải xuống an toàn hay không. Cụ thể, nếu tệp được tải xuống mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus, thì cho biết rằng tệp được tải xuống chứa virus và không an toàn; mặt khác, nếu tệp được tải xuống không mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus, thì cho biết rằng tệp được tải xuống là an toàn.

Ở bước S101: Nếu tệp được tải xuống an toàn, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không, và nếu công cụ tải xuống được chấp nhận là phần mềm IM, thì thực hiện ở bước S102.

Trong bước này, phần mềm IM có thể là các công cụ tải xuống như Tencent QQ và Ali Wangwang chẳng hạn.

Ở bước S102: Nếu công cụ tải xuống được chấp nhận là phần mềm IM, thì biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc được chạy trực tiếp.

Trong bước này, sau khi tệp được tải xuống hoàn toàn, vị trí lưu trữ của tệp được tải xuống có thể được tìm kiếm trước khi phần mở rộng tên tệp của tệp được tải xuống được biến đổi. Tính đến an ninh trong việc chuyển tệp, trong quá trình chuyển tệp chạy được hoặc các tệp khác, phần mềm IM, như Tencent QQ và Ali Wangwang, có thể đổi tên tệp được chuyển (chẳng hạn, biến đổi phần mở rộng tên tệp của tệp được tải xuống) để ngăn không cho tệp Trojan trong tệp được tải xuống chạy tự động. Chẳng hạn, khi tải xuống tệp, công cụ tải xuống Tencent QQ có thể thêm ".rename" vào sau phần mở rộng tên tệp của tệp được tải xuống; khi tải xuống tệp, công cụ tải xuống Ali Wangwang có thể thêm ".aliwangwang" vào sau phần mở rộng tên tệp của tệp được tải xuống. Vì vậy, trong bước này, để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp, tệp được tải xuống cần được đổi tên (để biến đổi phần mở rộng tên tệp của tệp được tải xuống). Chẳng hạn, đối với tệp được tải xuống bằng Tencent QQ, ".rename" được loại bỏ khỏi tên của tệp; đối với tệp được tải xuống bằng Ali Wangwang, ".aliwangwang" được loại bỏ khỏi tên của tệp.

Theo phương án của sáng chế, sáng chế thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không; nếu tệp được tải xuống an toàn, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không; nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp, sao cho an ninh trong quy trình chuyển tệp được bảo đảm, và trên cơ sở là người dùng được thông báo về an ninh, người dùng có thể mở hoặc chạy trực tiếp tệp, sao cho không làm ảnh hưởng đến việc sử dụng tệp được tải xuống bởi người dùng, nhờ đó tạo cho người dùng trải nghiệm dễ dàng hơn.

Fig.2 là lưu đồ phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế. Fig.2 là cải tiến dựa trên Fig.1. Dựa vào Fig.2, phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp theo phương án của sáng chế có thể bao gồm các bước từ S200-S208 dưới đây.

Ở bước S200: Khi phát hiện thao tác tải xuống tệp, thực hiện phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không, và nếu tệp được tải xuống an toàn, thì thực hiện bước S202.

Trong bước này, chẳng hạn, khi người dùng nhấp điều khiển để tải xuống tệp trên mạng hoặc thực hiện thao tác tải xuống tệp theo cách khác, bước này phát hiện thao tác tải xuống tệp. Khi việc phát hiện an ninh được thực hiện trên tệp được tải xuống, thì có thể xác định liệu tệp được tải xuống mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus hay không, để phát hiện liệu tệp được tải xuống an toàn hay không. Cụ thể, nếu tệp được tải xuống mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus, thì cho biết rằng tệp được tải xuống chứa virus và không an toàn; mặt khác, nếu tệp được tải xuống không mang các mã virus được lưu trữ trước trong cơ sở dữ liệu virus, thì cho biết rằng tệp được tải xuống an toàn.

Bước S200 có thể bao gồm bước: nếu tệp được tải xuống không an toàn, thực hiện bước S201.

Ở bước S201: Gửi thông tin rằng tệp được tải xuống không an toàn đến thiết bị đầu cuối khác, và kết thúc.

Ở bước S202: Nếu tệp được tải xuống an toàn, thì xác định liệu tệp được tải xuống là tệp chạy được hay không; nếu đúng, thì thực hiện bước S203, và nếu không đúng thì thực hiện bước S205.

Trong bước này, tệp chạy được có thể là, chẳng hạn, tệp với phần mở rộng tên tệp của tệp là exe.

Ở bước S203: xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không; nếu đúng thì thực hiện bước S206, và nếu không đúng thì thực hiện bước S207.

Trong bước này, phần mềm IM có thể là các công cụ tải xuống như Tencent QQ và Ali Wangwang.

Ở bước S205: Nếu tệp được tải xuống không phải là tệp chạy được, hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp, và kết thúc.

Trong bước này, nếu tệp được tải xuống không phải tệp chạy được, thông tin rằng tệp được tải xuống an toàn có thể được hiển thị ở thiết bị đầu cuối khách, và việc điều khiển "mở" có thể được hiển thị ở thiết bị đầu cuối khách, để nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp.

Ở bước S206: Nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp, và thực hiện bước S208.

Trong bước này, sau khi tệp được tải xuống hoàn toàn, vị trí lưu trữ của tệp được tải xuống có thể được tìm kiếm trước khi phần mở rộng tên tệp của tệp được tải xuống được biến đổi. Tính đến an ninh của việc chuyển tệp, trong suốt quá trình chuyển tệp chạy được hoặc các tệp khác, phần mềm IM, như Tencent QQ và Ali Wangwang, có thể đổi tên tệp được chuyển (chẳng hạn, biến đổi phần mở rộng tên tệp của tệp được tải xuống) để ngăn không cho tệp Trojan trong tệp được tải xuống chạy tự động. Chẳng hạn, khi tải xuống tệp, công cụ tải xuống Tencent QQ có thể thêm ".rename" vào sau phần mở rộng tên tệp của tệp được tải xuống; khi tải xuống tệp, công cụ tải xuống Ali Wangwang có thể thêm ".aliwangwang" vào sau phần mở rộng tên tệp của tệp được tải xuống. Vì vậy, trong bước này, để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy

trực tiếp, tệp được tải xuống cần được đổi tên (để biến đổi phần mở rộng tên tệp of tệp được tải xuống). Chẳng hạn, đối với tệp được tải xuống bằng Tencent QQ, ".rename" được loại bỏ khỏi tên của tệp; đối với tệp được tải xuống bằng Ali Wangwang, ".aliwangwang" được loại bỏ khỏi tên của tệp.

Ở bước S207: Nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, nhắc thiết bị đầu cuối khách biến đổi phần mở rộng tên tệp của tệp được tải xuống, và kết thúc.

Trong bước này, nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, thì thông tin rằng tệp được tải xuống an toàn có thể được hiển thị ở thiết bị đầu cuối khách, và thông tin về cách để biến đổi phần mở rộng tên tệp của tệp được tải xuống cũng có thể được hiển thị ở thiết bị đầu cuối khách, để nhắc thiết bị đầu cuối khách rằng thiết bị đầu cuối khách có thể biến đổi phần mở rộng tên tệp của tệp được tải xuống, để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp.

Ở bước S208: Hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp.

Trong bước này, phần minh họa được thể hiện trên Fig.3 là một ví dụ. Trên Fig.3, thông tin rằng tệp được tải xuống an toàn (chẳng hạn trên Fig.3, tệp được tải xuống an toàn) được hiển thị ở thiết bị đầu cuối khách, và tên và cách tải xuống tệp được tải xuống cũng được hiển thị trên Fig.3. Các điều khiển mở 301 và 303, và các thư mục mở 302 và 305 cũng được hiển thị ở thiết bị đầu cuối khách, để nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được chạy hoặc được mở trực tiếp.

Theo phương án của sáng chế, sáng chế thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không;

nếu tệp được tải xuống an toàn, xác định liệu tệp được tải xuống là tệp chạy được hay không; nếu đúng thì xác định thêm liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không; nếu công cụ tải xuống được chấp nhận là phần mềm IM, thì biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp; nếu tệp được tải xuống không phải tệp chạy được, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp, sao cho an ninh trong quy trình chuyển tệp được đảm bảo, và trên cơ sở được thông báo về an ninh, người dùng được phép mở hoặc chạy trực tiếp tệp theo các kết quả xác định khác nhau, để không làm ảnh hưởng đến việc sử dụng tệp được tải xuống bởi người dùng trong bất kỳ trường hợp nào, nhờ đó tạo trải nghiệm dễ dàng hơn cho người dùng.

Fig.4 là sơ đồ khối về khung chính của hệ thống thực hiện kiểm soát an ninh khi tải xuống tệp theo phương án khác của sáng chế. Dựa vào Fig.4, hệ thống thực hiện việc kiểm soát an ninh khi tải xuống tệp bao gồm: môđun phát hiện 401 và môđun xác định 403.

Môđun phát hiện 401 có thể được bố trí trong bộ dịch vụ mạng, và được tạo cấu hình để, khi phát hiện thao tác tải xuống tệp, thực hiện phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không. Nếu tệp được tải xuống an toàn, thì môđun xác định được thực hiện.

Môđun phát hiện 401 còn được cấu tạo để, nếu tệp được tải xuống không an toàn, gửi thông tin rằng tệp được tải xuống không an toàn đến thiết bị đầu cuối khách.

Môđun xác định 403 được tạo cấu hình để, nếu tệp được tải xuống an toàn, xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không, và nếu công cụ tải xuống được chấp nhận là phần

mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp.

Ngoài ra, môđun xác định 403 còn được tạo cấu hình để xác định liệu tệp được tải xuống là tệp chạy được hay không; nếu tệp được tải xuống không phải tệp chạy được, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp; nếu tệp được tải xuống là tệp chạy được, thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không.

Ngoài ra, môđun xác định 403 còn được tạo cấu hình để, nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách để biến đổi phần mở rộng tên tệp của tệp được tải xuống.

Ngoài ra, hệ thống thực hiện việc kiểm soát an ninh khi tải xuống tệp còn bao gồm môđun hiển thị 405.

Môđun hiển thị 405 có thể được bố trí tại thiết bị đầu cuối khách. Môđun hiển thị 405 hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp.

Theo phương án của sáng chế, sáng chế thực hiện phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không; nếu tệp được tải xuống an toàn, thì xác định liệu tệp được tải xuống là tệp chạy được hay không; nếu đúng, còn xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không; nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp; nếu tệp được tải xuống không phải tệp chạy được, hiển thị kết quả phát hiện an

ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp, sao cho an ninh trong quy trình chuyển tệp được đảm bảo, và trên cơ sở là người dùng được thông báo về an ninh, người dùng được phép để mở hoặc chạy trực tiếp tệp dưới các kết quả xác định khác nhau, để không làm ảnh hưởng đến việc sử dụng tệp được tải xuống bởi người dùng trong trường hợp bất kỳ, nhờ đó khiến trải nghiệm của người dùng dễ dàng hơn.

Theo một khía cạnh nữa của sáng chế, tất cả hoặc một phần của thủ tục trong phương pháp theo các phương án có thể được thực hiện bởi chương trình máy tính chỉ dẫn phần cứng liên quan. Chương trình có thể được lưu trữ trong vật ghi đọc được bằng máy tính không chuyển tiếp. Khi chương trình được chạy, thủ tục của phương pháp theo các phương án của sáng chế được thực hiện. Vật ghi bao gồm, nhưng không bị giới hạn vào, đĩa từ, đĩa quang, bộ nhớ chỉ đọc (ROM), bộ nhớ truy cập ngẫu nhiên (RAM), bộ nhớ ngẫu nhiên (RAM), bộ nhớ nhanh, hoặc các loại tương tự.

Phần mô tả trên đây về các phương án mẫu của sáng chế đã được thể hiện chỉ nhằm các mục đích minh họa và mô tả và không nhằm mục đích bao gồm tất cả hoặc giới hạn sáng chế vào đúng các dạng được bộc lộ. Các biến đổi và các thay đổi có thể thực hiện được theo phần mô tả ở trên.

Các phương án được chọn và được mô tả để giải thích các nguyên lý của sáng chế và ứng dụng thực tế của sáng chế để khiến những người có trình độ trung bình trong lĩnh vực sử dụng sáng chế và các phương án khác nhau với các biến đổi khác nhau tương ứng với việc sử dụng cụ thể được thiết kế. Các phương án thay thế sẽ trở nên rõ ràng với người có trình độ trung bình trong lĩnh vực của sáng chế mà không nằm ngoài phạm vi của sáng chế. Do đó, phạm vi của sáng chế được xác định bởi yêu cầu bảo hộ đính kèm thay vì phần mô tả và các phương án mẫu trên đây.

YÊU CẦU BẢO HỘ

1. Phương pháp thực hiện giám sát an ninh khi tải xuống tệp bao gồm các bước:

khi phát hiện thao tác tải xuống tệp, thực hiện phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không;

nếu tệp được tải xuống an toàn, xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm gửi tin nhắn tức thời (IM) hay không; và

nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp; và

xác định liệu tệp được tải xuống là tệp chạy được hay không, nếu tệp được tải xuống không phải tệp chạy được thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp; nếu tệp được tải xuống là tệp chạy được thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không.

2. Phương pháp theo điểm 1, trong đó nếu công cụ tải xuống được chấp nhận là phần mềm IM thì phương pháp còn bao gồm bước:

hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp.

3. Phương pháp theo điểm 1, trong đó nếu tệp được tải xuống an toàn, phương pháp còn bao gồm bước:

nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách,

và nhắc thiết bị đầu cuối khách biến đổi phần mở rộng tên tệp của tệp được tải xuống.

4. Phương pháp theo điểm 1, trong đó khi phát hiện thao tác tải xuống tệp, phương pháp còn bao gồm bước:

nếu tệp được tải xuống không an toàn, gửi thông tin rằng tệp được tải xuống không an toàn đến thiết bị đầu cuối khách.

5. Hệ thống thực hiện việc giám sát an ninh khi tải xuống tệp, bao gồm:

môđun phát hiện, được tạo cấu hình để, khi phát hiện thao tác tải xuống tệp, thực hiện phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn; và

môđun xác định, được tạo cấu hình để, nếu tệp được tải xuống an toàn, xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm gửi tin nhắn tức thời (IM) hay không, và nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp; và

xác định liệu tệp được tải xuống là tệp chạy được hay không, nếu tệp được tải xuống không phải tệp chạy được thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp; nếu tệp được tải xuống là tệp chạy được thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không.

6. Hệ thống theo điểm 5, hệ thống này còn bao gồm:

môđun hiển thị, được tạo cấu hình để hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp.

7. Hệ thống theo điểm 5, trong đó môđun xác định còn được tạo cấu hình để, nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách để biến đổi phần mở rộng tên tệp của tệp được tải xuống.

8. Hệ thống theo điểm 5, trong đó môđun phát hiện còn được tạo cấu hình để, nếu tệp được tải xuống không an toàn, gửi thông tin rằng tệp được tải xuống không an toàn đến thiết bị đầu cuối khách.

9. Vật ghi đọc được bằng máy tính lưu trữ các chỉ dẫn mà, khi được thực hiện bởi một hoặc nhiều bộ xử lý, khiến hệ thống thực hiện phương pháp thực hiện việc giám sát an ninh khi tải xuống tệp, phương pháp bao gồm các bước:

khi phát hiện thao tác tải xuống tệp, thực hiện việc phát hiện an ninh trên tệp được tải xuống để xác định liệu tệp được tải xuống an toàn hay không;

nếu tệp được tải xuống an toàn, xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm gửi tin nhắn tức thời (IM); và

nếu công cụ tải xuống được chấp nhận là phần mềm IM, biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp; và

xác định liệu tệp được tải xuống là tệp chạy được hay không, nếu tệp được tải xuống không phải tệp chạy được thì hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có thể được mở trực tiếp; nếu tệp được tải xuống là tệp chạy được thì xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không.

10. Vật ghi đọc được bằng máy tính theo điểm 9, trong đó nếu công cụ tải xuống được chấp nhận là phần mềm IM, phương pháp còn bao gồm bước:

hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách rằng tệp được tải xuống có khả năng được mở hoặc chạy trực tiếp.

11. Vật ghi đọc được bằng máy tính theo điểm 9, trong đó nếu tệp được tải xuống an toàn, phương pháp còn bao gồm bước:

nếu công cụ tải xuống được chấp nhận không phải phần mềm IM, hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở thiết bị đầu cuối khách, và nhắc thiết bị đầu cuối khách để biến đổi phần mở rộng tên tệp của tệp được tải xuống.

12. Vật ghi đọc được bằng máy tính theo điểm 9, trong đó khi phát hiện thao tác tải xuống tệp, phương pháp còn bao gồm bước:

nếu tệp được tải xuống không an toàn, gửi thông tin rằng tệp được tải xuống không an toàn đến thiết bị đầu cuối khách.

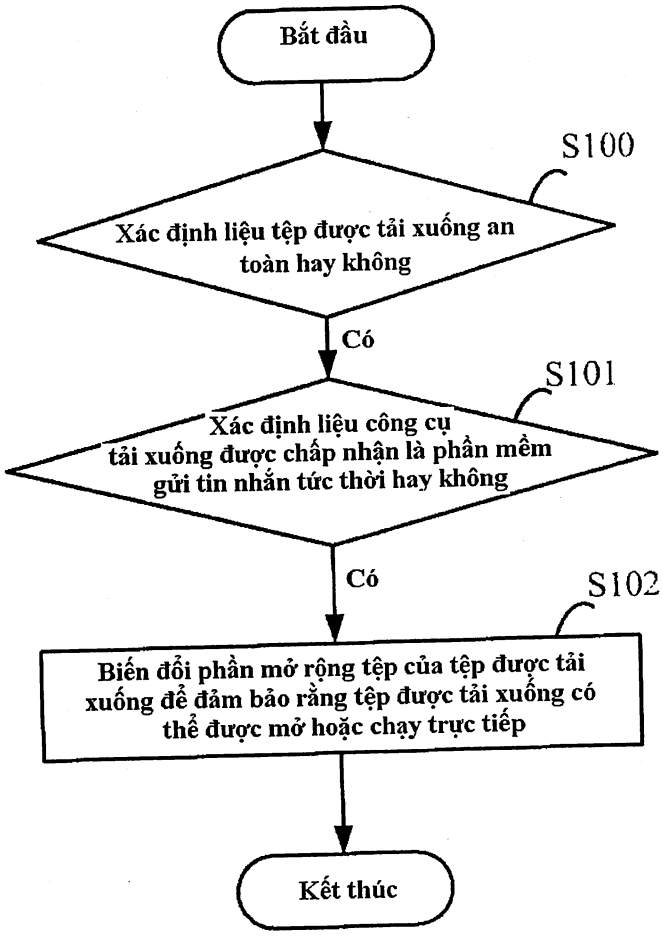

Bắt đầu
S100
Xác định liệu tệp được tải xuống an toàn hay không
Có
S101
Xác định liệu công cụ tải xuống được chấp nhận là phần mềm gửi tin nhắn tức thời hay không
Có
S102
Biến đổi phần mở rộng tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp
Kết thúc

FIG. 1

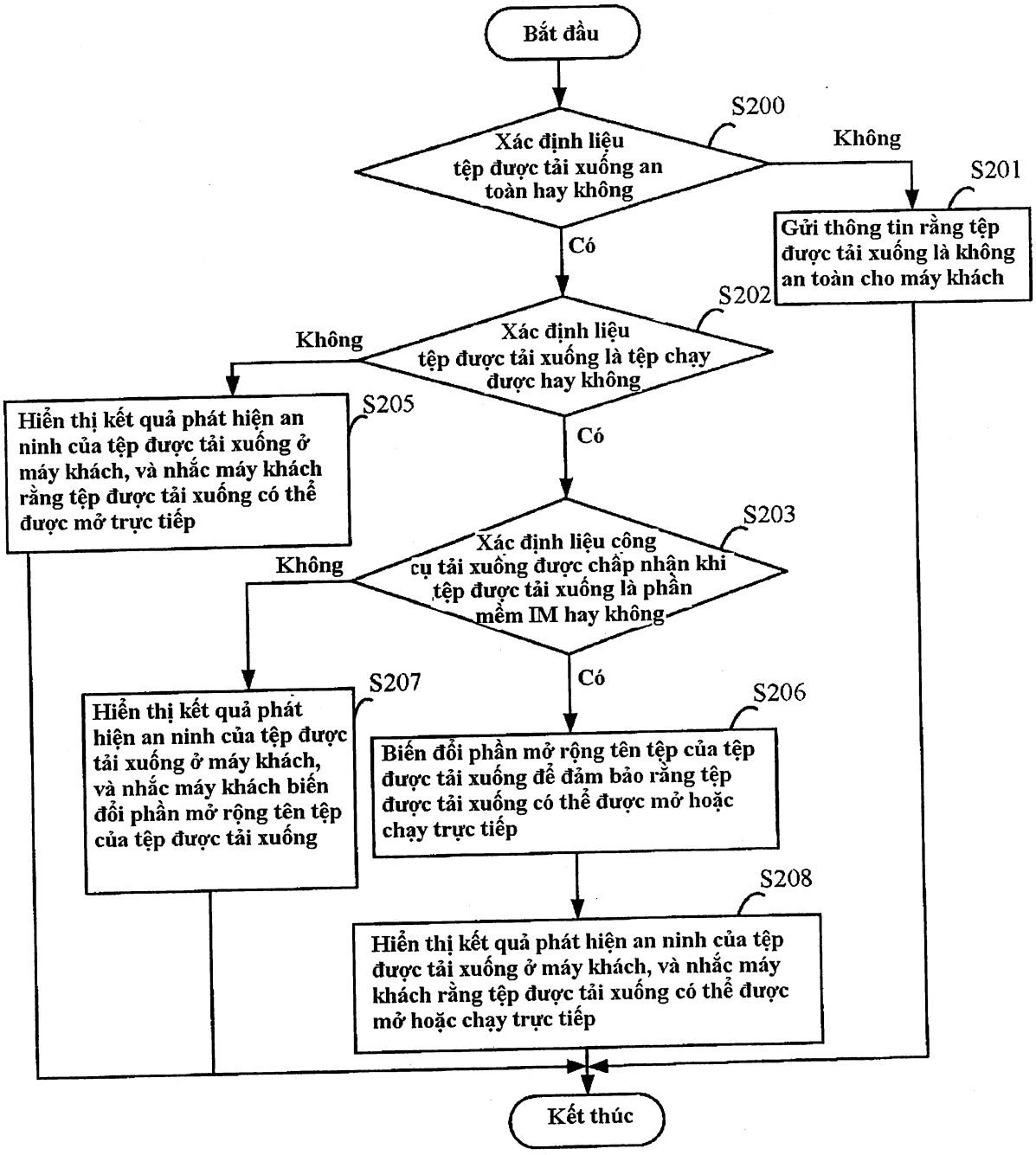

Bắt đầu
S200
Xác định liệu tệp được tải xuống an toàn hay không
Không
S201
Gửi thông tin rằng tệp được tải xuống là không an toàn cho máy khách
Có
S202
Xác định liệu tệp được tải xuống là tệp chạy được hay không
Không
S205
Hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở máy khách, và nhắc máy khách rằng tệp được tải xuống có thể được mở trực tiếp
Có
S203
Xác định liệu công cụ tải xuống được chấp nhận khi tệp được tải xuống là phần mềm IM hay không
Không
S207
Hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở máy khách, và nhắc máy khách biến đổi phần mở rộng tên tệp của tệp được tải xuống
Có
S206
Biến đổi phần mở rộng tên tệp của tệp được tải xuống để đảm bảo rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp
S208
Hiển thị kết quả phát hiện an ninh của tệp được tải xuống ở máy khách, và nhắc máy khách rằng tệp được tải xuống có thể được mở hoặc chạy trực tiếp
Kết thúc

FIG. 2

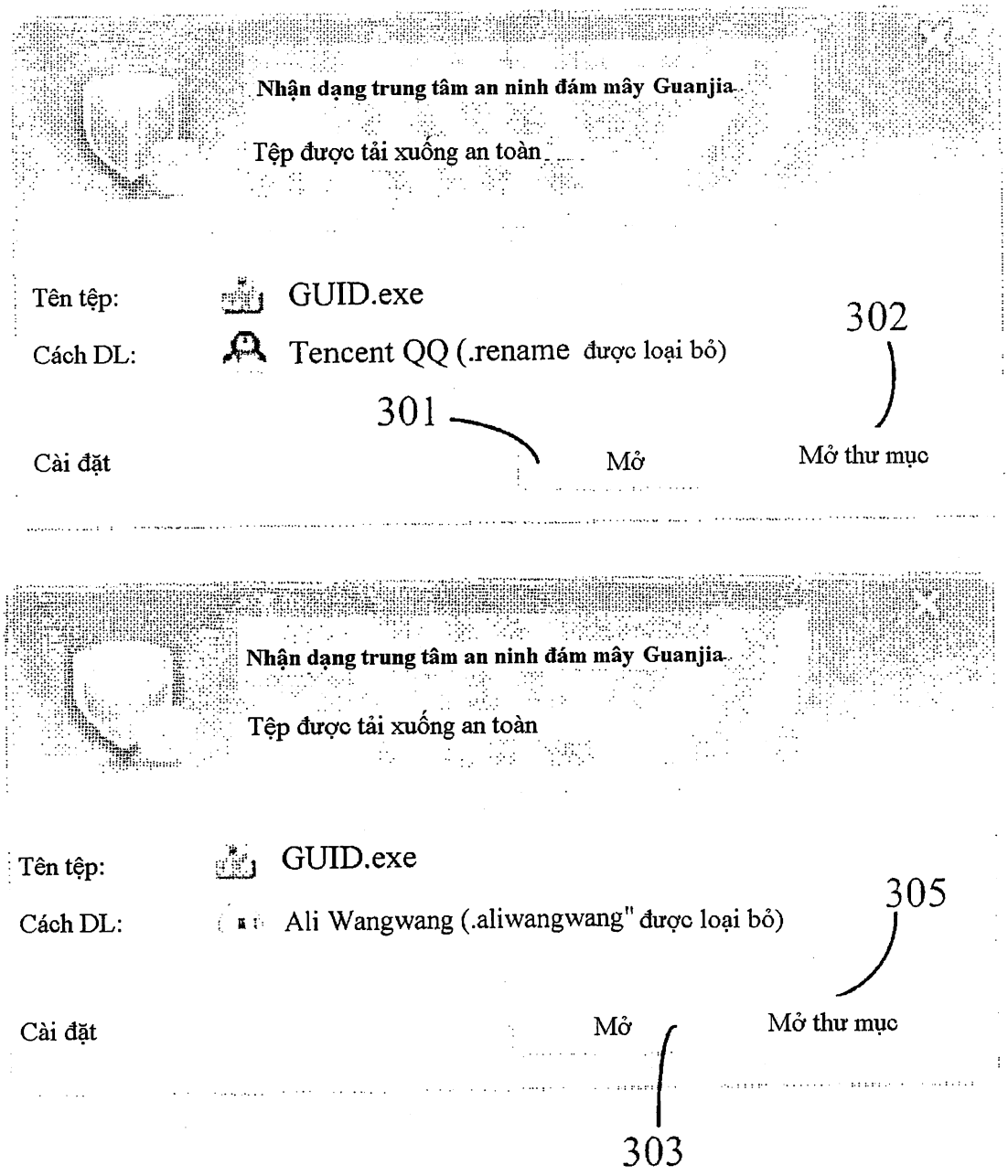

Nhận dạng trung tâm an ninh đám mây Guanjia
Tệp được tải xuống an toàn
Tên tệp:
GUID.exe
Cách DL:
Tencent QQ (.rename được loại bỏ)
302
301
Cài đặt
Mở
Mở thư mục
Nhận dạng trung tâm an ninh đám mây Guanjia
Tệp được tải xuống an toàn
Tên tệp:
GUID.exe
Cách DL:
Ali Wangwang (.aliwangwang" được loại bỏ)
305
Cài đặt
Mở
Mở thư mục
303

FIG. 3

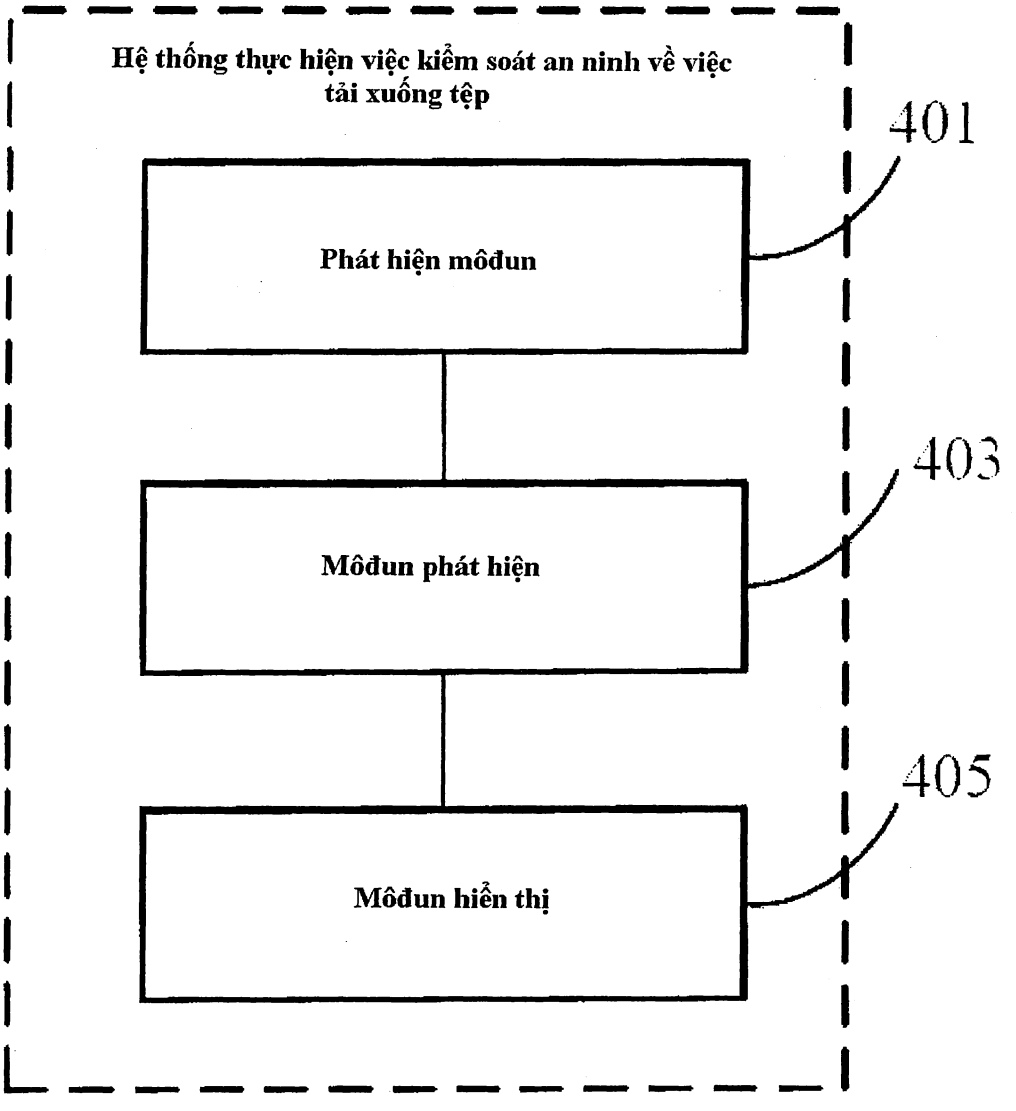

Hệ thống thực hiện việc kiểm soát an ninh về việc tải xuống tệp
401
Phát hiện môđun
403
Môđun phát hiện
405
Môđun hiển thị

FIG. 4