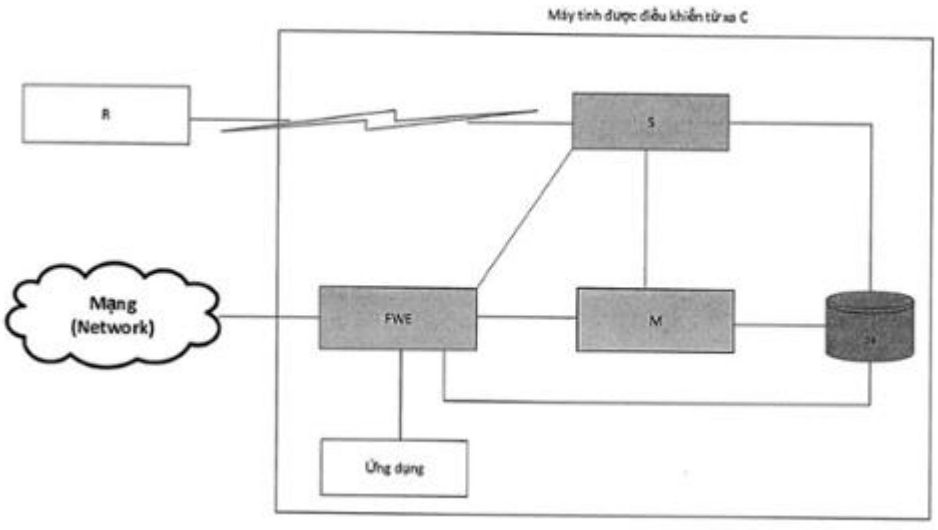
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0035291**
(51)[7] **G06F 21/00**; G06F 21/62
(13) **B**

(21) 1-2019-05644
(22) 14/10/2019
(45) 25/04/2023 421
(43) 26/04/2021 397
(73) Công ty cổ phần E LINK GATE (VN)
35 Nguyễn Thông, phường 7, quận 3, thành phố Hồ Chí Minh
(72) Nguyễn Xuân Hoàng (VN).
(74) Công ty Luật TNHH Tư vấn Quốc tế (INDOCHINE COUNSEL)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP KIỂM SOÁT VIỆC TRUY XUẤT DỮ LIỆU TRÊN MÁY TÍNH ĐƯỢC ĐIỀU KHIỂN TỪ XA TRONG GIAO DỊCH ĐIỀU KHIỂN TỪ XA

(57) Sáng chế này đề xuất hệ thống kiểm soát việc truy xuất trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa, bao gồm; (i) cơ sở dữ liệu cần bảo vệ (DB) chứa danh sách các tệp dữ liệu cần bảo vệ; và quy tắc ứng xử tương ứng của (các) phần mềm của hệ thống đối với các ứng dụng trên máy tính được điều khiển từ xa có truy xuất trực tiếp hoặc gián tiếp vào tệp dữ liệu cần bảo vệ (sau đây gọi là "ứng dụng có nguy cơ"); (ii)phần mềm kiểm soát ứng dụng (M) được kết nối với cơ sở dữ liệu cần bảo vệ (DB) để thực hiện việc giám sát và phát hiện ứng dụng có nguy cơ và thực hiện (các) hành vi xử lý đối với ứng dụng có nguy cơ phù hợp với quy tắc ứng xử tương ứng được thiết lập trong cơ sở dữ liệu cần bảo vệ (DB); và (iii)phần mềm phục vụ điều khiển từ xa (S) được kết nối với phần mềm kiểm soát ứng dụng M để liên lạc và lấy thông tin về ứng dụng có nguy cơ và thực hiện (các) hành vi xử lý đối với ứng dụng có nguy cơ phù hợp với quy tắc ứng xử tương ứng được thiết lập trong cơ sở dữ liệu cần bảo vệ (DB). Sáng chế cũng đề xuất phương pháp kiểm soát việc truy xuất hên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa bằng cách sử dụng hệ thống kiểm soát truy xuất dữ liệu nói trên.



Lĩnh vực kỹ thuật của sáng chế

Sáng chế đề xuất hệ thống và phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa, nhờ đó có thể ngăn chặn việc truy xuất không được phép dữ liệu cần bảo vệ trên máy tính được điều khiển từ xa bởi người điều khiển từ xa thông qua phần mềm điều khiển từ xa trên máy tính điều khiển từ xa.

Tình trạng kỹ thuật của sáng chế

Tác giả sáng chế này chưa biết đến giải pháp nào để bảo vệ ngăn chặn việc truy xuất không được phép dữ liệu cần bảo vệ trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa bởi người điều khiển từ xa.

Trên thực tế, hiện nay, dịch vụ hỗ trợ máy tính thông qua việc sử dụng phần mềm điều khiển từ xa (ví dụ như phần mềm Teamviewer, LogMeIn…) hay việc sử dụng các thiết bị phần cứng điều khiển từ xa như iDRAC, KVM over IP… là khá phổ biến. Nhược điểm của tất cả các giải pháp này là người điều khiển từ xa có toàn quyền thao tác và truy xuất đến bất cứ dữ liệu nào, bao gồm cả các dữ liệu quan trọng mà người dùng máy tính được điều khiển từ xa muốn bảo mật, chẳng hạn như tệp dữ liệu chứa các thông tin mật khẩu, mã số tài khoản, hình ảnh riêng tư… có trên máy tính được điều khiển từ xa và do vậy, người điều khiển từ xa có thể truy xuất trái phép, lấy cắp thông tin trên máy tính được điều khiển từ xa bằng cách tải dữ liệu trên máy tính được điều khiển từ xa thông qua giao tiếp mạng tới một địa chỉ khác, hoặc trực tiếp mở tệp chứa dữ liệu trên máy tính được điều khiển từ xa và chụp nội dung màn hình thông qua ứng dụng điều khiển từ xa.

Bản chất kỹ thuật của sáng chế

Nhằm mục đích giải quyết hạn chế nói trên trong việc ngăn chặn việc truy xuất trái phép dữ liệu cần bảo vệ trên máy tính được điều khiển từ xa bởi người điều khiển từ xa, theo mục đích thứ nhất, sáng chế đề xuất hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa (còn gọi tắt là "**hệ thống kiểm soát truy xuất dữ liệu**") bao gồm:

(i) Cơ sở dữ liệu cần bảo vệ (DB) chứa:

a. Danh sách các tệp dữ liệu cần bảo vệ được liệt kê theo đường dẫn (path) của các tệp dữ liệu cần bảo vệ hoặc thư mục chứa các tệp dữ liệu cần bảo vệ đó trên máy tính được điều khiển từ xa (C); và

b. Quy tắc ứng xử đối với mỗi ứng dụng trên máy tính được điều khiển từ xa (C), mà có thể thiết lập một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của hệ thống kiểm soát truy xuất dữ liệu đối với một ứng dụng trên máy tính được điều khiển từ xa có truy xuất trực tiếp hoặc gián tiếp vào tệp dữ liệu cần bảo vệ (sau đây gọi tắt là "**ứng dụng có nguy cơ**"): cấm việc truy xuất vào tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ; dừng hoạt động của tất cả các ứng dụng có nguy cơ đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ; cho phép ứng dụng có nguy cơ truy xuất vào tệp dữ liệu cần bảo vệ nhưng vùng dữ liệu màn hình tương ứng được loại bỏ trước khi được thu thập và gửi về máy tính điều khiển từ xa; cho phép một hoặc nhiều ứng dụng cụ thể được phép truy xuất vào tệp dữ liệu cần bảo vệ (sau đây gọi là "**ứng dụng ngoại lệ**").

(ii) Phần mềm kiểm soát ứng dụng (M) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối với và truy xuất, đọc danh sách các tệp dữ liệu cần bảo vệ trong cơ sở dữ liệu cần bảo vệ (DB), và có chức năng, khi có giao dịch

điều khiển từ xa, phát hiện và liệt kê ngay lập tức khi phát hiện (các) ứng dụng có nguy cơ, trừ (các) ứng dụng ngoại lệ trên máy tính được điều khiển từ xa (C) vào danh sách các ứng dụng có nguy cơ được thiết lập, lưu trữ và cập nhật tự động ngay trong phần mềm kiểm soát ứng dụng (M) này mỗi khi có ứng dụng có nguy cơ được phát hiện bởi phần mềm kiểm soát ứng dụng (M), và thực hiện một trong những hành vi ứng xử sau đây, tùy thuộc vào việc thiết lập quy tắc ứng xử trong cơ sở dữ liệu (DB): cấm việc truy xuất nội dung tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ đó; dừng hoạt động của tất cả các ứng dụng đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ; cho phép ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ;

(iii) Phần mềm phục vụ điều khiển từ xa (S) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối với phần mềm điều khiển từ xa trên máy tính từ xa khi thực hiện giao dịch điều khiển từ xa, và có thể kết nối với và truy xuất, đọc danh sách các tệp dữ liệu cần bảo vệ trong cơ sở dữ liệu cần bảo vệ (DB), kết nối với phần mềm kiểm soát ứng dụng (M) sao cho phần mềm phục vụ điều khiển từ xa (S) này có thể liên lạc và nhận chia sẻ thông tin về danh sách ứng dụng có nguy cơ từ phần mềm kiểm soát ứng dụng (M) để thực hiện các chức năng:

a. Cho phép thực hiện việc điều khiển từ xa máy tính được điều khiển từ xa bởi phần mềm điều khiển từ xa trên máy tính điều khiển từ xa;

b. Thu thập thông tin thay đổi dữ liệu màn hình máy tính được điều khiển từ xa (C);

c. Tùy thuộc vào việc thiết lập quy tắc ứng xử tương ứng trong cơ sở dữ liệu cần bảo vệ (DB), thực hiện việc loại bỏ dữ liệu màn hình tương ứng với ứng dụng có nguy cơ đó trên máy tính được điều khiển từ xa (C) trước khi gửi về phần mềm điều khiển từ xa;

d. Nén và mã hóa dữ liệu màn hình máy tính được điều khiển từ xa (C) để gửi về phần mềm điều khiển từ xa trên máy tính điều khiển từ xa; và

e. Gửi dữ liệu màn hình đã được nén và mã hóa tới ứng dụng điều khiển từ xa thông qua các kênh truyền dữ liệu được trang bị cho máy tính được điều khiển từ xa để phục vụ cho việc truyền dữ liệu trong giao dịch điều khiển từ xa.

Cơ chế vận hành của hệ thống kiểm soát truy xuất dữ liệu nêu trên được mô tả như sau:

Cơ sở dữ liệu cần bảo vệ (DB) gồm danh sách đường dẫn các tệp dữ liệu cần bảo vệ và quy tắc ứng xử cho từng ứng dụng trên máy tính được điều khiển từ xa được thiết lập sẵn bởi người dùng máy tính được điều khiển từ xa. Cơ sở dữ liệu cần bảo vệ (DB) như vậy có thể được cập nhật bất kỳ thời điểm nào bởi người dùng máy tính được điều khiển từ xa (C).

Tùy thuộc vào sự lựa chọn hoặc thiết lập của người dùng máy tính được điều khiển từ xa, phần mềm kiểm soát ứng dụng (M) có thể được kích hoạt tự động khi khởi động máy tính được điều khiển từ xa (C) hoặc kích hoạt chủ động bởi người dùng, hoặc kích hoạt khi có kết nối giữa phần mềm điều khiển từ xa và phần mềm phục vụ điều khiển từ xa (S) để thực hiện giao dịch điều khiển từ xa máy tính được điều khiển từ xa (C), và việc giám sát các ứng dụng có nguy cơ và thực hiện các hành vi ứng xử tương ứng phù hợp với các thiết lập của quy tắc ứng xử của cơ sở dữ liệu cần bảo vệ (DB) đối với các ứng dụng có nguy cơ đó được thực hiện trong giao dịch điều khiển từ xa đối với máy tính được điều khiển từ xa (C). Cụ thể, trong quá trình hoạt động, phần mềm kiểm soát ứng dụng (M) sẽ đọc danh sách các tệp dữ liệu cần bảo vệ trong cơ sở dữ liệu cần bảo vệ (DB), và giám sát và thu thập thông tin các ứng dụng có truy xuất vào các tệp tin cần bảo vệ và liệt kê các ứng dụng như vậy, ngay khi phát hiện ra, vào danh sách các ứng dụng có nguy cơ. Tùy thuộc vào quy tắc ứng xử được thiết lập trong cơ sở dữ liệu cần bảo vệ (DB) đối với một ứng dụng có nguy cơ, cụ thể trong một phiên giao dịch điều khiển từ xa, phần mềm kiểm soát ứng dụng (M) sẽ thực hiện hành vi ứng xử tương ứng

đối với ứng dụng đó, bao gồm việc: cấm việc truy xuất nội dung tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ đó; dừng hoạt động của tất cả các ứng dụng đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ; cho phép (các) ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ. Đồng thời, thông tin về các ứng dụng có nguy cơ sẽ được chia sẻ tới phần mềm phục vụ điều khiển từ xa (S) thông qua các giao tiếp trao đổi thông tin giữa các ứng dụng như pipe, socket, share memory…

Khi phần mềm điều khiển từ xa thực hiện kết nối tới phần mềm phục vụ điều khiển từ xa (S) trên máy tính được điều khiển từ xa (C) để thực hiện việc điều khiển từ xa, phần mềm phục vụ điều khiển từ xa (S) sẽ thu thập thông tin về sự thay đổi dữ liệu màn hình của máy tính được điều khiển từ xa (C) và gửi về phần mềm điều khiển từ xa cho mục đích điều khiển từ xa máy tính được điều khiển từ xa (C). Đồng thời, phần mềm phục vụ điều khiển từ xa (S) liên lạc tới phần mềm kiểm soát ứng dụng (M) để lấy thông tin về các ứng dụng có nguy cơ, và thực hiện việc loại bỏ dữ liệu màn hình tương ứng với (các) ứng dụng mà phần mềm phục vụ điều khiển từ xa (S) cần thực hiện việc loại bỏ dữ liệu màn hình như vậy theo các thiết lập của quy tắc ứng xử trong cơ sở dữ liệu cần bảo vệ (DB) đối với (các) ứng dụng đó trước khi nén, mã hóa dữ liệu và gửi tới phần mềm điều khiển từ xa. Kết quả là phần mềm điều khiển từ xa chỉ thấy được dữ liệu màn hình tương ứng với các ứng dụng không nằm trong danh sách các ứng dụng có nguy cơ.

Theo một phương án khác, sáng chế đề xuất hệ thống kiểm soát truy xuất dữ liệu như đã mô tả trên, trong đó:

(i) Quy tắc ứng xử của cơ sở dữ liệu cần bảo vệ (DB) có thể thiết lập thêm một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của hệ thống kiểm soát truy xuất dữ liệu đối với ứng dụng có nguy cơ: cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C); cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M);

và cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và

(ii) Hệ thống kiểm soát truy xuất dữ liệu bao gồm thêm phần mềm tường lửa mở rộng (FWE) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối và truy xuất, đọc nội dung trong cơ sở dữ liệu cần bảo vệ (DB), theo dõi và kiểm soát kết nối mạng của các ứng dụng/ phần mềm trên máy tính được điều khiển từ xa (C), có thể được kích hoạt trong đó việc kết nối với phần mềm kiểm soát ứng dụng (M) theo cách thức sao cho sao cho phần mềm tường lửa mở rộng (FWE) có thể liên lạc và nhận chia sẻ thông tin về ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M), và việc kết nối với phần mềm phục vụ điều khiển từ xa (S) theo cách thức sao cho khi có kết nối giữa phần mềm điều khiển từ xa và phần mềm phục vụ điều khiển từ xa (S) để thực hiện giao dịch điều khiển từ xa máy tính được điều khiển từ xa (C), thì phần mềm tường lửa mở rộng (FWE) sẽ thực hiện hành vi ứng xử tương ứng với thiết lập của cơ sở dữ liệu cần bảo vệ (DB) như được mô tả trong mục (i) ngay trên đây, bao gồm: cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C); cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M).

Với hệ thống kiểm soát truy xuất dữ liệu bao gồm thêm phần mềm tường lửa mở rộng (FWE) và các khả năng thiết lập hành vi ứng xử bổ sung cho quy tắc ứng xử của cơ sở dữ liệu cần bảo vệ (DB) như mô tả trên, người dùng máy tính được điều khiển từ xa sẽ có thêm lựa chọn trong việc kiểm soát việc truy xuất vào tệp dữ liệu cần bảo vệ bởi các ứng dụng có nguy cơ. Tùy thuộc vào thiết lập của người dùng máy tính được điều khiển từ xa (C), phần mềm tường lửa mở rộng (FWE) có thể được kích hoạt chủ động bởi người dùng máy tính được điều khiển từ xa (C), hoặc được kích hoạt tự động khi khởi động máy tính được điều khiển từ xa (C) hoặc được kích hoạt tự động khi phần mềm phục vụ điều khiển từ xa (S) được kích hoạt.

Có thể nhận biết một cách dễ dàng bởi người có kiến thức chuyên môn trong lĩnh vực chuyên môn rằng hoàn toàn có khả năng tích hợp phần mềm kiểm soát ứng dụng (M), phần mềm phục vụ điều khiển từ xa (S), và phần mềm tường lửa mở rộng (FWE), khi có mặt, trong một phần mềm duy nhất có các chức năng tương đương, mà việc tích hợp như vậy, cũng là một phương án thực hiện của sáng chế này.

Theo mục đích thứ hai, sáng chế này đề xuất phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa (C) trong giao dịch điều khiển từ xa bằng cách sử dụng hệ thống kiểm soát truy xuất dữ liệu như đã mô tả trên. Phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa bao gồm các việc sau:

(i) Thiết lập cơ sở dữ liệu cần bảo vệ (DB) trên máy tính được điều khiển từ xa (C) bằng cách liệt kê các tệp dữ liệu, thư mục cần bảo vệ vào danh sách tệp dữ liệu cần bảo vệ; và liệt kê quy tắc ứng xử cho từng ứng dụng trên máy tính được điều khiển từ xa (C), mà các quy tắc này có thể thiết lập một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của hệ thống kiểm soát truy xuất dữ liệu đối với một ứng dụng trên máy tính được điều khiển từ xa (C) có truy xuất vào tệp dữ liệu cần bảo vệ (sau đây gọi là "**ứng dụng có nguy cơ**"):

a. cấm việc truy xuất vào tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ; dừng hoạt động của tất cả các ứng dụng có nguy cơ đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ;

b. cho phép ứng dụng có nguy cơ truy xuất vào tệp dữ liệu cần bảo vệ nhưng vùng dữ liệu màn hình tương ứng được loại bỏ trước khi được thu thập và gửi về máy tính điều khiển từ xa;

c. chỉ cho phép (các) ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ;

và, khi hệ thống kiểm soát truy xuất dữ liệu có thêm phần mềm tường lửa mở rộng (FWE),

d. cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C);

e. cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và

f. cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M).

(ii) Kích hoạt chủ động phần mềm kiểm soát ứng dụng (M) bởi người dùng máy tính được điều khiển từ xa hoặc thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng (M) này khi khởi động máy tính được điều khiển từ xa (C), hoặc thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng (M) này khi có kết nối giữa phần mềm điều khiển từ xa với phần mềm phục vụ điều khiển từ xa (S) để thực hiện giao dịch điều khiển từ xa máy tính được điều khiển từ xa (C);

(iii) Kích hoạt chủ động phần mềm tường lửa mở rộng (FWE) bởi người dùng máy tính được điều khiển từ xa hoặc thiết lập chế độ kích hoạt tự động phần mềm tường lửa mở rộng (FWE) khi khởi động máy tính được điều khiển từ xa (C), hoặc thiết lập chế độ kích hoạt tự động phần mềm tường lửa mở rộng (FWE) khi có kết nối giữa phần mềm điều khiển từ xa và phần mềm phục vụ điều khiển từ xa (S) để thực hiện việc điều khiển từ xa máy tính được điều khiển từ xa (C); và

(iv) Cho phép phần mềm điều khiển từ xa kết nối với phần mềm phục vụ điều khiển từ xa (S) để thực hiện việc điều khiển từ xa đối với máy tính được điều khiển từ xa (C).

Các lợi ích của sáng chế

Hệ thống và phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa theo sáng chế này đạt được các lợi ích sau:

- Cho phép ngăn chặn việc gửi/tải không được phép các tệp tin cần bảo vệ thông qua giao tiếp mạng tới một địa chỉ khác bởi người điều khiển từ xa;

- Cho phép ngăn chặn việc mở và xem không được phép dữ liệu các tệp tin cần bảo vệ trên máy tính được điều khiển từ xa, và chụp nội dung màn hình dữ liệu đó bởi người điều khiển từ xa.

Mô tả vắn tắt hình vẽ

Mô tả chi tiết dưới đây về phương án thực hiện của sáng chế theo cách thức làm ví dụ để minh họa cho sáng chế, có đề cập đến các hình vẽ kèm theo, trong đó:

Fig. 1 là hình vẽ sơ đồ khối thể hiện hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo một phương án của sáng chế;

Fig. 2 là sơ đồ khối thể hiện hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo một phương án khác của sáng chế;

Fig. 3 là sơ đồ khối thể hiện cấu trúc của phần mềm kiểm soát ứng dụng (M) được thể hiện trên Fig. 1 và Fig. 2 trong mối liên hệ với các thành phần cơ bản khác của một máy tính;

Fig. 4 là giản đồ thể hiện cơ chế hoạt động của phần mềm phục vụ điều khiển từ xa (S) được thể hiện trên Fig. 1 và Fig. 2.

Mô tả chi tiết phương án thực hiện sáng chế

Như mô tả trong Fig. 1, hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa C theo một phương án của sáng chế bao gồm cơ sở dữ liệu cần bảo vệ DB, phần mềm kiểm soát ứng dụng M và phần mềm phục vụ điều khiển từ xa S. R thể hiện phần mềm điều khiển từ xa thực hiện việc điều khiển từ xa đối với máy tính được điều khiển từ xa C bằng việc kết nối với phần mềm phục vụ điều khiển từ xa S trên máy tính được điều khiển từ xa C thông qua các kênh truyền dữ liệu được trang bị cho máy tính được điều khiển từ xa để phục vụ cho việc truyền dữ liệu trong giao dịch điều khiển từ xa, chẳng hạn như kết nối mạng, thiết bị trung gian có hỗ trợ kết nối mạng trong trường hợp máy tính được điều khiển từ xa không kết nối mạng.

Tùy theo cách hiện thực cơ sở dữ liệu cần bảo vệ DB có thể định dạng ở dạng tệp văn bản thông thường, hoặc theo định dạng khác như XML, SQL database, … Việc xây dựng nội dung cơ sở dữ liệu cần bảo vệ DB có thể thực hiện theo cách thủ công là nhập nội dung các tệp, hay thư mục cần bảo vệ vào tệp văn bản bằng cách dùng phần mềm Notepad, hoặc dùng phần mềm được thiết kế chuyên dụng giúp người sử dụng dễ dàng chọn lựa các tệp và thư mục cần bảo vệ. Việc thực hiện cơ sở dữ liệu cần bảo vệ DB như vậy có thể dễ dàng được thực hiện bởi những người có kiến thức trong lĩnh vực chuyên môn. Cơ sở dữ liệu cần bảo vệ DB có thể được gán các quyền truy xuất đặc biệt chỉ có người dùng được phép mới có thể đọc/ghi/sửa đổi nội dung của cơ sở dữ liệu cần bảo vệ này, hoặc cơ sở dữ liệu cần bảo vệ DB có thể được mã hóa và xác thực bằng giải thuật mã hóa công khai (PKI) để tránh trường hợp cơ sở dữ liệu cần bảo vệ DB bị sửa đổi ngoài ý muốn của người dùng máy tính được điều khiển từ xa mà đã thiết lập cơ sở dữ liệu cần bảo vệ DB đó. Thậm chí cơ sở dữ liệu cần bảo vệ DB có thể được lưu trên các thiết bị khác bên ngoài máy tính được điều khiển từ xa C, nhưng có thể được truy xuất bởi các phần mềm liên quan trong máy tính được điều khiển từ xa C. Ngoài ra, để tăng

tính linh hoạt trong một số tình huống ngoại lệ, việc thay đổi nội dung cơ sở dữ liệu cần bảo vệ DB có thể được thực hiện bởi người điều khiển từ xa với sự cho phép và xác thực tại chỗ bởi người dùng máy tính được điều khiển từ xa. Việc thiết lập khả năng cho phép thay đổi cơ sở dữ liệu cần bảo vệ DB và khả năng xác thực tại chỗ như vậy có thể dễ dàng thực hiện bởi người có kiến thức trong lĩnh vực chuyên môn, chẳng hạn như bằng cách sử dụng phần mềm phục vụ điều khiển từ xa S hiện thực thêm một giao diện GUI cho phép người dùng từ xa yêu cầu một ứng dụng cụ thể được truy xuất tới một tệp tin cần bảo vệ, hoặc cho phép ứng dụng cụ thể kết nối mạng tới một địa chỉ mạng cụ thể, và khi đó người dùng của máy tính được điều khiển từ xa phải xác thực bằng thao tác vật lý như bấm phím trên bàn phím vật lý, hoặc kết nối một thiết bị USB để chấp nhận.

Quy tắc ứng xử được thiết lập bằng cách liệt kê các quy tắc ứng xử cho từng ứng dụng trên máy tính được điều khiển từ xa C, chẳng hạn như, cho mục đích làm ví dụ mà không nhằm hạn chế phạm vi của sáng chế này:

- FileAccessEnable = True: nghĩa là cho phép ứng dụng có nguy cơ truy xuất nội dung tệp dữ liệu cần bảo vệ;
- FileAccessEnable = False: nghĩa là không cho phép ứng dụng có nguy cơ truy xuất nội dung tệp dữ liệu cần bảo vệ;
- ScreenAccessEnable = False: nghĩa là cho phép ứng dụng có nguy cơ truy xuất vào nội dung tệp dữ liệu cần bảo vệ, nhưng loại bỏ vùng dữ liệu màn hình tương ứng trên máy tính được điều khiển từ xa trước khi được thu thập và gửi tới máy tính điều khiển từ xa bởi phần mềm phục vụ điều khiển từ xa S;
- ScreenAccessEnable = True: nghĩa là cho phép ứng dụng có nguy cơ truy xuất vào nội dung tệp dữ liệu cần bảo vệ và thấy được vùng dữ liệu màn hình tương ứng trên máy tính được điều khiển từ xa do phần mềm phục vụ điều khiển từ xa S thu thập và gửi tới máy tính điều khiển từ xa;
- Exception = "/Programs/Test1.exe, /Program/Test2.exe": nghĩa là Test1.exe, Test2.exe là ứng dụng ngoại lệ được phép truy xuất nội dung, và cho

phép thực hiện được thao tác gửi/ tải nội dung tệp dữ liệu cần bảo vệ tới địa chỉ khác bởi phần mềm phục vụ điều khiển từ xa S.

Phần mềm kiểm soát ứng dụng M là một phần mềm hệ thống có chức năng phát hiện và liệt kê ngay lập tức khi phát hiện (các) ứng dụng có nguy cơ trên máy tính được điều khiển từ xa C vào danh sách các ứng dụng có nguy cơ được thiết lập và cập nhật tự động ngay trong phần mềm kiểm soát ứng dụng M này mỗi khi có ứng dụng có nguy cơ được phát hiện bởi phần mềm kiểm soát ứng dụng M. Các ứng dụng có nguy cơ có thể bao gồm:

- Ứng dụng có truy xuất vào cơ sở dữ liệu cần bảo vệ DB bằng cách sử dụng thư viện hệ thống (system library) hoặc hàm dịch vụ của hệ điều hành (system service) (sau đây gọi chung là "**ứng dụng có nguy cơ trực tiếp**"); và
- Ứng dụng có liên lạc với (các) ứng dụng có nguy cơ trực tiếp thông qua các hàm (API) liên lạc; và ứng dụng có khả năng đọc nội dung màn hình của (các) ứng dụng có nguy cơ trực tiếp (sau đây được gọi chung là "**ứng dụng có nguy cơ gián tiếp**").

Tùy theo quy tắc ứng xử được cài đặt trong cơ sở dữ liệu cần bảo vệ DB mà phần mềm kiểm soát ứng dụng M có thể thực hiện (các) hành vi ứng xử tương ứng được thiết lập đối với mỗi ứng dụng có nguy cơ. Tùy thuộc vào thiết lập bởi người dùng máy tính được điều khiển từ xa C, phần mềm kiểm soát ứng dụng M này có thể được kích hoạt chủ động một cách vật lý bởi người dùng hoặc được kích hoạt tự động khi có giao dịch điều khiển từ xa.

Phần mềm kiểm soát ứng dụng M có thể được thiết lập chế độ kích hoạt tự động khi khởi động máy tính được điều khiển từ xa C hoặc được kích hoạt chủ động bởi người dùng máy tính được điều khiển từ xa khi cho phép thực hiện việc điều khiển từ xa. Trong

phương án thực hiện này, thì phần mềm kiểm soát ứng dụng M được thiết lập chế độ kích hoạt tự động khi khởi động máy tính được điều khiển từ xa C. Phần mềm kiểm soát ứng dụng M thực hiện việc giám sát và phát hiện các ứng dụng có nguy cơ trực tiếp và các ứng dụng có nguy cơ gián tiếp được thực hiện bằng các can thiệp (hook) vào thư viện hệ thống (system library) hoặc các hàm dịch vụ của hệ điều hành (system service) có liên quan tới việc truy xuất tệp tin, truy xuất bộ nhớ màn hình và trao đổi thông tin giữa các ứng dụng. Ngoại trừ các ứng dụng ngoại lệ được xác định theo quy tắc ứng xử được thiết lập bởi người dùng máy tính được điều khiển từ xa C mà các ứng dụng có nguy cơ đó vẫn được phép truy xuất các tệp dữ liệu cần được bảo vệ, thì tất cả các ứng dụng có nguy cơ được phát hiện bởi phần mềm kiểm soát ứng dụng M sẽ được liệt kê vào danh sách các ứng dụng có nguy cơ được thiết lập và lưu trữ ngay trên phần mềm kiểm soát ứng dụng M và danh sách này sẽ được phần mềm kiểm soát ứng dụng M trao đổi với phần mềm phục vụ điều khiển từ xa S và phần mềm tường lửa mở rộng FWE, khi có mặt, để thực hiện việc kiểm soát việc truy xuất tệp dữ liệu cần bảo vệ trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa phù hợp với quy tắc ứng xử đã được thiết lập trong cơ sở dữ liệu cần bảo vệ DB.

Cơ chế giám sát ứng dụng bởi phần mềm kiểm soát ứng dụng M có thể thực hiện bằng các phương pháp khác nhau như can thiệp vào hệ điều hành hoặc thư viện hệ thống (ví dụ tệp tin .dll trong Window, hoặc .so trong Linux). Trong hệ điều hành Window và tương tự cho các hệ điều hành khác, các ứng dụng muốn truy cập nội dung của một tệp thông thường sẽ sử dụng hàm thư viện của trình biên dịch ví dụ như Visual C++, các hàm thư viện này sẽ gọi hàm thư viện của hệ thống ví dụ như ntdll.dll và các hàm thư viện hệ thống sẽ gọi các dịch vụ (service) của hệ điều hành thông qua lệnh ngắt (INT), trong hệ điều hành Window NT/2000 sẽ là ngắt INT 0x2E với thanh ghi EAX chứa thứ tự (index) của dịch vụ và thanh ghi EDX chứa tham số cần xử lý. Hệ điều hành với các phần mềm hệ thống (driver) sẽ đáp ứng các dịch vụ yêu cầu từ ứng dụng.

Hình vẽ Fig. 3 mô tả các thành phần cơ bản của phần mềm kiểm soát ứng dụng M trong hệ điều hành Window để làm ví dụ cách thức thực hiện, mà không làm hạn chế phạm vi của sáng chế này. Các mô tả dưới đây liên quan đến Fig. 3 này không đề cập đến các thành phần khác của một máy tính mà cũng được thể hiện trên đó.

Theo đó, phần mềm kiểm soát ứng dụng M gồm mô-đun trung tâm M1 là mô-đun chính để kết nối với các mô-đun hệ thống gồm mô-đun giám sát truy xuất dữ liệu M2, mô-đun giám sát truy suất ổ đĩa M3, mô-đun giám sát liên lạc ứng dụng M4, và mô-đun giám sát truy xuất màn hình M5, thông qua giao tiếp IOCTL (system call for device-specific input/output operations) giữa ứng dụng và phần mềm hệ thống (device driver). Mô-đun trung tâm M1 dựa trên thông tin của các mô-đun giám sát truy xuất dữ liệu M2, mô-đun giám sát truy suất ổ đĩa M3, mô-đun giám sát liên lạc ứng dụng M4, và mô-đun giám sát truy xuất màn hình M5, để phát hiện các ứng dụng có nguy cơ và giao tiếp với các phần mềm khác thông qua kết nối socket, share memory, …

Mô-đun giám sát truy xuất dữ liệu M2 sẽ đăng ký vào phần mềm hệ thống để can thiệp (hook) vào hàm xử lý các dịch vụ liên quan tới việc truy xuất tệp tin ví dụ như NtOpenFile, NtCreateFile, … Các hàm can thiệp được thực hiện như sau:

- Kiểm tra xem tệp dữ liệu được truy xuất có nằm trong danh sách các tệp dữ liệu cần được bảo vệ không, nếu có thì ghi nhận ProcessId của ứng dụng bằng hàm GetCurrentProcessId và thông báo cho các mô-đun ứng dụng liên qua thông qua cơ chế IOCTL (a system call for device-specific input/output operations).
- Trong trường hợp quy tắc ứng xử quy định việc cấm truy xuất các tệp dữ liệu cần bảo vệ thì các hàm can thiệp sẽ trả về mã lỗi, tương ứng với lỗi từ chối truy xuất (access denied của hệ thống). Hoặc hàm can thiệp gọi lại hàm xử lý gốc NtOpenFile, NtCreateFile của hệ điều hành để đảm bảo sự hoạt động của hệ thống.

Việc can thiệp vào phần mềm hệ thống là một kỹ thuật phổ biến và cũng được mô tả trong sáng chế US 7,043,697 B1.

Tương tự như mô-đun giám sát truy xuất dữ liệu M2, mô-đun giám sát truy suất ổ đĩa M3 can thiệp vào phần mềm hệ thống để phát hiện các ứng dụng có sử dụng giao tiếp đọc dữ liệu cấp thấp (đọc sector) để đọc nội dung của các tệp tin cần bảo vệ.

Tương tự mô-đun giám sát truy xuất dữ liệu M2, mô-đun giám sát liên lạc ứng dụng M4 can thiệp vào hàm hệ thống liên quan tới hình thức liên lạc giữa các ứng dụng ví dụ như NtCreateChannel, NtConnectPort, … để phát hiện sự liên lạc giữa các ứng dụng.

Tương tự như mô-đun giám sát truy xuất dữ liệu M2, mô-đun giám sát truy xuất màn hình M5 can thiệp vào các hàm liên quan tới đồ họa để phát hiện các ứng dụng cố ý đọc nội dung màn hình.

Fig. 2 thể hiện hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo phương án khác có thêm phần mềm tường lửa mở rộng FWE để kiểm soát việc truy xuất mạng bởi các ứng dụng trên máy tính được điều khiển từ xa C. Phần mềm tường lửa mở rộng FWE được cài đặt và chạy trên máy tính được điều khiển từ xa C và có thể theo dõi và kiểm soát kết nối mạng với các ứng dụng/ phần mềm trên máy tính được điều khiển từ xa C, và liên lạc với phần mềm kiểm soát ứng dụng M và phần mềm phục vụ điều khiển từ xa S để kiểm soát việc kết nối mạng của các ứng dụng trên máy tính điều khiển từ xa C. Trong Fig. 2 này, các thành phần giống như các thành phần được thể hiện trên Fig. 1 sẽ được sử dụng cùng ký hiệu như trong Fig. 1. Trong phương án thực hiện này, phần mềm tường lửa mở rộng FWE sẽ được kích hoạt tự động ngay khi phần mềm điều khiển từ xa R thực hiện việc kết nối tới phần mềm phục vụ điều khiển từ xa S thông qua việc phần mềm phục vụ điều khiển từ xa S gọi khởi động phần mềm tường lửa mở rộng FWE hoặc gửi tín hiệu tới

phần mềm tường lửa mở rộng FWE để bắt đầu ngăn chặn việc kết nối mạng của các ứng dụng có nguy cơ. Phần mềm tường lửa mở rộng FWE sẽ liên lạc với phần mềm kiểm soát ứng dụng M và lấy thông tin về danh sách các ứng dụng có nguy cơ và gọi tới các API mạng của hệ điều hành, API của hệ thống tường lửa khác, hoặc gửi lệnh tới phần cứng tường lửa bên ngoài để thực hiện các hành vi tương ứng được thiết lập trong cơ sở dữ liệu cần bảo vệ DB đối với các ứng dụng có nguy cơ, bao gồm các hành vi: cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa C; cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng M; và cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ trong phần mềm kiểm soát ứng dụng M.

Có nhiều cách để hiện thực phần mềm tường lửa mở rộng FWE. Ví dụ, nhưng không làm hạn chế phạm vi của sáng chế này, phần mềm tường lửa mở rộng FWE có thể được hiện thực bằng một trong các cách thức sau:

- Bằng cách dựa trên hệ thống tường lửa có sẵn, ví dụ như Window Defender. Phần mềm tường lửa mở rộng FWE sẽ thực hiện kết nối tới phần mềm kiểm soát ứng dụng M để lấy thông tin về các ứng dụng có nguy cơ, sau khi có thông tin về ứng dụng và đường dẫn (path) của ứng dụng, phần mềm tường lửa mở rộng FWE sẽ gọi các tiện ích của Window Defender để ngăn các ứng dụng trên kết nối mạng. Ví dụ như dùng ứng dụng netsh như dưới đây để ngăn chặn ứng dụng telnet.exe kết nối mạng **netsh advfirewall firewall add rule name="Block Outbound Telnet" dir=out program=%SystemRoot%\System32\telnet.exe protocol=tcp localport=23 action=block**.
- Phần mềm tường lửa mở rộng FWE có thể kết nối với một thiết bị tường lửa bên ngoài thông qua giao tiếp ngoại vi với máy tính được điều khiển từ xa C, ví dụ như giao tiếp Serial port, Ethernet, USB…Trong trường hợp này phần mềm tường lửa mở rộng FWE sẽ dùng các hàm network của Window để xác định địa chỉ mạng (IP) và cổng (port) mà các ứng dụng có nguy cơ sử dụng. Dựa trên danh

sách các địa chỉ mạng (IP) và cổng (port) được tìm ra, phần mềm tường lửa mở rộng FWE sẽ gửi lệnh tới thiết bị tường lửa bên ngoài để cấm các kết nối mạng có dùng địa chỉ mạng (IP) và cổng (port) đó.

- Ở mức độ cao hơn phần mềm tường lửa mở rộng FWE có thể hiện thực lại một hệ thống tường lửa bằng phần mềm, qua đó phần mềm sẽ bao gồm một phần mềm hệ thống để can thiệp (hook) vào các dịch vụ hệ thống liên quan tới việc kết nối mạng của các ứng dụng trên máy tính được điều khiển từ xa.

Để tăng tính linh hoạt trong một số tình huống ngoại lệ, phần mềm tường lửa mở rộng FWE cũng có thể cung cấp cho người dùng máy tính được điều khiển từ xa khả năng xác nhận tại chỗ để cho phép một số ứng dụng nằm trong danh sách có khả năng truy xuất tới tệp dữ liệu cần bảo vệ được truy xuất tới một địa chỉ IP cụ thể. Tuy nhiên thao tác này cần được xác thực bằng cách tác động vật lý tới máy tính được điều khiển từ xa C ví dụ như bấm phím trên máy tính, hay xác thực bằng vân tay qua một thiết bị USB đang cắm vào máy tính.

Fig. 4 mô tả sơ đồ hiện thực phần mềm phục vụ điều khiển từ xa S được thể hiện trên các Fig. 1 và Fig. 2, được cài đặt và chạy trên máy tính được điều khiển từ xa C để thu thập dữ liệu màn hình của máy tính được điều khiển từ xa này và gửi tới phần mềm điều khiển từ xa R. Một ví dụ cụ thể, nhưng không làm hạn chế phạm vi của sáng chế về việc hiện thực phần mềm phục vụ điều khiển từ xa S trên hệ điều hành Window với giao tiếp mạng được mô tả như sau:

- Bước 1: Phần mềm phục vụ điều khiển từ xa S sẽ hiện thực việc kết nối với phần mềm điều khiển từ xa R thông qua giao tiếp mạng bằng cách sử dụng các hàm của thư viện WinSock;

- Bước 2: Sau khi kết nối được thực hiện, phần mềm phục vụ điều khiển từ xa S sẽ dùng hàm recv() để nhận các lệnh từ phần mềm điều khiển từ xa R. Nếu

phần mềm điều khiển từ xa R yêu cầu gửi thông tin về màn hình thì phần mềm phục vụ điều khiển từ xa S sẽ thực hiện qua bước 3;

- Bước 3: Phần mềm phục vụ điều khiển từ xa S sẽ thu thập thông tin màn hình bằng cách sử dụng các hàm hệ thống của hệ điều hành ví dụ như sử dụng thư viện DXGI của Window với các hàm GetFrameMoveRects, GetFrameDirtyRects, AcquireNextFrame… để lấy nội dung sự các vùng dữ liệu màn hình bị thay đổi trên máy tính được điều khiển từ xa. Để tăng tính hiệu quả cho việc nén dữ liệu, phần mềm phục vụ điều khiển từ xa S sẽ chỉ gửi thông tin những sự thay đổi so với dữ liệu được gửi trước đó, hoặc một cách khác là sử dụng Mirror driver như cơ chế được mô tả trong sáng chế Mỹ số US 7,043,697 B1;

- Bước 4: Phần mềm phục vụ điều khiển từ xa S sẽ kết nối tới phần mềm kiểm soát ứng dụng M thông qua các giao tiếp trao đổi dữ liệu giữa các ứng dụng (process) như cơ chế pipe, socket, share memory, … để lấy danh sách các ứng dụng có nguy cơ. Phần mềm phục vụ điều khiển từ xa S sẽ tính toán vùng dữ liệu màn hình của các ứng dụng thông qua GetWindowThreadProcessId() và hàm GetWindow() và duyệt qua danh sách các vùng dữ liệu màn hình thay đổi được thực hiện ở bước trên và loại bỏ các dữ liệu có liên quan tới vùng cửa sổ của ứng dụng có nguy cơ;

- Bước 5: Dữ liệu các vùng màn hình sau khi đã loại bỏ vùng dữ liệu màn hình tương ứng với các ứng dụng có nguy cơ ở bước 4 nói trên sẽ được nén bằng giải thuật jpeg, zlib…và mã hóa nếu cần để bảo mật; và

- Bước 6: Dữ liệu đã nén ở bước 5 sẽ được gửi tới phần mềm từ xa thông qua hàm socket send(). Cơ chế gửi (send) và nhận (recv) dữ liệu có thể được thực hiện theo các cách khác nhau, ví dụ như thông qua kết nối mạng, hoặc thông qua một thiết bị trung gian như được bộc lộ trong sáng chế Việt Nam số 1-2019-03916 nộp

ngày 19/07/2019 mà không được mô tả chi tiết trong sáng chế này, trong trường hợp mà người dùng máy tính được điều khiển từ xa C lựa chọn phương án cấm nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa khi có ứng dụng truy xuất vào tệp dữ liệu cần bảo vệ trong quá trình điều khiển từ xa được phát hiện bởi phần mềm kiểm soát ứng dụng M.

Có thể thấy rằng mô tả chi tiết phương án thực hiện đối với phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa bằng cách sử dụng hệ thống kiểm soát truy xuất dữ liệu theo sáng chế này đã được mô tả cùng với việc mô tả chi tiết phương án thực hiện đối với hệ thống kiểm soát truy xuất dữ liệu, mà phù hợp với hệ thống kiểm soát truy xuất dữ liệu trong phương án thực hiện trên đây, phương pháp như vậy bao gồm các việc sau:

(i) Thiết lập cơ sở dữ liệu cần bảo vệ DB trên máy tính điều khiển từ xa bằng cách liệt kê các tệp dữ liệu, thư mục cần bảo vệ vào danh sách tệp dữ liệu cần bảo vệ; và liệt kê quy tắc ứng xử cho từng ứng dụng trên máy tính được điều khiển từ xa C, mà các quy tắc này có thể thiết lập một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của thống kiểm soát truy xuất dữ liệu đối với một ứng dụng có nguy cơ:

a. cấm việc truy xuất vào tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ; dừng hoạt động của tất cả các ứng dụng có nguy cơ đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ;

b. cho phép ứng dụng có nguy cơ truy xuất vào tệp dữ liệu cần bảo vệ nhưng vùng dữ liệu màn hình tương ứng được loại bỏ trước khi được thu thập và gửi về máy tính điều khiển từ xa;

c. chỉ cho phép (các) ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ;

và, khi hệ thống kiểm soát truy xuất dữ liệu có thêm phần mềm tường lửa mở rộng FWE,

d. cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa C;

e. cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng M; và

f. cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng M.

(ii) Thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng M khi khởi động máy tính được điều khiển từ xa C;

(iii) Thiết lập chế độ kích hoạt tự động tường lửa mở rộng FWE khi phần mềm điều khiển từ xa kết nối với phần mềm phục vụ điều khiển từ xa S để thực hiện việc điều khiển từ xa đối với máy tính được điều khiển từ xa C; và

(iv) Cho phép phần mềm điều khiển từ xa được kết nối với phần mềm phục vụ điều khiển từ xa S để thực hiện việc điều khiển từ xa đối với máy tính được điều khiển từ xa C.

Việc thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng M và phần mềm tường lửa mở rộng FWE có thể dễ dàng thực hiện bởi người có trình độ chuyên môn trong lĩnh vực, chẳng hạn như bằng cách đăng ký tính năng chạy tự động vào registry của hệ điều hành Window.

Mô tả trên chỉ là phương án thực hiện trên đây của sáng chế là chỉ cho mục đích làm ví dụ, chứ không nhằm để hạn chế phạm vi của sáng chế này. Những người có kiến thức chuyên môn trong lĩnh vực có thể thực hiện các thay đổi và biến thể khác đối với sáng chế, ví dụ như có thể bổ sung, loại bớt hoặc thay thế các mô-đun của phần mềm kiểm

soát ứng dụng M để bổ sung, loại bớt hoặc thay thế chức năng tương đương của phần mềm này mà không nằm ngoài phạm vi bảo hộ và/hoặc phạm vi bộc lộ của sáng chế này.

YÊU CẦU BẢO HỘ

1. Hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa bao gồm:

(i) Cơ sở dữ liệu cần bảo vệ (DB) chứa:

a. Danh sách các tệp dữ liệu cần bảo vệ được liệt kê theo đường dẫn (path) của các tệp dữ liệu cần bảo vệ hoặc thư mục chứa các tệp dữ liệu cần bảo vệ đó trên máy tính được điều khiển từ xa (C); và

b. Quy tắc ứng xử đối với mỗi ứng dụng trên máy tính được điều khiển từ xa (C), mà có thể thiết lập một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của hệ thống kiểm soát truy xuất dữ liệu đối với một ứng dụng trên máy tính được điều khiển từ xa có truy xuất trực tiếp hoặc gián tiếp vào tệp dữ liệu cần bảo vệ (sau đây gọi tắt là "**ứng dụng có nguy cơ**"): cấm việc truy xuất vào tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ; dừng hoạt động của tất cả các ứng dụng có nguy cơ đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ; cho phép ứng dụng có nguy cơ truy xuất vào tệp dữ liệu cần bảo vệ nhưng vùng dữ liệu màn hình tương ứng được loại bỏ trước khi được thu thập và gửi về máy tính điều khiển từ xa; cho phép một hoặc nhiều hơn ứng dụng cụ thể được phép truy xuất vào tệp dữ liệu cần bảo vệ (sau đây gọi tắt là "**ứng dụng ngoại lệ**"),

(ii) Phần mềm kiểm soát ứng dụng (M) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối với và truy xuất, đọc danh sách các tệp dữ liệu cần bảo vệ trong cơ sở dữ liệu cần bảo vệ (DB), và có chức năng, khi có giao dịch điều khiển từ xa, phát hiện và liệt kê ngay lập tức khi phát hiện (các) ứng dụng có nguy cơ, trừ (các) ứng dụng ngoại lệ trên máy tính được điều khiển từ xa (C) vào danh sách các ứng dụng có nguy cơ được thiết lập, lưu trữ và cập nhật

tự động ngay trong phần mềm kiểm soát ứng dụng (M) này mỗi khi có ứng dụng có nguy cơ được phát hiện bởi phần mềm kiểm soát ứng dụng (M), và thực hiện một trong những hành vi ứng xử sau đây, tùy thuộc vào việc thiết lập quy tắc ứng xử trong cơ sở dữ liệu cần bảo vệ (DB): cấm việc truy xuất nội dung tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ đó; dừng hoạt động của tất cả các ứng dụng đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ; cho phép ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ;

(iii) Phần mềm phục vụ điều khiển từ xa (S) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối với phần mềm điều khiển từ xa trên máy tính từ xa khi thực hiện giao dịch điều khiển từ xa, và có thể kết nối với và truy xuất, đọc danh sách các tệp dữ liệu cần bảo vệ trong cơ sở dữ liệu cần bảo vệ (DB), kết nối với phần mềm kiểm soát ứng dụng (M) sao cho phần mềm phục vụ điều khiển từ xa (S) này có thể liên lạc và nhận chia sẻ thông tin về danh sách ứng dụng có nguy cơ từ phần mềm kiểm soát ứng dụng (M) để thực hiện các chức năng:

a. Cho phép thực hiện việc điều khiển từ xa máy tính được điều khiển từ xa bởi phần mềm điều khiển từ xa trên máy tính điều khiển từ xa;

b. Thu thập thông tin thay đổi dữ liệu màn hình máy tính được điều khiển từ xa (C);

c. Tùy thuộc vào việc thiết lập quy tắc ứng xử tương ứng trong cơ sở dữ liệu cần bảo vệ (DB), thực hiện việc loại bỏ dữ liệu màn hình tương ứng với ứng dụng có nguy cơ đó trên máy tính được điều khiển từ xa (C) trước khi gửi về phần mềm điều khiển từ xa;

d. Nén và mã hóa dữ liệu màn hình máy tính được điều khiển từ xa (C) để gửi về phần mềm điều khiển từ xa trên máy tính điều khiển từ xa; và

e. Gửi dữ liệu màn hình đã được nén và mã hóa tới ứng dụng điều khiển từ xa thông qua các kênh truyền dữ liệu được trang bị cho máy tính

được điều khiển từ xa để phục vụ cho việc truyền dữ liệu trong giao dịch điều khiển từ xa.

2. Hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo Điểm 1, trong đó:

(i) Quy tắc ứng xử của cơ sở dữ liệu cần bảo vệ(DB) có thể thiết lập thêm một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của hệ thống kiểm soát truy xuất dữ liệu đối với ứng dụng có nguy cơ: cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C); cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và

(ii) Hệ thống kiểm soát truy xuất dữ liệu bao gồm thêm phần mềm tường lửa mở rộng (FWE) được cài đặt và có thể chạy trên máy tính được điều khiển từ xa (C), có thể kết nối và truy xuất, đọc nội dung trong cơ sở dữ liệu cần bảo vệ (DB), theo dõi và kiểm soát kết nối mạng của các ứng dụng/ phần mềm trên máy tính được điều khiển từ xa (C), có thể được kích hoạt trong đó việc kết nối với phần mềm kiểm soát ứng dụng (M) theo cách thức sao cho sao cho phần mềm tường lửa mở rộng (FWE) có thể có thể liên lạc và nhận chia sẻ thông tin về ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M), và việc kết nối với phần mềm phục vụ điều khiển từ xa (S) theo cách thức sao cho khi có kết nối giữa phần mềm điều khiển từ xa và phần mềm phục vụ điều khiển từ xa (S) để thực hiện giao dịch điều khiển từ xa máy tính được điều khiển từ xa (C), thì phần mềm tường lửa mở rộng (FWE) sẽ thực hiện hành vi ứng xử tương ứng với thiết lập của cơ sở dữ liệu cần bảo vệ (DB) như được mô tả trong mục (i) ngay trên đây, bao gồm: cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C);

cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M).

3. Hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo Điểm 1 hoặc 2, trong đó phần mềm kiểm soát ứng dụng (M), phần mềm phục vụ điều khiển từ xa (S) và phần mềm tường lửa mở rộng (FEW), khi có mặt, được tích hợp trong một phần mềm duy nhất có các chức năng tương đương.

4. Phương pháp kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa bằng cách sử dụng hệ thống kiểm soát việc truy xuất dữ liệu trên máy tính được điều khiển từ xa trong giao dịch điều khiển từ xa theo Điểm 1 hoặc 2 nói trên, bao gồm các việc sau:

(i) Thiết lập cơ sở dữ liệu cần bảo vệ (DB) trên máy tính điều khiển từ xa bằng cách liệt kê các tệp dữ liệu, thư mục cần bảo vệ vào danh sách tệp dữ liệu cần bảo vệ; và liệt kê quy tắc ứng xử cho từng ứng dụng trên máy tính được điều khiển từ xa (C), mà các quy tắc này có thể thiết lập một hoặc nhiều các hành vi ứng xử tương ứng sau đây của (các) phần mềm của thống kiểm soát truy xuất dữ liệu đối với một ứng dụng trên máy tính được điều khiển từ xa có truy xuất vào tệp dữ liệu cần bảo vệ (sau đây gọi là "**ứng dụng có nguy cơ**"):

a. cấm việc truy xuất vào tệp dữ liệu cần bảo vệ bởi ứng dụng có nguy cơ; dừng hoạt động của tất cả các ứng dụng có nguy cơ đang hoặc bắt đầu truy xuất vào tệp dữ liệu cần bảo vệ;

b. cho phép ứng dụng có nguy cơ truy xuất vào tệp dữ liệu cần bảo vệ nhưng vùng dữ liệu màn hình tương ứng được loại bỏ trước khi được thu thập và gửi về máy tính điều khiển từ xa;

c. chỉ cho phép (các) ứng dụng ngoại lệ truy xuất vào tệp dữ liệu cần bảo vệ;

và, khi hệ thống kiểm soát truy xuất dữ liệu có thêm phần mềm tường lửa mở rộng (FWE),

d. cấm kết nối mạng đối với toàn bộ các ứng dụng trên máy tính được điều khiển từ xa (C);

e. cấm kết nối mạng đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M); và

f. cấm thao tác tải/ gửi dữ liệu đối với tất cả các ứng dụng trong danh sách ứng dụng có nguy cơ của phần mềm kiểm soát ứng dụng (M),

(ii) Kích hoạt chủ động phần mềm kiểm soát ứng dụng (M) bởi người dùng máy tính được điều khiển từ xa hoặc thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng (M) này khi khởi động máy tính được điều khiển từ xa (C), hoặc thiết lập chế độ kích hoạt tự động phần mềm kiểm soát ứng dụng (M) này khi có kết nối giữa phần mềm điều khiển từ xa với phần mềm phục vụ điều khiển từ xa (S) để thực hiện giao dịch điều khiển từ xa máy tính được điều khiển từ xa (C);

(iii) Kích hoạt chủ động phần mềm tường lửa mở rộng (FWE) bởi người dùng máy tính được điều khiển từ xa hoặc thiết lập chế độ kích hoạt tự động tường lửa mở rộng (FWE) khi khởi động máy tính được điều khiển từ xa (C), hoặc thiết lập chế độ kích hoạt tự động phần tường lửa mở rộng (FWE) khi có kết nối giữa phần mềm điều khiển từ xa và phần mềm phục vụ điều khiển từ xa (S) để thực hiện việc điều khiển từ xa máy tính được điều khiển từ xa (C); và

(iv) Cho phép phần mềm điều khiển từ xa kết nối với phần mềm phục vụ điều khiển từ xa (S) để thực hiện việc điều khiển từ xa đối với máy tính được điều khiển từ xa (C).

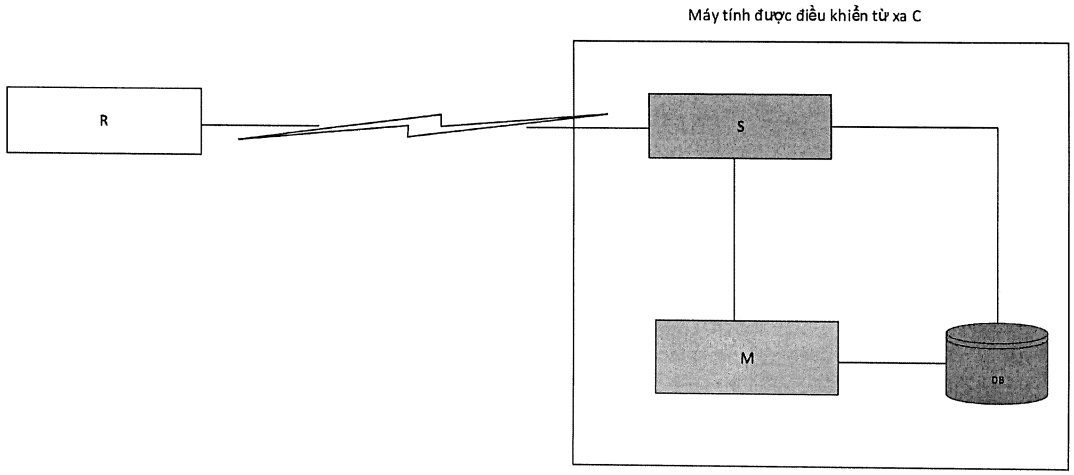

Máy tính được điều khiển từ xa C
R
S
M
DB

Fig. 1

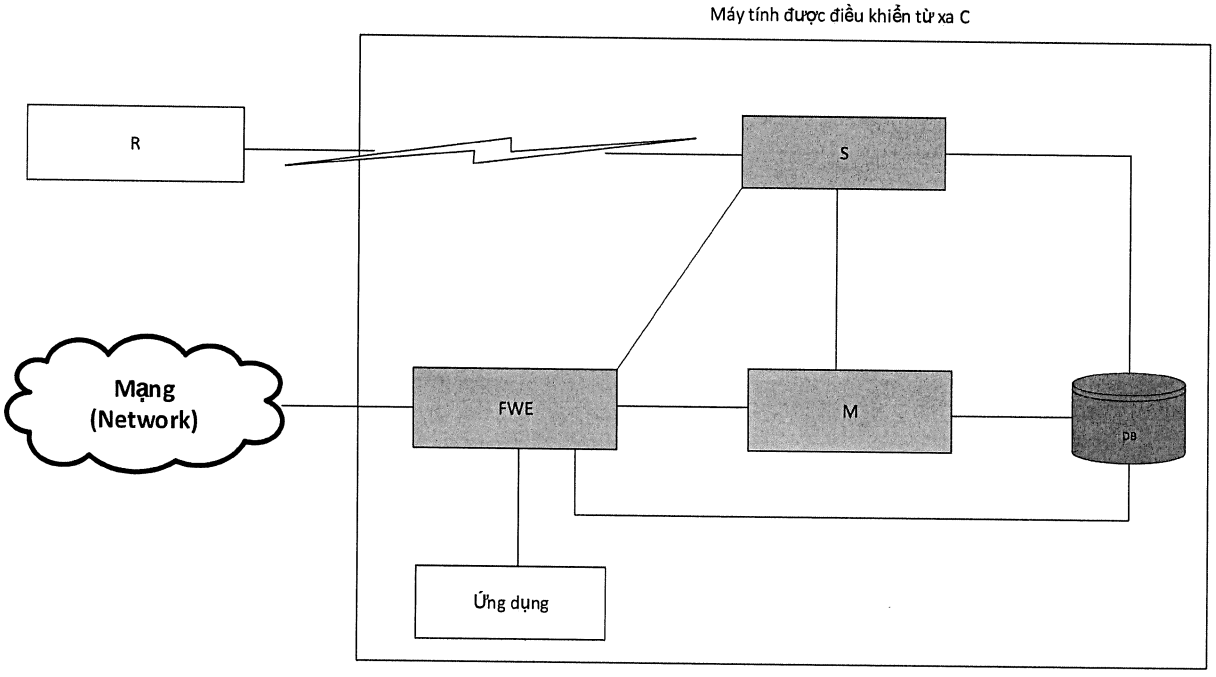

Máy tính được điều khiển từ xa C
R
S
Mạng
(Network)
FWE
M
DB
Ứng dụng

Fig. 2

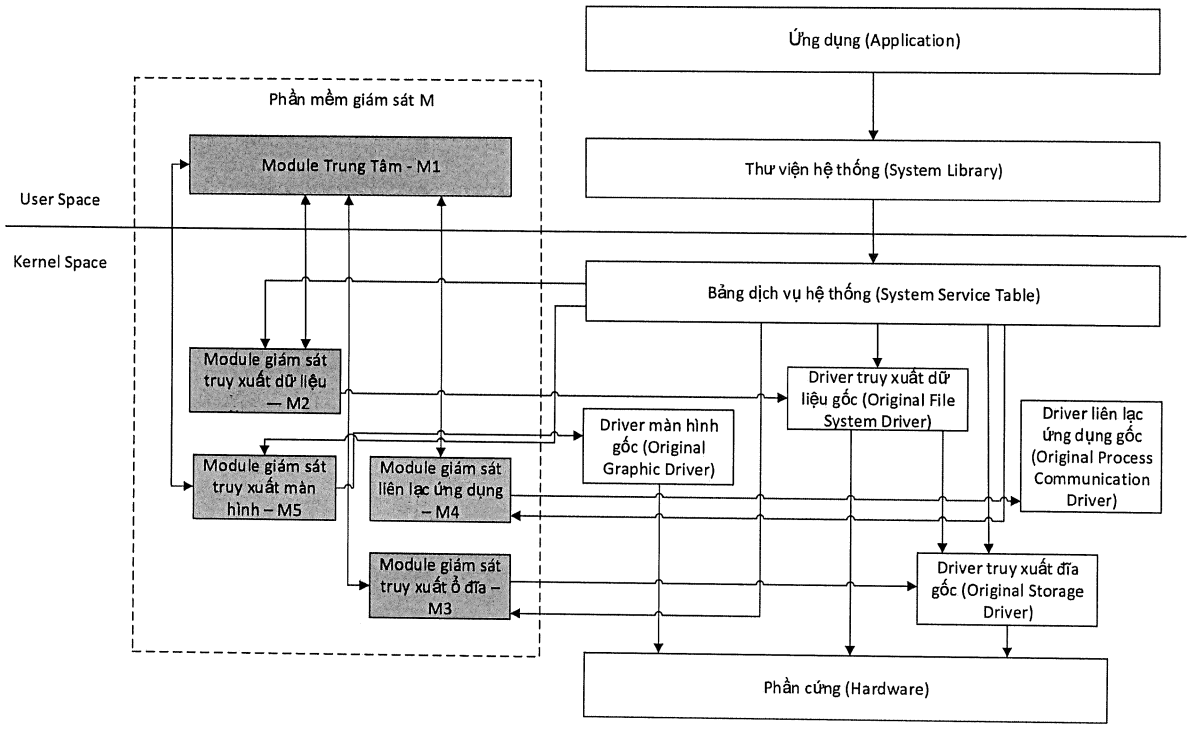

Ứng dụng (Application)
Phần mềm giám sát M
Module Trung Tâm - M1
Thư viện hệ thống (System Library)
User Space
Kernel Space
Bảng dịch vụ hệ thống (System Service Table)
Module giám sát truy xuất dữ liệu – M2
Driver truy xuất dữ liệu gốc (Original File System Driver)
Driver màn hình gốc (Original Graphic Driver)
Driver liên lạc ứng dụng gốc (Original Process Communication Driver)
Module giám sát truy xuất màn hình – M5
Module giám sát liên lạc ứng dụng – M4
Module giám sát truy xuất ổ đĩa – M3
Driver truy xuất đĩa gốc (Original Storage Driver)
Phần cứng (Hardware)

Fig. 3

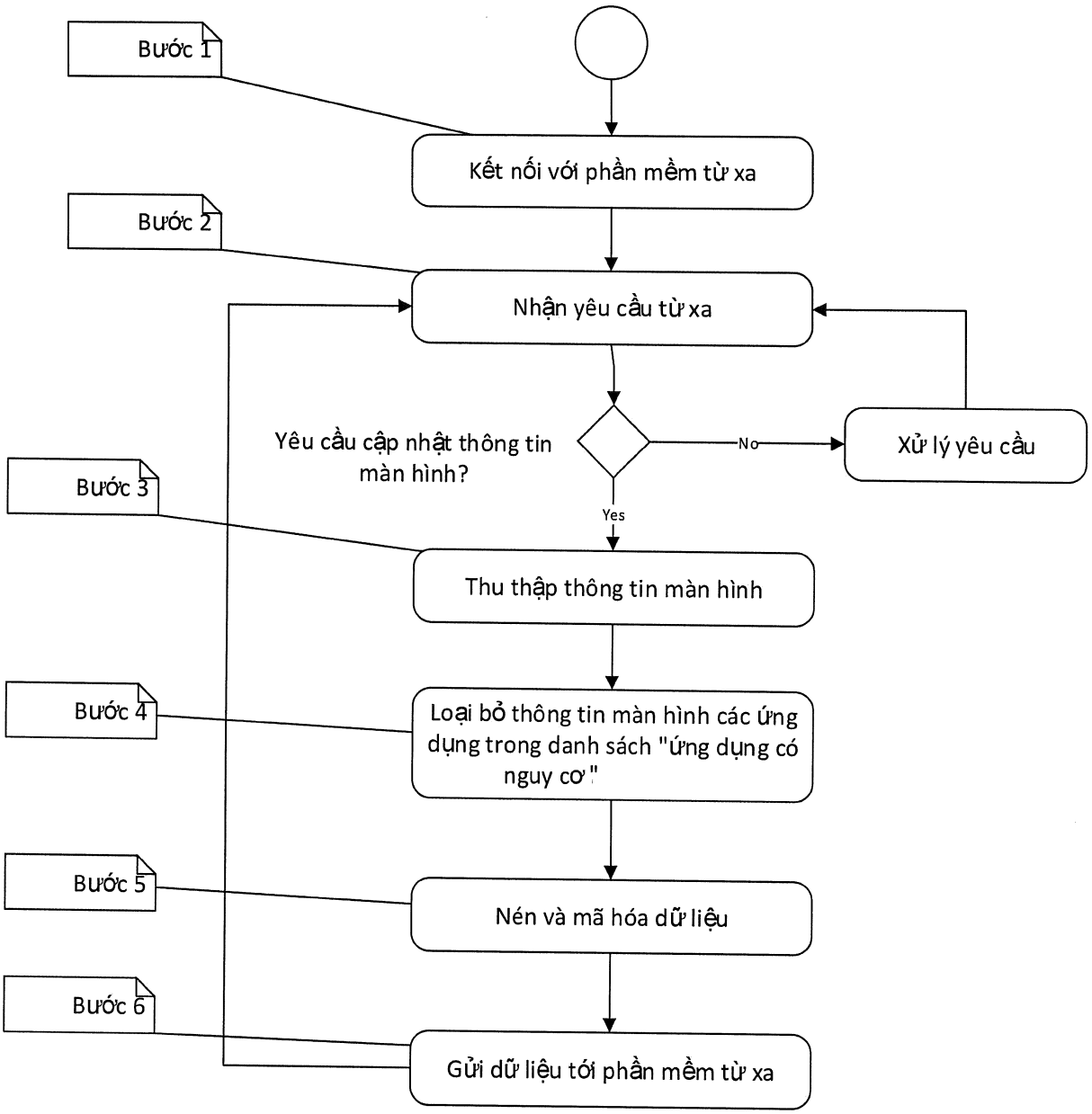

Bước 1
Kết nối với phần mềm từ xa
Bước 2
Nhận yêu cầu từ xa
Yêu cầu cập nhật thông tin màn hình?
No
Xử lý yêu cầu
Yes
Bước 3
Thu thập thông tin màn hình
Bước 4
Loại bỏ thông tin màn hình các ứng dụng trong danh sách "ứng dụng có nguy cơ"
Bước 5
Nén và mã hóa dữ liệu
Bước 6
Gửi dữ liệu tới phần mềm từ xa

Fig. 4