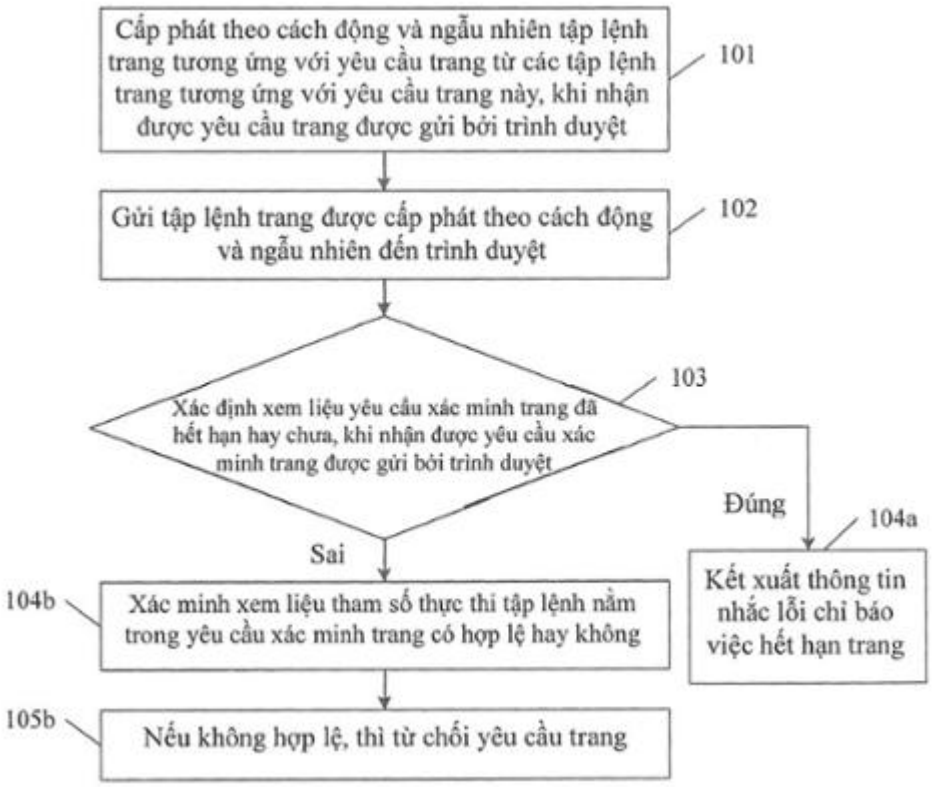
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0033781**
(51)[7] **H04L 29/02**
(13) **B**

(21) 1-2018-05571
(22) 18/04/2017
(86) PCT/CN2017/080862 18/04/2017
(87) WO 2017/206605 07/12/2017
(30) 201610377847.0 31/05/2016 CN
(45) 25/10/2022 415
(43) 25/04/2019 373A
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) LU, Yaran (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ NGĂN NGỪA MÁY CHỦ KHÔNG BỊ TẤN CÔNG

(57) Sáng chế đề xuất phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công, và liên quan đến lĩnh vực các công nghệ an ninh mạng, để giải quyết vấn đề sự bảo mật của máy chủ thấp. Các giải pháp kỹ thuật chính theo sáng chế bao gồm các bước sau: cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi nhận được yêu cầu trang được gửi bởi trình duyệt; gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh; xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt; và nếu đã hết hạn, thì kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang; hoặc nếu chưa hết hạn, thì xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không; và nếu không hợp lệ, thì từ chối yêu cầu trang. Sáng chế chủ yếu được sử dụng để ngăn ngừa máy chủ không bị tấn công.


Cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi nhận được yêu cầu trang được gửi bởi trình duyệt
101
Gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt
102
Xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt
103
Đúng
104a
Kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang
Sai
104b
Xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không
105b
Nếu không hợp lệ, thì từ chối yêu cầu trang

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực các công nghệ an ninh mạng và cụ thể là phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công.

Tình trạng kỹ thuật của sáng chế

Do các công nghệ Internet phát triển một cách nhanh chóng, nên việc bảo đảm an ninh mạng thu hút nhiều sự chú ý. Thông thường, an ninh mạng đề cập đến cách thức để ngăn ngừa máy chủ trong mạng không bị tấn công. Để tấn công máy chủ, kẻ tấn công sử dụng yêu cầu dịch vụ để chiếm quá nhiều tài nguyên dịch vụ của máy chủ, dẫn đến sự quá tải của máy chủ. Ngoài ra, máy chủ không thể đáp lại các yêu cầu khác, và do đó tài nguyên của máy chủ có thể bị cạn kiệt. Do vậy, kẻ tấn công làm cho máy chủ từ chối cung cấp các dịch vụ.

Hiện nay, trước tiên trình duyệt gửi yêu cầu dịch vụ đến máy chủ. Yêu cầu dịch vụ này bao gồm giá trị token trong tệp tin (cookie) (dữ liệu được máy chủ lưu trên thiết bị đầu cuối cục bộ của người dùng) được mã hóa bằng cách sử dụng thuật toán tóm lược tin báo 5 (Message Digest 5, MD5). Sau khi nhận được yêu cầu dịch vụ, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có hợp lệ hay không để ngăn ngừa máy chủ không bị tấn công. Tuy nhiên, giá trị token được mã hóa này được thu bằng cách thực thi mã tập lệnh tĩnh và mã tập lệnh tĩnh này được bộc lộ ở dạng văn bản gốc. Do đó, kẻ tấn công có thể trực tiếp thu được logic trong mã tập lệnh tĩnh và phân tích cú pháp phương pháp mã hóa giá trị token. Do vậy, kẻ tấn công có thể bỏ qua cơ chế phát hiện của máy chủ bằng cách mô phỏng yêu cầu dịch vụ của người dùng thông thường và sau đó tấn công máy chủ. Do đó, mức độ bảo vệ bảo mật đối với máy chủ hiện nay thấp.

Bản chất kỹ thuật của sáng chế

Từ quan điểm của vấn đề nêu trên, sáng chế được đề xuất để tạo ra phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công, để khắc phục vấn đề nêu trên hoặc ít nhất giải quyết được một phần vấn đề nêu trên.

Để đạt được mục đích nêu trên, sáng chế chủ yếu đề xuất các giải pháp kỹ thuật

dưới đây.

Theo một khía cạnh, một phương án thực hiện của sáng chế đề xuất phương pháp ngăn ngừa máy chủ không bị tấn công, và phương pháp này bao gồm các bước sau đây: cấp phát theo cách động và ngẫu nhiên tập lệnh trang (page script) tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với các yêu cầu trang này, khi nhận được yêu cầu trang được gửi bởi trình duyệt; gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh; xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt; nếu đã hết hạn, thì kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang; nếu chưa hết hạn, thì xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không; nếu không hợp lệ, thì từ chối yêu cầu trang.

Theo một khía cạnh khác, một phương án thực hiện của sáng chế còn đề xuất thiết bị ngăn ngừa máy chủ không bị tấn công và thiết bị này bao gồm: bộ phận cấp phát, được tạo cấu hình để cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi yêu cầu trang được gửi bởi trình duyệt được nhận; bộ phận gửi được tạo cấu hình để gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh; bộ phận xác định được tạo cấu hình để xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi yêu cầu xác minh trang được gửi bởi trình duyệt được nhận; bộ phận kết xuất được tạo cấu hình để kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang, nếu yêu cầu xác minh trang đã hết hạn; bộ phận xác minh được tạo cấu hình để xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không, nếu yêu cầu xác minh trang chưa hết hạn; và bộ phận từ chối, được tạo cấu hình để từ chối yêu cầu trang nếu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang không hợp lệ.

Dựa vào các thông tin nêu trên, các giải pháp kỹ thuật được đề xuất theo các phương án thực hiện của sáng chế có ít nhất các ưu điểm sau đây.

Theo phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công được đề xuất theo các phương án thực hiện của sáng chế, khi nhận được yêu cầu xác minh

trang được gửi bởi trình duyệt, thì trước tiên máy chủ xác định xem liệu yêu cầu xác minh trang này đã hết hạn hay chưa. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Nếu tham số thực thi tập lệnh không hợp lệ, thì máy chủ từ chối yêu cầu trang để ngăn ngừa máy chủ không bị tấn công. Hiện nay, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có hợp lệ hay không để ngăn ngừa máy chủ không bị tấn công. So với quy trình này, theo sáng chế, máy chủ xác minh tham số thực thi tập lệnh để ngăn ngừa máy chủ không bị tấn công. Tham số thực thi tập lệnh được thu dựa vào tập lệnh trang được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang, và logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu được logic tập lệnh trong mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi thời gian yêu cầu của yêu cầu xác minh trang vượt quá khoảng thời gian định trước, thì máy chủ từ chối yêu cầu trang. Trình duyệt cần phải tải lại yêu cầu xác minh trang để gửi lại yêu cầu xác minh trang, và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại. Do đó, kẻ tấn công không thể tấn công máy chủ theo các phương án thực hiện của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo các phương án thực hiện của sáng chế.

Mô tả vắn tắt các hình vẽ

Bằng cách đọc các phần mô tả chi tiết của các phương án thực hiện ưu tiên sau đây, nhiều ưu điểm và lợi ích khác có thể được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật. Các hình vẽ kèm theo chỉ được sử dụng cho mục đích minh họa các phương án thực hiện ưu tiên và không được xem là giới hạn đối với sáng chế. Ngoài ra, các ký hiệu chỉ dẫn giống nhau được sử dụng để thể hiện các thành phần giống nhau trên toàn bộ các hình vẽ kèm theo. Các hình vẽ kèm theo này bao gồm:

Fig.1 là lưu đồ minh họa phương pháp ngăn ngừa máy chủ không bị tấn công, theo một phương án thực hiện của sáng chế;

Fig.2 là lưu đồ minh họa phương pháp ngăn ngừa máy chủ không bị tấn công khác, theo một phương án thực hiện của sáng chế;

Fig.3 là sơ đồ khối minh họa thiết bị ngăn ngừa máy chủ không bị tấn công, theo một phương án thực hiện của sáng chế;

Fig.4 là sơ đồ khối minh họa thiết bị ngăn ngừa máy chủ không bị tấn công khác, theo một phương án thực hiện của sáng chế; và

Fig.5 là sơ đồ khối minh họa hệ thống ngăn ngừa máy chủ không bị tấn công, theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Phần tiếp theo mô tả chi tiết các phương án thực hiện làm ví dụ của sáng chế với tham chiếu đến các hình vẽ kèm theo. Mặc dù các hình vẽ kèm theo thể hiện các phương án thực hiện làm ví dụ của sáng chế, nhưng cần hiểu rằng sáng chế có thể được thực hiện ở các hình thức khác nhau, và không bị giới hạn ở các phương án thực hiện được mô tả ở đây. Thay vào đó, các phương án thực hiện này được đề xuất để giúp hiểu rõ sáng chế và truyền tải toàn bộ phạm vi của sáng chế cho người có hiểu biết trung bình trong lĩnh vực kỹ thuật.

Để làm rõ hơn các ưu điểm của các giải pháp kỹ thuật theo sáng chế, phần tiếp theo mô tả chi tiết sáng chế với tham chiếu đến các hình vẽ kèm theo và các phương án thực hiện.

Một phương án thực hiện của sáng chế đề xuất phương pháp ngăn ngừa máy chủ không bị tấn công. Như được thể hiện trên Fig.1, phương pháp này bao gồm các bước sau.

Bước 101: Cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi nhận được yêu cầu trang được gửi bởi trình duyệt.

Yêu cầu trang này bao gồm URL của trang và URL của trang là trang tương ứng với tập lệnh trang được yêu cầu bởi trình duyệt. Theo phương án thực hiện này của sáng chế, một URL của trang tương ứng với các tập lệnh trang. Logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang tương ứng với cùng URL của trang. Các tham số thực thi tập lệnh khác nhau được thu khi các tập lệnh trang tương ứng với cùng URL của trang được thực thi. Các kết quả thực thi trang của các tập lệnh trang tương ứng với cùng URL của trang giống nhau, tức là, các trang

được tạo ra sau khi trình duyệt tải và thực thi các tập lệnh trang giống nhau. Cần lưu ý rằng theo phương án thực hiện này của sáng chế, tập lệnh trang tương ứng với yêu cầu trang có thể được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang bằng cách sử dụng số ngẫu nhiên được tạo ra dựa vào thời điểm hiện tại hoặc số ngẫu nhiên được tạo ra dựa vào thời điểm gửi yêu cầu trang. Không có giới hạn cụ thể nào được áp đặt theo phương án thực hiện này của sáng chế.

Ví dụ, nếu người dùng nhập URL của AMAZON trên thanh địa chỉ của trình duyệt và ấn phím enter, thì máy chủ sẽ nhận được yêu cầu trang được gửi bởi trình duyệt. URL của trang trong yêu cầu trang này là AMAZON. Sau đó, máy chủ cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này. Tức là, máy chủ cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với AMAZON.

Bước 102: Gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt.

Ngoài ra, trình duyệt tải và thực thi tập lệnh trang để thu được tham số thực thi tập lệnh. Sau khi tải và thực thi tập lệnh trang, trình duyệt hiển thị trang tương ứng và thu được tham số thực thi tập lệnh. Các tham số thực thi tập lệnh là các tham số bổ sung trên trang và không ảnh hưởng đến trang được hiển thị. Theo phương án thực hiện này của sáng chế, khi các tập lệnh trang tương ứng với cùng URL của trang được thực thi, thì các tham số thực thi tập lệnh khác nhau được tạo ra theo các kết quả thực thi tập lệnh trang khác nhau.

Ví dụ, URL của trang cụ thể tương ứng với ba tập lệnh trang. Logic thu tham số thực thi tập lệnh trong tập lệnh trang để thu được giá trị token được mã hóa trong thông tin tệp tin. Logic thu tham số thực thi tập lệnh trong tập lệnh trang khác để thu được các giá trị mã hóa của tọa độ chuột hiện thời của người dùng. Logic thu tham số thực thi tập lệnh trong tập lệnh trang còn lại để thu được giá trị được mã hóa ở thời điểm hiện tại. Cần lưu ý rằng theo phương án thực hiện này của sáng chế, logic để thực thi tập lệnh trang và phương pháp mã hóa tham số thực thi tập lệnh không bị giới hạn, miễn là logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang theo sáng chế để phân biệt giữa các tập lệnh trang khác nhau.

Bước 103: Xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt.

Yêu cầu xác minh trang có thể được gửi bằng cách sử dụng trang được thu dựa vào bước tải và thực thi ở bước 102. Cụ thể là, yêu cầu này có thể được gửi bằng cách nhấp vào liên kết cụ thể trên trang, chọn nút lệnh cụ thể, nhập một số từ khóa, v.v.. Không có giới hạn cụ thể nào được áp đặt theo phương án thực hiện này của sáng chế. Yêu cầu xác minh trang này bao gồm tham số thực thi tập lệnh, và tham số thực thi tập lệnh này là tham số được mã hóa.

Theo phương án thực hiện này của sáng chế, quy trình cụ thể xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa có thể như sau: Trước tiên, máy chủ thu được thời gian yêu cầu đối với yêu cầu xác minh trang và thời gian để trình duyệt thực thi tập lệnh trang từ yêu cầu xác minh trang. Sau đó, máy chủ xác định xem liệu thời gian yêu cầu của yêu cầu xác minh trang có chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang hay không. Máy chủ xác định rằng yêu cầu xác minh trang đã hết hạn, nếu thời gian yêu cầu của yêu cầu xác minh trang chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang. Máy chủ xác định rằng yêu cầu xác minh trang chưa hết hạn, nếu thời gian yêu cầu của yêu cầu xác minh trang không chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang.

Khoảng thời gian định trước có thể được thiết lập dựa vào các yêu cầu thực tế, ví dụ, 10 phút, 20 phút hoặc 40 phút. Không có hạn chế nào được áp đặt theo phương án thực hiện này của sáng chế. Cần lưu ý rằng kẻ tấn công có thể tấn công máy chủ bằng cách mô phỏng hành vi của người dùng thông thường, và cần có thời gian để kẻ tấn công mô phỏng hành vi của người dùng thông thường. Do đó, theo phương án thực hiện này của sáng chế, trong điều kiện mà người dùng có thể gửi yêu cầu đến máy chủ một cách bình thường, khoảng thời gian định trước càng ngắn thì càng ít có khả năng kẻ tấn công tấn công máy chủ.

Ví dụ, nếu thời gian yêu cầu của yêu cầu xác minh trang được thu từ yêu cầu xác minh trang là 13:15, thời gian để trình duyệt thực thi tập lệnh trang là 12:34 và khoảng thời gian định trước là một giờ, thì máy chủ xác định rằng, thời gian yêu cầu của yêu cầu xác minh trang sớm hơn so với tổng khoảng thời gian định trước và thời

gian để trình duyệt thực thi tập lệnh trang, tức là 13:15 sớm hơn so với 13:34. Vì vậy, yêu cầu xác minh trang chưa hết hạn. Nếu thời gian yêu cầu của yêu cầu xác minh trang là 14:12, thì máy chủ có thể sử dụng phương pháp xác định trước để kết luận rằng yêu cầu xác minh trang đã hết hạn.

Bước 104a: Nếu đã hết hạn, thì kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang.

Theo phương án thực hiện này của sáng chế, thông tin nhắc lỗi chỉ báo việc hết hạn trang được kết xuất nếu yêu cầu xác minh trang đã hết hạn, để nhắc người dùng biết rằng trang hiện thời đã hết hạn. Nếu người dùng vẫn muốn thực hiện thao tác trên trang này, thì người dùng cần làm mới trang. Việc làm mới trang tương đương với việc gửi yêu cầu trang đến máy chủ. Sau khi nhận được yêu cầu, máy chủ cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này. Tức là, sau bước 104a, nếu nhận được lệnh làm mới từ người dùng, thì máy chủ chuyển sang bước 101 để thực hiện lại bước 101.

Bước 104b: Nếu chưa hết hạn, thì xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không.

Bước 104b song song với bước 104a. Máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không, nếu yêu cầu xác minh trang chưa hết hạn. Theo phương án thực hiện này của sáng chế, máy chủ có thể xác minh, dựa vào tập lệnh trang được thực thi để thu được tham số thực thi tập lệnh, xem liệu tham số thực thi tập lệnh có hợp lệ hay không. Quy trình cụ thể của bước 104b có thể như sau: Trước tiên, máy chủ thu được tham số tập lệnh cục bộ dựa vào tập lệnh trang và sau đó xác định xem liệu tham số tập lệnh cục bộ này có giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang hay không; nếu giống, thì chỉ báo rằng tham số thực thi tập lệnh hợp lệ; nếu không giống, thì chỉ báo rằng tham số thực thi tập lệnh không hợp lệ.

Ví dụ, sau khi yêu cầu xác minh trang được gửi bởi trình duyệt được nhận, nếu logic thu tham số thực thi tập lệnh trong tập lệnh trang được trích xuất theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang để thu được giá trị token theo thông tin tệp tin được mã hóa bằng cách sử dụng thuật toán tóm lược tin báo 5 (Message Digest 5, MD5), và yêu cầu xác minh trang trong khoảng thời gian

hợp lệ, thì máy chủ xác định, dựa vào logic thu tham số thực thi tập lệnh trong tập lệnh trang, xem liệu việc xác minh tham số tập lệnh có thể tiếp tục hay không. Tức là, máy chủ xác định, dựa vào giá trị MD5 được mã hóa của token trong thông tin tệp tin tương ứng được lưu trong máy chủ, xem liệu việc xác minh tham số tập lệnh được gửi bởi trình duyệt có thể tiếp tục hay không.

Bước 105b: Nếu không hợp lệ, thì từ chối yêu cầu trang.

Theo phương án thực hiện này của sáng chế, yêu cầu trang bị từ chối nếu tham số thực thi tập lệnh không hợp lệ sau khi xác minh. Sau đó, nếu người dùng vẫn muốn thực hiện thao tác trên trang, thì người dùng cần làm mới trang này. Việc làm mới trang tương đương với việc gửi yêu cầu trang đến máy chủ. Sau khi nhận được yêu cầu này, máy chủ cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này. Tức là, sau bước 105b, nếu nhận được lệnh làm mới từ người dùng, thì máy chủ chuyển sang bước 101 để thực hiện lại bước 101.

Cần lưu ý rằng theo sáng chế, yêu cầu trang có thể bị từ chối bằng cách sử dụng thông tin nhận dạng người dùng trong yêu cầu xác minh trang, và thông tin nhận dạng người dùng này là thông tin tệp tin được tạo ra bởi máy chủ. Sau khi nhận được thông tin tệp tin được gửi bởi máy chủ, trình duyệt lưu khóa/giá trị trong thông tin tệp tin thành tệp tin văn bản trong thư mục cụ thể. Trình duyệt gửi thông tin tệp tin đến máy chủ khi yêu cầu trang web lần tới. Nếu yêu cầu xác minh trang được gửi bởi trình duyệt đã hết hạn hoặc tham số thực thi tập lệnh không hợp lệ sau khi xác minh, thì máy chủ có thể thiết lập dịch vụ tương ứng với thông tin tệp tin trong yêu cầu xác minh trang thành "từ chối" để từ chối yêu cầu trang.

Theo phương pháp ngăn ngừa máy chủ không bị tấn công được đề xuất theo phương án thực hiện này của sáng chế, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, thì trước tiên máy chủ xác định xem liệu yêu cầu xác minh trang này đã hết hạn hay chưa. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Nếu tham số thực thi tập lệnh không hợp lệ, thì máy chủ từ chối yêu cầu trang để ngăn ngừa máy chủ không bị tấn công. Hiện nay, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có

hợp lệ hay không, để ngăn ngừa máy chủ không bị tấn công. So với quy trình này, theo sáng chế, máy chủ xác minh tham số thực thi tập lệnh để ngăn ngừa máy chủ không bị tấn công. Tham số thực thi tập lệnh này được thu dựa vào tập lệnh trang được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang, và logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu được logic tập lệnh trong mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi thời gian yêu cầu của yêu cầu xác minh trang vượt quá khoảng thời gian định trước, thì máy chủ từ chối yêu cầu trang. Trình duyệt cần phải tải lại yêu cầu xác minh trang để gửi lại yêu cầu xác minh trang, và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại. Do đó, kẻ tấn công không thể tấn công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Một phương án thực hiện của sáng chế đề xuất phương pháp ngăn ngừa máy chủ không bị tấn công khác. Như được thể hiện trên Fig.2, phương pháp này bao gồm các bước sau.

Bước 201: Thu được URL của trang trong yêu cầu trang khi nhận được yêu cầu trang được gửi bởi trình duyệt.

Bước 202: Trích xuất ngẫu nhiên tập lệnh trang từ các tập lệnh trang hiện có trong thư viện tập lệnh định trước và tương ứng với URL của trang.

Logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Theo phương án thực hiện này của sáng chế, trước bước 202, phương pháp này còn bao gồm bước tạo cấu hình các tập lệnh trang tương ứng với mỗi URL của trang trong thư viện tập lệnh định trước. Thư viện tập lệnh định trước lưu các tập lệnh trang lần lượt tương ứng với các URL của trang khác nhau. Logic thu tham số tập lệnh khác nhau được sử dụng trong các tập lệnh trang tương ứng với mỗi URL của trang. Theo phương án thực hiện này của sáng chế, tập lệnh trang được sử dụng để thực thi và tải trang mà trình duyệt yêu cầu, và thu được tham số thực thi tập lệnh từ kết quả thực thi. Khi các tập lệnh trang tương ứng với cùng URL của trang được thực thi, thì các tham số thực thi tập lệnh khác nhau được tạo ra từ bước thực thi các tập lệnh trang khác

nhau.

Cần lưu ý rằng, vì sự khác biệt duy nhất giữa các tập lệnh trang là sử dụng logic thu tham số thực thi tập lệnh khác nhau, nên các trang được tạo ra bằng cách tải và thực thi các tập lệnh trang giống nhau. Sự khác biệt duy nhất so với việc thực thi các tập lệnh trang là các tham số thực thi tập lệnh được tạo ra khác nhau.

Bước 203: Gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt.

Ngoài ra, trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh. Sau khi tải và thực thi tập lệnh trang, trình duyệt hiển thị trang tương ứng và thu được tham số thực thi tập lệnh. Các tham số thực thi tập lệnh là các tham số bổ sung trên trang và không ảnh hưởng đến trang được hiển thị.

Bước 204: Xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt.

Theo phương án thực hiện này của sáng chế, bước 204 bao gồm bước xác định xem liệu thời gian yêu cầu của yêu cầu xác minh trang có chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang hay không; và nếu chậm hơn, thì xác định rằng yêu cầu xác minh trang đã hết hạn; hoặc nếu không chậm hơn, thì xác định rằng yêu cầu xác minh trang chưa hết hạn. Khoảng thời gian định trước được sử dụng để giới hạn thời gian khi trình duyệt có thể gửi yêu cầu trang đến máy chủ, và khoảng thời gian định trước này có thể được xác định dựa vào các yêu cầu thực tế.

Cần lưu ý rằng, kẻ tấn công có thể tấn công máy chủ bằng cách mô phỏng hành vi của người dùng thông thường và cần có thời gian để kẻ tấn công mô phỏng hành vi của người dùng thông thường. Do đó, theo phương án thực hiện này của sáng chế, trong điều kiện mà người dùng có thể gửi yêu cầu đến máy chủ một cách bình thường, khoảng thời gian định trước càng ngắn thì càng ít có khả năng kẻ tấn công tấn công máy chủ.

Bước 205a: Nếu đã hết hạn, thì kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang.

Bước 205b: Nếu chưa hết hạn, thì xác minh xem liệu tham số thực thi tập lệnh

nằm trong yêu cầu xác minh trang có hợp lệ hay không.

Bước 205b song song với bước 205a. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Theo phương án thực hiện này của sáng chế, yêu cầu trang còn bao gồm thông tin mã định danh của tập lệnh trang được thực thi bởi trình duyệt. Bước 205b bao gồm các bước sau: tìm kiếm thư viện tập lệnh định trước cho tập lệnh trang tương ứng với thông tin mã định danh, trong đó thư viện tập lệnh định trước còn lưu thông tin mã định danh tương ứng với mỗi tập lệnh trang; và xác minh, dựa vào tập lệnh trang tương ứng với thông tin mã định danh, xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Tập lệnh trang được thực thi bởi trình duyệt là tập lệnh trang được gửi bởi máy chủ đến trình duyệt ở bước 203. Khi gửi tập lệnh trang đến trình duyệt, thì máy chủ đồng thời gửi thông tin mã định danh tương ứng với tập lệnh trang đến trình duyệt. Khi gửi yêu cầu xác minh trang đến máy chủ, thì trình duyệt đồng thời gửi thông tin mã định danh của tập lệnh trang đến máy chủ. Sau đó, máy chủ thu được tập lệnh trang tương ứng từ thư viện tập lệnh định trước dựa vào thông tin mã định danh của tập lệnh trang, và xác minh, dựa vào tập lệnh trang được thu, xem liệu tham số thực thi tập lệnh có chính xác hay không.

Theo phương án thực hiện này của sáng chế, bước xác minh dựa vào tập lệnh trang tương ứng với thông tin mã định danh, xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không, bao gồm các bước: thu được tham số tập lệnh cục bộ dựa vào tập lệnh trang tương ứng với thông tin mã định danh; xác định xem liệu tham số tập lệnh cục bộ này có giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang hay không; và nếu giống, thì xác định rằng tham số thực thi tập lệnh hợp lệ; hoặc nếu không giống, thì xác định rằng tham số thực thi tập lệnh không hợp lệ.

Bước 206b: Nếu không hợp lệ, thì từ chối yêu cầu trang.

Theo phương án thực hiện này của sáng chế, nếu tham số thực thi tập lệnh không hợp lệ sau khi xác minh, thì yêu cầu trang bị từ chối. Sau đó, nếu người dùng vẫn muốn thực hiện thao tác trên trang, thì người dùng cần làm mới trang này. Việc làm mới trang tương đương với việc gửi yêu cầu trang đến máy chủ. Sau khi nhận được yêu cầu, máy chủ cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương

ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này. Tức là, sau khi từ chối yêu cầu trang, nếu nhận được lệnh làm mới từ người dùng, thì máy chủ chuyển sang bước 201 để thực hiện lại bước 201 và trích xuất lại ngẫu nhiên tập lệnh trang sau khi thực hiện lại bước 201. Do đó, kẻ tấn công không thể tấn công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Theo phương án thực hiện này của sáng chế, trường hợp được thể hiện trên Fig.5 có thể được áp dụng, nhưng không bị giới hạn ở đó. Trường hợp này bao gồm các bước sau: ở bước 1 trên Fig.5, trước tiên trình duyệt gửi yêu cầu trang đến máy chủ. Yêu cầu trang này bao gồm URL của trang. Sau khi nhận được yêu cầu trang này, máy chủ trích xuất ngẫu nhiên tập lệnh trang tương ứng với URL của trang từ thư viện tập lệnh định trước và sau đó gửi tập lệnh trang đến trình duyệt. Tức là, máy chủ gửi tập lệnh trang được trích xuất ngẫu nhiên đến trình duyệt bằng cách sử dụng bước 2 trên Fig.5. Sau khi nhận được tập lệnh trang được gửi bởi máy chủ, trình duyệt thực thi tập lệnh trang và thu được tham số thực thi tập lệnh được thu bằng cách thực thi tập lệnh trang. Sau đó, trình duyệt gửi yêu cầu xác minh trang đến máy chủ. Yêu cầu xác minh trang này bao gồm tham số thực thi tập lệnh. Tức là, trình duyệt gửi yêu cầu xác minh trang đến máy chủ bằng cách sử dụng bước 3 trên Fig.5. Sau khi nhận được yêu cầu xác minh trang, trước tiên máy chủ xác định xem liệu thời gian yêu cầu xác minh trang có chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang hay không. Máy chủ xác minh xem liệu tham số thực thi tập lệnh có hợp lệ hay không, nếu thời gian yêu cầu xác minh trang sớm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang. Nếu không hợp lệ, thì máy chủ từ chối yêu cầu trang. Tham số thực thi tập lệnh theo sáng chế được thu bằng cách thực thi tập lệnh trang tương ứng với URL của trang và được trích xuất ngẫu nhiên từ thư viện tập lệnh định trước và logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu được logic tập lệnh theo mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi yêu cầu xác minh trang đã hết hạn, trình duyệt cần phải tải lại yêu cầu xác minh trang và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại tương ứng với URL của

trang. Do đó, kẻ tấn công không thể tấn công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Theo phương pháp ngăn ngừa máy chủ không bị tấn công khác được đề xuất theo phương án thực hiện này của sáng chế, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, thì trước tiên máy chủ xác định xem liệu yêu cầu xác minh trang này đã hết hạn hay chưa. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Nếu tham số thực thi tập lệnh không hợp lệ, thì máy chủ từ chối yêu cầu trang để ngăn ngừa máy chủ không bị tấn công. Hiện nay, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có hợp lệ hay không để ngăn ngừa máy chủ không bị tấn công. So với quy trình này, theo sáng chế, máy chủ xác minh tham số thực thi tập lệnh để ngăn ngừa máy chủ không bị tấn công. Tham số thực thi tập lệnh được thu dựa vào tập lệnh trang được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang, và logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu được logic tập lệnh trong mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi thời gian yêu cầu của yêu cầu xác minh trang vượt quá khoảng thời gian định trước, thì máy chủ từ chối yêu cầu trang. Trình duyệt cần phải tải lại yêu cầu xác minh trang để gửi lại yêu cầu xác minh trang, và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại. Do đó, kẻ tấn công không thể tấn công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Ngoài ra, một phương án thực hiện của sáng chế đề xuất thiết bị ngăn ngừa máy chủ không bị tấn công. Như được thể hiện trên Fig.3, thiết bị này bao gồm bộ phận cấp phát 31, bộ phận gửi 32, bộ phận xác định 33, bộ phận kết xuất 34, bộ phận xác minh 35 và bộ phận từ chối 36.

Bộ phận cấp phát 31 được tạo cấu hình để cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi yêu cầu trang được gửi bởi trình duyệt được nhận.

Bộ phận gửi 32 được tạo cấu hình để gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh.

Bộ phận xác định 33 được tạo cấu hình để xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi yêu cầu xác minh trang được gửi bởi trình duyệt được nhận.

Bộ phận kết xuất 34 được tạo cấu hình để kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang nếu yêu cầu xác minh trang đã hết hạn.

Bộ phận xác minh 35 được tạo cấu hình để xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không, nếu yêu cầu xác minh trang chưa hết hạn.

Bộ phận từ chối 36 được tạo cấu hình để từ chối yêu cầu trang nếu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang không hợp lệ.

Cần lưu ý rằng, đối với các phần mô tả tương ứng khác của các bộ phận chức năng trong thiết bị ngăn ngừa máy chủ không bị tấn công theo phương án thực hiện này của sáng chế, có thể thực hiện tham chiếu đến các phần mô tả tương ứng của phương pháp được thể hiện trên Fig.1. Nội dung chi tiết được lược bỏ ở đây cho đơn giản. Tuy nhiên, rõ ràng là thiết bị theo phương án thực hiện này có thể thực hiện tất cả nội dung tương ứng theo phương án thực hiện của phương pháp này.

Theo phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công được đề xuất theo các phương án thực hiện của sáng chế, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, thì trước tiên máy chủ xác định xem liệu yêu cầu xác minh trang này đã hết hạn hay chưa. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Nếu tham số thực thi tập lệnh không hợp lệ, thì máy chủ từ chối yêu cầu trang để ngăn ngừa máy chủ không bị tấn công. Hiện nay, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có hợp lệ hay không, để ngăn ngừa máy chủ không bị tấn công. So với quy trình này, theo sáng chế, máy chủ xác minh tham số thực thi tập lệnh để ngăn ngừa máy chủ không bị tấn công. Tham số thực thi tập lệnh được thu dựa vào tập lệnh trang được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu

cầu trang và logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu được logic tập lệnh trong mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi thời gian yêu cầu của yêu cầu xác minh trang vượt quá khoảng thời gian định trước, thì máy chủ từ chối yêu cầu trang. Trình duyệt cần phải tải lại yêu cầu xác minh trang để gửi lại yêu cầu xác minh trang và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại. Do đó, kẻ tấn công không thể tấn công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Ngoài ra, một phương án thực hiện của sáng chế đề xuất thiết bị ngăn ngừa máy chủ không bị tấn công khác. Như được thể hiện trên Fig.4, thiết bị này bao gồm bộ phận cấp phát 41, bộ phận gửi 42, bộ phận xác định 43, bộ phận kết xuất 44, bộ phận xác minh 45 và bộ phận từ chối 46.

Bộ phận cấp phát 41 được tạo cấu hình để cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi yêu cầu trang được gửi bởi trình duyệt được nhận.

Bộ phận gửi 42 được tạo cấu hình để gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh.

Bộ phận xác định 43 được tạo cấu hình để xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi yêu cầu xác minh trang được gửi bởi trình duyệt được nhận.

Bộ phận kết xuất 44 được tạo cấu hình để kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang, nếu yêu cầu xác minh trang đã hết hạn.

Bộ phận xác minh 45 được tạo cấu hình để xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không, nếu yêu cầu xác minh trang chưa hết hạn.

Bộ phận từ chối 46 được tạo cấu hình để từ chối yêu cầu trang nếu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang không hợp lệ.

Ngoài ra, bộ phận cấp phát 41 bao gồm môđun thu 411, được tạo cấu hình để thu URL của trang trong yêu cầu trang; và môđun trích xuất 412, được tạo cấu hình để trích xuất ngẫu nhiên tập lệnh trang từ các tập lệnh trang hiện có trong thư viện tập lệnh định trước và tương ứng với URL của trang, trong đó logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang.

Ngoài ra, bộ phận xác định 43 bao gồm môđun xác định 431, được tạo cấu hình để xác định xem liệu thời gian yêu cầu của yêu cầu xác minh trang có chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang hay không; và môđun xác định 432, được tạo cấu hình để xác định rằng yêu cầu xác minh trang đã hết hạn, nếu thời gian yêu cầu của yêu cầu xác minh trang chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang; hoặc môđun xác định 432, được tạo cấu hình để xác định rằng yêu cầu xác minh trang chưa hết hạn, nếu thời gian yêu cầu của yêu cầu xác minh trang không chậm hơn so với tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang.

Theo phương án thực hiện này của sáng chế, yêu cầu trang còn bao gồm thông tin mã định danh của tập lệnh trang được thực thi bởi trình duyệt, và bộ phận xác minh 45 bao gồm môđun tìm kiếm 451, được tạo cấu hình để tìm kiếm thư viện tập lệnh định trước cho tập lệnh trang tương ứng với thông tin mã định danh, trong đó thư viện tập lệnh định trước này còn lưu thông tin mã định danh tương ứng với mỗi tập lệnh trang; và môđun xác minh 452, được tạo cấu hình để xác minh, dựa vào tập lệnh trang tương ứng với thông tin mã định danh, xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không.

Theo phương án thực hiện này của sáng chế, môđun xác minh 452 được tạo cấu hình để thu được tham số tập lệnh cục bộ dựa vào tập lệnh trang tương ứng với thông tin mã định danh.

Môđun xác minh 452 được tạo cấu hình để xác định xem liệu tham số tập lệnh cục bộ có giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang hay không.

Môđun xác minh 452 được tạo cấu hình để xác định rằng tham số thực thi tập lệnh hợp lệ, nếu tham số tập lệnh cục bộ giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang.

Môđun xác minh 452 được tạo cấu hình để xác định rằng tham số thực thi tập lệnh không hợp lệ, nếu tham số tập lệnh cục bộ khác tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang.

Thiết bị này còn bao gồm bộ phận tạo cấu hình 47, được tạo cấu hình để tạo cấu hình các tập lệnh trang tương ứng với mỗi URL của trang trong thư viện tập lệnh định trước.

Cần lưu ý rằng, đối với các phần mô tả tương ứng khác của các bộ phận chức năng trong thiết bị ngăn ngừa máy chủ không bị tấn công khác theo phương án thực hiện này của sáng chế, có thể thực hiện tham chiếu đến các phần mô tả tương ứng của phương pháp được thể hiện trên Fig.2. Nội dung chi tiết được lược bỏ ở đây cho đơn giản. Tuy nhiên, rõ ràng là thiết bị theo phương án thực hiện này có thể thực hiện tất cả nội dung tương ứng theo phương án thực hiện của phương pháp này.

Theo phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công được đề xuất theo các phương án thực hiện của sáng chế, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, thì trước tiên máy chủ xác định xem liệu yêu cầu xác minh trang này đã hết hạn hay chưa. Nếu yêu cầu xác minh trang chưa hết hạn, thì máy chủ xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không. Nếu tham số thực thi tập lệnh không hợp lệ, thì máy chủ từ chối yêu cầu trang để ngăn ngừa máy chủ không bị tấn công. Hiện nay, máy chủ xác minh giá trị token được mã hóa để xác định xem liệu yêu cầu dịch vụ được gửi bởi trình duyệt có hợp lệ hay không để ngăn ngừa máy chủ không bị tấn công. So với quy trình này, theo sáng chế, máy chủ xác minh tham số thực thi tập lệnh để ngăn ngừa máy chủ không bị tấn công. Tham số thực thi tập lệnh này được thu dựa vào tập lệnh trang được cấp phát theo cách động và ngẫu nhiên từ các tập lệnh trang tương ứng với yêu cầu trang, và logic thu tham số thực thi tập lệnh khác được sử dụng trong các tập lệnh trang. Do đó, ngay cả khi kẻ tấn công thu logic tập lệnh trong mã động, thì kẻ tấn công này cũng không thể phân tích cú pháp phương pháp mã hóa tham số thực thi tập lệnh trong khoảng thời gian định trước. Ngoài ra, khi thời gian yêu cầu của yêu cầu xác minh trang vượt quá khoảng thời gian định trước, thì máy chủ từ chối yêu cầu trang. Trình duyệt cần phải tải lại yêu cầu xác minh trang để gửi lại yêu cầu xác minh trang và tham số thực thi tập lệnh trong yêu cầu xác minh trang được tải lại được thu bằng cách thực thi tập lệnh trang được trích xuất lại. Do đó, kẻ tấn công không thể tấn

công máy chủ theo phương án thực hiện này của sáng chế. Do vậy, sự bảo mật của máy chủ được cải thiện theo phương án thực hiện này của sáng chế.

Thiết bị ngăn ngừa máy chủ không bị tấn công bao gồm bộ xử lý và bộ nhớ. Bộ phận cấp phát, bộ phận gửi, bộ phận xác định, bộ phận kết xuất, bộ phận xác minh, bộ phận từ chối và bộ phận tạo cấu hình được lưu trong bộ nhớ là các bộ chương trình. Bộ xử lý thực thi các bộ chương trình được lưu trong bộ nhớ để thực hiện các chức năng tương ứng.

Bộ xử lý bao gồm nhân, và nhân này gọi ra bộ chương trình tương ứng từ bộ nhớ. Có thể có một hoặc nhiều nhân để cải thiện sự bảo mật của máy chủ bằng cách điều chỉnh tham số nhân.

Bộ nhớ có thể bao gồm thiết bị lưu trữ không ổn định, bộ nhớ truy cập ngẫu nhiên (RAM, Random Access Memory) và/hoặc bộ nhớ bất khả biến trong vật ghi đọc được bằng máy tính, ví dụ, bộ nhớ chỉ đọc (ROM, Read-Only Memory) hoặc bộ nhớ nhanh (flash RAM). Bộ nhớ này bao gồm ít nhất một chip lưu trữ.

Sáng chế còn đề xuất sản phẩm chương trình máy tính, và khi được thực thi trên thiết bị xử lý dữ liệu, sản phẩm này được sử dụng để khởi tạo mã chương trình bao gồm các bước sau: khi nhận được yêu cầu trang được gửi bởi trình duyệt, cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này; gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh; khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, thì xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa; và nếu đã hết hạn, thì kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang; hoặc nếu chưa hết hạn, thì xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không; và nếu không hợp lệ, thì từ chối yêu cầu trang.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án thực hiện của sáng chế có thể được đề xuất ở dạng phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng của các phương án thực hiện chỉ có phần cứng, các phương án thực hiện chỉ có phần mềm hoặc các phương án thực hiện kết hợp cả phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dạng của sản phẩm chương trình máy tính được thực hiện trên một

hoặc nhiều vật ghi lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị hạn chế ở thiết bị lưu trữ đĩa từ, CD-ROM, bộ nhớ quang học, v.v.) bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả với tham chiếu đến các lưu đồ và/hoặc các sơ đồ khối của phương pháp và thiết bị ngăn ngừa máy chủ không bị tấn công và sản phẩm chương trình máy tính, theo các phương án thực hiện của sáng chế. Cần hiểu rằng, các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi bước và/hoặc mỗi khối trên các lưu đồ và/hoặc các sơ đồ khối và tổ hợp bước và/hoặc khối trên các lưu đồ và/hoặc các sơ đồ khối này. Các lệnh chương trình máy tính này có thể được cấp cho máy tính đa năng, máy tính chuyên dùng, bộ xử lý nhúng hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra máy, để các lệnh này được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác để tạo ra thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều bước trên các lưu đồ và/hoặc trên một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được lưu trong bộ nhớ đọc được bằng máy tính có thể lệnh cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác làm việc theo cách cụ thể, để các lệnh được lưu trong bộ nhớ đọc được bằng máy tính tạo ra thành phần giả tượng (artifact) bao gồm thiết bị lệnh. Thiết bị lệnh này thực hiện chức năng cụ thể trong một hoặc nhiều bước trên các lưu đồ và/hoặc trên một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được tải vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, để các chuỗi bước vận hành và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra quá trình xử lý được thực hiện trên máy tính. Do đó, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước thực hiện chức năng cụ thể trong một hoặc nhiều bước trên các lưu đồ và/hoặc trên một hoặc nhiều khối trên các sơ đồ khối.

Theo một kết cấu điển hình, thiết bị tính toán bao gồm một hoặc nhiều bộ xử lý trung tâm (CPU, Central Processing Unit), giao diện đầu vào/đầu ra, giao diện mạng và bộ nhớ.

Bộ nhớ này có thể bao gồm thiết bị lưu trữ không ổn định, bộ nhớ truy cập ngẫu nhiên (RAM, Random Access Memory) và/hoặc bộ nhớ bất khả biến trong vật ghi đọc

được bằng máy tính, ví dụ, bộ nhớ chỉ đọc (ROM, Read-Only Memory) hoặc bộ nhớ nhanh (flash RAM). Bộ nhớ là một ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm vật ghi ổn định, vật ghi không ổn định, vật ghi di động và không di động có thể lưu thông tin bằng cách sử dụng phương pháp hoặc công nghệ bất kỳ. Thông tin này có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, môđun chương trình hoặc dữ liệu khác. Vật ghi lưu trữ máy tính bao gồm nhưng không giới hạn ở bộ nhớ truy cập ngẫu nhiên thay đổi pha (PRAM, Phase-change Random Access Memory), bộ nhớ truy cập ngẫu nhiên tĩnh (SRAM, Static Random Access Memory), bộ nhớ truy cập ngẫu nhiên động (DRAM, Dynamic Random Access Memory), kiểu khác của bộ nhớ truy cập ngẫu nhiên (RAM, Random Access Memory), bộ nhớ chỉ đọc (ROM, Read-Only Memory), bộ nhớ chỉ đọc có thể lập trình xóa được bằng tín hiệu điện (EEPROM, Electrically Erasable Programmable Read-Only Memory), bộ nhớ nhanh hoặc công nghệ bộ nhớ khác, bộ nhớ chỉ đọc dạng đĩa nén (CD-ROM, Compact Disc Read-Only Memory), đĩa đa năng kỹ thuật số (DVD, Digital Versatile Disc) hoặc thiết bị lưu trữ quang học, cát sét từ, băng từ, thiết bị lưu trữ đĩa từ, thiết bị lưu trữ từ tính khác hoặc vật ghi lâu dài khác bất kỳ. Vật ghi lưu trữ máy tính có thể được sử dụng để lưu thông tin truy cập được bằng thiết bị điện toán. Dựa vào định nghĩa trong bản mô tả này, vật ghi đọc được bằng máy tính không bao gồm các vật ghi đọc được bằng máy tính tạm thời (vật ghi tạm thời), ví dụ, tín hiệu dữ liệu được điều biến và sóng mang.

Các phần mô tả nêu trên chỉ là các phương án thực hiện của sáng chế và không nhằm giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể thực hiện các cải biên và các biến thể khác nhau đối với sáng chế. Các cải biên, các thay thế tương đương hoặc các cải tiến bất kỳ được thực hiện mà không vượt ra khỏi bản chất và nguyên lý của sáng chế sẽ nằm trong phạm vi yêu cầu bảo hộ theo sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp được thực hiện bằng máy tính để ngăn ngừa máy chủ không bị tấn công, phương pháp này bao gồm các bước:

để đáp lại việc nhận được yêu cầu trang được gửi bởi trình duyệt, thu được (201) URL của trang trong yêu cầu trang này;

trích xuất ngẫu nhiên tập lệnh trang từ các tập lệnh trang hiện có trong thư viện tập lệnh định trước và tương ứng với URL của trang, trong đó logic thu tham số thực thi tập lệnh khác nhau được sử dụng trong các tập lệnh trang (202);

gửi (203) tập lệnh trang được trích xuất ngẫu nhiên đến trình duyệt, để trình duyệt thực thi tập lệnh trang để thu được tham số thực thi tập lệnh;

để đáp lại việc nhận được yêu cầu xác minh trang được gửi bởi trình duyệt, xác định (204) xem liệu yêu cầu xác minh trang đã hết hạn hay chưa;

để đáp lại việc xác định rằng yêu cầu xác minh trang đã hết hạn, kết xuất (205a) thông tin nhắc lỗi chỉ báo việc hết hạn trang; hoặc

để đáp lại việc xác định rằng yêu cầu xác minh trang chưa hết hạn, xác minh (205b) xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không; và

nếu tham số thực thi tập lệnh không hợp lệ, thì từ chối yêu cầu trang (206b).

2. Phương pháp theo điểm 1, trong đó logic thu tham số thực thi tập lệnh bao gồm bước thu được giá trị token trong thông tin tệp tin (cookie) được mã hóa.

3. Phương pháp theo điểm 1, trong đó trước bước trích xuất ngẫu nhiên tập lệnh trang từ các tập lệnh trang hiện có trong thư viện tập lệnh định trước và tương ứng với URL của trang, phương pháp này còn bao gồm bước:

tạo cấu hình các tập lệnh trang tương ứng với mỗi URL của trang trong thư viện tập lệnh định trước và thông tin mã định danh tương ứng với các tập lệnh trang.

4. Phương pháp theo điểm 1, trong đó bước xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa bao gồm các bước:

xác định xem liệu thời gian yêu cầu của yêu cầu xác minh trang có chậm hơn tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang hay

không; và

để đáp lại việc xác định rằng thời gian yêu cầu của yêu cầu xác minh trang chậm hơn tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang, xác định rằng yêu cầu xác minh trang đã hết hạn; hoặc

để đáp lại việc xác định rằng thời gian yêu cầu của yêu cầu xác minh trang không chậm hơn tổng khoảng thời gian định trước và thời gian để trình duyệt thực thi tập lệnh trang, xác định rằng yêu cầu xác minh trang chưa hết hạn.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó yêu cầu trang còn bao gồm thông tin mã định danh của tập lệnh trang được thực thi bởi trình duyệt, và trong đó bước xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không bao gồm các bước:

tìm kiếm thư viện tập lệnh định trước cho tập lệnh trang tương ứng với thông tin mã định danh, trong đó thư viện tập lệnh định trước còn lưu thông tin mã định danh tương ứng với mỗi tập lệnh trang; và

xác minh, dựa vào tập lệnh trang tương ứng với thông tin mã định danh, xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không.

6. Phương pháp theo điểm 5, trong đó bước xác minh, dựa vào tập lệnh trang tương ứng với thông tin mã định danh, xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không bao gồm các bước:

thu được tham số tập lệnh cục bộ dựa vào tập lệnh trang tương ứng với thông tin mã định danh;

xác định xem liệu tham số tập lệnh cục bộ này có giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang hay không; và

để đáp lại việc xác định rằng tham số tập lệnh cục bộ giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang, xác định rằng tham số thực thi tập lệnh hợp lệ; hoặc

để đáp lại việc xác định rằng tham số tập lệnh cục bộ không giống tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang, xác định rằng tham số thực thi tập lệnh không hợp lệ.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó bước từ chối yêu cầu trang dựa vào thông tin nhận dạng người dùng nằm trong yêu cầu xác minh trang.

8. Phương pháp theo điểm 7, trong đó thông tin nhận dạng người dùng bao gồm thông tin tệp tin được tạo ra bởi máy chủ.

9. Thiết bị ngăn ngừa máy chủ không bị tấn công, thiết bị này bao gồm các môđun được tạo cấu hình để thực hiện các phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8.

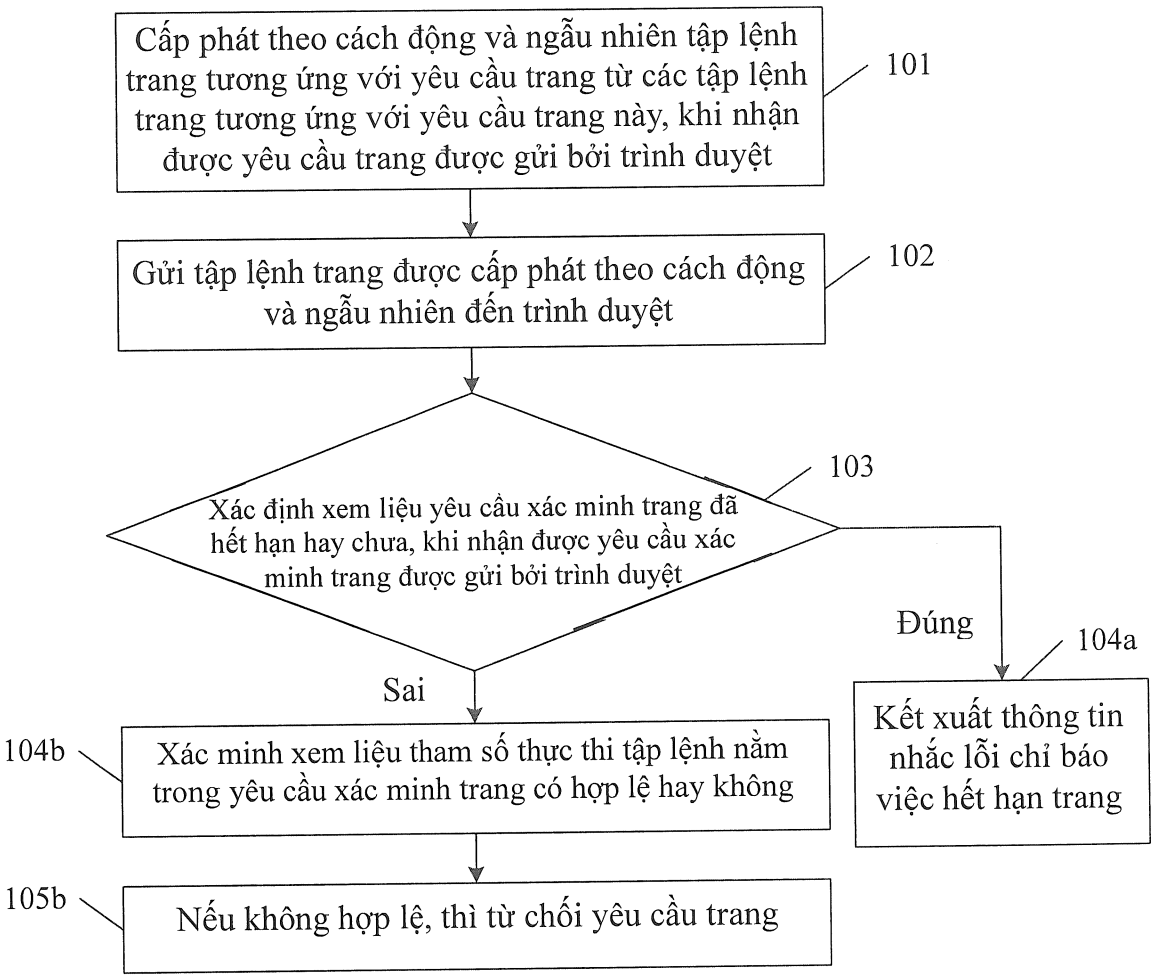

Cấp phát theo cách động và ngẫu nhiên tập lệnh trang tương ứng với yêu cầu trang từ các tập lệnh trang tương ứng với yêu cầu trang này, khi nhận được yêu cầu trang được gửi bởi trình duyệt
101
Gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt
102
Xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt
103
Đúng
104a
Kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang
Sai
104b
Xác minh xem liệu tham số thực thi tập lệnh nằm trong yêu cầu xác minh trang có hợp lệ hay không
105b
Nếu không hợp lệ, thì từ chối yêu cầu trang

Fig.1

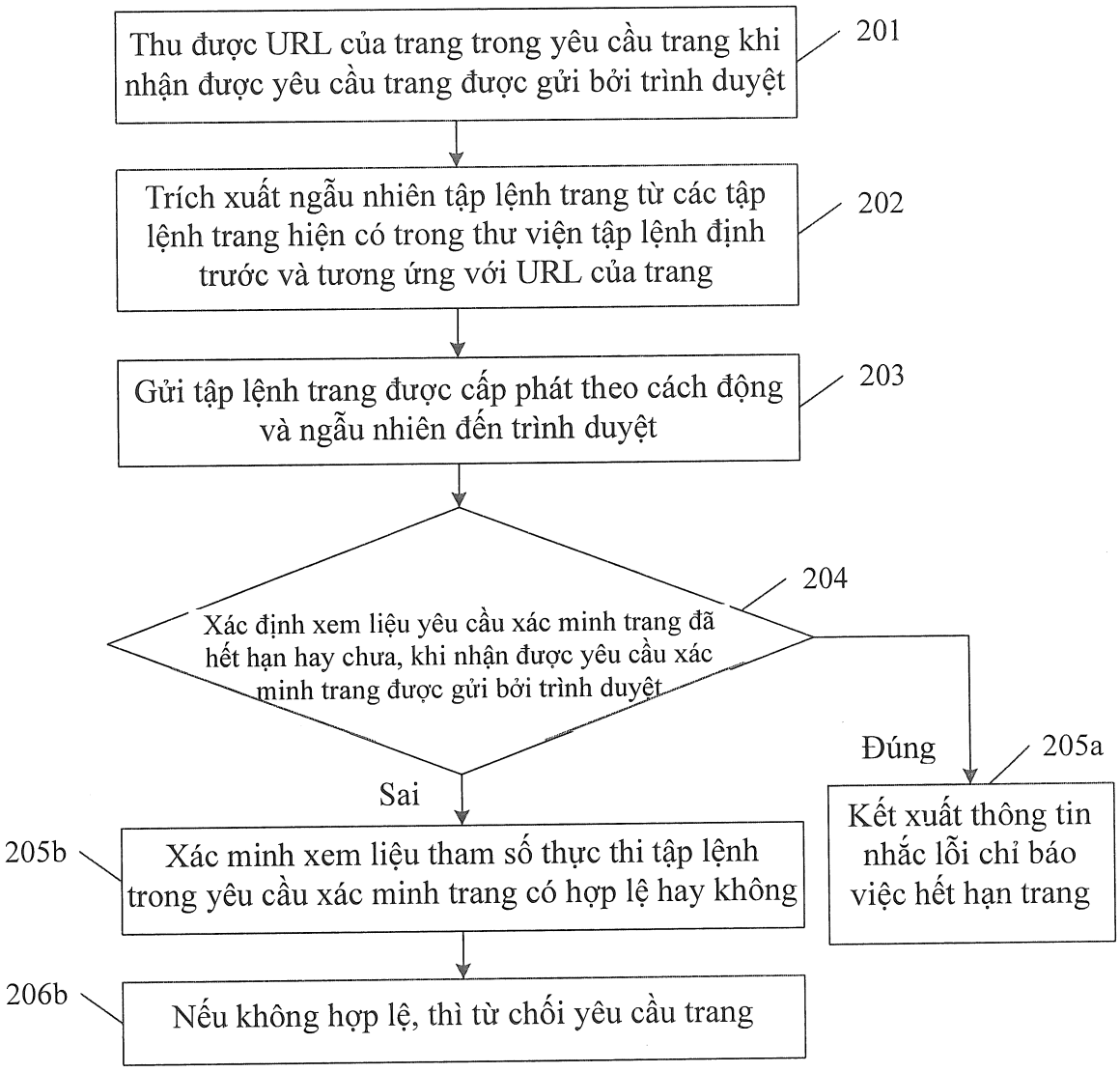

Thu được URL của trang trong yêu cầu trang khi nhận được yêu cầu trang được gửi bởi trình duyệt
201
Trích xuất ngẫu nhiên tập lệnh trang từ các tập lệnh trang hiện có trong thư viện tập lệnh định trước và tương ứng với URL của trang
202
Gửi tập lệnh trang được cấp phát theo cách động và ngẫu nhiên đến trình duyệt
203
Xác định xem liệu yêu cầu xác minh trang đã hết hạn hay chưa, khi nhận được yêu cầu xác minh trang được gửi bởi trình duyệt
204
Đúng
205a
Kết xuất thông tin nhắc lỗi chỉ báo việc hết hạn trang
Sai
205b
Xác minh xem liệu tham số thực thi tập lệnh trong yêu cầu xác minh trang có hợp lệ hay không
206b
Nếu không hợp lệ, thì từ chối yêu cầu trang

Fig.2

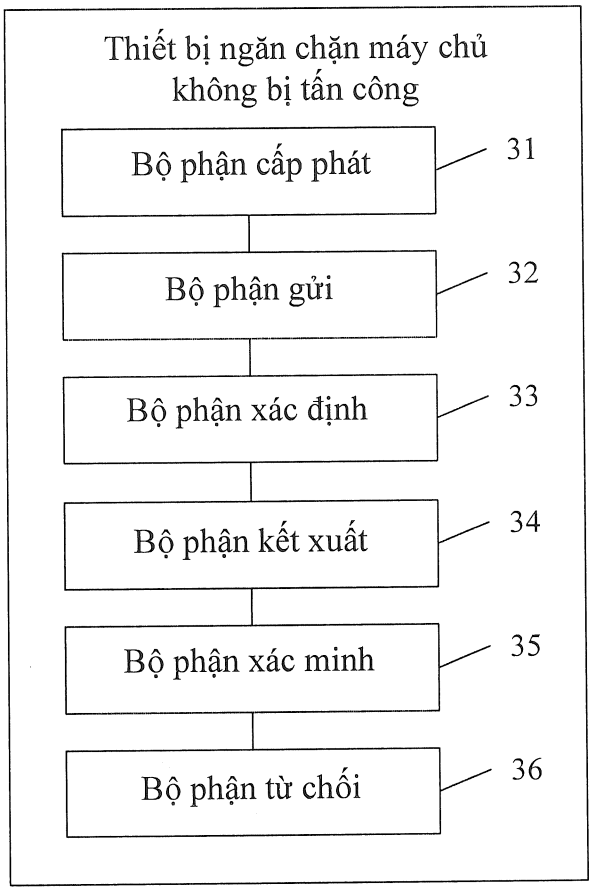

Thiết bị ngăn chặn máy chủ không bị tấn công
Bộ phận cấp phát
31
Bộ phận gửi
32
Bộ phận xác định
33
Bộ phận kết xuất
34
Bộ phận xác minh
35
Bộ phận từ chối
36

Fig.3

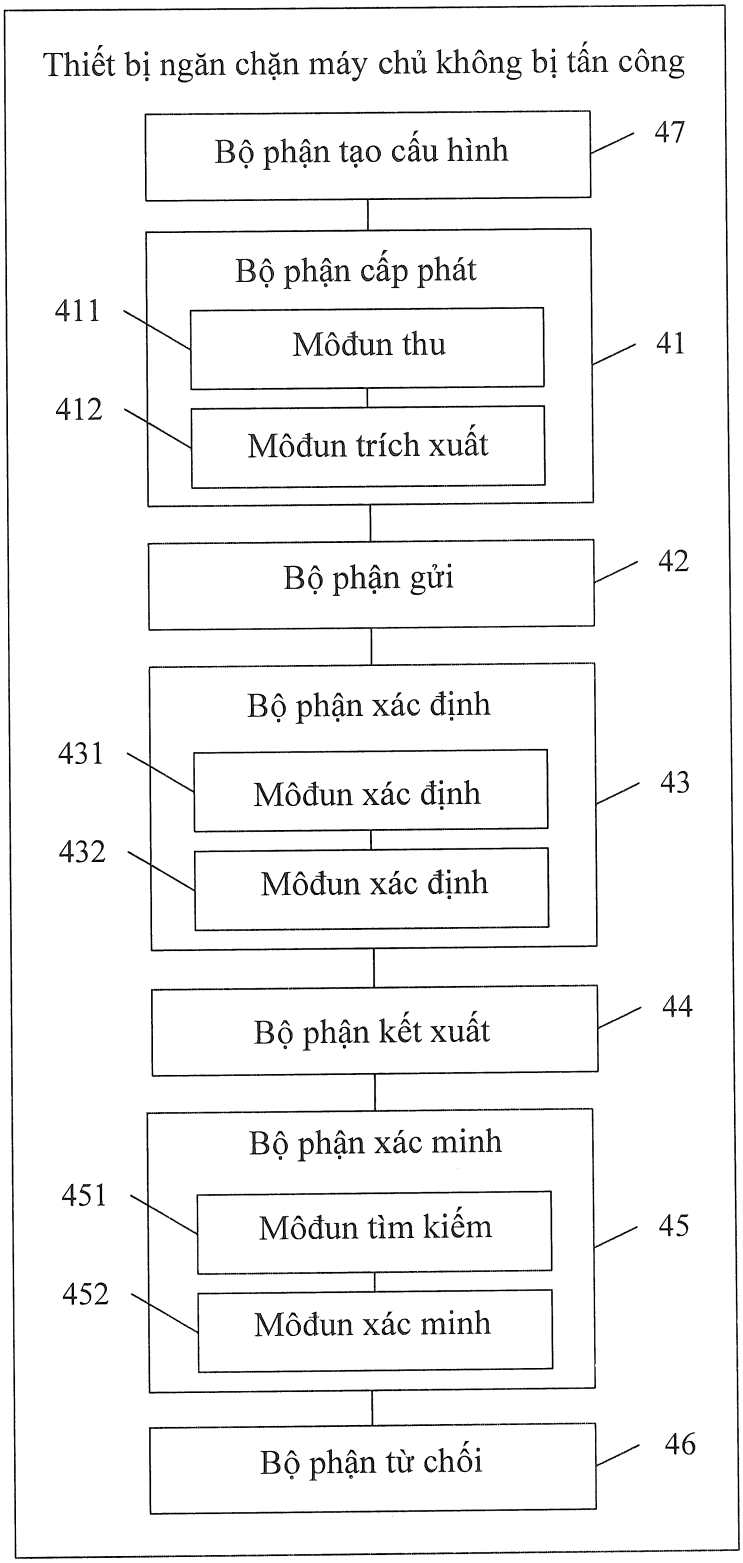

Thiết bị ngăn chặn máy chủ không bị tấn công
Bộ phận tạo cấu hình
47
Bộ phận cấp phát
411
Môđun thu
41
412
Môđun trích xuất
Bộ phận gửi
42
Bộ phận xác định
431
Môđun xác định
43
432
Môđun xác định
Bộ phận kết xuất
44
Bộ phận xác minh
451
Môđun tìm kiếm
45
452
Môđun xác minh
Bộ phận từ chối
46

Fig.4

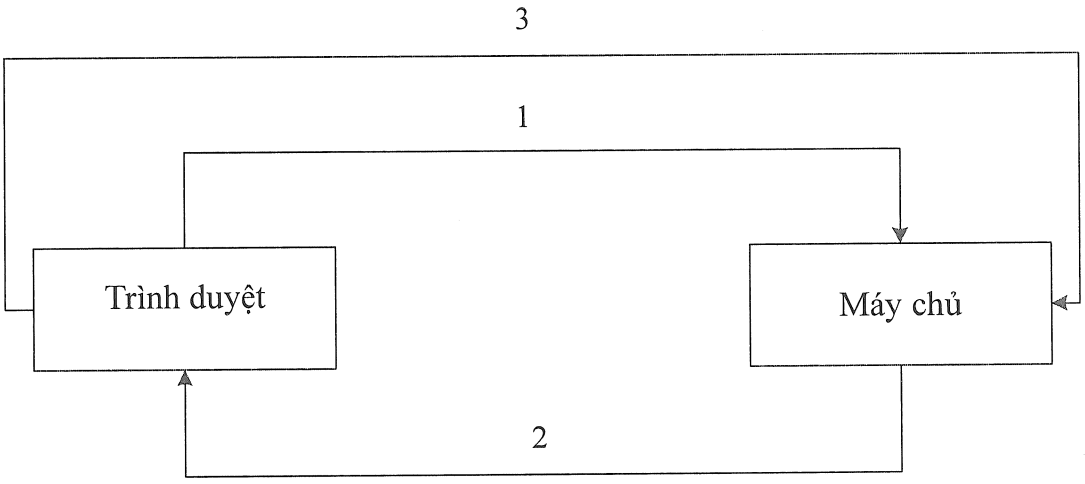


Fig.5