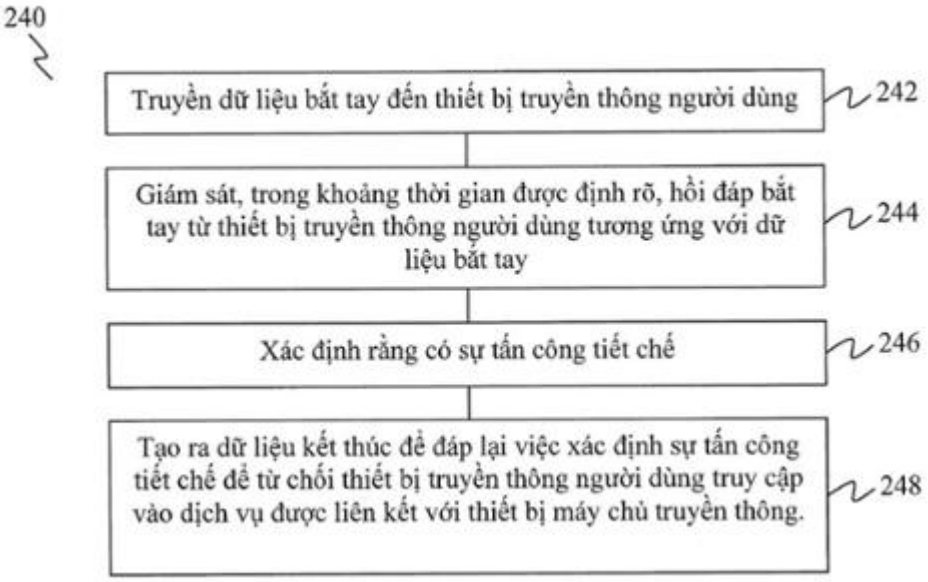
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0036204**
(51)[2020.01] **H04W 12/12**; G06F 21/56; H04L 29/06 (13) **B**

(21) 1-2022-01421 (22) 02/09/2019
(86) PCT/SG2019/050436 02/09/2019 (87) WO2021/045675 11/03/2021
(45) 25/07/2023 424 (43) 25/07/2022 412
(73) GRABTAXI HOLDINGS PTE. LTD. (SG)
3 MEDIA CLOSE, #01-03/06, SINGAPORE 138498, SINGAPORE
(72) KANAGASABAI, Prasanna (IN); PATHAK, Somesh (IN); NARAYANAN, Sreekanth (IN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) THIẾT BỊ MÁY CHỦ TRUYỀN THÔNG VÀ PHƯƠNG PHÁP ĐỂ XÁC ĐỊNH SỰ TẤN CÔNG TIẾT CHẾ VÀ PHƯƠNG TIỆN LƯU TRỮ KHÔNG CHUYỂN TIẾP

(57) Sáng chế này đề cập đến thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng, được tạo cấu hình để truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng, giám sát, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay, và để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay tương ứng với dữ liệu bắt tay được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông xác định sự có mặt của sự kiện mà biểu thị việc thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông, xác định rằng có sự tấn công tiết chế, và tạo ra dữ liệu kết thúc để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông. Sáng chế cũng đề cập đến phương pháp để xác định sự tấn công tiết chế và phương tiện lưu trữ không chuyển tiếp.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập chung đến lĩnh vực truyền thông. Một khía cạnh của sáng chế liên quan đến thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế (abstention) được liên kết với thiết bị truyền thông người dùng. Một khía cạnh khác của sáng chế liên quan đến phương pháp để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng.

Một khía cạnh của sáng chế có ứng dụng cụ thể, nhưng không độc quyền, để xác định việc nhận hồi đáp hoặc phần tải trong quy trình bắt tay, và/hoặc xác định sự tấn công tiết chế khi vắng mặt hồi đáp/phần tải thích hợp lúc hết hạn khoảng thời gian được định rõ.

Tình trạng kỹ thuật của sáng chế

Sự gian lận trên thiết bị di động là nguồn gốc cơ bản của sự mất doanh thu đối với các doanh nghiệp. Khi các tổ chức sử dụng các ứng dụng di động làm giao diện người tiêu dùng chính của họ, thì họ cũng phải xây dựng các chiến lược vững chắc để đối phó với sự gian lận xuất phát từ các nền tảng.

Dù các hệ thống ngăn chặn gian lận được dùng bởi các tổ chức, nhưng những người ác ý cũng đã nâng cao các hiểu biết và kỹ năng của họ để chống lại các hệ thống này, nên các sự tấn công "tiết chế" đã tăng lên. Các sự tấn công tiết chế là các phương pháp

né tránh sự kiểm soát của hệ thống ngăn chặn gian lận bằng cách không tham gia vào việc thu thập dữ liệu được liên kết với hệ thống. Chúng có thể có nhiều dạng, ví dụ:

- Người tấn công thay đổi ứng dụng mà theo cách này thì việc thu thập dữ liệu bị dừng lại;
- Người tấn công thay đổi ứng dụng mà theo cách này thì thủ tục gửi dữ liệu bị dừng lại;
- Người tấn công có thể thao túng kênh truyền thông đến máy chủ và chuyển hướng dữ liệu cụ thể đi đến nơi khác hoặc cắt nó, gây tổn thất toàn bộ gói tin đến máy chủ dự định.

Mặc dù có các biến thể của sự tấn công này đối với máy khách, nhưng các triệu chứng quan sát được trên máy chủ là sự thiếu truyền thông từ kẻ gian lận đối với việc thu thập dữ liệu.

Các giải pháp ngăn chặn gian lận đã bỏ qua vấn đề tiết chế vì khó giám sát. Các công ty sản xuất bỏ qua nó vì đây là một vấn đề phức tạp cần khắc phục trừ khi một công ty có quyền điều khiển tất cả các thành phần. Theo cách điển hình, giả định là phần tải đến máy chủ luôn được gửi và một khi rào cản này bị phá vỡ, thì các hệ thống sẽ không đưa ra cách phát hiện hoặc khắc phục tình trạng này. Trong những trường hợp như vậy, những kẻ gian lận tiếp tục truyền thông với các dịch vụ và nhận được chức năng bình thường, ngay cả khi chúng đã né tránh được sự phát hiện. Các loại gian lận điển hình có thể gồm giả mạo vị trí hoặc sửa đổi ứng dụng của nhà cung cấp dịch vụ để người ta có thể chọn một số tùy chọn nhất định (ví dụ, các dịch vụ) phù hợp với người đó, ví dụ, các dịch vụ hoặc chuyến đi liên quan đến du lịch, dẫn đến tổn thất tài chính cho nhà cung cấp dịch vụ.

Do đó, chúng tôi mong muốn giải quyết ít nhất một số vấn đề được đề cập ở trên.

Bản chất kỹ thuật của sáng chế

Các khía cạnh của sáng chế như được nêu trong các yêu cầu bảo hộ độc lập. Một số dấu hiệu tùy chọn được định rõ trong các yêu cầu bảo hộ phụ thuộc.

Cách triển khai của các kỹ thuật được bộc lộ ở đây có thể cung cấp các ưu điểm kỹ thuật đáng kể. Các cách triển khai này có thể gồm thiết bị máy chủ truyền thông gửi dữ liệu bắt tay đến thiết bị truyền thông người dùng (với sự kỳ vọng về hồi đáp bắt tay/phần tải trong hồi đáp của nó và tương ứng với dữ liệu bắt tay trong các tình huống bình thường), xác định rằng có sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng khi không có hồi đáp/phần tải thích hợp đã được nhận từ thiết bị truyền thông người dùng lúc hết hạn khoảng thời gian được định rõ, và tiếp đó tạo ra dữ liệu kết thúc mà cho phép việc chặn truy cập bởi thiết bị truyền thông người dùng vào thiết bị máy chủ truyền thông hoặc các dịch vụ được liên kết với thiết bị máy chủ truyền thông.

Trong ít nhất một số cách triển khai, các kỹ thuật được bộc lộ ở đây có thể cung cấp số nonce để được truyền đến thiết bị truyền thông người dùng (ví dụ, được gồm với dữ liệu bắt tay) để có thể tránh được sự tấn công phát lại bằng cách ngăn chặn truyền thông hoặc hồi đáp cũ không bị sử dụng lại để truy cập một lần nữa vào thiết bị máy chủ truyền thông hoặc các dịch vụ được liên kết với nó.

Trong ít nhất một số cách triển khai, các kỹ thuật được bộc lộ ở đây có thể cho phép việc nhớ đệm cho các sự cố mạng tiềm ẩn, ví dụ, các kết nối mạng chậm, bằng cách triển khai khung thời gian hoặc khoảng phù hợp mà nếu vượt quá khung thời gian hoặc khoảng này thì sự tấn công tiết chế có thể bị gắn cờ nếu không có hồi đáp phù hợp từ thiết bị truyền thông người dùng.

Mô tả vắn tắt các hình vẽ

Bây giờ, sáng chế sẽ được mô tả, theo cách làm ví dụ, dựa vào các hình vẽ kèm theo, trong đó:

Fig.1 là sơ đồ khối sơ lược minh họa hệ thống truyền thông làm ví dụ liên quan tới thiết bị máy chủ truyền thông.

Fig.2A thể hiện sơ đồ khối sơ lược minh họa thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng.

Fig.2B thể hiện lưu đồ minh họa phương pháp được thực hiện trong thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng.

Fig.3A thể hiện sơ đồ sơ lược minh họa chuỗi luồng ứng dụng vô hại.

Fig.3B thể hiện sơ đồ sơ lược minh họa trình tự luồng ứng dụng tiết chế.

Mô tả chi tiết sáng chế

Các phương án khác nhau có thể liên quan đến thiết bị và phương pháp luận để phát hiện và ngăn chặn sự tấn công tiết chế, ví dụ, trên mạng ngăn chặn gian lận di động được phân tán.

Các phương án khác nhau có thể liên quan đến việc kiểm tra gian lận trong hệ thống di động. Có thể có các hệ thống phát hiện gian lận mà có thể yêu cầu thành phần trên thiết bị di động (hoặc thiết bị truyền thông) mà đóng vai trò như là "chương trình đại lý (agent)" để thu thập dữ liệu và gửi dữ liệu được thu thập một cách an toàn đến hệ thống xử lý được tập trung hoặc được phân tán. Dữ liệu mà có thể được thu thập có thể gồm, nhưng không bị giới hạn ở, các kiểm tra tổng ứng dụng để phát hiện nếu ứng dụng (App) được sử dụng để truyền thông với máy chủ được sửa đổi hoặc đã được sửa đổi,

thông tin cảm biến để kiểm tra nếu thiết bị bị chiếm quyền truy cập gốc (root)/bị bẻ khóa (jailbrake), và DeviceID được tạo ra. Chương trình đại lý có thể an toàn hơn so với ứng dụng, để ít bị sửa đổi hơn. Chương trình đại lý có thể là, ví dụ, đoạn mã C++ với các biện pháp bảo vệ tại chỗ để bảo vệ chính nó.

Trong các phương án khác nhau, hệ thống di động có thể xác thực người dùng trên hệ thống, việc truy cập vào hệ thống được cấp phép và hệ thống có thể ghi lại sự có mặt của người dùng trong bộ lưu trữ dữ liệu. Để đạt được mục đích kiểm tra gian lận, tách biệt với quy trình đăng nhập/xác thực, thì hệ thống phát hiện gian lận khởi tạo sự bắt tay với người dùng, gửi lời mời bắt tay thực sự là gì. Hệ thống phát hiện gian lận giám sát việc nhận hồi đáp bắt tay mà, trong sự sắp xếp được ưu tiên, gồm một số dữ liệu từ chương trình đại lý trên thiết bị của người dùng. Người dùng vô hại sẽ gửi hồi đáp bắt tay trở lại, và việc nhận hồi đáp được phát hiện. Trong sự sắp xếp được ưu tiên, hồi đáp - hoặc ít nhất sự việc hồi đáp đã được nhận - được ghi lại trong bộ lưu trữ dữ liệu. Những người dùng ác ý thường tìm cách trốn tránh gửi việc hồi đáp. Nếu hồi đáp bắt tay không được phát hiện trong khung thời gian cụ thể, thì người dùng được nhận dạng là người có tiềm năng là ác ý và hệ thống truy cập cho người dùng bị thu hồi.

Một cách hiệu quả, việc khởi tạo bắt tay có thể phục vụ để thu hút hồi đáp cụ thể hoặc được định rõ mà hệ thống có thể đang mong đợi, cùng với, tốt hơn là, thông tin hoặc một số dữ liệu từ "chương trình đại lý" trên thiết bị. Tất cả các khách hành (hoặc người dùng) bình thường hoặc không ác ý được mong đợi là sẽ phản hồi dữ liệu từ thiết bị (ví dụ, kiểm tra tổng để kiểm tra nếu ứng dụng không được sửa đổi, dữ liệu để kiểm tra nếu thiết bị bị chiếm quyền truy cập gốc/bị bẻ khóa, v.v.). Khi những người ác ý cố gắng để tránh gửi hồi đáp bắt tay, nên hệ thống có thể phát hiện một cách hiệu quả việc

người này không sẵn lòng gửi "phần tải" (ví dụ, dữ liệu từ chương trình đại lý) đến hệ thống.

Lúc xác định được hoặc phát hiện được rằng có sự tấn công tiết chế, thì truyền thông từ người xấu (qua thiết bị truyền thông người dùng) có thể bị chấm dứt, hoặc tất cả các phiên từ người xấu (ví dụ, được khởi tạo với một hoặc nhiều (vi) dịch vụ) có thể bị chấm dứt hoặc bị bỏ đi. Một cách hiệu quả, người xấu có thể bị trục xuất khỏi hệ thống.

Các kỹ thuật hiện tại có thể triển khai quy trình bắt tay hạn chế thời gian giữa các hệ thống khác nhau để phát hiện sự tấn công tiết chế (vốn sẽ được mô tả chi tiết hơn dưới đây). Lúc sự tấn công tiết chế được phát hiện, thì các hệ thống có thể trục xuất những người ác ý (hoặc những người dùng) này bằng cách chấm dứt các phiên hoạt động mà nhưng người dùng nắm giữ với các vi dịch vụ bất kỳ. Các kỹ thuật hiện tại có thể cung cấp một hoặc nhiều ưu điểm sau đây:

(i) Giải quyết vấn đề đã bị bỏ qua, ví dụ, trong không gian ngăn chặn gian lận di động;

(ii) Thiết kế linh hoạt có thể cho phép tinh chỉnh các thông số khác nhau để cho phép việc sửa khẳng định giả (ví dụ, do các kết nối mạng chậm, v.v.);

(iii) Tỷ lệ phát hiện gần 100% cho vấn đề cụ thể đang được giải quyết. Điều này đề cập đến một tình huống trong đó các kỹ thuật hoặc hệ thống có thể trả về một khẳng định giả, trái ngược với việc bỏ sót một người xấu hoặc không bắt được một người dùng ác ý.

Đối với việc thiết kế linh hoạt, thì điều này có thể gồm việc điều chỉnh thông số thời gian và/hoặc tính linh hoạt để thực hiện kiểm tra gian lận ở giai đoạn bất kỳ. Ví dụ,

khoảng thời gian được định rõ trước khi việc kiểm tra sự tấn công tiết chế có thể dẫn đến sự chậm trễ tiềm năng trong thời gian xử lý và di chuyển dữ liệu. Hơn nữa, có thể kiểm tra việc liệu người/người dùng có đang làm việc trên dịch vụ (các dịch vụ) khác bất kỳ hay không nhưng không gửi phần tải bảo mật được yêu cầu trong quy trình bắt tay, mà sau đó chỉ báo rõ ràng về sự tấn công và hành động sẽ được thực hiện để chống lại người dùng.

Thứ nhất, tham khảo đến Fig.1, hệ thống truyền thông 100 được minh họa, vốn có thể áp dụng được trong các phương án khác nhau. Hệ thống truyền thông 100 gồm thiết bị máy chủ truyền thông 102, thiết bị truyền thông người dùng (hoặc máy khách) thứ nhất 104 và thiết bị truyền thông người dùng (hoặc máy khách) thứ hai 106. Các thiết bị 102, 104, 106 này được kết nối trong hoặc với mạng truyền thông 108 (ví dụ, Internet) thông qua các đường liên kết truyền thông tương ứng 110, 112, 114 triển khai, ví dụ, các giao thức truyền thông Internet. Các thiết bị truyền thông 104, 106 có thể có khả năng truyền thông thông qua các mạng truyền thông khác, như là các mạng điện thoại chuyển đổi công cộng (Public Switched Telephone Networks, PSTN), gồm các mạng truyền thông dạng ô di động, nhưng chúng được lược bỏ khỏi Fig.1 để cho rõ ràng. Cần thấy rõ rằng có thể có một hoặc nhiều thiết bị truyền thông khách tương tự với các thiết bị 104, 106.

Thiết bị máy chủ truyền thông 102 có thể là để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng (ví dụ, 104 và/hoặc 106).

Thiết bị máy chủ truyền thông 102 có thể là một máy chủ như được minh họa một cách sơ lược trên Fig.1, hoặc có chức năng được thực hiện bởi thiết bị máy chủ truyền thông 102 được phân tán qua nhiều thành phần máy chủ. Trong ví dụ trên Fig.1, thiết bị máy chủ truyền thông 102 có thể gồm một số thành phần riêng lẻ gồm, nhưng không bị

giới hạn ở, một hoặc nhiều bộ vi xử lý (μP) 116, bộ nhớ 118 (ví dụ, bộ nhớ khả biến như là bộ nhớ truy cập ngẫu nhiên (Random Access Memory, RAM)) để tải các lệnh có thể thực thi được 120, các lệnh có thể thực thi được 120 định rõ chức năng mà thiết bị máy chủ 102 thi hành dưới sự điều khiển của bộ xử lý 116. Thiết bị máy chủ truyền thông 102 cũng có thể gồm môđun đầu vào/đầu ra (Input/Output, I/O) 122 cho phép thiết bị máy chủ 102 truyền thông qua mạng truyền thông 108. Giao diện người dùng (User Interface, UI) 124 được cung cấp cho việc điều khiển của người dùng và có thể gồm, ví dụ, một hoặc nhiều thiết bị ngoại vi điện toán như là các màn hình hiển thị, các bàn phím máy tính và tương tự. Thiết bị máy chủ truyền thông 102 cũng có thể gồm cơ sở dữ liệu (Database, DB) 126, mục đích của chúng sẽ trở nên rõ ràng hơn nhờ phần thảo luận sau đây.

Thiết bị truyền thông người dùng 104 có thể gồm một số thành phần riêng lẻ gồm, nhưng không bị giới hạn ở, một hoặc nhiều bộ vi xử lý (μP) 128, bộ nhớ 130 (ví dụ, bộ nhớ khả biến như là RAM) để tải các lệnh có thể thực thi được 132, các lệnh có thể thực thi được 132 định rõ chức năng thiết bị truyền thông người dùng 104 thi hành dưới sự điều khiển của bộ xử lý 128. Thiết bị truyền thông người dùng 104 cũng gồm môđun đầu vào/đầu ra (I/O) 134 cho phép thiết bị truyền thông người dùng 104 truyền thông qua mạng truyền thông 108. Giao diện người dùng (UI) 136 được cung cấp cho việc điều khiển của người dùng. Nếu thiết bị truyền thông người dùng 104 là, chẳng hạn, điện thoại thông minh hoặc thiết bị dạng bảng, thì giao diện người dùng 136 có thể có bộ phận hiển thị dạng tấm chạm phổ biến như trong nhiều điện thoại thông minh và thiết bị cầm tay khác. Theo cách thay thế, nếu thiết bị truyền thông người dùng 104 là, chẳng hạn, máy tính để bàn hoặc máy tính xách tay, thì giao diện người dùng có thể có, ví dụ, một hoặc nhiều thiết bị ngoại vi điện toán như là các màn hình hiển thị, các bàn phím máy tính và tương tự.

Thiết bị truyền thông người dùng 106 có thể là, ví dụ, điện thoại thông minh hoặc thiết bị dạng bảng với cùng kiến trúc phần cứng hoặc kiến trúc phần cứng tương tự với kiến trúc phần cứng của thiết bị truyền thông người dùng 104.

Fig.2A thể hiện sơ đồ khối sơ lược minh họa thiết bị máy chủ truyền thông 202 để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng. Thiết bị máy chủ truyền thông 202 gồm bộ xử lý 216 và bộ nhớ 218, mà tại đó thiết bị máy chủ truyền thông 202 được tạo cấu hình, dưới sự điều khiển của bộ xử lý 216 để thực thi các lệnh trong bộ nhớ 218 để, truyền dữ liệu bắt tay 238 đến thiết bị truyền thông người dùng, giám sát, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay 238, để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay tương ứng với dữ liệu bắt tay 238 được nhận bởi thiết bị máy chủ truyền thông 202, và, hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông 202 xác định sự có mặt của sự kiện mà biểu thị việc thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông 202, xác định rằng có sự tấn công tiết chế, và tạo ra dữ liệu kết thúc 239 để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông 202. Bộ xử lý 216 và bộ nhớ 218 có thể được ghép nối với nhau (như được biểu diễn bởi đường 2179), ví dụ, được ghép nối theo kiểu vật lý và/hoặc được ghép nối theo kiểu điện. Bộ xử lý 216 có thể giống như được mô tả trong ngữ cảnh của bộ xử lý 116 (Fig.1) và/hoặc bộ nhớ 218 có thể giống như được mô tả trong ngữ cảnh của bộ nhớ 118 (Fig.1).

Nói cách khác, thiết bị máy chủ truyền thông 202 có thể được cung cấp. Thiết bị máy chủ truyền thông 202 có thể được tạo cấu hình để phát hiện sự tấn công tiết chế được liên kết với hoặc bắt nguồn từ thiết bị truyền thông người dùng (ví dụ, 104, 106,

Fig.1). Người dùng của thiết bị truyền thông người dùng có thể, ví dụ, cố gắng giành quyền truy cập vào một hoặc nhiều (vi) dịch vụ được liên kết với hoặc được cung cấp bởi thiết bị máy chủ truyền thông 202. Thiết bị máy chủ truyền thông 202 có thể truyền dữ liệu bắt tay 238 cần được nhận bởi thiết bị truyền thông người dùng (ví dụ, thiết bị máy chủ truyền thông 202 có thể truyền dữ liệu bắt tay 238 như là một phần của quy trình bắt tay, hoặc thiết bị máy chủ truyền thông 202 có thể khởi tạo quy trình bắt tay bằng cách truyền dữ liệu bắt tay 238). Sau đó, thiết bị máy chủ truyền thông 202 có thể giám sát, trong khoảng thời gian được định rõ (hoặc được xác định trước), hồi đáp bắt tay (ví dụ, vốn có thể là phần tải hoặc có thể gồm phần tải) từ thiết bị truyền thông người dùng để đáp lại dữ liệu bắt tay 238. Hồi đáp bắt tay có thể cụ thể cho dữ liệu bắt tay 238. Hồi đáp bắt tay có thể được truyền bởi thiết bị truyền thông người dùng đến thiết bị máy chủ truyền thông 202 như là một phần của quy trình bắt tay.

Trong các phương án khác nhau, dữ liệu bắt tay 238 có thể được truyền đến thiết bị truyền thông người dùng để đáp lại việc thiết bị máy chủ truyền thông 202 xác thực người dùng của thiết bị truyền thông người dùng, hoặc tại thời điểm bất kỳ sau quy trình xác thực.

Nếu khoảng thời gian được định rõ (hoặc quãng thời gian nhất định) đã đi qua hoặc trôi qua (tức là, bị hết hạn) mà thiết bị máy chủ truyền thông 202 đã không được nhận hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay 238, và, hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông 202 đã được xác định hoặc được phát hiện sự có mặt (hoặc sự tồn tại) của sự kiện (ví dụ, sự kiện truyền thông hoặc mạng) mà biểu thị rằng thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông 202, thì thiết bị máy chủ truyền thông 202 có thể xác định rằng sự tấn công tiết chế đã xảy ra, và, sau đấy, thiết bị máy chủ truyền thông 202

có thể tạo ra dữ liệu kết thúc 239 để chặn việc truy cập bởi thiết bị truyền thông người dùng vào dịch vụ (ví dụ, vi dịch vụ) được liên kết với thiết bị máy chủ truyền thông 202. Việc truy cập bởi thiết bị truyền thông người dùng vào một hoặc nhiều hoặc tất cả các (vi) dịch vụ được liên kết với thiết bị máy chủ truyền thông 202 có thể bị từ chối. Dữ liệu kết thúc 239 có thể gồm hoặc có thể biểu thị phán quyết hoặc thông báo trục xuất.

Chi tiết hơn, nếu không có hồi đáp thích hợp được nhận bởi thiết bị máy chủ truyền thông 202 từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay 238 trước khi hết hạn khoảng thời gian được định rõ, thì thiết bị máy chủ truyền thông 202 có thể xác định liệu có thể có sự kiện cung cấp chỉ báo rằng thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông 202 hay không, tức là, liệu thiết bị truyền thông người dùng có thể ở trong trạng thái truyền thông với thiết bị máy chủ truyền thông 202 hay không, hoặc ở trong trạng thái là có khả năng truyền thông với thiết bị máy chủ truyền thông 202 hay không. Nếu nó được xác định rằng có sự kiện như vậy, thì thiết bị máy chủ truyền thông 202 tiến hành từ chối truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông bằng cách tạo ra dữ liệu kết thúc 239 vì thiết bị máy chủ truyền thông 202 có thể nhận ra sự có mặt của sự kiện như vậy, được tổ hợp việc thiếu hồi đáp bắt tay tương ứng với dữ liệu bắt tay 238 từ thiết bị truyền thông người dùng, biểu thị của ý định ác ý từ phía người dùng hoặc của sự tấn công tiết chế, và, do đó, chặn truy cập.

Vì yếu tố thời gian liên quan đến hồi đáp bắt tay đối với dữ liệu bắt tay 238, do đó, quy trình bắt tay hạn chế thời gian được cung cấp.

Cần thấy rõ rằng việc xác định rằng có sự tấn công tiết chế có thể là bước chủ động của việc xác định rằng có sự tấn công như vậy, hoặc việc xác định là quy trình tiếp theo như là hệ quả hoặc kết luận được rút ra từ sự tổ hợp của việc không có hồi đáp bắt tay

tương ứng với dữ liệu bắt tay 238 trong khoảng thời gian được định rõ và sự có mặt của sự kiện.

Sự kiện mà biểu thị rằng thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông 202 có thể gồm, nhưng không bị giới hạn ở, ít nhất một việc trong số (i) truyền thông đang diễn ra giữa thiết bị truyền thông người dùng và thiết bị máy chủ truyền thông 202, ví dụ, liên quan đến một hoặc nhiều dịch vụ khác được liên kết với (hoặc được cung cấp bởi) thiết bị máy chủ truyền thông 202, (ii) thiết bị truyền thông người dùng còn cố gắng truy cập thêm vào thiết bị máy chủ truyền thông 102 hoặc dịch vụ được liên kết với nó, hoặc cố gắng truyền thông với thiết bị máy chủ truyền thông 202, (iii) thiết bị truyền thông người dùng thực hiện cuộc gọi đến cổng nối của thiết bị máy chủ truyền thông 202, (iv) thiết bị truyền thông người dùng kiểm tra các cuộc gọi mạng, hoặc (v) kết nối giao thức điều khiển truyền dẫn (Transmission Control Protocol, TCP) mở. Việc kiểm tra sự tồn tại của truyền thông/kết nối mở có thể ở trên thiết bị máy chủ; như đã biết rằng người dùng đã được hỏi để phản hồi thử thách (bắt tay), nhưng đã không phản hồi, và nếu cùng một mã thông báo (token) xác thực được gửi cho các lệnh gọi đến API, thì mã thông báo xác thực này có thể kích hoạt việc phát hiện trên máy chủ.

Theo các ví dụ không giới hạn, có thể không có hồi đáp nào tại tất cả từ thiết bị truyền thông người dùng (ví dụ, mà tại đó người dùng trốn tránh việc gửi hồi đáp), hoặc hồi đáp mà được gửi bởi người dùng để đáp lại dữ liệu bắt tay 238 không phải là hồi đáp thích hợp hoặc không phải là hồi đáp được mong đợi, ví dụ, mà tại đó hồi đáp có thể gồm dữ liệu từ thiết bị truyền thông người dùng chỉ ra ít nhất một việc trong số các việc sau đây: (i) chương trình đại lý (trên thiết bị truyền thông người dùng) để gửi hồi đáp bắt tay đã được sửa đổi hoặc bị xâm phạm, (ii) ứng dụng (App) mà được sử dụng để

truyền thông với thiết bị máy chủ truyền thông 202 đã được sửa đổi hoặc bị xâm phạm, hoặc (iii) thiết bị truyền thông người dùng (hoặc hệ thống vận hành của nó) đã được sửa đổi hoặc bị xâm phạm. "Chương trình đại lý" trên thiết bị truyền thông người dùng có thể đề cập đến tập hợp mã hoặc các lệnh nằm trên thiết bị truyền thông người dùng.

Trong ngữ cảnh của các phương án khác nhau, thiết bị máy chủ truyền thông 202 có thể thiết lập thời gian bắt đầu trong khoảng thời gian được định rõ và/hoặc lưu trữ dữ liệu biểu thị thời gian bắt đầu (ví dụ, trong một hoặc nhiều bộ lưu trữ dữ liệu). Thời gian bắt đầu có thể tương ứng với thời gian mà sự có mặt của người dùng của thiết bị truyền thông người dùng được nhận dạng.

Trong ngữ cảnh của các phương án khác nhau, dịch vụ hoặc vi dịch vụ được liên kết với thiết bị máy chủ truyền thông 202 có thể gồm việc đăng nhập, ghi nhật ký, (nhiều) lôgic nghiệp vụ, v.v.

Trong ngữ cảnh của các phương án khác nhau, việc truyền dữ liệu bắt tay 238 đến thiết bị truyền thông người dùng và giám sát hồi đáp có thể thông qua mạng quyết định gian lận (Fraud Decision Network, FDN) của thiết bị máy chủ truyền thông 202. Việc tạo ra dữ liệu kết thúc 239 có thể thông qua FDN.

Trong các phương án khác nhau, để xác định rằng có sự tấn công tiết chế, thì thiết bị máy chủ truyền thông 202 có thể được tạo cấu hình để xác định rằng có sự tấn công tiết chế để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay có dữ liệu xác minh (tương ứng với dữ liệu bắt tay 238) được nhận bởi thiết bị máy chủ truyền thông 202, và hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông 202 xác định sự có mặt của sự kiện. Dữ liệu xác minh có thể là từ chương trình đại lý trên thiết bị truyền thông người dùng. Dữ liệu xác minh có thể gồm dữ liệu biểu thị tình trạng hoặc điều kiện của thiết bị truyền thông người dùng và/hoặc tình trạng của ứng

dụng (App) được sử dụng bởi người dùng của thiết bị truyền thông người dùng để truyền thông với thiết bị máy chủ truyền thông 202, ví dụ, liệu ứng dụng đã được sửa đổi và/hoặc thiết bị truyền thông người dùng đã trải qua việc bị chiếm quyền truy cập gốc/bẻ khóa hay chưa. Các ví dụ về dữ liệu như vậy có thể gồm kiểm tra tổng để kiểm tra liệu ứng dụng có được sửa đổi hay không, dữ liệu về việc liệu thiết bị có bị chiếm quyền truy cập gốc/bị bẻ khóa hay không, v.v..

Trong các phương án khác nhau, dữ liệu bắt tay 238 có thể gồm số nonce. Thuật ngữ "số nonce" có thể đề cập đến mã, ký tự, số hoặc giá trị mà có thể được sử dụng (chỉ) một lần cho mục đích xác thực. Số nonce có thể được sử dụng trong truyền thông mật mã, và có thể được mật mã hóa bởi khóa cá nhân được định rõ hoặc cụ thể mà chỉ được thiết bị máy chủ truyền thông 202 biết đến (ví dụ, chỉ được FDN biết đến rằng tạo thành một phần của thiết bị máy chủ 202). Thông tin tương ứng với số nonce có thể được lưu trữ trong thiết bị máy chủ truyền thông 202 (ví dụ, trong FDN). Số nonce có thể được gửi đến chương trình đại lý trên thiết bị truyền thông người dùng. Việc sử dụng số nonce có thể tránh sự tấn công phát lại để truyền thông hoặc hồi đáp cũ không thể được sử dụng lại.

Với dữ liệu bắt tay 238 có số nonce, thì dữ liệu xác minh (để được truyền với hồi đáp bắt tay) có thể gồm số nonce được ký hoặc hồi đáp tương ứng với số nonce được truyền bởi thiết bị máy chủ truyền thông 202.

Trong ngữ cảnh của các phương án khác nhau, khoảng thời gian được định rõ có thể nằm giữa khoảng 2 phút và khoảng 10 phút, ví dụ, giữa khoảng 2 phút và khoảng 8 phút, giữa khoảng 2 phút và khoảng 6 phút, giữa khoảng 2 phút và khoảng 5 phút, giữa khoảng 5 phút và khoảng 10 phút, giữa khoảng 5 phút và khoảng 8 phút, hoặc giữa

khoảng 3 phút và khoảng 6 phút, ví dụ, khoảng 2 phút, khoảng 3 phút, khoảng 5 phút (tốt hơn là), khoảng 6 phút, khoảng 8 phút hoặc khoảng 10 phút.

Trong các phương án khác nhau, trước khi truyền dữ liệu bắt tay 238 đến thiết bị truyền thông người dùng, thì thiết bị máy chủ truyền thông 202 có thể còn được tạo cấu hình để phát hành mã thông báo phiên đến thiết bị truyền thông người dùng. Mã thông báo phiên có thể phục vụ việc nhận dạng hoặc chứng minh việc xác thực của người dùng. Mã thông báo phiên có thể được phát hành để đáp lại việc thiết bị máy chủ truyền thông 202 xác thực người dùng của thiết bị truyền thông người dùng.

Trong ngữ cảnh của các phương án khác nhau, để xác thực người dùng của thiết bị truyền thông người dùng, thì thiết bị máy chủ truyền thông 202 có thể được tạo cấu hình để, để đáp lại việc nhận dữ liệu người dùng (từ thiết bị truyền thông người dùng) có một hoặc nhiều trường dữ liệu biểu thị sự nhận dạng của người dùng, xác thực người dùng dựa trên dữ liệu người dùng. Dữ liệu người dùng có thể gồm ID người dùng và mật khẩu được liên kết với người dùng.

Mã thông báo phiên có thể hợp lệ cho tất cả các (vi) dịch vụ được liên kết với thiết bị máy chủ truyền thông 202.

Mã thông báo phiên có thể được phát hành bởi môđun cung cấp nhận dạng (Identity Provider, IDP) của thiết bị máy chủ truyền thông 202.

Trong ngữ cảnh của các phương án khác nhau, IDP và FDN là các tập hợp hoặc các đoạn mã đang chạy trên thiết bị máy chủ truyền thông 202. IDP và FDN có thể khác nhau hoặc tách biệt với nhau, hoặc có thể ở trong một môđun.

Trong các phương án khác nhau, để đáp lại dữ liệu kết thúc 239 được tạo ra, thì thiết bị máy chủ truyền thông 202 có thể còn được tạo cấu hình để làm mất hiệu lực

(hoặc thu hồi) mã thông báo phiên. Nói cách khác, thiết bị máy chủ truyền thông 202 có thể gây ra sự hết hạn của mã thông báo phiên để chặn truy cập bởi thiết bị truyền thông người dùng vào dịch vụ được liên kết với thiết bị máy chủ truyền thông 202. Mã thông báo phiên có thể bị làm mất hiệu lực bởi môđun IDP để đáp lại phán quyết hoặc thông báo trục xuất được phát hành bởi FDN.

Trước khi truyền dữ liệu bắt tay 238 đến thiết bị truyền thông người dùng, và để đáp lại việc thiết bị máy chủ truyền thông 202 xác thực người dùng của thiết bị truyền thông người dùng, thì thiết bị máy chủ truyền thông 202 có thể còn được tạo cấu hình để tạo ra dữ liệu để nhận dạng sự có mặt của người dùng, và lưu trữ dữ liệu trong một hoặc nhiều bộ lưu trữ dữ liệu (ví dụ, bộ lưu trữ dữ liệu có thể là bảng băm được phân tán) trong thiết bị máy chủ truyền thông 202. Theo ví dụ không giới hạn, dữ liệu có thể gồm "khóa" được định rõ và giá trị được định rõ (ví dụ, giá trị rỗng) được liên kết với khóa. Một hoặc nhiều bộ lưu trữ dữ liệu hoặc bảng (các bảng) băm được phân tán có thể là một phần của FDN.

Dữ liệu có thể gồm dữ liệu thời gian biểu thị thời gian nhận dạng sự có mặt của người dùng.

Trong các phương án khác nhau, để đáp lại hồi đáp bắt tay (tương ứng với dữ liệu bắt tay 238) được nhận bởi thiết bị máy chủ truyền thông 202 trong khoảng thời gian được định rõ, thì thiết bị máy chủ truyền thông 202 có thể còn được tạo cấu hình để tạo ra dữ liệu truy cập để cho phép thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông 202. Hồi đáp có thể gồm dữ liệu xác minh. Dữ liệu xác minh có thể gồm số nonce được ký hoặc hồi đáp tương ứng với số nonce được truyền bởi thiết bị máy chủ truyền thông 202 như là một phần của dữ liệu bắt tay 238.

Thiết bị máy chủ truyền thông 202 có thể còn được tạo cấu hình để tạo ra dữ liệu thứ hai biểu thị việc nhận hồi đáp bắt tay bởi thiết bị máy chủ truyền thông 202, và cập nhật dữ liệu được lưu trữ trong một hoặc nhiều bộ lưu trữ dữ liệu với dữ liệu thứ hai. Theo ví dụ không giới hạn, dữ liệu thứ hai có thể gồm giá trị thứ hai được định rõ (ví dụ, giá trị không rỗng) để được liên kết với "khóa" được định rõ.

Theo ví dụ không giới hạn, hồi đáp bắt tay có thể được nhận tại thời điểm bất kỳ trong khoảng thời gian được định rõ. Nếu hồi đáp bắt tay được nhận trong khoảng thời gian được định rõ, thì người dùng có thể, ví dụ, bị loại bỏ khỏi bảng dò tìm. Vào cuối khoảng thời gian được định rõ, thì người dùng bất kỳ mà đã không gửi hồi đáp bắt tay có thể bị coi là có khả năng ác ý và sau khi kiểm tra thêm, thì người dùng có thể bị xử lý, ví dụ, bị loại bỏ hoặc bị trục xuất.

Trong ngữ cảnh của các phương án khác nhau, thiết bị máy chủ truyền thông 202 có thể là máy chủ đơn lẻ, hoặc có chức năng được thực hiện bởi thiết bị máy chủ truyền thông 202 được phân tán ngang qua các thành phần máy chủ.

Trong ngữ cảnh của các phương án khác nhau, "app" hoặc "ứng dụng" có thể được cài đặt trong thiết bị truyền thông (người dùng) và có thể gồm các lệnh có thể thực thi được bởi bộ xử lý để thực thi trên thiết bị. Theo ví dụ không giới hạn, người dùng của thiết bị truyền thông người dùng có thể cố gắng truyền thông với thiết bị máy chủ truyền thông 202 hoặc truy cập vào dịch vụ được liên kết với (hoặc được cung cấp bởi) thiết bị máy chủ truyền thông 202 qua ứng dụng.

Fig.2B thể hiện lưu đồ 240 minh họa phương pháp, được thực hiện trong thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng.

Tại 242, dữ liệu bắt tay được truyền đến thiết bị truyền thông người dùng.

Tại 244, việc giám sát được thi hành, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay.

Để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay tương ứng với dữ liệu bắt tay được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại xác định sự có mặt của sự kiện mà biểu thị việc thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông,thì tại 246, xác định được rằng có sự tấn công tiết chế, và tại 248, dữ liệu kết thúc được tạo ra để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

Tại 246, có thể xác định được rằng có sự tấn công tiết chế để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay có dữ liệu xác minh được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại xác định sự có mặt của sự kiện.

Tại 242, dữ liệu bắt tay gồm số nonce có thể được truyền đến thiết bị truyền thông người dùng.

Trong các phương án khác nhau, khoảng thời gian được định rõ có thể nằm giữa khoảng 2 phút và khoảng 10 phút, ví dụ, giữa khoảng 2 phút và khoảng 8 phút, giữa khoảng 2 phút và khoảng 6 phút, giữa khoảng 2 phút và khoảng 5 phút, giữa khoảng 5 phút và khoảng 10 phút, giữa khoảng 5 phút và khoảng 8 phút, hoặc giữa khoảng 3 phút và khoảng 6 phút, ví dụ, khoảng 2 phút, khoảng 3 phút, khoảng 5 phút (tốt hơn là), khoảng 6 phút, khoảng 8 phút hoặc khoảng 10 phút.

Trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng tại 242, thì phương pháp có thể còn gồm việc phát hành mã thông báo phiên đến thiết bị truyền thông người dùng.

Để đáp lại dữ liệu kết thúc được tạo ra, thì phương pháp có thể còn gồm việc làm mất hiệu lực mã thông báo phiên.

Trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng tại 242, và để đáp lại việc xác thực người dùng của thiết bị truyền thông người dùng, thì phương pháp có thể còn gồm việc tạo ra dữ liệu để nhận dạng sự có mặt của người dùng, và lưu trữ dữ liệu trong một hoặc nhiều bộ lưu trữ dữ liệu trong thiết bị máy chủ truyền thông.

Dữ liệu có thể gồm dữ liệu thời gian biểu thị thời gian nhận dạng sự có mặt của người dùng.

Để đáp lại hồi đáp bắt tay được nhận bởi thiết bị máy chủ truyền thông trong khoảng thời gian được định rõ, thì dữ liệu truy cập có thể được tạo ra để cho phép thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

Dữ liệu thứ hai biểu thị việc nhận hồi đáp bắt tay bởi thiết bị máy chủ truyền thông có thể được tạo ra, và dữ liệu được lưu trữ trong một hoặc nhiều bộ lưu trữ dữ liệu có thể được cập nhật với dữ liệu thứ hai.

Cần thấy rõ rằng các phần mô tả trong ngữ cảnh của thiết bị máy chủ 202 có thể áp dụng được một cách tương ứng liên quan đến các phương pháp như được mô tả trong ngữ cảnh của lưu đồ 240.

Cần thấy rõ rằng các sự mô tả trong ngữ cảnh của thiết bị máy chủ truyền thông 102 có thể áp dụng được một cách tương ứng liên quan đến thiết bị máy chủ truyền thông 202.

Trong ngữ cảnh của các phương án khác nhau, thiết bị truyền thông người dùng có thể gồm, nhưng không bị giới hạn bởi, điện thoại thông minh, máy tính bảng, thiết bị

truyền thông cầm tay/khả chuyển, máy tính để bàn hoặc máy tính xách tay, máy tính đầu cuối, v.v.

Sáng chế cũng đề xuất sản phẩm chương trình máy tính có các lệnh để triển khai phương pháp để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng như được mô tả ở đây.

Sáng chế cũng đề xuất chương trình máy tính có các lệnh để triển khai phương pháp để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng như được mô tả ở đây.

Sáng chế cũng đề xuất phương tiện lưu trữ không chuyển tiếp lưu trữ các lệnh, mà, khi được thực thi bởi bộ xử lý, thì làm cho bộ xử lý thực hiện phương pháp để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng như được mô tả ở đây.

Bây giờ các phương án hoặc các kỹ thuật khác nhau sẽ được mô tả chi tiết hơn nữa.

Các kỹ thuật được bộc lộ ở đây có thể liên quan đến việc triển khai quy trình bắt tay hạn chế thời gian giữa các hệ thống hoặc các môđun sau đây: nhà cung cấp nhận dạng (IDP), mạng quyết định gian lận (FDN), và chương trình đại lý trên thiết bị người dùng.

IDP có thể chịu trách nhiệm đăng nhập (Login) để IDP có thể đóng vai trò như cổng nối.

Fig.3A thể hiện sơ đồ sơ lược 350a minh họa chuỗi luồng ứng dụng vô hại, trong khi Fig.3B thể hiện sơ đồ sơ lược 350b minh họa trình tự luồng ứng dụng tiết chế.

Thứ nhất, tham khảo đến Fig.3A, quy trình bắt đầu với việc thiết bị truyền thông người dùng 352a kết nối với IDP 354 để phát hành mã thông báo phiên (1, tương ứng

với mũi tên định hướng của cùng một số (trong vòng tròn) trên Fig.3A). IDP 354 có thể xác thực người dùng và nhận dạng người dùng (việc xác thực hợp lệ dẫn đến sự nhận dạng của người dùng), và sau đó có thể phát hành mã thông báo phiên (2) và có thể ghi lại (3) sự có mặt của người hoặc người dùng này trên mạng vào bảng băm được phân tán 356. Bảng băm 356 hiện tại có thể ghi lại khóa, nhưng có thể gán giá trị rỗng cho cặp khóa-giá trị, chỉ ra rằng người có mặt trên mạng đang chờ xác minh. Dấu thời gian của sự kiện này có thể được ghi lại và được theo dõi để kiểm tra hạn chế.

Mã thông báo phiên hoặc cookie phiên IDP có thể là loại bất kỳ để xác thực nhận dạng, gồm trong dạng mã thông báo Web JSON (JSON Web Token, JWT). Mã thông báo có thể được yêu cầu để chứng minh việc xác thực và có thể được đòi hỏi trong tất cả sự vấn tin đối với nền phụ (background).

IDP mã thông báo phiên có thể hợp lệ cho tất cả các (vi) dịch vụ trong chương trình phụ trợ (backend).

Mạng quyết định gian lận (FDN) 358 có thể nhận thấy sự có mặt của người (4) và bây giờ có thể phát hành số nonce mật mã (5) được mật mã hóa bởi khóa cá nhân cụ thể mà chỉ được FDN 358 biết đến. Số nonce được gửi đến chương trình đại lý cụ thể trên thiết bị 352a dưới dạng hồi đáp. Trong các phương án khác nhau, khi người dùng/người đăng nhập, thì IDP 354 có thể thông báo cho FDN 358 về sự có mặt của người này. FDN 358 có thể lưu trữ thông tin liên quan đến người dùng, và thông tin số nonce.

Nếu người này vô hại, thì chương trình đại lý gửi số nonce được ký này trở lại máy chủ (tức là, FDN 358) cùng với phần tải hồi đáp (6). Hồi đáp này được ghi lại trong bảng băm được phân tán 356 dựa vào sự nhận dạng của người dùng như là giá trị cho khóa tương ứng (7). Sự cần thiết của số nonce là để tránh sự tấn công phát lại mà tại đó

người gian lận có thể sao chép phần tải hồi đáp trước đó và gửi nó đến FDN 358. Sau đó, quy trình tiếp tục cho phép thiết bị 352a truy cập dịch vụ mong muốn.

Số nonce có thể là mã xác thực thông điệp hoặc gồm mã xác thực thông điệp mà được gửi từ FDN 358 thiết bị khách 352a. Đối với số nonce được ký, thì cùng một thông điệp được mong đợi là sẽ được máy khách 352a trả lại cho FDN 358 như là một phần của phần tải từ máy khách 352a. Điều này là để đảm bảo rằng phần tải được tạo ra tại một thời điểm cụ thể và không bị "phát lại" (ví dụ, sử dụng hồi đáp hoặc phần tải trước đó).

Cùng một thông điệp được mong đợi là sẽ được máy khách 352a trả lại cho FDN 358 như là một phần của phần tải.

Cần thấy rõ rằng, dù bảng băm được phân tán 356 được thể hiện là tách biệt với FDN 358, nhưng bảng băm được phân tán 356 có thể là một phần của FDN 358.

Cần thấy rõ rằng một hoặc nhiều bảng băm được phân tán (ví dụ, mỗi bảng băm được phân tán tương tự với bảng băm được phân tán 356) có thể được cung cấp để lưu trữ dữ liệu.

IDP 354 và FDN 358 nằm trên thiết bị máy chủ truyền thông, ví dụ, trên cùng máy chủ. IDP 354 và FDN 358 là các đoạn mã đang chạy trên thiết bị máy chủ truyền thông. IDP 354 và FDN 358 có thể là các môđun khác nhau hoặc chúng có thể ở trong một môđun.

Bây giờ, đề cập đến Fig.3B, (1) đến (5) là giống với (1) đến (5) trên Fig.3A và do đó phần mô tả của chúng bị lược bỏ. Nếu chương trình đại lý trên thiết bị truyền thông người dùng 352b đã được thay đổi (ví dụ, được sửa đổi để dừng gửi hồi đáp hoặc phần tải), hoặc nếu người/người dùng cố gắng trốn tránh việc gửi phần tải, mà tại đó không

có hồi đáp từ ứng dụng tiết chế (6), thì FDN 358 chờ cho đến khi bộ định thời 359 hết hạn (7). Sự hết hạn của bộ định thời 359 có nghĩa là khoảng thời gian nhất định đã đi qua hoặc trôi qua mà không có phần tải nào được nhận. Theo ví dụ không giới hạn, có thể có khoảng thời gian 5 phút để bộ định thời 359 hết hạn. FDN 358 có thể lưu trữ thời gian khi IDP 354 thông báo về sự có mặt của người làm tham chiếu hoặc cơ sở cho bộ định thời 359.

Tất cả các khách hành (hoặc người dùng) bình thường hoặc không ác ý được mong đợi để phản hồi dữ liệu từ thiết bị. Chỉ những người ác ý sẽ không gửi hồi đáp (hoặc phần tải), và sự lược bỏ hành động gửi hồi đáp sẽ được phát hiện trên FDN 358.

Sau khi bộ định thời 359 hết hạn, thì sau đó FDN 358 có thể kiểm tra sự có mặt của một hoặc nhiều sự kiện mạng từ người/người dùng, vốn có thể ở trong dạng kiểm tra các cuộc gọi mạng hoặc các kết nối TCP mở. Một sự kiện mạng khác có thể là nơi mà tại đó FDN 358 xác định rằng vẫn có các kết nối hoạt động với các dịch vụ trong mạng lưới các vi dịch vụ. Điều này có thể được thực hiện, ví dụ, bằng cách dò tìm cổng nối giao diện lập trình ứng dụng (Application Programming Interface Gateway, API G/W), vốn có thể đóng vai trò là cổng nối cho tất cả các vi dịch vụ trong hệ sinh thái. Trong các phương án khác nhau, API G/W có thể là thành phần phần mềm mà đóng vai trò như là cổng nối cho tất cả các cuộc gọi API. Sự tồn tại của cuộc gọi đến G/W có thể là chỉ báo của ý định ác ý sau một thời lượng nhất định.

Nếu các sự kiện mạng hoạt động được phát hiện và đã không có phần tải hồi đáp từ người này, vốn được chỉ ra bởi giá trị rỗng cho khóa trên bảng băm được phân tán 356 (8), thì FDN 358 phát hành phán quyết trục xuất cho người cụ thể này (9). Sau đó, IDP 354 có thể hành động theo phán quyết trục xuất và loại bỏ người này khỏi mạng bằng cách làm mất hiệu lực phiên hiện tại (vốn hợp lệ cho tất cả các (vi) dịch vụ trong chương

trình phụ trợ) bằng cách thu hồi (hoặc làm hết hạn) mã thông báo phiên (10). Theo ví dụ không giới hạn, mã thông báo phiên có tính hợp lệ phiên và điều này có thể mỗi khi thiết bị người dùng 352b thực hiện cuộc gọi. Nếu mã thông báo phiên bị làm mất hiệu lực trên máy chủ, vào lần tiếp theo khi người dùng thực hiện cuộc gọi, qua thiết bị người dùng 352b, thì sẽ xác định được rằng mã thông báo phiên không còn hợp lệ, và vì vậy phiên bị chấm dứt.

Một cách hiệu quả, sự tấn công tiết chế có thể được phát hiện nếu người dùng hoặc người này không gửi phần tải được yêu cầu, nhưng vẫn có mặt hoặc khả dụng trong hệ thống.

Trong các phương án khác nhau, tổng số lần đăng nhập và số lượng phần tải được nhận có thể được theo dõi. Các số này, lý tưởng là bằng nhau, nhưng có thể bị mất do các vấn đề về mạng. Tuy nhiên, nếu số lượng phần tải được nhận là quá nhỏ so với số lần đăng nhập, thì hành động đăng xuất người/người dùng có thể được thực hiện.

Như được mô tả ở trên, các kỹ thuật được bộc lộ ở đây có thể đề xuất phương pháp luận để giải quyết sự tấn công tiết chế, ví dụ, trên mạng ngăn chặn gian lận di động.

Cần thấy rõ rằng sáng chế đã được mô tả chỉ theo cách làm ví dụ. Các sửa đổi khác nhau có thể được thực hiện đối với các kỹ thuật được mô tả ở đây mà không vượt ra khỏi mục đích và phạm vi của các yêu cầu bảo hộ kèm theo. Các kỹ thuật được bộc lộ bao gồm các kỹ thuật vốn có thể được cung cấp theo cách thức độc lập, hoặc tổ hợp với nhau. Do đó, các dấu hiệu được mô tả đối với một kỹ thuật cũng có thể được trình bày trong tổ hợp với một kỹ thuật khác.

YÊU CẦU BẢO HỘ

1. Thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng, thiết bị máy chủ truyền thông bao gồm bộ xử lý và bộ nhớ, thiết bị máy chủ truyền thông được tạo cấu hình, dưới sự điều khiển của bộ xử lý, để thực thi các lệnh trong bộ nhớ để:

truyền dữ liệu bắt tay bao gồm số nonce đến thiết bị truyền thông người dùng;

giám sát, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay; và

để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay tương ứng với dữ liệu bắt tay được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông xác định sự có mặt của sự kiện mà biểu thị việc thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông,

xác định rằng có sự tấn công tiết chế; và

tạo ra dữ liệu kết thúc để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

2. Thiết bị máy chủ truyền thông theo điểm 1,

trong đó, để xác định rằng có sự tấn công tiết chế, thì thiết bị máy chủ truyền thông được tạo cấu hình để xác định rằng có sự tấn công tiết chế để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay bao gồm dữ liệu xác minh được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại việc thiết bị máy chủ truyền thông xác định sự có mặt của sự kiện.

3. Thiết bị máy chủ truyền thông theo điểm 1 hoặc 2, trong đó, khoảng thời gian được định rõ là nằm giữakhoảng2 phút và khoảng 10 phút.

4. Thiết bị máy chủ truyền thông theo một điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó, trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng, thì thiết bị máy chủ truyền thông còn được tạo cấu hình để phát hành mã thông báo (token) phiên đến thiết bị truyền thông người dùng.

5. Thiết bị máy chủ truyền thông theo điểm 4,

trong đó, để đáp lại dữ liệu kết thúc được tạo ra, thì thiết bị máy chủ truyền thông còn được tạo cấu hình để làm mất hiệu lực mã thông báo phiên.

6. Thiết bị máy chủ truyền thông theo một điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó, trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng, và để đáp lại việc thiết bị máy chủ truyền thông xác thực người dùng của thiết bị truyền thông người dùng, thì thiết bị máy chủ truyền thông còn được tạo cấu hình để:

tạo ra dữ liệu để nhận dạng sự có mặt của người dùng; và

lưu trữ dữ liệu trong một hoặc nhiều bộ lưu trữ dữ liệu trong thiết bị máy chủ truyền thông.

7. Thiết bị máy chủ truyền thông theo điểm 6, trong đó, dữ liệu bao gồm dữ liệu thời gian biểu thị thời gian nhận dạng sự có mặt của người dùng.

8. Thiết bị máy chủ truyền thông theo một điểm bất kỳ trong số các điểm từ 1 đến 7,

trong đó, để đáp lại hồi đáp bắt tay được nhận bởi thiết bị máy chủ truyền thông trong khoảng thời gian được định rõ, thì thiết bị máy chủ truyền thông còn được tạo cấu hình để tạo ra dữ liệu truy cập để cho phép thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

9. Thiết bị máy chủ truyền thông theo điểm 8, khi phụ thuộc vào điểm 6, còn được tạo cấu hình để:

tạo ra dữ liệu thứ hai biểu thị việc nhận hồi đáp bắt tay bởi thiết bị máy chủ truyền thông; và

cập nhật dữ liệu được lưu trữ trong một hoặc nhiều bộ lưu trữ dữ liệu với dữ liệu thứ hai.

10. Phương pháp, được thực hiện trong thiết bị máy chủ truyền thông để xác định sự tấn công tiết chế được liên kết với thiết bị truyền thông người dùng, thì phương pháp bao gồm các bước, dưới sự điều khiển của bộ xử lý của thiết bị máy chủ truyền thông:

truyền dữ liệu bắt tay bao gồm số nonce đến thiết bị truyền thông người dùng;

giám sát, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay; và

để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không có hồi đáp bắt tay tương ứng với dữ liệu bắt tay được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại xác định sự có mặt của sự kiện mà biểu thị việc thiết bị truyền thông người dùng ở trong chế độ truyền thông với thiết bị máy chủ truyền thông,

xác định rằng có sự tấn công tiết chế; và

tạo ra dữ liệu kết thúc để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

11. Phương pháp theo điểm 10,

trong đó, bước xác định rằng có sự tấn công tiết chế bao gồm việc xác định rằng có sự tấn công tiết chế để đáp lại sự hết hạn của khoảng thời gian được định rõ mà không

có hồi đáp bắt tay bao gồm dữ liệu xác minh được nhận bởi thiết bị máy chủ truyền thông, và, hơn nữa, để đáp lại xác định sự có mặt của sự kiện.

12. Phương pháp theo điểm 10 hoặc 11, trong đó, khoảng thời gian được định rõ là nằm giữa khoảng 2 phút và khoảng 10 phút.

13. Phương pháp theo điểm bất kì trong số các điểm từ 10 đến 12,

trong đó, trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng, thì phương pháp còn bao gồm bước phát hành mã thông báo phiên đến thiết bị truyền thông người dùng.

14. Phương pháp theo điểm 13,

trong đó, để đáp lại dữ liệu kết thúc được tạo ra, thì phương pháp còn bao gồm bước làm mất hiệu lực mã thông báo phiên.

15. Phương pháp theo một điểm bất kỳ trong số các điểm từ 10 đến 14, trong đó, trước khi truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng, và để đáp lại việc xác thực người dùng của thiết bị truyền thông người dùng, thì phương pháp còn bao gồm các bước:

tạo ra dữ liệu để nhận dạng sự có mặt của người dùng; và

lưu trữ dữ liệu trong một hoặc nhiều bộ lưu trữ dữ liệu trong thiết bị máy chủ truyền thông.

16. Phương pháp theo điểm 15, trong đó, dữ liệu bao gồm dữ liệu thời gian biểu thị thời gian nhận dạng sự có mặt của người dùng.

17. Phương pháp theo điểm bất kì trong số các điểm từ 10 đến 16,

trong đó, để đáp lại hồi đáp bắt tay được nhận bởi thiết bị máy chủ truyền thông trong khoảng thời gian được định rõ, thì phương pháp còn bao gồm bước tạo ra dữ liệu truy cập để cho phép thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.

18. Phương pháp theo điểm 17, khi phụ thuộc vào điểm 15, còn bao gồm bước các bước:

tạo ra dữ liệu thứ hai biểu thị việc nhận hồi đáp bắt tay bởi thiết bị máy chủ truyền thông; và

cập nhật dữ liệu được lưu trữ trong một hoặc nhiều bộ lưu trữ dữ liệu với dữ liệu thứ hai.

19. Phương tiện lưu trữ không chuyển tiếp lưu trữ các lệnh, mà khi được thực thi bởi bộ xử lý thì khiến bộ xử lý thực hiện phương pháp theo một điểm bất kỳ trong số các điểm từ 10 đến 18.

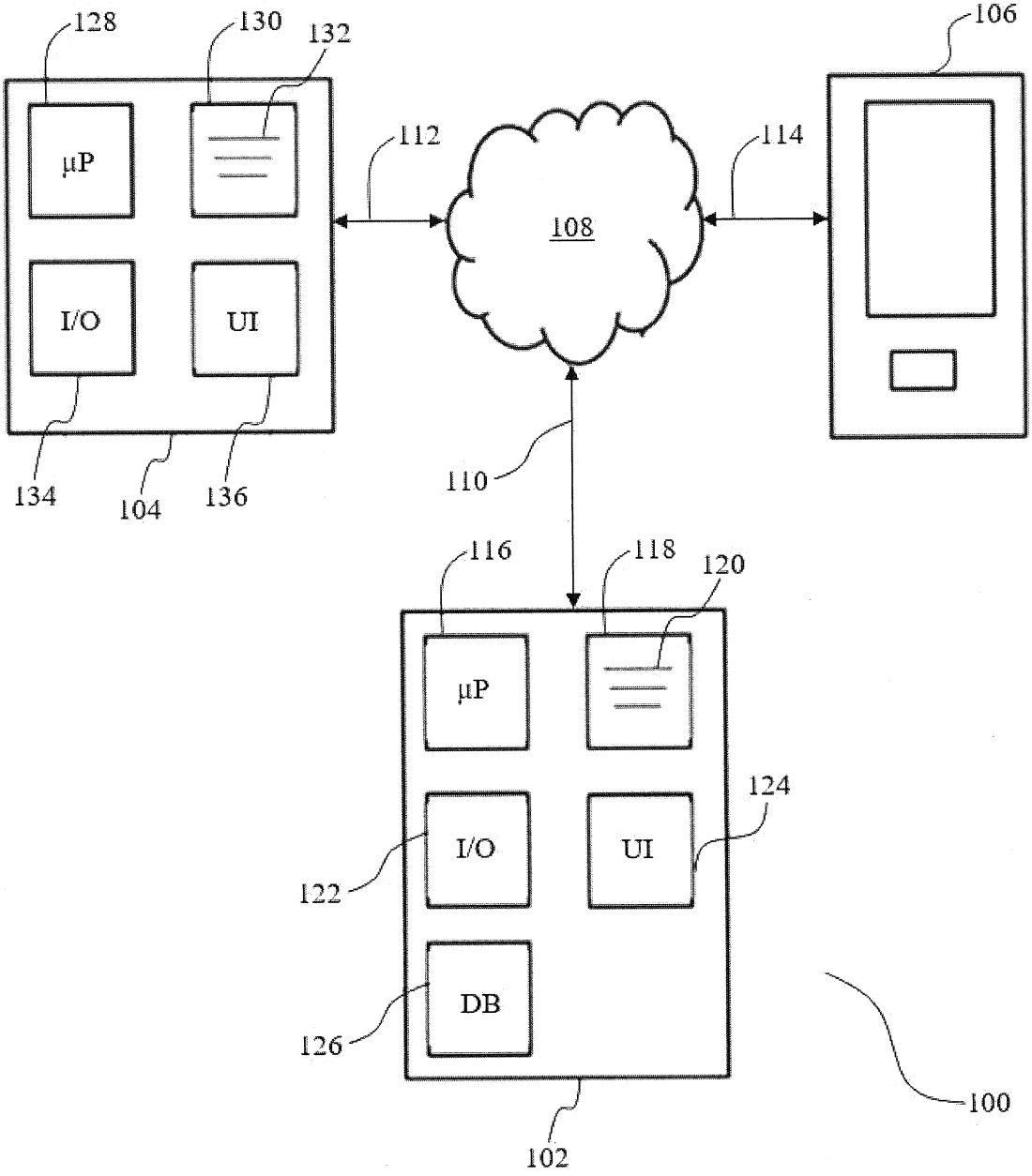

128
130
132
106
µP
112
114
108
I/O
UI
110
134
104
136
116
118
120
µP
124
I/O
UI
122
DB
126
100
102

FIG. 1

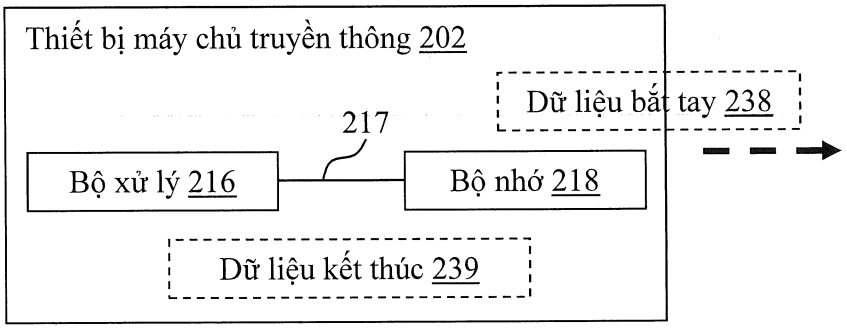

Thiết bị máy chủ truyền thông 202
Dữ liệu bắt tay 238
217
Bộ xử lý 216
Bộ nhớ 218
Dữ liệu kết thúc 239

FIG. 2A

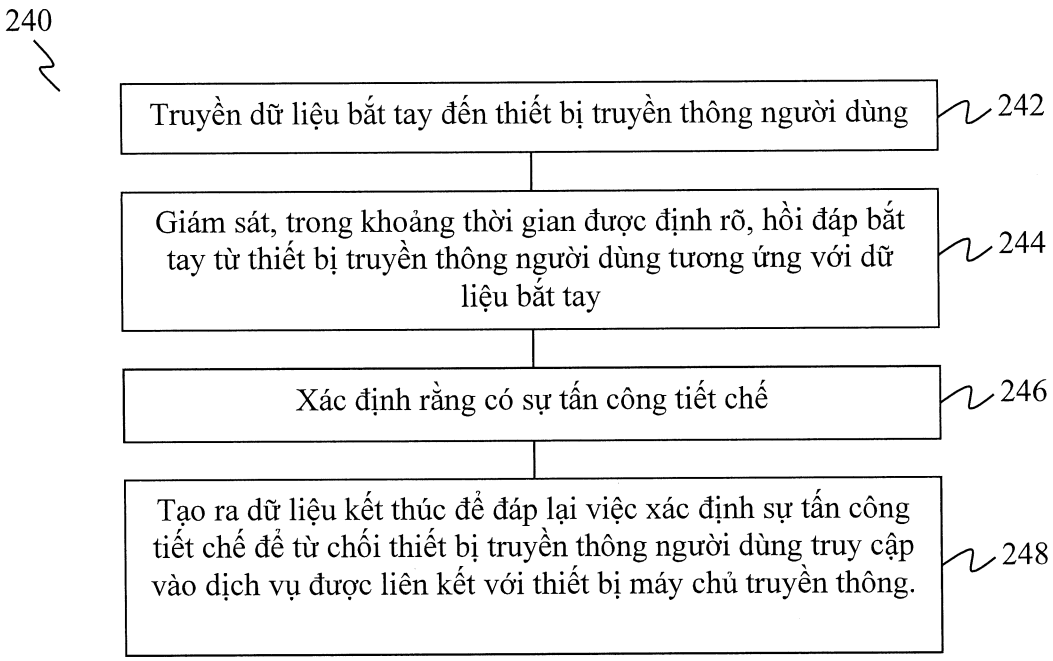

240
Truyền dữ liệu bắt tay đến thiết bị truyền thông người dùng
242
Giám sát, trong khoảng thời gian được định rõ, hồi đáp bắt tay từ thiết bị truyền thông người dùng tương ứng với dữ liệu bắt tay
244
Xác định rằng có sự tấn công tiết chế
246
Tạo ra dữ liệu kết thúc để đáp lại việc xác định sự tấn công tiết chế để từ chối thiết bị truyền thông người dùng truy cập vào dịch vụ được liên kết với thiết bị máy chủ truyền thông.
248

FIG. 2B

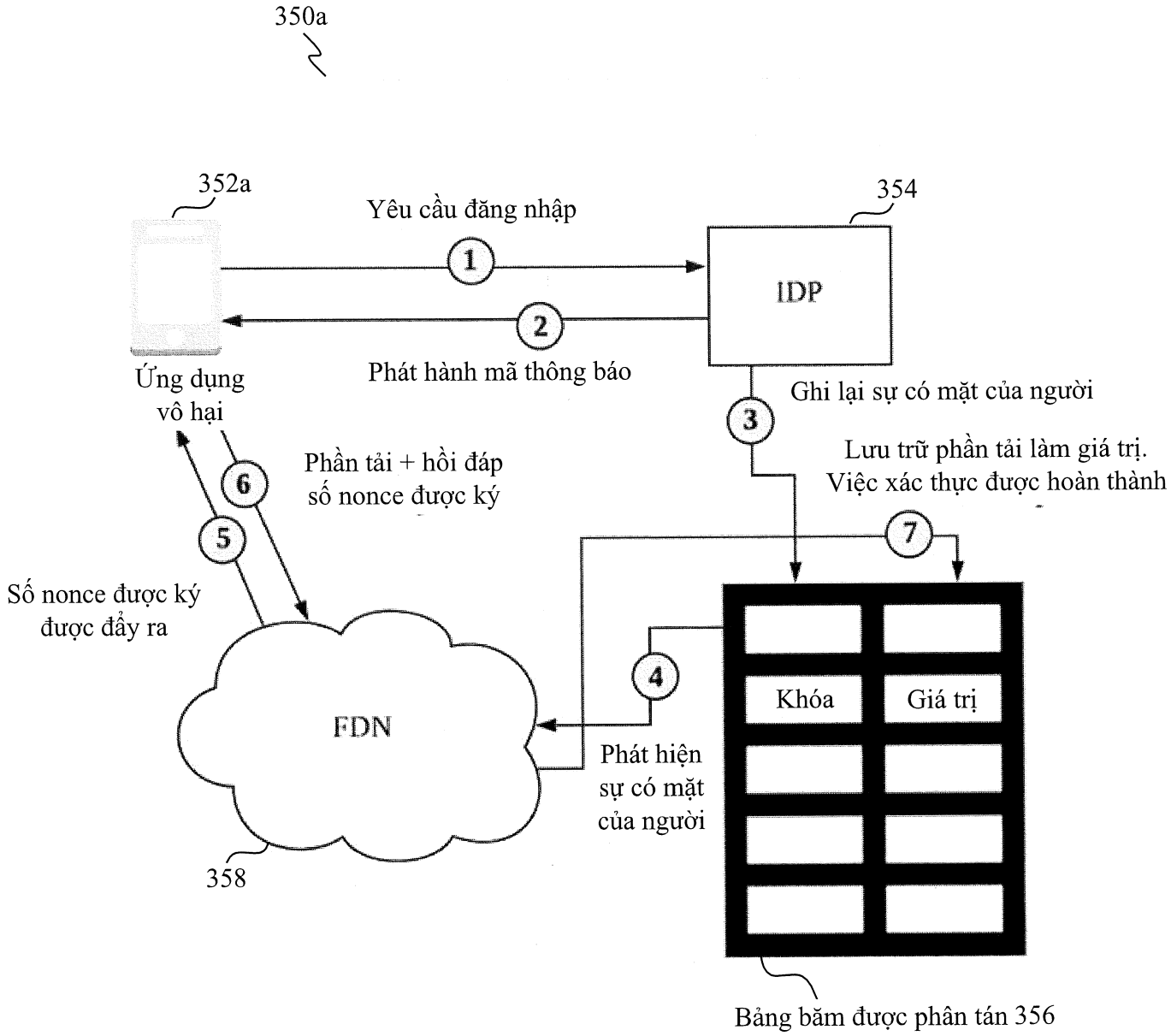

350a
352a
Yêu cầu đăng nhập
354
1
IDP
2
Phát hành mã thông báo
Ứng dụng
vô hại
Ghi lại sự có mặt của người
3
Lưu trữ phần tải làm giá trị.
Việc xác thực được hoàn thành
Phần tải + hồi đáp
số nonce được ký
6
5
7
Số nonce được ký
được đẩy ra
4
Khóa
Giá trị
FDN
Phát hiện
sự có mặt
của người
358
Bảng băm được phân tán 356

FIG. 3A

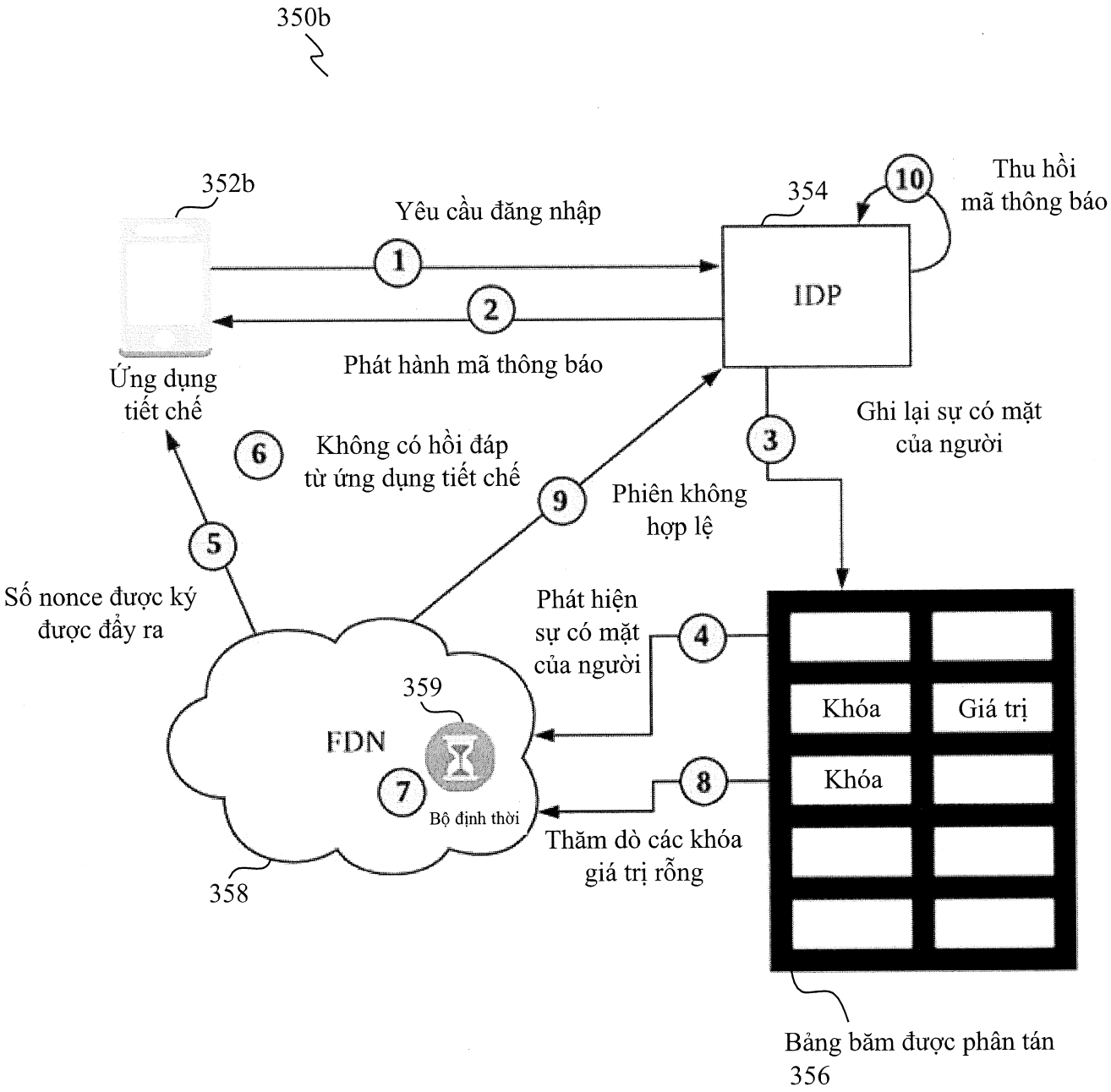

350b
352b
Yêu cầu đăng nhập
1
2
Phát hành mã thông báo
Ứng dụng tiết chế
354
10
Thu hồi mã thông báo
IDP
3
Ghi lại sự có mặt của người
6
Không có hồi đáp từ ứng dụng tiết chế
9
Phiên không hợp lệ
5
Số nonce được ký được đẩy ra
Phát hiện sự có mặt của người
4
359
FDN
7
Bộ định thời
8
Thăm dò các khóa giá trị rỗng
358
Khóa
Giá trị
Khóa
Bảng băm được phân tán
356

FIG. 3B