(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 806 514 A8**

(12) **CORRECTED EUROPEAN PATENT APPLICATION**

(15) Correction information:
Corrected version no 1 (W1 A1)
Corrections, see
Bibliography INID code(s) 15
Remarks
Remarks deleted

(48) Corrigendum issued on:
26.05.2021 Bulletin 2021/21

(43) Date of publication:
14.04.2021 Bulletin 2021/15

(21) Application number: **20199911.7**

(22) Date of filing: **13.06.2016**

(51) Int Cl.:
H04W 12/06 *(2021.01)* ***H04W 12/08*** *(2021.01)*
H04W 12/12 *(2021.01)* ***G06F 21/31*** *(2013.01)*
G06F 21/36 *(2013.01)* ***G06N 20/00*** *(2019.01)*
H04L 29/06 *(2006.01)* ***H04W 4/02*** *(2018.01)*
H04W 4/029 *(2018.01)* ***H04W 12/10*** *(2021.01)*
H04W 12/126 *(2021.01)* ***H04W 12/30*** *(2021.01)*

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **15.06.2015 US 201514739107**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
16734091.8 / 3 259 931

(71) Applicant: **Google LLC**
Mountain View, CA 94043 (US)

(72) Inventors:
- **SHARIFI, Matthew**
Mountain View, CA California 94043 (US)
- **WANG, Kai**
Mountain View, CA California 94043 (US)
- **PETROU, David**
Mountain View, CA California 94043 (US)

(74) Representative: **Derry, Paul Stefan et al**
Venner Shipley LLP
200 Aldersgate
London EC1A 4HD (GB)

Remarks:
•This application was filed on 02-10-2020 as a divisional application to the application mentioned under INID code 62.
•Claims filed after the date of filing of the application (Rule 68(4) EPC).

(54) **SCREEN-ANALYSIS BASED DEVICE SECURITY**

(57) Systems and methods are provided for a content-based security for computing devices. An example method includes identifying content rendered by a mobile application, the content being rendered during a session, generating feature vectors from the content and determining that the feature vectors do not match a classification model. The method also includes providing, in response to the determination that the feature vectors do not match the classification model, a challenge configured to authenticate a user of the mobile device. Another example method includes determining a computing device is located at a trusted location, capturing information from a session, the information coming from content rendered by a mobile application during the session, generating feature vectors for the session, and repeating this until a training criteria is met. The method also includes training a classification model using the feature vectors and authenticating a user of the device using the trained classification model.

EP 3 806 514 A8

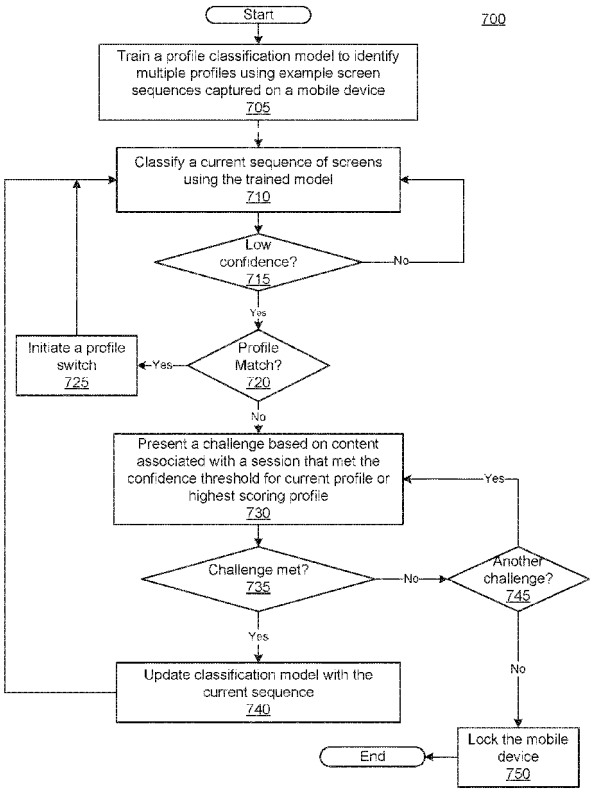
Start
700
Train a profile classification model to identify multiple profiles using example screen sequences captured on a mobile device
705
Classify a current sequence of screens using the trained model
710
Low confidence?
715
No
Yes
Initiate a profile switch
725
Yes
Profile Match?
720
No
Present a challenge based on content associated with a session that met the confidence threshold for current profile or highest scoring profile
730
Yes
Challenge met?
735
No
Another challenge?
745
Yes
Update classification model with the current sequence
740
No
Lock the mobile device
750
End

FIG. 7