(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 209 459 A1** 2015.11.19

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 209 459.3**
(22) Anmeldetag: **19.05.2014**
(43) Offenlegungstag: **19.11.2015**

(51) Int Cl.: ***H04W 12/06*** (2009.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333 München, DE

(72) Erfinder:
Rothmaier, Gerrit, Plainsboro, N.J., US;
Wambach, Tim, 85579 Neubiberg, DE

(56) Ermittelter Stand der Technik:

DE 10 2012 205 462 A1
US 2002 / 0 174 336 A1

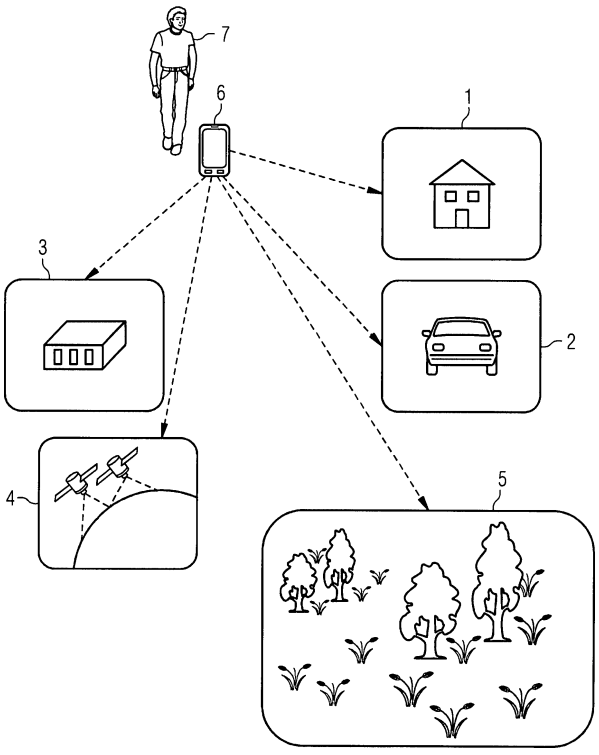
NAZARIAN, Robert: How to automatically disable Android's security lock screen when connected to your home Wi-Fi, Bluetooth device or by location. 01.10.2013. URL: http://www.talkandroid.com/guides/beginner/how-to-automatically-disable-androids-security-lock-screen-when-connected-to-your-home-wi-fi-bluetooth-device-or-by-location/ [abgerufen am 12.12.2014]

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Authentifizierung für mobile Geräte mit Zugangskontrolle**

(57) Zusammenfassung: Es wird ein Verfahren zur Authentifizierung bei mobilen Kommunikationsgeräten (6) mit Zugangsschutz beschrieben, wobei in Abhängigkeit von einer aktuellen Position des mobilen Kommunikationsgerätes ein Grad des Zugangsschutzes zum mobilen Kommunikationsgerät (6) festgelegt und dem mobilen Kommunikationsgerät zugeordnet wird, eine Kombination aus der aktuellen Position des mobilen Kommunikationsgerätes (6) mit dem Grad des Zugangsschutzes zum mobilen Kommunikationsgerät (6) abspeichert wird, und zur anfänglichen Endsperrung des mobilen Kommunikationsgerätes (6) der Grad des Zugangsschutzes für die aktuelle Position oder den Bereich am mobilen Kommunikationsgerät (6) aktiviert ist.



Beschreibung

[0001] Die Erfindung betrifft ein Authentifizierungssystem für mobile Kommunikationsgeräte, welche durch eine Zugangskontrolle am Gerät vor nicht autorisierter Benutzung des Gerätes schützt.

[0002] Der zunehmende Umgang von Menschen mit elektronischen Systemen im Alltagsleben erfordert sichere, jedoch auch einfach verwendbare Authentisierungsmechanismen. Eine große Anzahl verschiedener Verfahren die für unterschiedliche Schutzklassen eingesetzt werden können sind sowohl frei, als auch kommerziell, verfügbar.

[0003] Die große Herausforderung von sicheren, alltagstauglichen Authentisierungssystemen besteht darin, die Benutzbarkeit, durch eine hohe Komplexität bei der Anwendung nicht zu sehr einzuschränken. Ein Smartphone ist üblicherweise erst dann nutzbar, nachdem eine korrekte, meist vierstellige PIN, persönliche Identifizierungs-Nummer, eingegeben worden ist. Für eine achtstellige PIN oder sogar ein alphanumerisches Passwort ist der Aufwand für den Benutzer meist sehr groß und wird nicht akzeptiert. Die Folge ist, dass die Sicherheitsmaßnahmen vom Benutzer umgangen bzw. komplett abgeschaltet werden. Insbesondere für Smartphones wurden deshalb in den letzten Jahren neue Mechanismen umgesetzt, wie beispielsweise das Aufmalen eines Musters per Finger auf einem Touchscreen, wie es in Zusammenhang mit den Betriebssystemen "Android" oder "Windows 8" bekannt ist oder ein biometrischer Fingerabdrucksensor, bekannt vom "IPhone 5s".

[0004] Bei gängigen Mobiltelefonen ist eine statische Konfiguration des Authentisierungssystems möglich. Somit kann bisher beim Zugangsschutz zwischen PIN, Passwort, Bild basiert bzw. Muster basiert oder biometrisch gewählt werden.

[0005] Der Erfindung liegt die Aufgabe zugrunde, eine einfache Konfiguration des Authentifizierungssystems bei mobilen Geräten mit Zugangskontrolle zu beschreiben, um deren Bedienungskomfort zu verbessern.

[0006] Die Lösung dieser Aufgabe geschieht durch die jeweilige Merkmalskombination eines unabhängig formulierten Patentanspruchs.

[0007] Vorteilhafte Ausgestaltungen können den Unteransprüchen entnommen werden.

[0008] Der Erfindung liegt die Erkenntnis zugrunde, dass nicht zu jeder Zeit und an jedem Ort der gleiche Zugangsschutz eines Gerätes, insbesondere eines Kommunikationsgerätes, notwendig ist.

[0009] Der Benutzer oder Besitzer eines betreffenden Kommunikationsgerätes, beispielsweise eines Smartphones, gibt die Stufe oder den Grad für die Authentifizierung für jede gewünschte Position oder gewünschten Bereich vor.

[0010] Ein Authentifizierungskonzept, welches Standortinformationen zu der Wahl einer Stärke eines Authentifizierungsschutzes, kontinuierlich oder gestuft verlaufend, entsprechend einem Grad oder einer Stufe des Zugangsschutzes zum mobilen Kommunikationsgerät, mit einbezieht, erleichtert dem Benutzer die Handhabung des mobilen Gerätes.

[0011] So ist beispielsweise das Mobiltelefon zu Hause vor einem Zugriff, wie bei einem Diebstahl, durch physikalische Gegebenheiten, wie Haustür, Wohnungseingangstür, etc. geschützt. In diesem Fall wäre für ein Mobiltelefon ein geringerer oder gar kein technischer Zugangsschutz notwendig.

[0012] Ist das mobile Kommunikationsgerät in einem bestimmten Netz oder über eine bestimmte Verbindungsart angemeldet und befindet es sich innerhalb des Empfangsbereichs, so hat bereits ein anfänglicher Datenaustausch zwischen mobilem Kommunikationsgerät und Netz, wie WLAN, Bluetooth oder weitere Dienste oder Verbindungsmöglichkeiten, stattgefunden, so dass bereits mit einer Kennung ein bestimmter Grad der Authentifizierung verbunden oder festgelegt ist und die Kennung nicht weiter abgefragt wird.

[0013] Dem mobilen Kommunikationsgerät bekannte Kennungen werden mit einer Stufe der Authentifizierung als Zugangsschutz für einen bestimmten Bereich zu diesem Gerät verknüpft und abgespeichert. Dabei wird jeweils einer bestimmten Adresse oder Kennung eine bestimmte Stufe für den Zugangsschutz zum Smartphone zugeordnet.

[0014] Die Datenspeicherung der Daten kann an beliebigen Orten geschehen, solange das mobile Kommunikationsgerät darauf zugreifen kann.

[0015] Ermöglicht werden kann dies durch die Einbeziehung Standortspezifischer Faktoren. Zusätzlich können GPS-Koordinaten verwendet werden um die aktuelle Position des Benutzers zu ermitteln oder einen bestimmten Bereich festzulegen, in welchem dann eine bestimmte Stufe des Zugangsschutzes vorliegt oder vorgegeben ist.

[0016] Die Wahl einer Stufe der Authentifizierung wird von weiteren bzw. zusätzlichen Faktoren, wie dem Standort, der aktuellen Position oder einem Aufenthaltsbereich abhängig gemacht. So benötigt das Smartphone für den Bereich "zu Hause" gar keine Authentifizierung und bei der "Arbeitsstelle" reicht eine vierstellige PIN zur Authentifizierung aus. Auf die-

se Weise kann der Benutzer an ausgewählten Orten oder Bereichen auf einfachem Wege Zugang zum Gerät und damit auf die Daten seines elektronischen Gerätes bekommen.

[0017] Sobald sich der Benutzer außerhalb eines solchen Bereiches aufhält, wird als Zugangskontrolle ein stärkeres beispielsweise 8-stelliges alphanumerisches Passwort für eine Zugangskontrolle, zugrunde gelegt.

[0018] Darüber hinaus ist es auch möglich bekannte kabellose WLAN Accesspoints, Verbindungsknotenpunkte, mit einzubeziehen. Ist das Smartphone beispielsweise in der Lage einen Einwahlvorgang in ein WLAN-Netz zu tätigen, wie dies beim WLAN Router zu Hause der Fall ist, so ist in vorteilhafter Weise, innerhalb der Reichweite dieses WLANs, keine Authentifizierung notwendig.

[0019] Auf diese Weise kann der Benutzer zu Hause auf möglichst bequeme Art mit dem Gerät umgehen; ist allerdings außerhalb dieses Bereiches weiterhin vor unzulässiger Benutzung durch einen höheren Grad der Zugangskontrolle geschützt.

[0020] Falls das Mobiltelefon verloren geht, müsste ein Dieb das Gerät zur Benutzung in einen bevorzugten Bereich bringen, um ohne Authentifizierung, also ohne PIN, zugreifen zu können. Der Benutzer könnte in diesem Fall zur Abhilfe das Kommunikationsgerät für den Zugriff auf das betreffende WLAN sperren.

[0021] Ebenfalls ist der Einsatz von Übertragungsstandards, wie Bluetooth denkbar. So könnte sich in einem bestimmten Raum beispielsweise auf dem Tisch eines Konferenzzimmers, ein Bluetooth basiertes Gerät befinden, welches den erforderlichen Grad der Authentifizierung in diesem Raum vorgibt. Sobald sich das Gerät außerhalb dieses Bereiches befindet, ist wieder ein höherer Schutz für den Zugang zu dem mobilen Gerät notwendig.

[0022] Moderne Autoradios lassen sich via Bluetooth mit dem Mobiltelefon koppeln. Das so mit dem Autoradio verbundene Mobiltelefon kann diesen Bereich "Auto" ebenfalls als eine "vertrauenswürdige Zone" erkennen und es wird die niedrigste Stufe des Authentisierungssystems entsprechend "keine PIN" verlangt.

[0023] Gleiches gilt z.B. bei über Bluetooth ansprechbaren Lautsprechern, mit Funkradius ca. 5–10 Meter. Zur Benutzung eines Smartphones zur Ansteuerung der Lautsprecher ist kein Zugangsschutz erforderlich.

[0024] Die abgestufte Authentifizierung in ausgewählten Bereichen kann auch dadurch erreicht werden, dass der Benutzer selbst ein Authentifizierungsmerkmal mit sich trägt:
Befindet sich ein RFID-Chip am Schlüsselbund des Benutzers oder im Portemonnaie des Benutzers, so kann dieser ein Signal geben, dass das Smartphone dann ohne PIN zugänglich ist, aber nur, wenn sich der RFID-Chip in der Nähe befindet. Sobald RFID-Chip und Smartphone zunehmend voneinander getrennt werden, wird ein höherer Aufwand, entsprechend einer höheren Stufe zur Authentifizierung, entsprechend einer komplizierteren PIN, vom Benutzer gefordert.

[0025] Im Folgenden werden anhand der begleitenden Figur schematische, die Erfindung nicht einschränkende, Ausführungsbeispiele beschrieben:

[0026] Die Figur zeigt eine Übersicht verschiedener Bereiche **1**–**5**, wobei jeweils unterschiedliche Stufen einer Authentifizierung eingerichtet sind.

[0027] Es werden exemplarisch am Beispiel eines Smartphones, eines intelligenten Mobiltelefons, Ausführungsbeispiele dargestellt. Weitere Anwendungsfälle sind ebenso denkbar, wie bei einem "Notebook".

[0028] Befindet sich der Benutzer im Bereich **1**, zu Hause, so hat er Zugriff auf sein WLAN, das drahtlose lokale Verwaltungsnetz seines Heimnetzwerks. In diesem Fall bedarf es keiner Authentifizierung des Benutzers am Kommunikationsgerät.

[0029] Während des Aufenthaltes im Bereich **2**, im Auto, beispielsweise bei einer Autofahrt, ist das Kommunikationsgerät **6** via Bluetooth mit dem Bluetooth fähigen Autoradio verbunden. Eine erste Anmeldung des Kommunikationsgerätes am Autoradio erfordert eine Eingabe einer Kennung des Autoradios, womit diese Verbindung selbst einen bestimmten Grad für die Authentifizierung des Benutzers zu seinem Kommunikationsgerät aufweist.

[0030] Bewegt sich der Benutzer im Bereich **3**, Arbeitsstelle, so genügt in diesem Fall die Eingabe einer 4-stelligen PIN.

[0031] Weiterhin kann der Benutzer in einem Bereich **4**, in einem GPS-Bereich, via GPS lokalisiert werden, woraus sich eine weitere Stufe der Authentifizierung ergibt. Es kann ein GPS-Bereich definiert werden durch GPS-Koordinaten, für den ein bestimmter Grad der Authentifizierung vorgegeben wird.

[0032] Außerhalb der Bereiche **1** bis **4** wird im Bereich **5**, im Außenbereich, eine starke Authentifizierung, wie mit einem 8-stelligen alphanumerischen Passwort, gefordert.

[0033] Die Erfindung basiert auf der Berücksichtigung von Umgebungsfaktoren, die am aktuellen Aufenthaltsort des Smartphones, vorliegen.

[0034] Eine eingerichtete Bluetooth-Verbindung mit bestimmtem Grad der Authentifizierung oder ein RFID-Chip am Benutzer **7**, kann zur dynamischen Anpassung des notwendigen Grades der Authentifizierung beitragen. Weiterhin kann im jeweiligen Bereich **1**, zu Hause, Bereich **2**, im Auto, Bereich **3**, am Arbeitsplatz, Bereich **4**, im GPS-Bereich, der Grad der Authentifizierung angepasst werden.

[0035] Der wesentliche Vorteil der Erfindung liegt in der Erleichterung der Benutzung des Kommunikationsgerätes durch den Benutzer bei gleichzeitiger Etablierung eines höheren Sicherheitsniveaus in dem jeweiligen Bereich **1**–**5**.

[0036] Beispiel: Jeweils vorgegebener Grad der Authentifizierung:
Bereich **1**, keine PIN,
Bereich **2**, keine PIN, Bluetooth-Verbindung eingerichtet,
Bereich **3**, 4-stellige PIN,
Bereich **4**, 8-stellige PIN,
Bereich **5**, 8-stellige alphanumerische PIN.

Patentansprüche

1. Verfahren zur Authentifizierung bei mobilen Kommunikationsgeräten (**6**) mit Zugangsschutz, wobei
– in Abhängigkeit von einer aktuellen Position des mobilen Kommunikationsgerätes ein Grad des Zugangsschutzes zum mobilen Kommunikationsgerät (**6**) festgelegt und dem mobilen Kommunikationsgerät zugeordnet wird,
– eine Kombination aus der aktuellen Position des mobilen Kommunikationsgerätes (**6**) mit dem Grad des Zugangsschutzes zum mobilen Kommunikationsgerät (**6**) abspeichert wird, und
– zur anfänglichen Entsperrung des mobilen Kommunikationsgerätes (**6**) der Grad des Zugangsschutzes für die aktuelle Position am mobilen Kommunikationsgerät (**6**) aktiviert ist.

2. Verfahren nach Anspruch 1, wobei, falls das mobile Kommunikationsgerät (**6**) in einem Netz oder für eine Verbindungsart angemeldet ist, in einem anfänglichen Datenaustausch zwischen dem mobilen Kommunikationsgerät und dem Netz eine Authentifizierung stattgefunden hat und damit keine weitere Authentifizierung notwendig ist.

3. Verfahren nach Anspruch 1 oder 2, wobei
der Verlauf des jeweiligen Grades des Zugangsschutzes stufenförmig ist, entsprechend einer variablen Authentifizierung, für verschiedene aktuelle Positionen oder Bereiche (1–5) mit aufsteigender Stärke des Zugangsschutzes und wie folgt eingeteilt ist:
Bereich (**1**), zu Hause, keine PIN,
Bereich (**2**), im Auto, keine PIN; falls Bluetooth- Verbindung eingerichtet,
Bereich (**3**), Arbeitsstelle, 4-stellige PIN,
Bereich (**4**), GPS-Bereich, 8-stellige PIN,
Bereich (**5**), im Außenbereich, 8-stellige alphanumerische PIN;
mit PIN entspricht:‚Persönliche Identifizierung Nummer‘.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Festlegung des Grades des Zugangsschutzes durch den Einsatz eines RFID-Chips geschieht, welcher sich beim Benutzer des mobilen Kommunikationsgeräts (**6**) befindet, womit dem mobilen Kommunikationsgerät der Grad des Zugangsschutzes signalisiert wird, solange sich der RFID-Chips in der Nähe des Benutzers des mobilen Kommunikationsgeräts befindet.

5. Verfahren nach einem der Ansprüche 1–3, wobei die Festlegung des Grades des Zugangsschutzes zum mobilen Kommunikationsgerät durch die Kennung bei der Anmeldung am WLAN, Bluetooth, an weiteren Diensten oder weiteren Verbindungsmöglichkeiten, geschieht, womit dem mobilen Kommunikationsgerät der Grad des Zugangsschutzes signalisiert wird, solange sich das mobile Kommunikationsgerät in einem entsprechenden Sendebereich befindet.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Benutzer (**7**) einen Bereich (**4**) mittels GPS-Koordinaten vorgibt, dem ein bestimmter Grad des Zugangsschutzes zugeordnet wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Grad der Authentifizierung für jede aktuelle Position oder jeden gewünschten Bereich vom Benutzer des mobilen Kommunikationsgeräts vorgegeben wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei für den außerhalb der aktuellen Position oder eines Bereichs (1–4) befindlichen Benutzer (**7**) mit mobilem Kommunikationsgerät, als Zugangsschutz einen stärkeren Grad des Zugangsschutzes, insbesondere ein 8-stelliges alphanumerisches Passwort, beachten muss.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei durch eine Einwahl in bekannte kabellose WLAN-Accesspoints, Verbindungsknotenpunkte, sich in ein bestimmtes WLAN-Netz einwählen können, so kann, innerhalb der Reichweite des WLANs, eine Authentifizierung entfallen.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei Autoradios über Bluetooth mit dem mobilen Kommunikationsgerät gekoppelt werden, womit am mobilen Kommunikationsgerät ein sehr niedriger Grad des Zugangsschutzes oder gar keiner verlangt wird.

11. Verfahren nach einem der Ansprüche 1–10, wobei über Bluetooth ansprechbare Lautsprecher, mit einem Funkradius im Bereich von 3–10 Meter, über Bluetooth mit dem mobilen Kommunikationsgerät gekoppelt werden, womit am mobilen Kommunikationsgerät ein sehr niedriger Grad des Zugangsschutzes oder gar keiner verlangt wird.

12. Verfahren nach einem der vorhergehenden Ansprüche, wobei ein Bluetooth basiertes Gerät, welches den erforderlichen Grad der Authentifizierung in einem Raum vorgibt, signalisiert dem mobilen Kommunikationsgerät den Bereichs abhängigen Grad des Zugangsschutzes.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen