(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-502128
(P2005-502128A)
(43)公表日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330A	5B076
G06F 1/00	G06F	9/06	660C	5B085

審査請求 未請求　予備審査請求 有　（全 41 頁）

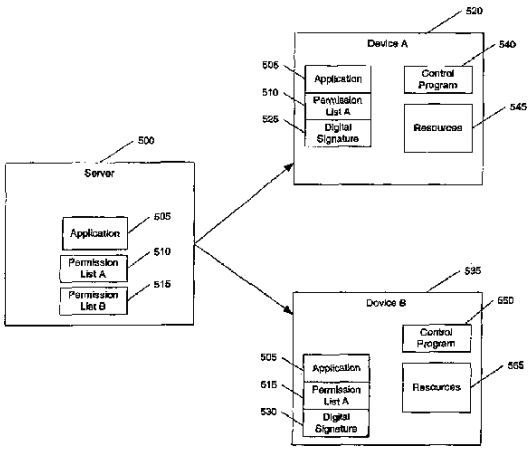
(21)出願番号	特願2003-525489(P2003-525489)
(86)(22)出願日	平成14年8月13日(2002.8.13)
(85)翻訳文提出日	平成16年2月13日(2004.2.13)
(86)国際出願番号	PCT/US2002/025746
(87)国際公開番号	WO2003/021467
(87)国際公開日	平成15年3月13日(2003.3.13)
(31)優先権主張番号	60/312,146
(32)優先日	平成13年8月13日(2001.8.13)
(33)優先権主張国	米国(US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】アプリケーションにデバイスリソースを割り当てるための許可の使用

(57)【要約】
【課題】アプリケーションにデバイスリソースを割り当てるための許可の使用
【解決手段】デバイス（５２０）に対するリソースは、アプリケーション（５０５）に対するアクセスを、該アプリケーション（５０５）に関連付けられた特権に基づいて与えられる。許可リスト（５１０、５１５）がサーバ（５００）によって作成され、アプリケーション（５０５）がどのリソース（５４５）にアクセスしてよいのかを示している。アプリケーション（５０５）がリソース（５４５）を要求するアプリケーション実行中、デバイス（５２０）上で実行している制御プログラム（５４０）は、アプリケーション（５０５）と関連付けられる許可リスト（５１０）をチェックし、アプリケーション（５０５）がリソース（５４５）にアクセスしてよいかどうかを判断するために使用される。



【特許請求の範囲】
【請求項１】
デバイスにアプリケーションを記憶する方法であって、
前記デバイスでアプリケーションを受信する工程と、
前記デバイスで許可リストを受信する工程であって、前記許可リストは、前記アプリケーションがデバイス上でアクセスしてよいリソースを示す工程と、
前記デバイスに前記アプリケーション及び許可リストを記憶する工程と、
を備える方法。
【請求項２】
前記許可リストは権限保持者からのインプットを使用して作成される、請求項１に記載の方法。
【請求項３】
前記権限保持者はデバイスとは別個のエンティティである、請求項２に記載の方法。
【請求項４】
前記デバイスで前記アプリケーションを実行する工程と、
前記許可リストに基づいてデバイスリソースへのアプリケーションのアクセスを許可する工程と、
をさらに備える、請求項１に記載の方法。
【請求項５】
修正検出方法を受信する工程とをさらに備え、デジタル署名が前記許可リストからの情報に基づき作成される、請求項１に記載の方法。
【請求項６】
前記デバイスは無線装置である、請求項１に記載の方法。
【請求項７】
アプリケーションを実行するデバイスであって、
ハンドセットリソースとアプリケーションとを接続するように動作可能な制御プログラムを備え、
前記制御プログラムがアプリケーションからデバイスリソースに対する要求を受信し、該アプリケーションと関連付けられる許可リストに含まれるデータに基づいて、該アプリケーションに該デバイスリソースへのアクセスを許可するように動作可能であるデバイス。
【請求項８】
前記デバイスは無線装置である、請求項７に記載のデバイス。
【請求項９】
前記制御プログラムは、前記許可リストに関連付けられるデジタル署名を評価するようにさらに動作可能である、請求項７に記載のデバイス。
【請求項１０】
デバイスリソースへのアクセスを可能にする方法であって、
アプリケーションから前記デバイスリソースに対する要求を受信する工程と、
前記アプリケーションと関連付けられた許可リストを評価する工程であって、前記許可リストはアプリケーションがアクセスできるリソースを示す工程と、
前記許可リスト中の表示に基づき、前記デバイスリソースへのアクセスを前記アプリケーションに許可する工程と、
を備える方法。
【請求項１１】
少なくとも前記許可リストと関連付けられたデジタル署名を受信する工程と、
前記許可リストが修正されたかどうかを判断するために前記デジタル署名を評価する工程と、
をさらに備える、請求項１０に記載の方法。
【請求項１２】
前記許可リスト中の表示に基づき、前記デバイスリソースへのアプリケーションアクセス

を拒絶する工程と、
をさらに備える、請求項１０に記載の方法。
【請求項１３】
前記デバイスリソースは、前記デバイスに接続される第２のデバイスに位置する、請求項１０に記載の方法。
【請求項１４】
前記許可リストはサーバから受信され、該サーバは権限保持者からの要件に基づき前記許可リストを作成する、請求項１０に記載の方法。
【請求項１５】
デバイスリソースへのアクセスを可能にする方法であって、
アプリケーションから前記デバイスリソースに対する要求を受信する工程と、
前記アプリケーションに関連付けられた許可リストを評価する工程であって、前記許可リストは、アプリケーションがアクセスできるリソースを示す工程と、
前記許可リスト中の表示に基づき、前記デバイスリソースへのアプリケーションアクセスを拒絶する工程と、
を備える方法。
【請求項１６】
許可リストをアプリケーションと関連付ける方法であって、
アプリケーションを受信する工程と、
１つまたは複数のデバイスリソースと関連付けられた少なくとも１つまたは複数の特権を受信する工程であって、前記特権が、前記関連付けられたデバイスリソースへのアクセスを示す工程と、
前記１つまたは複数のデバイスリソースのそれぞれに関連付けられた前記１つまたは複数の特権及びフィールドを使用して許可リストを作成する工程と、
を備え、
前記許可リストはアプリケーションに関連付けられ、該アプリケーションが該１つまたは複数のデバイスリソースにアクセスしてよいかどうかを評価するために使用される方法。
【請求項１７】
デバイスに許可リストを送信する工程とをさらに備える、請求項１６に記載の方法。
【請求項１８】
前記許可リストの中の情報を使用してデジタル署名を作成することと、該デジタル署名を該デバイスに送信することとをさらに備える請求項１７に記載の方法。
【請求項１９】
第２のデバイスのために１つまたは複数のデバイスリソースと関連付けられる少なくとも１つのまたは複数の特権を受信する工程であって、前記特権が、該関連付けられた第２のデバイスリソースへのアクセスを示す工程と、
前記１つまたは複数の特権及び前記１つまたは複数の第２のリソースのそれぞれの関連付けられるフィールドを使用して許可リストを作成する工程と、
をさらに備え、
前記許可リストが前記アプリケーションと関連付けられ、該アプリケーションが該１つまたは複数の第２のデバイスリソースにアクセスしてよいかどうかを評価するために使用される、請求項１６に記載の方法。
【請求項２０】
デバイスにアプリケーションを記憶するシステムであって、
前記デバイスでアプリケーションを受信する手段と、
前記デバイスで許可リストを受信する手段であって、前記許可リストは、アプリケーションがデバイス上でアクセスしてよいリソースを示す手段と、
前記デバイスに前記アプリケーション及び許可リストを記憶する手段と、
を備えるシステム。
【請求項２１】

デバイスリソースへのアクセスを許可するシステムであって、
アプリケーションから前記デバイスリソースに対する要求を受信する手段と、
前記アプリケーションと関連付けられる許可リストを評価する手段であって、前記許可リストは、前記アプリケーションがアクセスできるリソースを示す手段と、
前記許可リスト中の表示に基づき、前記デバイスリソースへのアクセスを前記アプリケーションに許可する手段と、
を備えるシステム。
【請求項２２】
許可リストをアプリケーションと関連付けるシステムであって、
アプリケーションを受信する手段と、
１つまたは複数のデバイスリソースと関連付けられた少なくとも１つまたは複数の特権を受信する手段であって、前記特権が関連デバイスリソースへのアクセスを示す手段と、
前記１つまたは複数の特権、及び前記１つまたは複数のデバイスリソースのそれぞれに関連付けられたフィールドを使用して許可リストを作成する手段と、
を備え、
前記許可リストが前記アプリケーションと関連付けられ、該アプリケーションが該１つまたは複数のデバイスリソースにアクセスしてよいかどうかを評価するために使用されるシステム。
【請求項２３】
デバイス上にアプリケーションを記憶するためのコンピュータ実行可能命令を含むコンピュータ読み取り可能媒体であって、
前記デバイスでアプリケーションを受信する工程と、
前記デバイスで許可リストを受信する工程であって、前記許可リストは、前記アプリケーションが前記デバイス上でアクセスできるリソースを示す工程と、
前記デバイスに前記アプリケーションと前記許可リストを記憶する工程と、
を備える、コンピュータ読み取り可能媒体。
【請求項２４】
デバイスリソースへのアクセスを可能にするためのコンピュータ実行可能命令を含むコンピュータ読み取り可能媒体であって、
アプリケーションから前記デバイスリソースに対する要求を受信する工程と、
前記アプリケーションと関連付けられる許可リストを評価する工程であって、前記許可リストは、前記アプリケーションがアクセスできるリソースを示す工程と、
前記許可リスト中の表示に基づき、前記デバイスリソースへのアクセスを前記アプリケーションに許可する工程と、
を備える、コンピュータ読み取り可能媒体。
【請求項２５】
アプリケーションに許可リストを関連付けるためのコンピュータ実行可能な命令を含むコンピュータ読み取り可能媒体であって、
アプリケーションを受信する工程と、
１つまたは複数のデバイスリソースに関連付けられる１つまたは複数の特権を受信する工程であって、前記特権が、該関連デバイスリソースへのアクセスを示す工程と、
前記１つまたは複数の特権、及び前記１つまたは複数のデバイスリソースのそれぞれに関連付けられたフィールドを使用して許可リストを作成する工程と、
を備え、
前記許可リストが前記アプリケーションと関連付けられ、該アプリケーションが該１つまたは複数のデバイスリソースにアクセスしてよいかどうかを評価するために使用される、コンピュータ読み取り可能媒体。
【請求項２６】
前記修正検出方法は前記アプリケーションからの情報に基づいて作成される、請求項５に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータデバイスで使用するためのアプリケーションの処理に関し、さらに詳細にはアプリケーションごとにデバイスリソースを許可することに関する。
【背景技術】
【０００２】
近年無線通信は爆発的な増加を経験している。消費者及び企業がさらに携帯電話及び携帯情報端末（ＰＤＡ）などの無線装置に依存するにつれて、無線サービスプロバイダ、つまり、通信事業者はこれらの無線装置で追加の機能を提供しようと躍起になる。この追加の機能は無線装置に対する需要を高めるだけではなく、現在のユーザの間での使用量も増加するだろう。
【０００３】
無線装置の環境は、無線装置でのアプリケーションの実行を考えるときに独特の課題を生じさせる。アプリケーションをダウンロードし、アプリケーションを削除する方法を開発する必要がある。加えて、無線装置でのセキュリティに対するニーズもある。無線装置でのセキュリティの懸念事項は、アプリケーションが意図的にあるいは意図的にではなく、無線装置でまたは無線装置が通信する回路網で他のファイルを劣化させるあるいは壊すことができないように考えられる最善の方法で環境を管理することを含む。
【０００４】
アプリケーションは、実行中それらが実行しているデバイス上で多様なリソースを必要とする。これらのリソースは（一次記憶装置と二次記憶装置を含む）メモリ、ＣＰＵ時間及び／またはアクセス、Ｉ／Ｏポートならびに特にディスプレイ、スピーカ、キーボードまたはキーパッド及びマイクを含む。デバイスが回路網に接続されると、アプリケーションは、例えばデバイスでのダイヤラーなど、回路網を使用するためにデバイスリソースにアクセスすることを希望してよい。
【０００５】
アプリケーションがデバイス、またはデバイスに接続される他のデバイス上で被る可能性がある損傷を制限するセキュリティ手段として、デバイスリソースへのアプリケーションのアクセスを制御することが望ましい。この損傷はアプリケーション上のウィルスを介して意図されるか、あるいは意図的にではなくリソースを支配し、それを他のアプリケーションが使えないようにするか、損傷を受けた状態にする低い程度で作成された符号を用いてアプリケーションが実行する場合に意図されない場合がある。
【０００６】
一般にデバイスのリソースを制御する方法は、ユーザ特権レベルに基づいていた。ユーザがシステム上の典型的なユーザである場合、ユーザは、ユーザが必要とすると予想されるリソースに対するアクセスレベルを与えられていた。ユーザがデバイスに搭載した、あるいはデバイスで実行したアプリケーションがなんであろうと、アプリケーションがそれらのユーザ特権の元で実行している限り、それらのアプリケーションはすべてデバイスに対して同じアクセス権を与えられていた。
【０００７】
例えば、ユーザがデバイスが接続されている回路網のシステム管理者またはシステムエンジニアである場合、そのユーザは例えば「スーパーユーザ」などのさらに高い特権レベルを与えられ、デバイス及びネットワークリソースにさらに多くのアクセスを与えられてよい。しかしながら、典型的なユーザでの場合と同様に、このスーパーユーザの特権はスーパーユーザが実行するすべてのアプリケーション全体で同じままであった。このシナリオでは、典型的なユーザによって実行される同じアプリケーションは、スーパーユーザによって実行される場合の追加リソースを与えられてよい。
【０００８】
しかしながら、このやり方ではデバイスがデバイスのリソースをアプリケーションごとに

制限することは不可能である。ユーザ自体がアプリケーションのリソースに対するアクセスを制限しようと試みることがあるが、これはデバイス及びデバイスが位置する回路網を管理する人たちになんのセキュリティも提供しなかった。ユーザはリソースを制限することを回避し、そのためユーザに設定された特権レベルに基づきデバイスリソースまたはネットワークリソースに損害を与えていただろう。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

その結果、技術で必要とされているのは、デバイス及び接続されている回路網のリソースを保護し、アプリケーションごとのリソースに対する供与権利を可能にすることによりデバイスのリソースを管理する柔軟性も高めるシステムと方法である。

【課題を解決するための手段】

【００１０】

本発明に適合したシステム及び方法により、デバイスのリソースに対するアプリケーションアクセスをアプリケーションに関連付けられた一組の許可に基づいて可能にすることにより既存のシステムの欠点を克服する。

【００１１】

一実施形態では、本発明は、デバイスにアプリケーションを記憶する方法であって、前記デバイスでアプリケーションを受信する工程と、前記デバイスで許可リストを受信する工程であって、前記許可リストは、前記アプリケーションが前記デバイス上でアクセスしてよいリソースを示す工程と、前記アプリケーションと許可リストを前記デバイスに記憶する工程とを備える。

【００１２】

別の実施形態では、本発明は、デバイスリソースへのアクセスを可能にする方法であって、アプリケーションから前記デバイスリソースに対する要求を受信する工程と、前記アプリケーションに関連付けられた許可リストを評価する工程であって、前記許可リストは、前記アプリケーションがアクセスできるリソースを示す工程と、許可リスト内の表示に基づき、前記デバイスリソースへのアプリケーションアクセスを許可する工程とを備える。

【００１３】

さらに別の実施形態では、本発明は、アプリケーションに許可リストを関連付ける方法であって、アプリケーションを受信する工程と、１つまたは複数のデバイスリソースと関連付けられた少なくとも１つまたは複数の特権を受信する工程であって、前記特権は関連デバイスリソースへのアクセスを示す工程と、該１つまたは複数のデバイスリソースに関連付けられた１つまたは複数の特権及びフィールドを使用して許可リストを作成する工程とを備え、前記許可リストはアプリケーションと関連付けられ、当該アプリケーションが該１つまたは複数のデバイスリソースにアクセスしてよいかどうかを評価するために使用される。

【００１４】

本発明の追加の実施形態も続く説明及び添付図面に説明される。

【００１５】

明細書に組み込まれ、明細書の一部を構成する添付図面は、本発明の現在好まれている実施形態を、前述された一般的な説明及び後述される好適実施形態の詳細な説明とともに図解し、本発明の原理を説明する役目を果たしている。

【発明の効果】

【００１６】

本発明によれば、デバイス及び接続されている回路網のリソースを保護し、アプリケーションごとのリソースに対する供与権利が可能になり、デバイスのリソースを管理する柔軟性が高まる。

【発明を実施するための最良の形態】

【００１７】

ここでは、類似する参照文字がいくつかの図面を通じて類似するパーツまたは対応するパーツを示す添付図面に図解されるような本発明の現在の例示的且つ好ましい実施形態を詳しく参照する。本発明の性質、目的及び優位点は添付図面に関連して以下の詳細な説明を考慮した後に当業者により明らかになるだろう。

【００１８】

はじめに

本発明と一貫するシステム及び方法はコンピュータデバイス上でのデバイスリソースに対するアプリケーションのアクセスを制限する。デバイスリソースへのアクセスを制限する特権レベルはユーザに設定されてよいが、本発明に一貫するシステム及び方法はデバイスリソースに対するアプリケーションのアクセスをアプリケーションごとに制限し、このようにしてデバイスリソースを管理する上で高められた柔軟性とセキュリティを提供する。デバイスリソースは機能に対するアクセスを提供する、あるいは機能を実行するデバイスのそれらすべての構成要素を含む。これらは、デバイスのメモリ、一次記憶装置と二次記憶装置、入力／出力（「入出力」）ポート、ネットワークアクセス、ダイヤラー、スピーカ、ディスプレイ、キーボード／キーパッド、マイク、ファイル及びデバイス自体にあるか、デバイスがアクセスできる回路網全体に位置するかに関係なくリソースを含むが、それらに制限されない。

【００１９】

本発明は、アプリケーションと許可リストを関連付ける。アプリケーションの開発者、システム管理者、または事業者やデバイスの製造メーカなどの他の権限保持者は、デバイスで使用されるときのアプリケーションについてこの許可リストを作成してよい、あるいは作成にインプットを提供してよい。加えて、デバイスでアプリケーションを実行することに関わる権限保持者、エンティティまたは関係者からのインプットに基づき許可リストを作成するためにサーバが使用されてよい。アプリケーション及び許可リストがデバイスにインストールされると、アプリケーションは実行時許可リスト内で許可されたリソースに対するアクセスだけを許される。デバイスが許可リスト外のリソースに対するアプリケーションのアクセスをさらに制限してよいことは当業者によって認識されるだろう。例えば、ユーザに、アプリケーションが許可を与えられるデバイス上のリソースに対する権利がない可能性がある。本発明のこの代替実施形態は、デバイスが追加の制限を提供し、その結果許可がデバイス及び／またはユーザと関連付けられた他の特権レベルに基づき許可リストで与えられているとしてもリソースに対するアクセスを拒絶してよいというものである。

【００２０】

デバイスのリソースを許可リストのアプリケーションに関連付けることにより、同じアプリケーションとともに使用するために複数の許可リストが作成されてよい。その結果、様々なデバイスで様々なリソースに同じアプリケーションに対するアクセスが許される可能性がある。

【００２１】

前記したことは、説明を簡単にするため分散され、実行されているアプリケーションファイルタイプを説明していることが当業者により認識されるだろう。「アプリケーション」は、オブジェクトコード、スクリプト、ジャバファイル、ブックマークファイル（またはＰＱＡファイル）、ＷＭＬスクリプト、バイトコード及びパールスクリプトなどの実行可能なコンテンツを有するファイルも含んでよい。さらに、ここで参照される「アプリケーション」は、開く必要がある文書、またはアクセスする必要がある他のデータファイルなどの本質的に実行可能ではないファイルも含んでよい。

【００２２】

図１は、本発明の例示的な実施形態が実践されてよいシステムアーキテクチャ環境を示すブロック図である。デバイス１１５はアプリケーション１０５を実行できる。デバイス１１５は、パソコン、移動無線装置と固定無線装置を含む無線装置、ともに接続される計算機の組み合わせなどの任意の計算機であってよい。デバイス１１５は、デバイス１１５に

関連付けられたリソース１２０を有する。これらのリソースは、デバイス１１５の内部、または外部で機能を提供する、あるいは機能にアクセスするデバイスの構成要素を含む。デバイスのリソース１２０の例は一次記憶装置と二次記憶装置を含むメモリ、マイク、デバイスに接続される回路網、回路網を介して接続されるものを含む、デバイスに接続される他のデバイスにアクセスするためのダイヤラー、このようなファイル上での読み取り動作、書き込み動作及び修正動作を含むメモリに記憶されるファイル、Ｉ／Ｏポート、衛星利用測位システム（「ＧＰＳ」）機能などのデバイスによってサポートされる他の構成要素を含む。

【００２３】

アプリケーション１０５は、回路網１１０を介して、あるいはローカルドライブを使用するＣＤ－ＲＯＭ、または直接接続を介する別のコンピュータからのファイル転送を介してなどなんらかの他のインストール機構を通してデバイスにインストールされる。アプリケーション１０５は、通常、デバイスのリソース１２０の使用を要求する。例えば、アプリケーション１０５の機能が回路網を介して他のデバイスにダイヤルすることである場合、アプリケーションはデバイスのアドレスまたはダイヤル番号が位置するメモリへのアクセスを要求し、メモリから受け取られる番号を使用して別のデバイスに電話をかけるためにデバイスのダイヤラーへのアクセスを要求してもよい。

【００２４】

サーバ１００はデバイス１１５にアプリケーション１０５を転送するために本発明によって使用される１つの機構である。許可リスト（図示せず）は、サーバ１００によって作成され、デバイス１１５で使用するためにアプリケーション１０５と関連付けられてよい。任意の他のデータ転送だけではなく、アプリケーションの安全な伝送のためにも、サーバは当業者に周知であるデジタル署名などの修正検出方法を組み込んでよい。この方法を使用することにより、アプリケーションなどの情報は、それがデバイスによって受信される前に修正されたかどうかを判断するためにデバイスによってチェックできる。さらにこのチェックは、デバイスによって受信された後にも情報に対して修正が発生したかどうかを判断するためにアプリケーションが実行されるたびに行われることもある。

【００２５】

回路網１１０は、ＬＡＮ及び／またはインターネットなどの任意の私設網または公衆網であってよい。回路網１１０は、完全にワイヤレスＲＦネットワークであるか、あるいはワイヤレスＲＦネットワークを組み込んでもよい。さらに、回路網１１０は専用回線、公衆電話交換網を組み込み、データ、音声またはその任意の組み合わせをサポートしてよい。

【００２６】

図２は、本発明の例示的な実施形態においてリソースを有する無線装置を含む無線システムアーキテクチャを示すブロック図である。中央サーバ２０２は、単独でまたは認証サーバと組み合わされてのどちらかでアプリケーションプログラムを定義された一式のプログラミング規定または規約として認証するエンティティである。前述されたように、これらのプログラミング規定は、アプリケーションがクアルコム社（ＱＵＡＬＣＯＭＭ　Ｉｎｃｏｒｐｏｒａｔｅｄ）によって開発されたＢＲＥＷ（商標）ソフトウェアプラットホームで実行するように確立されてよい。

【００２７】

一実施形態では、中央サーバデータベース２０４は、回路網２００の中のそれぞれの無線装置２３０につねにダウンロードされるアプリケーションプログラムごとの識別のレコードと、アプリケーションプログラムをダウンロードした個人のための電子サーバ番号（「ＥＳＮ」）と、そのアプリケーションプログラムを搬送する無線装置２３０に一意のモバイル識別番号（「ＭＩＮ」）から構成される。代わりに、中央サーバデータベース２０４は無線装置モデルの回路網２００内の無線装置２３０、無線網事業者、無線装置２３０が使用される領域、及びどの無線装置２３０がどのアプリケーションプログラムを搬送するのかを識別するために有効な任意の他の情報のレコードを含む。さらに、中央サーバデータベースは、アプリケーションと関連付けられる情報を識別するこの開発者も記憶してよ

い。

【００２８】

中央サーバ２０２は、１つまたは複数のコンピュータサーバ２０６と（好ましくは保護されている）インターネットなどの回路網２０８上で通信する。サーバ２０６は回路網２０８を介してキャリヤネットワーク２１０とも通信する。キャリヤネットワーク２１０はインターネットと（図２の中で２１１として集合的に識別される）ＰＯＴＳ（従来のアナログ電話回線サービス）の両方によってＭＳＣ２１２と通信する。キャリヤネットワーク２１０とＭＳＣ２１２間のインターネット接続２１１はデータを転送し、ＰＯＴＳ２１１は音声情報を転送する。ＭＳＣ２１２は、代わりに複数の基地局（「ＢＴＳ」）２１４に接続される。ＭＳＣ２１２は、（データ転送用の）インターネット２１１と（音声情報用の）ＰＯＴＳ２１１の両方によってＢＴＳに接続される。ＢＴＳ２１４は、ショートメッセージングサービス（「ＳＭＳ」）または他の無線の方法によって無線装置２３０に無線でメッセージを送信する。

【００２９】

前記回路網は、無線装置２３０などのコンピュータデバイスにアプリケーション及び／または許可リストを送信するために使用されてよい。アプリケーションは、ある実施態様では、それを他のアプリケーションと区別するための一意の識別子を有している。アプリケーションと許可リストは、デバイスによる受け取り前に、アプリケーションを実行する前に、及びアプリケーションに対してリソースへのアクセスを許可する前に、修正を検出するためにデジタル署名を組み込んでよい。デジタル署名は、アプリケーションと許可リストに結び付けられ、結び付けられてまたは別々にのどちらかであるが、依然としてアプリケーションと許可リストに関連付けられて、無線装置で記憶されてよい。アプリケーション及び許可リストは、中央サーバから無線装置に、ＭＳＣとＢＴＳを通して無線装置２３０に多様なサーバ２０６の１台に、無線装置２３０に送信される。

【００３０】

図３は、本発明の例示的な実施形態における無線装置の構成要素を示すブロック図である。無線装置３００は制御プログラム３０５、それぞれに許可リスト３２０とデジタル署名３２５が付いたアプリケーション３１０、及びリソース３１５を含む。アプリケーション３１０が様々なタスクを実行してよいことが当業者によって認識されるだろう。さらに、各アプリケーション１１０は、そのアプリケーションと、通常アプリケーションと許可リストごとに一意であるデジタル署名と関連付けられる別個の許可リストを有してよい。３１５に一覧表示されているリソースが多くのデバイスリソースの例であることも当業者によって認識されるだろう。デバイスがアクセスしてよいデバイスの外のリソースを含む、デバイスと関連付けられた多くのリソースがあり、そのアクセスは許可リストに基づきアプリケーションに与えられてよい。

【００３１】

一実施形態では、制御プログラム３０５はリソース３１５へのアクセスを管理するのに役立つためにデバイス上に位置している。制御プログラム３０５の機能は、無線装置のオペレーティングシステムに組み込まれてよいか、あるいはクアルコム社によって開発されたＢＲＥＷ（商標）ＡＰＩなどの別個のＡＰＩであってよい。制御プログラム３０５は、アプリケーションに授けられる特権に基づきアプリケーションへのリソースのアクセスを許可または拒絶してよい。

【００３２】

一実施形態では、これらの特権はアプリケーションに関連付けられた許可リスト３２０を介して決定される。許可リスト３２０はリソース３１５のリスティング、及びアプリケーションがデバイス上の特定のリソース３１５のどれかにアクセスする許可を有しているかどうかの表示を含む。例えば、許可リスト３２０は「マイク」及び「スピーカ」のフィールドを含んでよい。フィールドのそれぞれのフラグの設定が、アプリケーションがマイクにアクセスできるのか、あるいはスピーカにアクセスできるのかを示す。いくつかの例では、マイクフィールドにセットされたフラグは、アプリケーションがマイクにアクセスし

てよいことを示している。フラグがセットされておらず、それによってアクセスを拒絶する場合もある。許可リスト内で可能な限り多くのリソースを明らかにさせ、フラグを、アプリケーションが関連リソースにアクセスできるかどうかを示すそれぞれのものと関連させることが好ましい。

【００３３】

許可リスト３２０はサーバによって作成され、アプリケーションとともに無線装置３００に送信されてよい。しかしながら、許可リストは、アプリケーション開発者または中間権限保持者を含む多くの方法で作成されてよい。これにより、デバイスのリソースの悪用によって影響を受ける可能性があるそれらの権限保持者、エンティティまたは関係者による、デバイスリソースに対するアプリケーションのアクセスの決定が可能になる。その結果、通信事業者などの第三者は、無線装置によって実行され、キャリヤネットワーク上で使用されるアプリケーションと関連付けられた許可を設定することにより無線装置のリソースへのアクセスを管理してよい。

【００３４】

デジタル署名３２５は、アプリケーション３１０及び／または許可リスト３２０が修正されたかどうかを判断するのに役立つ。デジタル署名３２５は、許可リスト、アプリケーション、またはその組み合わせを使用して作成されてよい。デジタル署名、または他のなんらかの修正検出方法が使用されるのが好ましい。許可リストまたはアプリケーションが修正されたかどうかを検出することにより、デバイスは、どの他のプロセスまたはアプリケーションもアプリケーションまたは許可リストを意図的に、または意図的にではなく破壊しないというさらに高い度合いの信頼を有する。これにより、アプリケーションは、それが最初に許可を与えられなかったリソースに対するアクセスを獲得しないようになり、アプリケーションの信頼でき、且つ安全な実行が強化される。

【００３５】

図４は、本発明の例示的な実施形態においてデバイス上でリソースの許可リストを有するアプリケーションを実行するプロセスを示すフローチャートである。許可リストが作成され、アプリケーションと関連付けられる（ステップ４００）。一実施形態では、許可リストは、アプリケーションが実行するデバイスのリソースのフィールドを含む。フィールドは、アプリケーションがフィールドに関連付けられるリソースにアクセスできるようにするために許可が与えられているかどうかに応じてセットされる、またはセットされないフラグを含んでいる。

【００３６】

許可リストは、アプリケーション開発者からのインプットに基づいて作成されてよい。また、許可リストはデバイスのリソース使用を承認することを所望する権限保持者からのインプットに基づいてもよい。無線網の通信事業者などの権限保持者が、回路網でアプリケーションが実行してよいことの範囲を制限することを希望する場合がある。デバイスリソースに対するアプリケーションのアクセスを制限することにより、権限保持者はアプリケーションが実行できることの範囲を制限した。

【００３７】

次にデジタル署名がアプリケーションと許可リストを使用して作成される（ステップ４０５）。デジタル署名の使用は当業者に周知である。これにより、デジタル署名を作成するために使用されるファイルに対する修正の検出が可能になる。デジタル署名はアプリケーションとデジタル署名の両方に適用されるのが好ましい。これによってデバイスはアプリケーションと許可リストが修正されたかどうかをチェックできる。それらが修正されていた場合、デバイスはアプリケーションを実行しないことを選び、このようにして破壊したアプリケーションまたは許可リストがデバイスのリソースにアクセスするのを防いでよい。

【００３８】

許可リストとデジタル署名の作成は、デバイスにアプリケーションをインストールする前にサーバで実行されてよい。

【００３９】
次に、デバイスはアプリケーション、許可リスト、及びデジタル署名を受信する（ステップ４１０）。これは、回路網からこの情報をダウンロードすることによって、あるいはデバイスに直接的に接続される別のコンピュータからの、またはローカルデバイスを介するＣＤ－ＲＯＭなどのなんらかの他の転送機構によるファイル転送を使用してデバイスの上にじかにそれをインストールすることによって達成されてよい。
【００４０】
デバイスは許可リストとアプリケーションと対照してデジタル署名を評価し、デバイスによって受信される前にアプリケーションの修正があったかどうかを判断する（ステップ４１５）。一実施形態では、デバイス上で実行している制御プログラムがこの評価を実行する。
【００４１】
アプリケーション及び／または許可リストが修正されていたと判断されると（ステップ４２０）、処理は終了する（ステップ４５５）。デバイスはこの時点で、アプリケーションと許可リストを削除すること、破壊されたデータとしてそれにタグを付けること、及び／またはアプリケーションと許可リストの創設者に、アプリケーション及び／または許可リストが修正され、別のインストールを開始するところであることを通知することを含む任意の数の機能を実行してよい。
【００４２】
ステップ４２０において、修正が発生しなかったと判断されると、アプリケーションはデバイス上で実行する（ステップ４２５）。この実行は、ユーザによって、または別のアプリケーションまたはプロセスの要求によって要求を開始した結果として発生する場合がある。
【００４３】
次に、アプリケーションはデバイス上でリソースを要求する（ステップ４３０）。この実施形態では、アプリケーションは、デバイス上のリソースが機能を実行することを希望する。例えば、アプリケーションは無線装置で呼を起動することを希望し、デバイスでのダイヤラーのアクセスを要求している。
【００４４】
制御プログラムはアプリケーションと関連付けられた許可リストを評価する（ステップ４３５）。許可リストが、アプリケーションが要求されたリソースにアクセスする特権を有していることを示すと（ステップ４４０）、アプリケーションはリソースへのアクセスを許可される（ステップ４４５）。それからプロセスは終了する（ステップ４５５）。
【００４５】
許可リストが、アプリケーションがステップ４００で要求されたリソースにアクセスする特権を有していないことを示すと、リソースにアクセスするという要求は拒絶される（ステップ４５０）。それからプロセスは終了する（ステップ４５５）。終了する前に、デバイス及び／または制御プログラムは、アプリケーションの実行を終了する、リソースにアクセスしないが実行を続行できるようにする、及び／または創設者または他の権限保持者に、アプリケーションがリソースを要求し、それが拒絶された旨を知らせることを含む複数の処置を講じることができる。
【００４６】
図５は、本発明の例示的な実施形態の様々なデバイスのために同じアプリケーションに複数の許可を割り当てる能力を示すブロック図である。サーバ５００は、複数のデバイス（デバイスＡ５２０とデバイスＢ５３５）によって使用されるアプリケーションを含んでいる。この実施形態では、サーバは１つのデバイスのためにアプリケーションと関連付けられた許可リストを作成する。サーバ２００は、デバイスＡ５２０とデバイスＢ５３５が接続される回路網通信事業者（図示せず）、デバイスの製造メーカ（図示せず）及びアプリケーション開発者（図示せず）などの複数のソースからのインプットを使用してよい。代替実施形態では、許可リストは他のところで作成され、サーバ５００に記憶される。いず

れにしても、許可リストが定義され、特定の回路網に接続される全デバイスなどの、１台の特定のデバイスまたはデバイスのクラスについてアプリケーションが利用できるリソースを示す。

【００４７】

サーバ５００は、それぞれデバイスＡ５２０とデバイスＢ５３５と使用するために、許可リストＡ５１０と許可リストＢ５１５を含む。サーバ５００は、許可リストＡ５１０とともにアプリケーション５０５をデバイスＡ５２０に送信する。一実施形態では、サーバはアプリケーション５０５と許可リストＡ５１０の情報を使用して作成されたデジタル署名５２５を使用する。アプリケーション５０５、許可リストＡ５１０及びデジタル署名５２５は、アプリケーション５０５にデバイスＡのリソース５４５へのアクセスを許可するために図４に関して説明されたようにデバイスＡ５２０によって評価されてよい。

【００４８】

また、サーバは許可リストＢ５１５とともにアプリケーション５０５をデバイスＢ５３５に送信する。一実施形態では、サーバ５００はアプリケーション５０５と許可リストＢ５１５の情報を使用して作成されたデジタル署名５３０を使用する。アプリケーション５０５、許可リストＢ５１５及びデジタル署名５３０は、アプリケーション５０５にデバイスＢのリソース５５５に対するアクセスを許可するために図４に関して説明されたようにデバイスＢ５３５によって評価されてよい。

【００４９】

許可リストＡ５１０と許可リストＢ５１５がその中に設定される様々なリソースアクセス権を有してよいことが当業者によって認識されるだろう。このようなことが当てはまる場合、アプリケーション５０５は、それが同じアプリケーションであるとしても、様々なアプリケーションを基づかせるだろう。さらに、これらのアクセス権はアプリケーションに依存しており、ユーザに基づいていない。

【００５０】

代わりに、本発明の別の実施形態は、アプリケーションと関連付けられる複数の許可リストを有する単一のデバイスを含む。環境に応じて、特定の許可リストは実行のためにアプリケーションとともに使用されてよい。

【００５１】

結論

このようにして、本発明は、実行されるアプリケーションに基づいて１台のデバイスの、または複数のデバイスのリソースへのアクセスを可能にする。ユーザ特権レベルは、ユーザが実行するすべてのアプリケーション全体でのリソースに対するアクセスに影響を及ぼす一方で、ここに説明され、本発明によって請求されるようにリソース割り当ての粒度の増加を実現しない。本発明は、アプリケーション単位でリソースへのアクセスを許可し、このようにしてデバイスのリソース管理にさらに直接的な制御と柔軟性、及びアプリケーションの実行により安全な環境を提供するという追加の改良点を可能にする。

【００５２】

さらに、本発明はデバイスの制御の外の権限保持者が、アプリケーションに基づき、ユーザの特権レベルとは無関係にリソース割り当てに対する決定を下すことができるようにする。これは、アプリケーションがデバイスだけではなく、回路網に接続される他の構成要素にも影響を及ぼす可能性がある回路網環境で特に有効である。

【００５３】

本発明の実現の前記説明は、図解及び説明の目的で提示された。それは網羅的ではなく、発明を開示された正確な形式に制限しない。変型及び変化は前記教示を鑑みて可能であるか、あるいは本発明の実践から獲得されてよい。例えば、説明された実現はソフトウェアを含むが、本発明の一実施形態はハードウェアとソフトウェアの組み合わせあるいはハードウェア単独で実現されてよい。本発明は、オブジェクト指向プログラミングシステムと非オブジェクト指向プログラミングシステムの両方で実現されてよい。さらに、本発明の態様はメモリに記憶されているとして説明されているが、当業者は、これらの態様がハー

ドディスク、フロッピーディスク、またはＣＤ－ＲＯＭのような二次記憶装置、インターネットや他の伝搬媒体からの搬送波、または他の形式のＲＡＭまたはＲＯＭなどの他の種類のコンピュータ読み取り可能媒体に記憶することもできることを理解するだろう。本発明の範囲は請求項及びその同等物によって定義される。

【図面の簡単な説明】

【００５４】

【図１】本発明の例示的な実施形態が実践されてよいシステムアーキテクチャ環境を示すブロック図である。

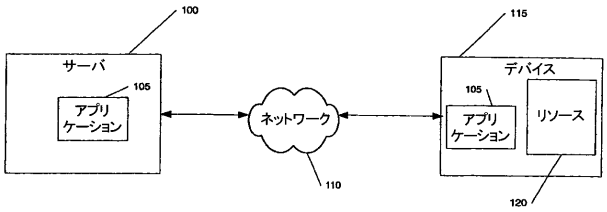
【図２】本発明の例示的な実施形態においてリソースを有する無線装置を含む無線システムアーキテクチャを示すブロック図である。

【図３】本発明の例示的な実施形態における無線装置の構成要素を示すブロック図である。

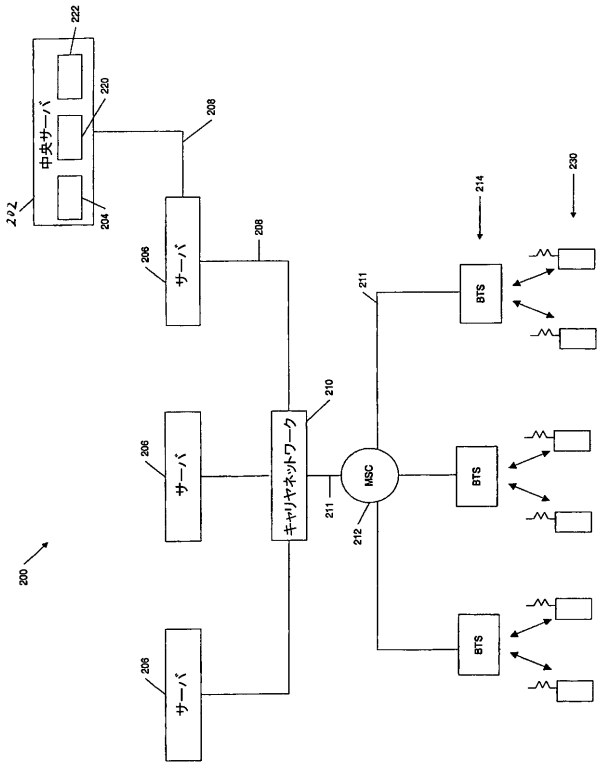
【図４】本発明の例示的な実施形態におけるデバイスでリソースの許可リストを有するアプリケーションを実行するプロセスを示すフローチャートである。

【図５】本発明の例示的な実施形態における様々なデバイスについて同じアプリケーションに複数の許可リストを割り当てる能力を示すブロック図である。

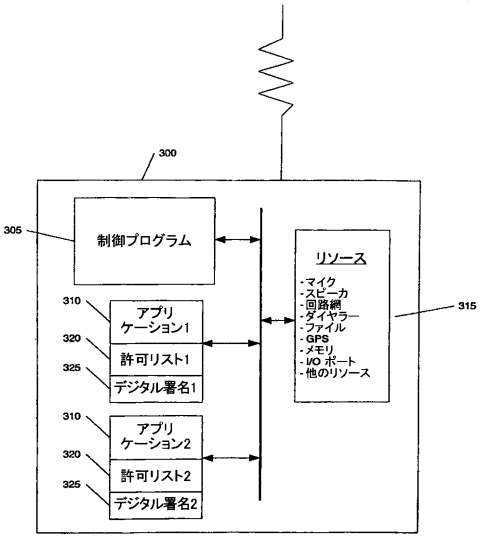
【図１】



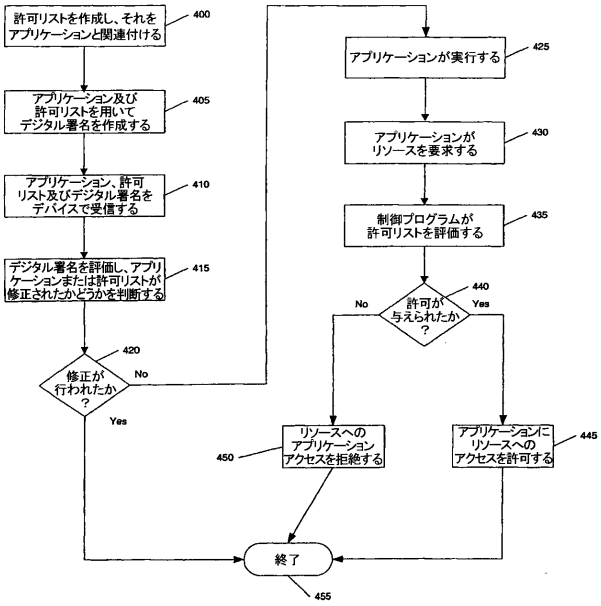
【図２】



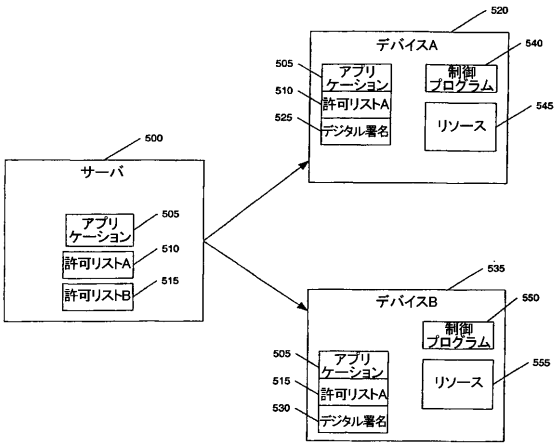
【図３】


300
305
制御プログラム
リソース
- マイク
- スピーカ
- 回路網
- ダイヤラー
- ファイル
- GPS
- メモリ
- I/O ポート
- 他のリソース
315
310
アプリケーション1
320
許可リスト1
325
デジタル署名1
310
アプリケーション2
320
許可リスト2
325
デジタル署名2

【図４】


許可リストを作成し、それをアプリケーションと関連付ける
400
アプリケーション及び許可リストを用いてデジタル署名を作成する
405
アプリケーション、許可リスト及びデジタル署名をデバイスで受信する
410
デジタル署名を評価し、アプリケーションまたは許可リストが修正されたかどうかを判断する
415
修正が行われたか？
420
No
Yes
アプリケーションが実行する
425
アプリケーションがリソースを要求する
430
制御プログラムが許可リストを評価する
435
許可が与えられたか？
440
No
Yes
リソースへのアプリケーションアクセスを拒絶する
450
アプリケーションにリソースへのアクセスを許可する
445
終了
455

【図５】


サーバ
500
アプリケーション
505
許可リストA
510
許可リストB
515
デバイスA
520
505
アプリケーション
510
許可リストA
525
デジタル署名
制御プログラム
540
リソース
545
デバイスB
535
制御プログラム
550
505
アプリケーション
515
許可リストA
530
デジタル署名
リソース
555

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2003 (13.03.2003)

PCT

(10) International Publication Number
WO 03/021467 A1

(51) International Patent Classification⁷: G06F 15/177

(21) International Application Number: PCT/US02/25746

(22) International Filing Date: 13 August 2002 (13.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/312,146 13 August 2001 (13.08.2001) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM, INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPRIGG, Stephen, A.** [US/US]; 12124 Travertine Court, Poway, CA 92064 (US). **LUNDBLADE, Laurence** [US/US]; 3062 Naugatuck, San Diego, CA 92117 (US).

(74) Agents: **WADSWORTH, Philip, R.** et al.; 5775 Morehouse Drive, San Diego, CA 92121 (US).

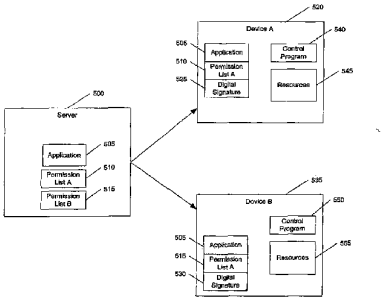
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** USING PERMISSIONS TO ALLOCATE DEVICE RESOURCES TO AN APPLICATION



(57) **Abstract:** Resources to a device (520) are granted access to an application (505) based on privileges associated with the application (505). A permission list (510, 515) is created by a server (500), which indicates what resource (545) the application (505) may access. During application execution when the application (505) requests a resource (545), a control program (540) executing on the device (520) is used to check the permission list (510) associated with the application (505) to determine if the application (505) may access the resource (545).

WO 03/021467 A1

USING PERMISSIONS TO ALLOCATE DEVICE RESOURCES TO AN APPLICATION

Field of the Invention

[0001] The present invention relates to processing of applications for use in a computer device, and more particularly, to the granting of device resources per application.

Background

[0002] Wireless communication has experienced explosive growth in recent years. As consumers and businesses rely more on their wireless devices, such as mobile phones and personal digital assistants (PDAs), wireless service providers, i.e., carriers, strive to provide additional functionality on these wireless devices. This additional functionality will not only increase the demand for wireless devices but also increase the usage among current users.

[0003] The environment of a wireless device creates unique challenges when one considers the execution of application on a wireless device. Methods of downloading the applications and removing the applications need to be developed. In addition, there is a need for security on the wireless device. Security concerns on the wireless device include controlling the environment the best way possible so that an application cannot, intentionally or unintentionally, degrade or corrupt other files on the wireless device or the network on which the wireless device communicates.

[0004] Applications, during execution, require various resources on the device they are executing. These resources include memory (including primary and secondary storage), CPU time and/or access, I/O ports and particularly, the display, speakers, keyboard or keypad and a microphone. If the device is connected to a network, the application may also want to access a device resource to use the network, e.g., a dialer on the device.

[0005] It is desirable control the application's access to the device resources as a security measure to limit any damage an application may have on the device, or other devices connected to the device. This damage may be intended via a virus on the application or may be unintended where the application executes with poorly written

code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.

[0006] Currently, the method of controlling the resources of a device was based on a user privilege level. If the user was a typical user on the system, he or she was provided a level of access to the resources that was anticipated they would need. No matter what applications the user put on or executed on the device, as long as the applications were executing under those user privileges, those applications were all given the same access rights to the device.

[0007] If, for example, the user was a systems administrator or systems engineer on the network the device was connected, that user may be given a higher privilege level, e.g., a "super user," and given more access to the device and network resources. Similarly as with the typical user though, this super user's privileges remained the same across all the applications the super user executed. In this scenario, the same application executed by the typical user may be granted additional resources if executed by the super user.

[0008] However, this practice does not allow for the device to limit a device's resources per application. While the user itself may attempt to limit the application's access to resources, this provided no security to those maintaining the device and the network the device was located. The user could avoid limiting the resources and, therefore, damage the device resources or network resources based on the privilege levels defined to the user.

[0009] Consequently, what is needed in the art is a system and method for protecting the resources of a device and the connected network and also increasing the flexibility of managing the device's resources by allowing the granting rights to the resources per application.

SUMMARY OF THE INVENTION

[0010] Systems and methods consistent with the present invention overcome the shortcomings of existing systems by allowing an application access to a device's resources based on a set of permissions associated with the application.

[0011] In one embodiment, the present invention provides a method for storing an application on a device comprising the steps of receiving an application at the device,

receiving a permission list at the device, wherein the permission list indicates a resource the application may access on the device and storing the application and permission list on the device.

[0012] In another embodiment, the present invention provides a method for allowing access to a device resource comprising the steps of receiving a request for the device resource from an application, evaluating a permission list associated with the application, wherein the permission list indicates the resources the application can access, and granting the application access to the device resource based on the indication in the permission list.

[0013] In yet another embodiment, the present invention provides a method for associating a permission list with an application comprising the steps of receiving an application, receiving at least one or more privilege rights associated with one or more device resources, wherein the privilege right indicates access to the associated device resource, and creating a permission list using the one or more privilege rights and a field associated with each of the one or more device resources, wherein, the permission list is associated with an application and is used to evaluate whether the application may access the one or more device resources.

[0014] Further embodiments of the present invention are also described in the following description and attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention and, together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention. In the drawings:

[0016] Fig. 1 is a block diagram depicting a system architecture environment in which an exemplary embodiment of the present invention may be practiced;

[0017] Fig. 2 is a block diagram depicting a wireless system architecture containing wireless devices having resources in an exemplary embodiment of the present invention;

[0018] Fig. 3 is a block diagram depicting components of a wireless device in an exemplary embodiment of the present invention;

[0019] Fig. 4 is a flowchart depicting the process of executing an application having a permission list for resources on a device in an exemplary embodiment of the present invention; and

[0020] Fig. 5 is a block diagram depicting the ability to assign multiple permission list to the same application for different devices in an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0021] Reference will now be made in detail to the presently exemplary and preferred embodiments of the invention as illustrated in the accompanying drawings, in which like reference characters designate like or corresponding parts throughout the several drawings. The nature, objectives and advantages of the present invention will become more apparent to those skilled in the art after considering the following detailed description in connection with the accompanying drawings.

Introduction

[0022] Systems and methods consistent with the present invention limits an application's access to a device's resources on a computer device. While a privilege level may be defined to the user that limits access to the device's resources, systems and methods consistent with the present invention limit an application's access to the device's resources per application, thus providing increased flexibility and security in managing the device's resources. The device resources include all those components of the device that provides access to or performs a function. These include, but are not limited to, the device's memory, primary and secondary storage, Input/Output ("I/O") ports, network access, dialers, speakers, display, keyboard/keypad, microphones, files and resources whether on the device itself or located across a network that the device can access.

[0023] The present invention associates a permission list with the application. The developer of the application, system administrator, or other authority, such as a carrier

or device manufacturer, may create or provide input to creating this permission list for the application when used on the device. In addition a server may be used to create the permission list based on the input from the authorities, entities or parties involved with executing the application on the device. When the application and permission list is installed on the device, the application when executed will only be allowed access to the resources granted in the permission list. It will be recognized by those skilled in the art that a device may further limit an applications access to resources outside of the permission list. For example, a user may not have rights to a resource on the device that the application is granted permission. This alternative embodiment of the present invention is that the device may provide an additional limitation and, consequently, refuse access to the resource even if the permission has been granted in the permission list based on other privilege levels associated with the device and/or user.

[0024] By associating the resources of a device to an application in a permission list, multiple permission lists may be created for use with the same application. Consequently, on different devices, different resources may be granted access to the same application.

[0025] It will be recognized to those skilled in the art that the forgoing describes an application file type being distributed and executed for simplicity of description. An "application" may also include files having executable content, such as: object code, scripts, java file, a bookmark file (or PQA files), WML scripts, byte code, and perl scripts. In addition, an "application" referred to herein, may also include files that are not executable in nature, such as documents that may need to be opened or other data files that need to be accessed.

[0026] Figure 1 is a block diagram depicting an system architecture environment in which an exemplary embodiment of the present invention may be practiced. A device 115 is capable of executing an application 105. The device 115 may be any computing device, such as a personal computer, a wireless device, including mobile and fixed wireless devices, a combination of computing devices connected together. The device 115 has resources 120 associated with the device 115. These resources include components of the device that provide a function or access to a function within or external to the device 115. Examples of a device's resources 120 include

memory, including primary and secondary storage, a microphone, the network connected to the device, dialers to access other devices connected to the device, including those connected via the network, files stored in memory, including the read, write and modify operations on such files, I/O port, other components supported by the device, such as a Global Positioning Satellite ("GPS") function.

[0027] The application 105 is installed on the device via a network 110 or through some other installation mechanism, such as via a CD-ROM using a local drive or a file transfer from another computer via a direct connection. The application 105 will typically request the use of the device's resources 120. For example, if the application's 105 function is to dial other devices via a network, the application may request access to memory where the device's address or dialing numbers are located, it may also request access to the device's dialer to place a call to another device using the number received from memory.

[0028] A server 100 is one mechanism used by the present invention to transfer the application 105 to the device 115. A permission list (not shown) may be created by the server 100 and associated with the application 105 for use on the device 115. For secure transmission of the application, as well as any other data transfer, the server may incorporate a modification detection technique, such as a digital signature well known to those in the art. By using this technique, information, such as an application, can be check by the device to determine if it was modified prior to being received by the device. Furthermore, this checking can also occur before every execution of the application to determine if any modification occurred to the information even after being received by the device.

[0029] The network 110 may be any private or public network, such as a LAN and/or Internet. The network 110 may also be entirely or incorporate a wireless RF network. In addition, the network 110 may incorporate dedicated lines, a public switched telephone network and support data, voice, or any combination thereof.

[0030] Figure 2 is a block diagram depicting a wireless system architecture containing wireless devices having resources in an exemplary embodiment of the present invention. A central server 202 is an entity that certifies, either by itself or in combination with a certification server, the application programs as compatible with a defined set of programming standards or conventions. As described earlier, these

programming standards may be established so that the application will execute on a BREW™ software platform, developed by QUALCOMM Incorporated.

[0031] In one embodiment, the central server database 204 consists of a record of the identifications for each application program downloaded at any time onto each wireless device 230 in the network 200, an Electronic Service Number ("ESN") for the individual who downloaded the application program, and a Mobile Identification Number ("MIN") unique to the wireless device 230 carrying that application program. Alternatively, the central server database 204 contains records for each wireless device 230 in the network 200 of the wireless device model, wireless network carrier, the region where the wireless device 230 is used, and any other information useful to identify which wireless device 230 are carrying which application programs. In addition, the central server database may also store this developer identifying information associated with an application.

[0032] The central server 202 communicates with one or more computer servers 206, over a network 208, such as the Internet (preferably secured). The servers 206 also communicate with a carrier network 210 via a network 208. The carrier network 210 communicates with the MSC 212 by both the Internet and POTS (plain ordinary telephone system) (collectively identified in Figure 2 as 211). The Internet connection 211 between the carrier network 210 and the MSC 212 transfers data, and the POTS 211 transfers voice information. The MSC 212, in turn, is connected to multiple base stations ("BTS") 214. The MSC 212 is connected to the BTS by both the Internet 211 (for data transfer) and POTS 211 (for voice information). The BTS 214 sends messages wirelessly to the wireless devices 230 by short messaging service ("SMS"), or any other over-the-air method.

[0033] The above network may be used to send an application and/or permission list to a computer device, such as the wireless device 230. The application, in one embodiment, has a unique identifier to distinguish it from other applications. The application and permission list may incorporate a digital signature to detect modifications prior to receipt by the device, prior to executing the application, and prior to granting access to a resource to the application. This digital signature may be bound to the application and permission list and stored on the wireless device either bound or separate, but still associated with, the application and permission list. The

application and permission list are sent to the wireless device from the central server to one of the various servers 206 through the MSC and BTS to the wireless devices 230.

[0034] Figure 3 is a block diagram depicting components of a wireless device in an exemplary embodiment of the present invention. A wireless device 300 contains a control program 305, applications 310 each with a permission list 320 and a digital signature 325 and resources 315. It will be recognized by those skilled in the art the applications 310 may perform different tasks. Furthermore, each application 110 may have a separate permission list associated with that application and a digital signature that will typically be unique for each application and permission list. It will also be recognized by those skilled in the art that the resources listed in 315 are examples of many device resources. There may be many resources associated with a device, including those outside of the device that the device may access, that access may be granted to an application based on the permission list.

[0035] In one embodiment, the control program 305 is located on the device to help manage access to the resources 315. The functions of the control program 305 may be incorporated into the operating system for the wireless device, or may be a separate API, such as the BREW™ API developed by QUALCOMM Incorporate. The control program 305 may grant or deny access of a resource to an application based on the privileges awarded to the application.

[0036] In one embodiment, these privileges are determined via a permission list 320 associated with the application. The permission list 320 contains a listing of the resources 315 and an indication whether the application has permission to access any of the specific resources 315 on the device. For example, the permission list 320 may contain a field for "microphone" and "speaker." The setting of a flag in each of the fields indicates whether the application has access to the microphone or speaker. In some instances, a flag set in the microphone field indicates that the application may access the microphone. In other instances, the flag may not be set thereby denying access. It is preferable to have as many resources as possible accounted for in the permission list and a flag associated with each one indicating whether the application has access to the associated resource or not.

[0037] The permission lists 320 may be created by a server and transmitted along with the application to the wireless device 300. The permission list may be created many ways, though, including by the application developer or intermediate authority. This allows the determination of the application's access to the device's resources by those authorities, entities, or parties that may be affected by the misuse of a device's resource. Consequently, a third party, such as a carrier, may control the access to the wireless device's resources by defining permissions associated with an application that will be executed by the wireless device and used on the carrier network.

[0038] The digital signatures 325 help determine if the application 310 and/or the permission list 320 was modified. The digital signature 325 may be created using the permission list, application, or combination thereof. It is preferable that digital signatures, or some other modification detection technique, be used. By detecting whether the permission list or application was modified, the device has a higher degree of confidence that no other process or application has intention or unintentionally, corrupted the application or permission list. This prevents the application from obtaining access to resources that it was not originally granted permission and increases reliable and safe execution of the application.

[0039] Figure 4 is a flowchart depicting the process of executing an application having a permission list for resources on a device in an exemplary embodiment of the present invention. A permission list is created and associated with an application (Step 400). In one embodiment, the permission list contains the fields of resources of a device on which the application will run. The fields contain flags that are set or not depending on whether the permission is granted to allow the application to access the resource associated with the field.

[0040] The permission list may be created based on input from the application developer. Also, it may be based on input from an authority that desires to approve the resource usage of the device. An authority, such as a carrier in a wireless network, may want to limit the extent of what an application may do on a network. By limiting the application's access to the device's resources, the authority has limited the extent to what an application can do.

[0041] A digital signature is then created using the application and permission list (Step 405). The use of digital signatures is well known to those skilled in the art; it

allows for the detection of any modification to the files used to create the digital signature. While a digital signature is not necessary to implement one embodiment of the present invention, it is preferable that the digital signature be applied to both the application and the digital signature. This allows the device to check whether the application and the permission list were modified. If they were modified, the device may elect not to execute the application and thus prevent a corrupted application or permission list from accessing the device's resources.

[0042] Creating the permission list and the digital signature may be performed at a server prior to installing the application on the device.

[0043] The device then receives the application, permission list and the digital signature (Step 410). This may be performed by downloading this information from a network or by installing it directly onto the device using a file transfer from another computer directly connected to the device or by some other transfer mechanism, such as a CD-ROM via a local drive.

[0044] The device evaluates the digital signature against the permission list and the application to determine if there was a modification of the application prior to being received by the device (Step 415). In one embodiment, the control program executing on the device performs this evaluation.

[0045] If it is determined that the application and/or permission list was modified (Step 420), processing ends (Step 455). The device may perform any number of functions at this point, including removing the application and permission list, tagging it as corrupted data, and/or notifying the originator of the application and permission list that the application and/or permission list was modified and to initiate another installation.

[0046] If in Step 420 it is determined that no modification occurred, the application executes on the device (Step 425). This execution can occur as a result of an initiating request by a user or by the request of another application or process.

[0047] The application then requests a resource on the device (Step 430). In this embodiment, the application wants a resources on the device to perform a function. For example, the application may want to initiate a call on the wireless device and is requesting access to a dialer on the device.

[0048] The control program evaluates the permission list associated with the application. (Step 435). If the permission list indicates that the application has the privilege to access the requested resource (Step 440), the application will be granted access to the resource (Step 445). The process then ends (Step 455)

[0049] If the permission list indicates that the application does not have the privilege to access the requested resource in Step 440, then the request to access the resource is denied (Step 450). The process then ends (Step 455). Prior to ending, the device and/or control program can take several actions, including terminating executing of the application, allowing execution to continue but without access to the resource, and/or notifying the originator or other authority that the application has requested a resource and that it was denied.

[0050] Figure 5 is a block diagram depicting the ability to assign multiple permission list to the same application for different devices in an exemplary embodiment of the present invention. The server 500 contains the application to be used by multiple devices (device A 520 and device B 535). In this embodiment, the server generates the permission list associated with an application for a device. The server 200 may use input from multiple sources, such as the network carriers (not shown) that device A 520 and device B 535 will be connected to, device manufacturers (not shown), and the application developers (not shown). In an alternative embodiment, the permission list is generated elsewhere and stored on the server 500. In any event, a permission list is defined and indicates the resources available to an application for a specific device or class of devices, such as all devices connected to particular network).

[0051] The server 500 contains permission list A 510 and permission list B 515, for use with device A 520 and device B 535, respectively. The server 500 transmits the application 505 along with permission list A 510 to Device A 520. In one embodiment, the server uses a digital signature 525 created using application 505 and permission list A 510 information. The application 505, permission list A 510 and digital signature 525 may be evaluated by device A 520 as described with respect to figure 4 in order to grant application 505 access to device A's resources 545.

[0052] The server also transmits the application 505 along with permission list B 515 to Device B 535. In one embodiment, the server 500 uses a digital signature 530 created using application 505 and permission list B 515 information. The application

505, permission list B 515, and digital signature 530 may be evaluated by device B 535 as described with respect to figure 4 in order to grant application 505 access to device B's resources 555.

[0053] It will be recognized by those skilled in the art that permission list A 510 and permission list B 515 may have different resource access rights defined in them. If such is the case, the application 505 will have different access rights based even though it is the same application. Furthermore, these access rights are application dependent and not based on the user.

[0054] Alternatively, another embodiment of the present invention includes a single device having multiple permission lists associated with the application. Depending on a circumstance, a particular permission list may be used with an application for execution.

CONCLUSION

[0055] In this manner, the present invention allows for access to a device's, or multiple devices', resources based on the application being executed. The user privilege level, while impacting the access to resources across all applications the user executes, does not provide the increased granularity of resource allocation as described herein and claimed by the present invention. The present invention allows for a further refinement of granting access to resources on a per application basis, thus providing more direct control and flexibility in the device's resource management and a more secure environment for application execution.

[0056] Furthermore, the present invention allows for an authority outside of the device's control to make decisions on resource allocation based on the application and independent of the user privilege level. This is particularly useful in network environments where an application may not only impact a device, but other components connected to the network.

[0057] The foregoing description of an implementation of the invention has been presented for purposes of illustration and description. It is not exhaustive and does not limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the invention. For example, the described implementation includes software but one

embodiment of the present invention may be implemented as a combination of hardware and software or in hardware alone. The invention may be implemented with both object-oriented and non-object-oriented programming systems. Additionally, although aspects of the present invention are described as being stored in memory, those skilled in the art will appreciate that these aspects can also be stored on other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or CD-ROM; a carrier wave from the Internet or other propagation medium; or other forms of RAM or ROM. The scope of the invention is defined by the claims and their equivalents.

WHAT IS CLAIMED IS:

CLAIMS

[c1] 1. A method for storing an application on a device, comprising the steps of:

receiving an application at the device;

receiving a permission list at the device, wherein the permission list indicates a resource the application may access on the device; and

storing the application and permission list on the device.

[c2] 2. The method of claim 1, wherein the permission list is created using input from an authority.

[c3] 3. The method of claim 2, wherein the authority is a separate entity from the device.

[c4] 4. The method of claim 1 further comprising the steps of:

executing the application on the device; and

granting the application access to the device's resource based on the permission list.

[c5] 5. The method of claim 1 further comprising the step of receiving a modification detection technique, wherein the digital signature is created based on information from the permission list.

[c6] 6. The method of claim 1, wherein the device is a wireless device.

[c7] 7. A device for executing an application, comprising:

a control program operable to interface between the handset resources and an application,

wherein the control program is operable to receive a request for a device resource from an application and to grant the application access to the device resource based on data contained in a permission list associated with the application.

[c8] 8. The device of claim 7, wherein the device is a wireless device.

[c9] 9. The device of claim 7, wherein the control program is further operable to evaluate a digital signature associated with the permission list.

[c10] 10. A method of allowing access to a device resource, comprising the steps of:

receiving a request for the device resource from an application;

evaluating a permission list associated with the application, wherein the permission list indicates the resources the application can access; and

granting the application access to the device resource based on the indication in the permission list.

[c11] 11. The method of claim 10, further comprising the step of:

receiving a digital signature associated with at least the permission list; and

evaluating the digital signature to determine whether the permission list was modified.

[c12] 12. The method of claim 10, further comprising the steps of:

denying the application access to the device resource based on the indication in the permission list.

[c13] 13. The method of claim 10, wherein the device resource is located on a second device connected to the device.

[c14] 14. The method of claim 10, wherein the permission list was received from a server and the server created the permission list based on requirements from an authority.

[c15] 15. A method of allowing access to a device resource, comprising the steps of:

receiving a request for the device resource from an application;

evaluating a permission list associated with the application, wherein the permission list indicates the resources the application can access; and

denying the application access to the device resource based on the indication in the permission list.

[c16] 16. A method of associating a permission list with an application, comprising the steps of:

receiving an application;

receiving at least one or more privilege rights associated with one or more device resources, wherein the privilege right indicates access to the associated device resource; and

creating a permission list using the one or more privilege rights and a field associated with each of the one or more device resources,

wherein, the permission list is associated with an application and is used to evaluate whether the application may access the one or more device resources.

[c17] 17. The method of claim 16 further comprising the step of transmitting the permission list to a device.

[c18] 18. The method of claim 17 further comprising creating a digital signature using information in the permission list and transmitting the digital signature to the device.

[c19] 19. The method of claim 16 further comprising the steps of:

receiving at least one or more privilege rights associated with one or more device resources for a second device, wherein the privilege right indicates access to the associated second device resource; and

creating a permission list using the one or more privilege rights and a field associated with each of the one or more second device resources,

wherein, the permission list is associated with the application and is used to evaluate whether the application may access the one or more second device resources.

[c20] 20. A system for storing an application on a device, comprising:

means for receiving an application at the device;

means for receiving a permission list at the device, wherein the permission list indicates a resource the application may access on the device; and

means for storing the application and permission list on the device.

[c21] 21. A system for allowing access to a device resource, comprising:

means for receiving a request for the device resource from an application;

means for evaluating a permission list associated with the application, wherein the permission list indicates the resources the application can access; and

means for granting the application access to the device resource based on the indication in the permission list.

[c22] 22. A system for associating a permission list with an application, comprising:

means for receiving an application;

means for receiving at least one or more privilege rights associated with one or more device resources, wherein the privilege right indicates access to the associated device resource; and

means for creating a permission list using the one or more privilege rights and a field associated with each of the one or more device resources,

wherein, the permission list is associated with an application and is used to evaluate whether the application may access the one or more device resources.

[c23] 23. A computer-readable medium containing computer-executable instructions for storing an application on a device that when executed perform a method, comprising the steps of:

receiving an application at the device;

receiving a permission list at the device, wherein the permission list indicates a resource the application may access on the device; and

storing the application and permission list on the device.

[c24] 24. A computer-readable medium containing computer-executable instructions for allowing access to a device resource that when executed perform a method, comprising the steps of:

receiving a request for the device resource from an application;

evaluating a permission list associated with the application, wherein the permission list indicates the resources the application can access; and

granting the application access to the device resource based on the indication in the permission list.

[c25] 25. A computer-readable medium containing computer-executable instructions for associating a permission list with an application that when executed perform a method, comprising the steps of:

receiving an application;

receiving at least one or more privilege rights associated with one or more device resources, wherein the privilege right indicates access to the associated device resource; and

creating a permission list using the one or more privilege rights and a field associated with each of the one or more device resources,

wherein, the permission list is associated with an application and is used to evaluate whether the application may access the one or more device resources.

[c26] 26. The method of claim 5, wherein the modification detection technique is created based on information from the application.

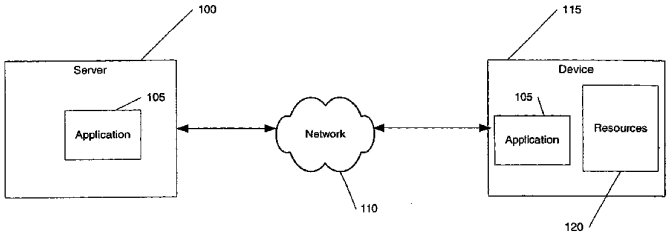
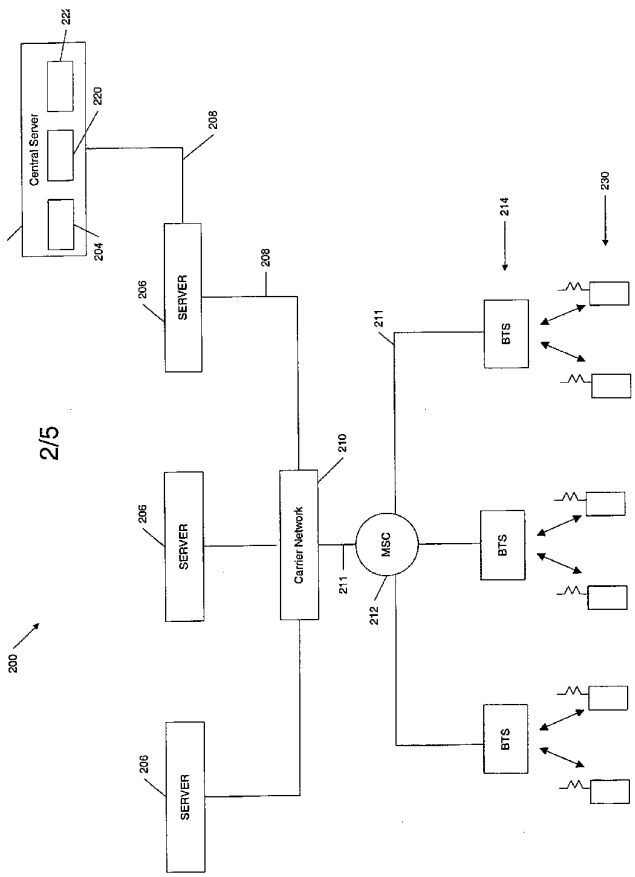

100
Server
105
Application
Network
110
115
Device
105
Application
Resources
120

Fig. 1


Central Server
220
208
204
SERVER
206
208
SERVER
206
210
Carrier Network
211
MSC
212
211
BTS
214
BTS
BTS
230
200

2/5

Fig. 2

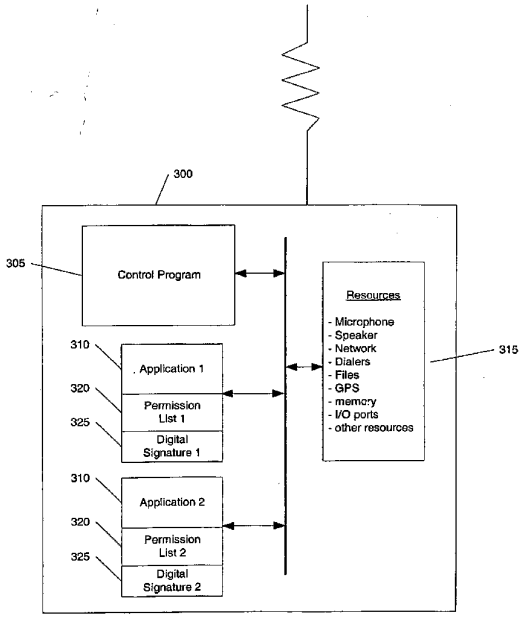

300
305
Control Program
Resources
- Microphone
- Speaker
- Network
- Dialers
- Files
- GPS
- memory
- I/O ports
- other resources
315
310
Application 1
320
Permission List 1
325
Digital Signature 1
310
Application 2
320
Permission List 2
325
Digital Signature 2

Fig. 3

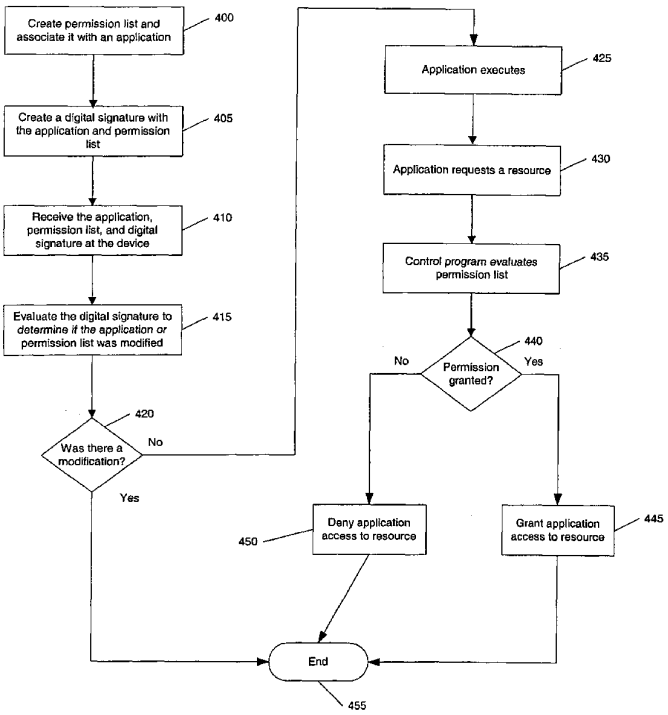

Create permission list and associate it with an application
400
Create a digital signature with the application and permission list
405
Receive the application, permission list, and digital signature at the device
410
Evaluate the digital signature to determine if the application or permission list was modified
415
Was there a modification?
420
No
Yes
Application executes
425
Application requests a resource
430
Control program evaluates permission list
435
Permission granted?
440
No
Yes
Deny application access to resource
450
Grant application access to resource
445
End
455

Fig. 4

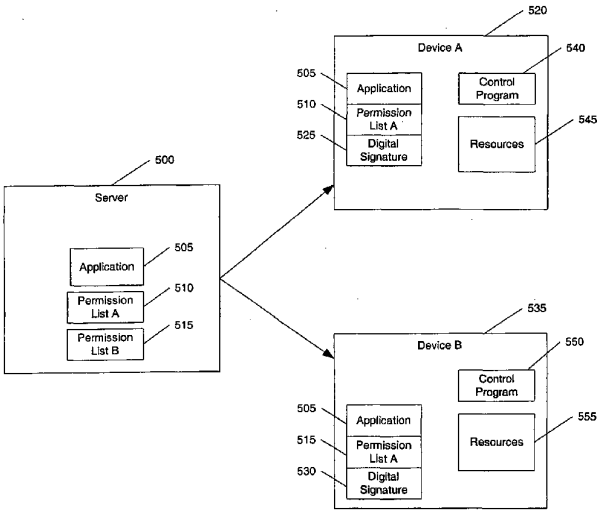

520
Device A
540
505
Application
Control Program
510
Permission List A
545
525
Digital Signature
Resources
500
Server
505
Application
510
Permission List A
515
Permission List B
535
Device B
550
Control Program
505
Application
555
515
Permission List A
Resources
530
Digital Signature

Fig. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/25746

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 15/177
US CL : 709/220
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/220, 227, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,689,708 A (REGNIER et al.) 18 November 1997 (18.11.1997), col. 4, line 1 - col. 8, line 7.	1-26
Y	US 6,105,066 A (HAYES, JR.) 15 August 2000 (15.08.2000), col. 13, line 10 - col. 16, line 54.	1-26
A	US 5,745,879 A (WYMAN) 28 April 1998 (28.04.1998), col. 11, line 38 - col. 14, line 42.	1-26
A	US 6,158,010 A (MORICONI et al.) 05 December 2000 (05.12.2000), see entire document.	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
03 November 2002 (03.11.2002)

Date of mailing of the international search report
06 DEC 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Jason D Cardone
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US02/25746

Continuation of B. FIELDS SEARCHED Item 3:
EAST (BRS)
search terms: PDA, wireless, WML, firewall, network access, download, application, executable

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
フロッピー

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 スプリッグ、スティーブン・エー
アメリカ合衆国、カリフォルニア州 ９２０６４、ポウェイ、トラバーティン・コート １２１２４
(72)発明者 ルンドブレード、ローレンス
アメリカ合衆国、カリフォルニア州 ９２１１７、サン・ディエゴ、ノーガタック・アベニュー ３０６２

Ｆターム(参考) 5B076 FB01
5B085 AE00 AE06