(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2018-536932
(P2018-536932A)
(43)公表日　平成30年12月13日(2018.12.13)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/56	***(2013.01)***	G06F	21/56	360
G06F 21/53	***(2013.01)***	G06F	21/53	

審査請求 未請求　予備審査請求 有　（全 39 頁）

(21)出願番号　特願2018-521349 (P2018-521349)
(86)(22)出願日　平成28年10月11日 (2016.10.11)
(85)翻訳文提出日　平成30年4月25日 (2018.4.25)
(86)国際出願番号　PCT/US2016/056438
(87)国際公開番号　WO2017/083043
(87)国際公開日　平成29年5月18日 (2017.5.18)
(31)優先権主張番号　14/935,522
(32)優先日　平成27年11月9日 (2015.11.9)
(33)優先権主張国　米国 (US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　セイド・アリ・アハマドザデ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】動的ハニーポットシステム

(57)【要約】
様々な実施形態は、挙動解析アルゴリズムおよび動的リソース供給を使用して、悪意のあるアプリケーションによる悪意のある活動をトリガするように構成されたハニーポットシステムを含む。モバイルコンピューティングデバイスであり得るコンピューティングデバイスのプロセッサによって実行される方法は、解析に少なくとも部分的に基づいて、コンピューティングデバイス上で現在実行中のターゲットアプリケーションが潜在的に悪意があるか否かを決定することと、ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、ターゲットアプリケーションのトリガ条件を予測することと、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することと、供給された1つまたは複数のリソースに対応する、ターゲットアプリケーションの活動を監視することと、監視された活動に少なくとも部分的に基づいて、ターゲットアプリケーションが悪意のあるアプリケーションであるか否かを決定することとを含み得る。リソースは、デバイス構成要素(たとえば、ネットワークインターフェース、

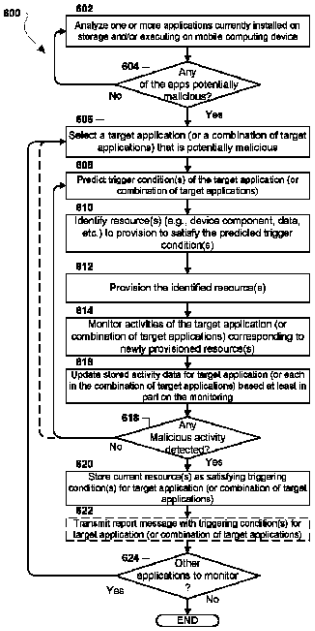


FIG. 6

【特許請求の範囲】
【請求項１】
アプリケーションによる悪意のある活動をトリガするためにハニーポットシステムにおいて実施される方法であって、
ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションのトリガ条件を、コンピューティングデバイスのプロセッサを介して予測するステップと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを前記プロセッサを介して供給するステップと、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップと、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるか否かを、前記プロセッサを介して決定するステップと
を備える、方法。
【請求項２】
前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、同じトリガ条件を有し得るアプリケーションのグループを監視するステップを備える、請求項1に記載の方法。
【請求項３】
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを、前記プロセッサを介して決定するステップと、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションを前記ターゲットアプリケーションとして指定するステップと
をさらに備える、請求項1に記載の方法。
【請求項４】
前記コンピューティングデバイス上で現在実行中の前記アプリケーションが潜在的に悪意があるかどうかを、前記プロセッサを介して決定するステップが、
前記コンピューティングデバイスのリソースにアクセスすることに対応する、前記アプリケーションのパーミッション、および前記アプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して解析するステップ
を備える、請求項3に記載の方法。
【請求項５】
前記1つまたは複数のリソースが、1つまたは複数のデバイス構成要素およびデータのうちの一方または両方を備える、請求項1に記載の方法。
【請求項６】
前記1つまたは複数のデバイス構成要素が、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサからなるグループの少なくとも1つのメンバーを備える、請求項5に記載の方法。
【請求項７】
前記データが、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータからなるグループの少なくとも1つのメンバーを備える、請求項5に記載の方法。
【請求項８】
前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションの前記トリガ条件を、前記プロセッサを介して予測するステップが、
前記ターゲットアプリケーションのパーミッション、前記ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および前記ターゲットアプリケー

ションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項９】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを、前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記ターゲットアプリケーションにとって以前に認識可能であったリソースを、前記プロセッサを介して調整するステップ、および
前記ターゲットアプリケーションにとって以前に認識可能でなかったリソースを、前記ターゲットアプリケーションにとって前記リソースが認識可能になるように、前記プロセッサを介して構成するステップ
のうちの少なくとも1つを備える、請求項1に記載の方法。
【請求項１０】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを、前記プロセッサを介して作成するステップを備え、前記仮想リソースが、前記コンピューティングデバイス内に実際には存在しないかまたは前記コンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す、
請求項1に記載の方法。
【請求項１１】
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、
前記ターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを、前記プロセッサを介して検出するステップ
を備える、請求項1に記載の方法。
【請求項１２】
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるかどうかを前記プロセッサを介して決定するステップが、
前記監視された活動、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項１３】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して供給されたリソースに関する情報を含む、前記ターゲットアプリケーションに対して記憶された活動データを、前記プロセッサを介して更新するステップをさらに備える、請求項1に記載の方法。
【請求項１４】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して、前記ターゲットアプリケーションに対する前記トリガ条件を示す報告メッセージを送信するステップをさらに備える、請求項1に記載の方法。
【請求項１５】
コンピューティングデバイスであって、
メモリと、
前記メモリに結合され、動作を実行するためのプロセッサ実行可能命令を用いて構成されたプロセッサとを備え、前記動作が、
ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションのトリガ条件を予測することと、

前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することと、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を監視することと、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意があるか否かを決定することと
を備える、コンピューティングデバイス。
【請求項１６】
前記ターゲットアプリケーションの活動を監視することが、同じトリガ条件を有し得るアプリケーションのグループを監視することを備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項１７】
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することと、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションを前記ターゲットアプリケーションとして指定することと
をさらに備える動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項１８】
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することが、
前記コンピューティングデバイスのリソースにアクセスすることに対応する、前記1つまたは複数のターゲットアプリケーションのパーミッション、および前記1つまたは複数のターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを解析すること
を備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項17に記載のコンピューティングデバイス。
【請求項１９】
前記1つまたは複数のリソースが、1つまたは複数のデバイス構成要素およびデータのうちの一方または両方を備える、請求項15に記載のコンピューティングデバイス。
【請求項２０】
前記1つまたは複数のデバイス構成要素が、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサからなるグループの少なくとも1つのメンバーを備える、請求項19に記載のコンピューティングデバイス。
【請求項２１】
コンピューティングデバイスがモバイルコンピューティングデバイスであり、前記データが、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータからなるグループの少なくとも1つのメンバーを備える、請求項19に記載のコンピューティングデバイス。
【請求項２２】
前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションの前記トリガ条件を予測することが、
前記ターゲットアプリケーションのパーミッション、前記ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを評価すること
を備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサ

が構成される、請求項15に記載のコンピューティングデバイス。
【請求項２３】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを供給することが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記ターゲットアプリケーションにとって以前に認識可能であったリソースを調整すること、および
前記ターゲットアプリケーションにとって以前に認識可能でなかったリソースを、前記ターゲットアプリケーションにとって前記リソースが認識可能になるように構成することのうちの少なくとも1つを備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２４】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを供給することが、
前記予測されたトリガ条件に少なくとも部分的に基づいて仮想リソースを作成することを備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成され、前記仮想リソースが、前記コンピューティングデバイス内に実際には存在しないかまたは前記コンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す、
請求項15に記載のコンピューティングデバイス。
【請求項２５】
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を監視することが、
前記ターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを検出すること
を備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２６】
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意があるかどうかを決定することが、
前記監視された活動、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データを評価すること
を備えるような動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２７】
前記ターゲットアプリケーションが悪意があるという決定に応答して供給されたリソースに関する情報を含む、前記ターゲットアプリケーションに対して記憶された活動データを更新することをさらに備える動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２８】
前記ターゲットアプリケーションが悪意があるという決定に応答して、前記ターゲットアプリケーションに対する前記トリガ条件を示す報告メッセージを送信することをさらに備える動作を実行するための、プロセッサ実行可能命令を用いて前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２９】
コンピューティングデバイスのプロセッサに動作を実行させるように構成されたプロセッサ実行可能命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作が、
1つまたは複数のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記1つまたは複数のターゲットアプリケーションのトリガ条件を予測することと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソース

を供給することと、
前記供給された1つまたは複数のリソースに対応する、前記1つまたは複数のターゲットアプリケーションの活動を監視することと、
前記監視された活動に少なくとも部分的に基づいて、前記1つまたは複数のターゲットアプリケーションのいずれかが悪意があるか否かを決定することと
を備える、非一時的プロセッサ可読記憶媒体。
【請求項３０】
コンピューティングデバイスであって、
1つまたは複数のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記1つまたは複数のターゲットアプリケーションのトリガ条件を予測するための手段と、
前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給するための手段と、
前記供給された1つまたは複数のリソースに対応する、前記1つまたは複数のターゲットアプリケーションの活動を監視するための手段と、
前記監視された活動に少なくとも部分的に基づいて、前記1つまたは複数のターゲットアプリケーションのいずれかが悪意があるか否かを決定するための手段と
を備える、コンピューティングデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、動的ハニーポットシステムに関する。
【背景技術】
【０００２】
「ハニーポットシステム」(または、単に「ハニーポット」)とは、悪意のあるソフトウェアを発見、識別、および特徴づけるために、そのようなソフトウェアによってプロービングされ、攻撃され、脅かされるように、意図的に配備されるコンピュータシステムである。一般のハニーポットシステムは、制御できない攻撃を悪意のあるソフトウェアがそれ以上起動できるようにすることなく、悪意のあるソフトウェアをシステムの制御される機能性にとどめるようにロックダウンされる。一般のハニーポットシステムは、広範なシステムおよびアプリケーションの監視およびロギングが可能である。ハニーポットシステムは、しばしば、悪意のあるソフトウェアにとってネットワーク(たとえば、ローカルエリアネットワーク(LAN)上で発見可能など)を経由して容易にアクセス可能である。ハニーポットシステムの監視および制御の機能性は、ハニーポットを認識および回避するように構成されたマルウェアによって検出されることを回避するようにうまく偽装される。そのような特性を伴って、ハニーポットシステムは、しばしば、ネットワーク内での攻撃を誘引または隔離するとともに、悪意のあるソフトウェアがどのように動作するのかを示す有用なデータを生成するために使用される。たとえば、ハニーポットシステムは、早期警戒システムの働きをするために、他のデバイスと共有され得るマルウェアによって生じる潜在的な脅威を示すデータを提供することができる。概して、良好なハニーポットシステムは、データ、ネットワーク、およびネットワーク上のコンピューティングデバイスへの実際の損害の恐れなしに、悪意のあるソフトウェアから学習するための制御された機会をもたらす。
【発明の概要】
【課題を解決するための手段】
【０００３】
様々な実施形態は、ハニーポットシステムがアプリケーションによる悪意のある活動をトリガするための方法、デバイス、システム、および非一時的プロセス可読記憶媒体を提供する。様々な実施方法は、ハニーポットシステムを実装するコンピューティングデバイスのプロセッサによって実行され得る。様々な実施形態を実施するコンピューティングデ

バイスは、モバイルコンピューティングデバイスであり得る。様々な実施形態は、1つまたは複数のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、1つまたは複数のターゲットアプリケーションのトリガ条件を予測することを含み得る。様々な実施形態は、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することと、供給された1つまたは複数のリソースに対応する、1つまたは複数のターゲットアプリケーションの活動を監視することとをさらに含み得る。様々な実施形態は、監視された活動に少なくとも部分的に基づいて、1つまたは複数のターゲットアプリケーションが悪意があるか否かを決定することをさらに含み得る。いくつかの実施形態は、コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することと、アプリケーションが潜在的に悪意があるという決定に応答して、アプリケーションを1つまたは複数のターゲットアプリケーションのうちの1つとして指定することとをさらに含み得る。いくつかの実施形態では、コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することは、コンピューティングデバイスのリソースにアクセスすることに対応する、1つまたは複数のターゲットアプリケーションのパーミッションのうちの少なくとも1つを解析することを含み得る。いくつかの実施形態では、コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することは、1つまたは複数のターゲットアプリケーションの以前の活動を示す記憶された活動データを解析することを含み得る。

【０００４】

いくつかの実施形態では、1つまたは複数のリソースは、1つまたは複数のデバイス構成要素およびデータのうちの一方または両方を含み得る。いくつかの実施形態では、1つまたは複数のデバイス構成要素は、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサからなるグループの少なくとも1つのメンバーを含み得る。いくつかの実施形態では、データは、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータからなるグループの少なくとも1つのメンバーを含み得る。

【０００５】

いくつかの実施形態では、1つまたは複数のターゲットアプリケーションのトリガ条件を予測することは、1つまたは複数のターゲットアプリケーションのパーミッション、1つまたは複数のターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および1つまたは複数のターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを評価することを含み得る。

【０００６】

いくつかの実施形態では、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することは、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のターゲットアプリケーションにとって以前に認識可能であったリソースを調整することを含み得る。いくつかの実施形態では、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することは、1つまたは複数のターゲットアプリケーションにとって以前に認識可能でなかったリソースを、1つまたは複数のターゲットアプリケーションにとってリソースが認識可能になるように構成することを含み得る。いくつかの実施形態では、予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給することは、予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを作成することを含み得、仮想リソースは、コンピューティングデバイス内に実際には存在しないかまたはコンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す。

【０００７】

いくつかの実施形態では、供給された1つまたは複数のリソースに対応する、1つまたは

複数のターゲットアプリケーションの活動を監視することは、1つまたは複数のターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを検出することを含み得る。いくつかの実施形態では、監視された活動に少なくとも部分的に基づいて、1つまたは複数のターゲットアプリケーションが悪意があるかどうかを決定することは、監視された活動、および1つまたは複数のターゲットアプリケーションの以前の活動を示す記憶された活動データを評価することを含み得る。

【０００８】

いくつかの実施形態は、1つまたは複数のターゲットアプリケーションの監視された活動が1つまたは複数のターゲットアプリケーションが悪意があるという決定をもたらすときに供給されたリソースに関する情報を含む、1つまたは複数のターゲットアプリケーションに対して記憶された活動データを更新することをさらに含み得る。いくつかの実施形態は、1つまたは複数のターゲットアプリケーションが悪意があるという決定に応答して、1つまたは複数のターゲットアプリケーションに対するトリガ条件を示す報告メッセージを送信することをさらに含み得る。

【０００９】

さらなる実施形態は、上記で説明した方法の動作を実行するためのプロセッサ実行可能命令を用いて構成されたコンピューティングデバイスを含む。さらなる実施形態は、上記で説明した方法の動作をコンピューティングデバイスに実行させるように構成されたプロセッサ実行可能命令が記憶された非一時的プロセッサ可読媒体を含む。さらなる実施形態は、上記で説明した方法の動作を実行するためのプロセッサ実行可能命令を用いて構成されたコンピューティングデバイスを含むシステムを含む。

【００１０】

本明細書に組み込まれ、本明細書の一部を構成する添付図面は、様々な実装形態を示し、上記の一般的な説明および下記の詳細な説明とともに、特許請求の範囲の特徴を説明するのに役立つ。

【図面の簡単な説明】

【００１１】

【図１】様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイスを含むシステム図である。

【図２】様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイスのリソースに関連する動的データを示す図である。

【図３】様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイスのリソースに関連する動的データを示す図である。

【図４】様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイスのリソースに関連する動的データを示す図である。

【図５】様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイスのリソースに関連する動的データを示す図である。

【図６】様々な実装形態による、アプリケーションによる悪意のある活動を誘引または刺激するためのリソースを動的に供給するための動作を実行すべきコンピューティングデバイスハニーポットのための方法を示すプロセスフロー図である。

【図７】一実装形態における使用に適したモバイルコンピューティングデバイスの構成要素ブロック図である。

【発明を実施するための形態】

【００１２】

様々な実施形態および実装形態が、添付の図面を参照しながら詳細に説明される。可能な場合はいつでも、同一または同様の部分を指すために図面全体にわたって同じ参照番号が使用される。特定の例および実装形態になされる参照は説明の目的のためであり、実装形態の範囲および特許請求の範囲を限定するものではない。

【００１３】

様々な実施形態および実装形態は、悪意のある挙動を引き出すように、予測された方法

でリソースおよび機能性の様々な組合せをアプリケーションに提示することによって、プロセッサ上で実行中のアプリケーションの悪意のある挙動を識別するように構成されている、コンピューティングデバイス内でインスタンス化される動的ハニーポットシステムを含む。コンピューティングデバイスは、限定はしないが、モバイルコンピューティングデバイスであり得る。潜在的に悪意のあるアプリケーションごとに、ハニーポットシステムは、アプリケーションの活動および状態を観測し得、観測されたデータを使用して解析を実行し得る。ハニーポットシステムは、潜在的に悪意のある各アプリケーションに悪意のあるアクションを実行させるのに必要とされる可能性が高い、利用可能なデバイス機能性およびシステムの動作状態などの状況を予測し得る。ハニーポットシステムは、それに応じて、様々なデバイス構成要素(たとえば、センサ、ネットワークインターフェース、メモリロケーション、プロセッサ、無線など)および/またはデータ(たとえば、連絡先リスト、ファイル、メッセージコンテンツなど)をアクセス可能または認識可能にさせることなどによってリソースを供給し得る。ハニーポットシステムは、潜在的に悪意のあるアプリケーションを監視し続けてよく、潜在的に悪意のあるアプリケーションが悪意のある活動を提示するまで、利用可能なリソースを反復的に調整してよい。スマートフォンなどのモバイルコンピューティングデバイスにおいて一般的であるデバイス構成要素をアクセス可能または認識可能にさせることによって、様々な実施形態および実装形態は、モバイルコンピューティングデバイスの一般のファイルおよび機能を悪意のある目的のために悪用し得るアプリケーションを評価するための、モバイルハニーポットシステムとして機能し得る。

【００１４】

「コンピューティングデバイス」という用語は、本明細書では少なくともプロセッサを装備した電子デバイスを指すために使用される。コンピューティングデバイスの例は、モバイルコンピューティングデバイス(たとえば、セルラー電話、ウェアラブルデバイス、スマートフォン、ウェブパッド、タブレットコンピュータ、インターネット対応セルラー電話、Wi-Fi対応電子デバイス、携帯情報端末(PDA)、ラップトップコンピュータなど)、パーソナルコンピュータ、およびサーバコンピューティングデバイスを含み得る。たとえば、モバイルコンピューティングデバイスは、異種または同種のマルチコアスマートフォンを含んでよい。様々な実装形態では、コンピューティングデバイスは、メモリおよび/またはストレージ、ならびにワイドエリアネットワーク(WAN)接続(たとえば、セルラーネットワーク接続など)および/またはローカルエリアネットワーク(LAN)接続(たとえば、Wi-Fiルータを経由したインターネットへの有線/ワイヤレスの接続など)を確立するように構成されたネットワークトランシーバおよびアンテナなどのネットワーキング機能とともに構成され得る。

【００１５】

「悪意のある挙動」、「悪意のある活動」、および「悪意のあるアクション」という用語は、コンピューティングデバイスおよび/または関連するユーザにとって攻撃、漏洩、障害、データ損失、および/または他の不要もしくは不正な状態をもたらし得る、コンピューティングデバイス上で実行中のアプリケーション(たとえば、マルウェア)による任意の1つまたは複数の動作を指すために、本明細書で互換的に使用される。たとえば、悪意のある活動は、不正もしくは不要なデータアクセス(たとえば、読み取ること、コピーすることなど)、データ送信(たとえば、リモートデバイスに転送される機密データなど)、および/またはデータ変更(たとえば、改名すること、書き込むこと、上書きすること、削除すること、破損させること、暗号化すること、解読すること、パーミッションを変更することなど)を含み得る。別の例として、悪意のある活動は、システムまたはサブシステムをリブートすること、プロセッサに過負荷をかけること、センサを非活動化させること、記憶デバイスを切断することなどの、不正または不要なデバイス構成要素変更を含み得る。悪意のある活動は、組み合わせて実行されたときにのみ不要または不正な結果を引き起こす、複数の動作を含み得る。たとえば、悪意のある活動は、機密データをコピーするための、通常は良性の要求と組み合わせて、結合された外部記憶デバイスの、通常は良性

のポールを含み得る。

【００１６】

典型的なハニーポットシステムの様々なタイプがある。「アクティブ」ハニーポットシステムは、悪意のあるアプリケーションから検出される脅威を監視するとともにそうした脅威に応答するように構成され得る。「パッシブ」ハニーポットシステムは、悪用および悪意のある活動の解析のための監視データ(たとえば、検出されたアプリケーションプログラミングインターフェース(API)呼出しなど)を単に収集するように構成され得る。いくつかのハニーポットシステムは、悪意のある特定のアプリケーションに関係し得るコンピューティングシステムの機能性へのアクセスのみを提供するように設計されている。たとえば、ハニーポットシステムは、完全に機能するシステムを提供することなく、既知の脆弱なサブシステムを再作成することによって、既知のマルウェアアプリによる活動をターゲットにし得る。そのようなハニーポットシステム技法は、悪意のあるアプリケーションの相互作用を、悪意のある特定のアプリケーションによって脆弱であるものと知られているサブシステムに限定してよい。他のハニーポットシステム技法は、大きいオーバーヘッドを犠牲にして通常の特性およびリソースを模倣することなどによって完全に機能するシステムを再作成する、高い相互作用設計を採用し得る。

【００１７】

悪意のある活動を評価するのに適した環境を提供するために必要とされるリソースに起因して、ハニーポットシステムは、しばしば、動作条件および/またはデバイス構成要素を定義しているサーバまたは静的コンピューティングシステムの中に実装される。いくつかのハニーポットシステムはまた、モバイルコンピューティングシステムの中に実装されてよいが、しばしば、モバイルシステムの限定された処理機能、メモリ、およびパワーに起因してもっと小さい範囲しか有しない。たとえば、広範なまたは絶え間ない監視動作は、限定されたバッテリー寿命および処理馬力に起因して、モバイルデバイス上で時間の長い期間にわたって達成することがより困難であり得る。

【００１８】

悪意のあるいくつかの精巧なアプリケーションは、コンピューティングシステムをいつ攻撃すべきかを選択的に決めることができるとともに、攻撃において使用すべき様々なリソースを決定することができる。たとえば、マルウェアアプリは、マルウェアアプリがシステム上にダウンロードおよびインストールされたずっと後まで、悪意のある活動(たとえば、セキュアなデータをモバイル電話から送信することなど)を見せないことがある。別の例として、マルウェアアプリは、実行時間の大部分にわたって無害の動作を実行することがあり、ホストコンピューティングシステムのいくつかの動作条件が満たされるときにのみ、悪意のある活動(たとえば、ファイルを削除することなど)に関与する。悪意のある活動がいつ行われ得るのか、またはどのリソースが悪意のある活動のために使用され得るのかを知らないと、典型的なハニーポットシステムは、アプリケーション活動の、コストがかかる絶え間ない監視を採用するように強制される。

【００１９】

モバイルデバイスは、しばしば、悪意のある活動のために使用され得る幅広いデバイス構成要素、機能性、およびシステム状態を含むので、悪意のあるいくつかのアプリケーションの精巧な性質は、モバイルコンピューティングデバイス上に実装されるハニーポットシステムにとって追加として問題となる。たとえば、モバイル電話上のマルウェアアプリは、複数の通信インターフェース、幅広いデバイス構成および動作シナリオ(たとえば、利用可能な無線アクセス技術、チャネル条件)、様々なユーザ挙動(たとえば、入力を与えることなど)、ならびに同時に実行中のアプリケーションの任意の組合せを利用し得、または別の方法でそれらに依拠し得る。悪意のあるアプリケーションは、いくつかのリソースを利用するように設計されてよく、その結果、コンピューティングデバイスの動作条件の極めて特定かつ複雑なセットが所与の時間において満足されるときにのみ、悪意のある活動がトリガされる。たとえば、マルウェアは、悪意のある活動を起動すべきかどうかを決定するために、1つまたは複数の他の要因と組み合わせてスマートフォンの現在位置を

使用し得る。モバイルシステムにおける悪意のある活動に対する極めて多くのオプションが、そのような悪意のある活動を誘引またはトリガできるハニーポットの設計を複雑にしており、これらの一般的なモバイルコンピューティング環境を特に脆弱なままにしている。

【００２０】

様々な実施形態は、因果解析および/または挙動予測を使用して、悪意のあるアプリケーションによる悪意のある活動をトリガするための方法、デバイス、および非一時的プロセス可読記憶媒体を提供する。概して、コンピューティングデバイス(たとえば、図1に示すモバイルコンピューティングデバイス102)は、ハニーポットシステムとして動作するように構成され得る。例示的な一実装形態では、ハニーポットシステムは、ネットワーク上で認識可能(たとえば、発見可能)であるように構成されるとともに、外部エンティティ/ユーザなどにとって利用可能ないくつかの制御された機能性を有する、スマートフォンであってよい。ハニーポットシステムは、コンピューティングデバイスのプロセッサ(たとえば、図1におけるプロセッサ121)を介して実行している様々なアプリケーションの様々な特性、事前の活動、およびパーミッションを解析し得る。ハニーポットシステムはまた、アプリケーションのすべての要求、メッセージ、ポーリング、コピー/書込み、アクセス、および他の活動を監視し得る。そのような解析および監視に少なくとも部分的に基づいて、ハニーポットシステムは、アプリケーションの悪意のある活動をトリガし得る条件(たとえば、コンピューティングデバイスのいくつかのデバイス構成要素の存在、システム状態、および/または他の動作条件)を予測し得る。ハニーポットシステムは、次いで、新たなリソースを供給し得、アプリケーションが悪意をもって行動し始めるか否かを決定するために監視を継続し得る。ハニーポットシステムは、悪意のあるアプリケーションを首尾よく露呈させるリソースの組合せを見つけるために、そのような動作を反復的に継続してよい。挙動解析に少なくとも部分的に基づくそのような予測を用いて、以前に知られていない脅威および脆弱性が、低減されたシステム監視および検出オーバーヘッドを伴って識別され得る。

【００２１】

いくつかの実装形態では、ハニーポットシステムは、潜在的に悪意のあるアプリケーションを識別するために、機械学習アルゴリズム、およびアプリケーションの履歴的活動データを使用し得る。いくつかの実装形態では、アプリケーションが悪意のある活動を起動することが可能であるかまたは起動するように配置されている確率の計算に少なくとも部分的に基づいて、アプリケーションは、潜在的に悪意があるものとして識別され得る。たとえば、ハニーポットシステムは、アプリケーションの現在のパーミッションおよびアプリケーションによって以前に観測されたアクション(たとえば、データアクセス、接続要求など)の解析に少なくとも部分的に基づいて、確率値を計算し得る。そのような計算された確率値は、既定のしきい値、または観測されたアクションが、疑わしいかもしくは潜在的に悪意のある活動に整合することに少なくとも部分的に基づいて、経時的に更新される動的なしきい値などの、しきい値と比較され得る。

【００２２】

潜在的に悪意のあるアプリケーションの活動の解析を使用して、ハニーポットシステムは、潜在的に悪意のあるアプリケーションが、悪意のある活動を提示する前に、モバイルコンピューティングデバイスの中に存在することを必要とする条件(すなわち、トリガ条件)を予測し得る。たとえば、ハニーポットシステムは、潜在的に悪意のあるアプリケーションが待っていることがあるネットワーキング状態(たとえば、信号強度、帯域幅、および接続タイプ)を推定し得る。そのような推定されるネットワーキング状態は、異なるネットワークインターフェースが利用可能であったとき、または利用可能でなかったときなどの、コンピューティングデバイスの以前の動作条件中に記録された潜在的に悪意のあるアプリケーションのアクションに、少なくとも部分的に基づいてよい。予測されたトリガ条件は、潜在的に悪意のあるアプリケーションを動作するように刺激するために利用可能であるべき正確なリソース(たとえば、活動化されたデバイス構成要素、利用可能なネ

ットワークインターフェースなど)を、ハニーポットシステムが識別することを可能にし得る。さらに、予測されたトリガ条件はまた、潜在的に悪意のあるアプリケーションを適切にだまして動作させるために必要とされ得る間接条件(たとえば、システム状態、ロケーション、構成パラメータなど)を、ハニーポットシステムが識別することを可能にし得る。

【００２３】

ハニーポットシステムは、デバイス構成要素を活動化させることおよび/または記憶されたデータの値を調整することなどによって、識別されたリソースを供給し得る。概して、供給することは、モバイルコンピューティングデバイスの様々な機能性を非活動化させること、活動化させること、調整すること、構成すること、隠すこと、見せること、作成すること、削除すること、および/または別の方法で利用可能(または、利用不可能)にさせることを含み得る。供給されるリソースは、ハニーポットシステムの他の要素から隔離された(たとえば、サンドボックス化された)現実のリソースであってよく、またはハニーポットシステムによってエミュレートされてよい。供給されるリソースは、アプリケーションのグループまで、または潜在的に悪意のあるアプリケーションのみまで、システム全体に認識可能にされてよい。

【００２４】

いくつかの実装形態では、供給されるリソースまたは他の関連するリソースは、ハニーポットシステムの性質を潜在的に悪意のあるアプリケーションから隠すように構成され得る。たとえば、ハニーポットシステムが移動している(または、移動をシミュレートしている)とき、偽のWi-Fiアクセスポイントは、行き来しているものとして識別され得る。別の例として、ハニーポットシステムは、実際のユーザのスマートフォン上の現実の連絡先リストに類似して見えるように、多様な市外局番を有する偽の連絡先リストを作成してよい。

【００２５】

様々な実装形態では、供給され得るリソースは、ハニーポットシステムを提供するコンピューティングデバイスの仕様によって決定されてもされなくてもよい。たとえば、いくつかの実装形態では、ハニーポットシステムは、実際には存在しないかまたはコンピューティングデバイスにとって利用可能でない機能性(たとえば、全地球測位システム(GPS)受信機、加速度計センサ、4G接続性など)を、調整および/またはエミュレートするように構成され得る。

【００２６】

ハニーポットシステムは、供給される任意のリソースに対応する、潜在的に悪意のあるアプリケーションの活動を、密に監視および解析し得る。たとえば、ハニーポットシステムは、潜在的に悪意のあるアプリケーションからの発信メッセージおよび/またはアプリケーションプログラミングインターフェース(API)呼出しを傍受し得る。

【００２７】

潜在的に悪意のあるアプリケーションが、供給されるリソースに悪意のある活動を伴って応答しない場合、ハニーポットシステムは、トリガ条件を予測すること、および後続の監視/予測に少なくとも部分的に基づいて新たな(または、調整された)リソースを供給することを、反復的に継続してよい。たとえば、潜在的に悪意のあるアプリケーションが使用しようと待っている可能性が高いリソースを識別するために、潜在的に悪意のあるアプリケーションの活動の新たな観測値が解析器に転送されてよい。別の例として、潜在的に悪意のあるアプリケーションからの発信メッセージおよび/またはアプリケーションプログラミングインターフェース(API)呼出しの傍受に応答して、ハニーポットシステムは、誤った情報(たとえば、利用可能なネットワーキング接続、連絡先リストデータ、送信確認など)を用いて応答してよい。そのような反復プロセスは、悪意のある活動が検出されるかまたは完全に解析されるまで、ハニーポットシステムのリソースを潜在的に悪意のあるアプリケーションに継続的に適合させてよい。

【００２８】

上記で説明したように、様々な実施形態のハニーポットシステムは、スマートフォンなどのモバイルコンピューティングデバイスのファイル、構成要素、および機能を悪用し得るモバイルアプリケーションを評価する際に特に有用である。この理由で、様々な実施形態および実装形態が、実施ハニーポットシステムを実施するのに適したコンピューティングデバイスの一例として、モバイルコンピューティングデバイスを参照しながら説明される。しかしながら、モバイルコンピューティングデバイスへの参照は例示するためのものであり、特許請求の範囲を限定するものではない。

【００２９】

以下のことは、様々な実装形態による、モバイルコンピューティングデバイス(たとえば、スマートフォン)上で実行中のハニーポットシステムの非限定的な例示である。ハニーポットシステムがウクライナに配置されるときにしか悪意のある活動(たとえば、パスワードを漏洩することなど)を実行しないように、特定のアプリケーションが設計されることがある。言い換えれば、ウクライナに配置される前、アプリケーションは悪意のあるいかなる活動も提示しない。ハニーポットシステムは、アプリケーションが、記憶されたデータ、ワイドエリアネットワーク(WAN)接続、およびロケーションサービスにアクセスするためのパーミッションを有することを観測し得る。リソースは、実際のリソース、またはハニーポットシステムによって作成された仮想リソースの、任意の組合せであってよい。ハニーポットシステムは、モバイルコンピューティングデバイスがカリフォルニアのサンフランシスコにあることを示す、偽のGPS座標を提供し得る。ある期間にわたって、ハニーポットシステムは、アプリケーションが周期的にロケーションデータ(たとえば、GPSデータ)を読み取るかまたはロケーションデータへのアクセスを有するが、限定されるかまたは良性のネットワーク活動しか提示しないことを観測し得る。

【００３０】

パーミッションに少なくとも部分的に基づいて、ハニーポットシステムは、情報を漏洩する高い確率をアプリケーションが有すると結論付けてよい。ハニーポットシステムは、悪意のある活動をトリガするために特定のロケーションをアプリケーションが必要とし得ることを予測し得る。それに応答して、ハニーポットシステムは、世界中の異なる場所におけるロケーションを示すための様々な偽のロケーションデータを生成し得る。ウクライナ内の現在位置を示すロケーションデータを生成すると、アプリケーションはトリガされ得、機密情報を漏洩するための動作の実行を開始し得、したがって、アプリケーションが悪意があることを確証し得る。ハニーポットシステムは、必要な場合にそのような漏洩を阻止してよく、特定のアプリケーションに対する正確なトリガ条件として利用可能な条件/リソースを記録し得る。

【００３１】

いくつかの実装形態では、ハニーポットシステムは、遅延したまたは特定のトリガを有する悪意のある活動を検出するために、ある時間期間にわたってすべてのアプリケーションの履歴および状態を維持し得る。いくつかの実装形態では、潜在的に悪意のあるアプリケーションは、後続の活動に少なくとも部分的に基づいて、悪意がないものと決定され得る。

【００３２】

様々な実装形態では、ハニーポットシステムによって供給され得るリソースは、様々なデバイス構成要素(および/または、関連する設定)およびデータ(および/または、関連する設定)を含み得る。たとえば、リソースは、インストール済みアプリケーション(たとえば、ウィルス保護ソフトウェア、ファイアウォールソフトウェアなど)、オペレーティングシステム(たとえば、Android、Windowsなど)、ネットワークインターフェース(たとえば、トランシーバ、アンテナ、コントローラなどの、様々なネットワーク、ローカルエリアネットワーク、および/またはワイドエリアネットワークを介した通信を確立するためのハードウェアおよび/またはソフトウェアなど)、無線アクセス技術(RAT)(たとえば、ロングタームエボリューション(LTE)、3G、2G、Wi-Fi、Bluetooth(登録商標)など)、処理ユニット(たとえば、デジタル信号プロセッサ(DSP)、中央処理ユニット(CPU)、グラフィッ

クス処理ユニット(GPU)など)、データ記憶ユニット(たとえば、メモリ、キャッシュ、ハードドライブなど)、結合されたデバイス(たとえば、ユニバーサルシリアルバス(USB)接続を介して接続された外部ハードドライブ、USBサムドライブ、セキュアデジタル(SD)カードなど)、出力ユニット(たとえば、ディスプレイ、スピーカなど)、入力ユニット(たとえば、キーボード、タッチスクリーンなど)、および/またはセンサ(たとえば、カメラ、マイクロフォン、加速度計、ジャイロスコープなど)のうちの、1つまたは複数の任意の組合せを含み得る。別の例として、リソースは、連絡先リスト、記憶されたファイル、セキュア情報または個人情報(たとえば、ピクチャ、ビデオ、セーブされたパスワード、メッセージコンテンツ、電子メールなど)、ネットワーキング状態データ(たとえば、アクセスポイント名(APN)、インターネットプロトコル(IP)アドレス、ラウンドトリップ時間(RTT)、利用可能なスループット、オープン利用可能ポート、バックホール情報、モビリティ、信号強度、アップロード/ダウンロードレート、帯域幅など)、加入情報(たとえば、利用可能な加入者識別情報/識別モジュール(SIM)カード、パブリックランドモバイルネットワーク(PLMN)、モバイルネットワーク事業者(MNO)、トラッキングエリアなど)、ロケーション情報(たとえば、全地球測位システム(GPS)利用可能性、位置座標など)、システム情報(たとえば、利用可能なメモリ、中央処理ユニット(CPU)情報、CPU使用量、動作中のサービス、活動化されたスクリーン/ディスプレイ、利用可能なタッチ機能など)、既知の脆弱性情報(たとえば、OSバージョン、OSインストール済みパッチなどの、オペレーティングシステム(OS)情報、セキュアソケットレイヤ(SSL)バージョン、SSL実装などの、セキュリティ情報、輸出レベルAESなどの弱いかまたは古くなったセキュリティアルゴリズムなど)、およびセンサデータ(たとえば、センサ利用可能性、センサデータなど)のうちの、1つまたは複数の任意の組合せを含むデータであってよい。

【００３３】

いくつかの実装形態では、ハニーポットシステムは、因果解析動作および/または挙動解析動作、監視、ならびに/あるいはモバイルコンピューティングデバイス内の活動を検出、制御、および/または予測するための他の動作を実行するために、様々なモジュール、構成要素、命令、動作、回路構成、および/またはルーチンを利用し得る。いくつかの実装形態では、ハニーポットシステムは、ハニーポットシステム制御モジュール(たとえば、図1におけるハニーポットシステム制御モジュール140)を介して可能にされてよい。たとえば、そのようなハニーポットシステム制御モジュールは、システムレベルリソースへのアクセスおよび/またはモバイルコンピューティングデバイス内でのシグナリングとともに構成されている、OSサービス、ソフトウェア、回路構成、モジュール、ルーチンなどであり得る。いくつかの実装形態では、ハニーポットシステムは、Qualcomm IncorporatedからのQualcomm Snapdragon Smart Protectなどのリアルタイム解析プラットフォームを使用して、潜在的に悪意のあるアプリケーションを識別し得る。

【００３４】

様々な実施形態は、制御されたモバイル環境においてアプリケーションの隠された悪意のある活動をトリガまたは誘致するために、挙動解析および予測を使用する動的ハニーポットシステムを提供する。詳細には、開示する様々な実装形態は、潜在的に悪意のあるアプリケーションによって必要とされるトリガ条件を反復的に予測し、悪意のある活動が観測されるまで、利用可能なリソースを継続的に調整する。様々な実装形態が既定のトリガ条件を必要とせず、代わりに、アプリケーション挙動および特性を解析して、テストにおいて使用すべきリソースを動的に識別するので、これらの新規の技法は、未知のマルウェアの脆弱性、または他の脅威を検出するのに適する。そのような技法はまた、監視コストおよび検出コストを低減し得る。

【００３５】

様々な実施形態は、マルウェアを識別するためにアプリケーションを監視する既存の技法とは異なる。たとえば、いくつかの既存の技法は、既知のマルウェアによって予期され得るデバイス入力(たとえば、ダミーキーストローク)を単に提供するが、モバイルコンピューティングデバイス動作条件または環境を動的に変更しない。そのような既存の技法は

予測的でなく、アプリケーションの観測された悪意のない活動に少なくとも部分的に基づいて、異なるリソースを反復的に供給しない。様々な実装形態は、未確認または未知の、悪意のあるソフトウェアの悪意のある活動を引き起こすために、モバイルコンピューティングデバイスの状態情報およびシステムリソース情報を使用し得、したがって、既知のマルウェアを活動化させる自明型入力メカニズムを使用することに依拠しない。

【００３６】

他の既存の技法とは異なり、様々な実装形態は、ソフトウェアまたはコンピューティングシステムの静的な構成をまったく採用しない。たとえば、本明細書で開示する様々な実装形態は、異なるオペレーティングシステムまたはアーキテクチャのための既定のソフトウェアインストール(または、システムイメージ)のセットを反復的に実施しない。代わりに、様々な実装形態は、潜在的に悪意のあるアプリケーションの挙動解析(たとえば、現在のパーミッション、履歴的活動)に少なくとも部分的に基づいて、個々のリソース(たとえば、利用可能なハードウェアデバイス構成要素、システム状態変数値など)を動的に変更する。そのような動的な変更は、知られている悪用、またはマルウェア活動を引き起こすために知られている特定のシナリオに基づいていない。たとえば、未知のアプリの現在の挙動に基づいて、様々な実装形態を用いて構成されたモバイルデバイスは、挙動を評価し得、任意の数の利用可能なデバイス構成要素、デバイス構成要素構成、もしくは動作状態(たとえば、接続性)、および/またはシステム条件(たとえば、バッテリー電力レベルなど)を反復的に変更し得る。

【００３７】

いくつかの既存の技法は、コンピュータシステム内での特定のコンテンツの移動(たとえば、発信送信におけるデータ)を監視する。様々な実装形態は、特定のデータまたはファイルが移動しているかどうかに、まさにウォーターマークを入れず、またはそれをまったく監視しない。代わりに、様々な実装形態は、悪意のある活動を強制するのに必要とされるトリガ条件を予測するために、潜在的に悪意のあるアプリケーションの様々な活動を評価する。言い換えれば、様々な実装形態は、いくつかの漏洩されているデータをまったく追跡せず、ウォーターマークを提供せず、または機密データへのアクセスルートを識別しない。

【００３８】

図1は、様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイス102を含む通信システム100を示す。モバイルコンピューティングデバイス102は、有線またはワイヤレスの接続103(たとえば、Wi-Fiネットワーク接続、セルラーネットワーク接続など)を経由して、1つまたは複数のネットワーク105を介して通信を交換し得る。たとえば、モバイルコンピューティングデバイス102は、有線またはワイヤレスの接続111を経由してやはり1つまたは複数のネットワーク105に接続されている1つまたは複数のリモートサーバ110と、データを交換し得る。様々な実装形態では、ネットワーク105は、ローカルエリアネットワーク(LAN)および/またはワイドエリアネットワーク(WAN)を含んでよく、Wi-Fiルータ、セルラーネットワーク基地局などの、様々なアクセスポイントに関連付けられてよい。

【００３９】

様々な実装形態では、モバイルコンピューティングデバイス102は、タブレット、スマートフォン、およびラップトップコンピュータなどの、様々なタイプのモバイルコンピューティングデバイスのいずれかであり得る。いくつかの実装形態では、1つまたは複数のリモートサーバ110は、様々なサードパーティサーバ(たとえば、インターネットを経由してアクセス可能なウェブサーバ、アプリ記憶サーバなど)、および/またはハニーポットシステム監視に関連するサーバコンピューティングデバイス(たとえば、マルウェアアプリケーションに関するデータを管理するセキュリティサーバなど)を含み得る。

【００４０】

様々な実装形態では、モバイルコンピューティングデバイス102は、1つまたは複数のプロセッサ121を含み得る。たとえば、モバイルコンピューティングデバイス102は、1つま

たは複数の中央処理ユニット(CPU)(または、アプリケーションプロセッサ)、デジタル信号プロセッサ(DSP)、グラフィックス処理ユニット(GPU)、またはそれらの任意の組合せを含んでよい。モバイルコンピューティングデバイス102はまた、プロセッサ実行可能命令(たとえば、アプリケーション、プログラム、ルーチン、オペレーティングシステムなど)、データ(たとえば、アプリケーションデータ、メッセージ、プロファイル、ピクチャ、オーディオファイルなど)、および/または本明細書で説明するような様々な動作を実行するための他の情報を記憶することが可能な、様々なメモリ/データ記憶ユニット122(たとえば、RAM、キャッシュ、ハードドライブ、フラッシュドライブなど)を含み得る。モバイルコンピューティングデバイス102の様々な構成要素(たとえば、121～130)は、バス132を経由するなどの有線および/またはワイヤレスの接続を経由して、互いに結合され得る。

【００４１】

モバイルコンピューティングデバイス102はまた、様々な実装形態によるハニーポットシステムを実施するために必要であってもなくてもよい随意の構成要素を含み得る。たとえば、モバイルコンピューティングデバイス102は、他のデバイスおよび/またはネットワークと通信を交換するための1つまたは複数のネットワーキングインターフェース130を含んでよい。簡単にするために、ネットワーキングインターフェースは、様々な無線アクセス技術、プロトコル、および/またはフォーマットに従ってワイヤレス信号を交換するための、任意のハードウェア(たとえば、トランシーバ、アンテナ、コネクタなど)および/またはソフトウェア(たとえば、論理、ファームウェアなど)を指すことがあり、さもなければそれを含むことがある。たとえば、ネットワーキングインターフェースは、Wi-Fi、Bluetooth(登録商標)、RF、および/または近距離通信(NFC)無線を含んでよい。モバイルコンピューティングデバイス102は、1つまたは複数のセンサ124(たとえば、カメラ、マイクロフォン、光センサ、加速度計、ジャイロスコープなど)を含み得る。モバイルコンピューティングデバイス102はまた、タッチスクリーン入力部、周辺機器(たとえば、マウス、キーボードなど)などの、様々な入力デバイス126を含み得る。モバイルコンピューティングデバイス102はまた、タッチスクリーンディスプレイ、電球、スピーカなどの、様々な出力デバイス128を含み得る。いくつかの実装形態では、モバイルコンピューティングデバイス102はまた、全地球測位システム(GPS)受信機を含み得る。

【００４２】

いくつかの実装形態では、モバイルコンピューティングデバイス102が、モバイルコンピューティングデバイス102内に存在すべき実際の構成要素を必要とすることなく、そのような構成要素または関連する機能性を単にエミュレートするように構成され得るので、様々な随意の構成要素は随意と見なされてよい。たとえば、モバイルコンピューティングデバイス102は、実際のBluetooth(登録商標)無線を含まなくてよいが、プロセッサ121上で実行中のアプリケーションによる悪意のある活動をトリガするために、Bluetooth(登録商標)リソースをアプリケーションにとって利用可能にさせる目的で、Bluetooth(登録商標)無線の存在をエミュレートするように構成されてよい。

【００４３】

様々な実装形態では、モバイルコンピューティングデバイス102は、モバイルコンピューティングデバイス102(すなわち、ハニーポットシステム)上での悪意のあるアプリケーション活動の少なくとも監視、解析、および予測を可能にする、様々なソフトウェア、サービス、構成要素、モジュール、回路構成、および/または他の機能性を用いて構成され得る。本質的に、ハニーポットシステムは、潜在的に悪意のあるアプリケーションにとって認識可能でなくてよいが、その様々なシステム構成要素との潜在的に悪意のあるアプリケーションのすべての相互作用、データ、およびモバイルコンピューティングデバイス102の能力を制御することが可能であり得る。いくつかの実装形態では、モバイルコンピューティングデバイス102のプロセッサ121は、ハニーポットシステム制御モジュール140を実行することによってハニーポットシステムを有効化し得る。ハニーポットシステム制御モジュール140は、潜在的に悪意のあるアプリケーションによる使用のために利用可能な情報およびリソースを制御するために、システム内の信号を継続的に生成、傍受、および

フィルタ処理するように構成され得る。たとえば、ハニーポットシステム制御モジュール140は、センサをポーリングするための、または記憶されたデータをメモリもしくは他のデータ記憶ユニットから受信するための、インストールされたアプリケーションからの要求などの、API呼出しならびに任意のデバイスレベルまたはOSレベルのメッセージングを傍受または別の方法で検出し得る。

【００４４】

いくつかの実装形態では、ハニーポットシステム制御モジュール140は、ハニーポットシステムに提供すべき様々なモジュール(たとえば、論理、ソフトウェア、回路構成など)を含み得、かつ/またはそれを利用し得る。たとえば、ハニーポットシステム制御モジュール140は、システム情報(たとえば、状態変数、アクセスなど)を評価するとともに、潜在的な悪意のあるアプリケーションの存在を識別するための機械学習を実行するように構成されている、挙動観測および解析モジュール144を利用し得る。たとえば、挙動観測および解析モジュール144は、アプリケーションがマルウェアであるか否かという確率を計算するために、アプリケーションパーミッション、以前に実行されたAPI呼出し、および/またはいくつかのアプリケーションによるリソースアクセス(たとえば、メモリアクセス、ネットワーク接続性照会など)を評価するように構成され得る。そのような解析に少なくとも部分的に基づいて、挙動観測および解析モジュール144は、潜在的に悪意があるか否かとしてアプリケーションを識別し得る。

【００４５】

ハニーポットシステム制御モジュール140はまた、ターゲットアプリケーションに悪意のある活動を提示させ得るトリガ条件を予測するように構成されている、アプリケーション挙動予測モジュール146を利用し得る。たとえば、アプリケーション挙動予測モジュール146は、以前に利用可能でなかったが利用可能にされた場合にマルウェアを活動化させ得る、モバイルコンピューティングデバイス102の1つまたは複数のリソースまたは動作条件を識別するために、ターゲットアプリケーション、関連する特性、および以前に観測された活動の第2の解析を実行し得る。

【００４６】

ハニーポットシステム制御モジュール140は、潜在的に悪意のあるアプリケーションの悪意のある活動をトリガするように利用可能にさせられてよく、かつ/または調整されてよい、様々なリソースおよび/またはシステム状態を選択するように構成されている、動的リソース選択モジュール148を利用し得る。これらのリソースおよび/またはシステム状態の選択は、識別されるトリガ条件を満足する可能性を高めるように設計された方法で行われてよい。

【００４７】

ハニーポットシステム制御モジュール140はまた、選択されたリソースを潜在的に悪意のあるアプリケーションに提供するように構成されている、動的リソース供給モジュール150を利用し得る。たとえば、動的リソース供給モジュール150は、仮想的な(または、エミュレートされた)リソース(たとえば、Wi-Fiネットワーク接続、特定のMNOへの登録などの、仮想ネットワーク接続またはインターフェースなど)を作成および/または調整し得る。別の例として、動的リソース供給モジュール150は、認識可能であるがアプリケーションへの限定されたアクセスしか有しないように(たとえば、写真を撮ることができないカメラセンサを認識可能にさせることなど)、実際のリソースを構成してよい。動的リソース供給モジュール150は、アプリケーションのグループまで、または特定のアプリケーションのみまで、リソースをシステム全体に認識可能にさせ得る。

【００４８】

ハニーポットシステム制御モジュール140はまた、様々なリソース(たとえば、システム状態情報、デバイス状態など)ならびに潜在的に悪意のあるアプリケーションの任意の動作および/または状態を監視および観測するように構成されている、ハニーポットシステム監視モジュール152を利用し得る。たとえば、ハニーポットシステム監視モジュール152は、特定のターゲットアプリケーションからの任意のAPI呼出し、OS要求、割込み、信号

、および/または他の通信を傍受および評価するように構成され得る。

【００４９】

ハニーポットシステム制御モジュール140はまた、新たな観測値を潜在的に悪意のあるアプリケーションに対応する以前に観測された情報と組み合わせて、悪意のある活動を検出するように構成されている、悪意活動検出モジュール154を利用し得る。たとえば、悪意活動検出モジュール154は、挙動解析のいくつかの反復にわたってターゲットアプリケーションによるアクションの動向を検出し得、アクションの組合せが悪意のある活動を表す可能性が高いと決定し得る。

【００５０】

図2～図5は、様々な実装形態による、ハニーポットシステムとして働くように構成されたモバイルコンピューティングデバイス102によって使用され得る動的データ200の一例を示す図である。動的データ200は、本明細書で説明する様々な実装形態に従って、潜在的に悪意のあるアプリケーションに対するトリガ条件を決定するために、反復挙動解析アルゴリズムの実行中にモバイルコンピューティングデバイス102によって記憶された情報に相当し得る。いくつかの実装形態では、動的データ200および反復挙動解析アルゴリズムは、説明したようにハニーポットシステム制御モジュール140によって更新、管理、実行、および別の方法で制御され得る。

【００５１】

非限定的な例示のために、図2～図5は、モバイルコンピューティングデバイス102が潜在的に悪意のあるアプリケーションとしてターゲットアプリケーション250(または、ターゲット「アプリ」)を識別しているシナリオを対象とする。この識別は、説明したように挙動観測および解析モジュール144を介した、ターゲットアプリケーション250のパーミッションおよび/または以前の活動の解析に少なくとも部分的に基づいていてよい。動的データ200は、ターゲットアプリケーション250に関して反復挙動解析アルゴリズムの実行中にモバイルコンピューティングデバイス102によって記憶された情報に相当し得る。動的データ200は、所与の時間におけるターゲットアプリケーション250による使用のために供給されるかまたは別の方法で「認識可能」である現在のリソース(たとえば、デバイス構成要素、システム状態のデータ)を示すリソースデータセグメント202a～202d、ターゲットアプリケーション250のパーミッションを示すパーミッションデータセグメント204、および現在のターゲットアプリケーション250活動(たとえば、リソースおよび/または状態情報の調整に応答して行われるAPI呼出しなど)を示す活動データセグメント206a～206dを含み得る。図2～図5に示す例では、パーミッションデータセグメント204は、ターゲットアプリケーション250が、様々なネットワーキング機能性(たとえば、セルラーネットワーク接続、Wi-Fiネットワーク接続など)ならびにメモリおよび/または記憶デバイスアクセス(たとえば、メモリ、ディスク、外部記憶装置へのデータの読取り/書込みなど)にアクセスするためのパーミッションを有することを示し得る。

【００５２】

様々な実装形態では、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250および/または挙動解析アルゴリズムに関連するデータを記憶、定義、提示(または、アクセス可能にさせること)、および追跡するための、様々なデータ構造および記録方式を使用し得る。図2～図5に示すいかなるデータまたはデータ構造も、データ管理の他の方式に対して単に例示的かつ非限定的であることを意図する。

【００５３】

図2は、挙動解析アルゴリズムの第1の反復の後、モバイルコンピューティングデバイス102によって記憶された動的データ200を示す。詳細には、動的データ200は、セルラーネットワークインターフェースがモバイルコンピューティングデバイス102の中に存在することを示すデータを含む、リソースデータセグメント202aを含み得る。動的データ200はまた、ターゲットアプリケーション250が、いかなるアクションも実行していないこと、または代替として、利用可能なセルラーネットワーク接続を伴い潜在的に悪意のあるいかなるアクションも実行していないことを示す、活動データセグメント206aを含み得る。詳

細には、ターゲットアプリケーション250は、モバイルコンピューティングデバイス上で実行中の多くの良性アプリケーションにとって一般の動作であり得る、現在のネットワーク接続のチェックを単に実行していてよい。

【００５４】

挙動解析アルゴリズムの第1の反復の後、悪意のある活動が検出されないので、モバイルコンピューティングデバイス102は、動的データ200の中のデータの任意の組合せを使用して、ターゲットアプリケーション250に対するトリガ条件を予測するための挙動解析アルゴリズムの第2の反復を実行し得る。詳細には、モバイルコンピューティングデバイス102は、悪意のあるアクションを実行する前にターゲットアプリケーション250が待っていることがある条件および/またはリソースを予測するために、ターゲットアプリケーション250にとって利用可能にされた現在のリソース(たとえば、セルラーネットワーク)と組み合わせて、ターゲットアプリケーション250のパーミッション(たとえば、ネットワークおよびストレージ/メモリアクセス)を評価し得る。そのような予測は、説明したようにアプリケーション挙動予測モジュール146を使用して行われてよい。

【００５５】

たとえば、挙動解析アルゴリズムを介して、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250が、ネットワークアクセスパーミッションを有すること、機密データへのアクセスを有すること、およびセルラーネットワーク接続を伴う良性活動しか実行しないことを観測し得る(たとえば、利用可能なネットワーク接続(たとえば、RAT利用可能性、特定の非共通アドレスへのドメインネームシステム(DNS)照会)をチェックするなど)。この観測に応答して、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250がWAN接続を使用して機密情報を漏洩する高い確率を有すると結論付けてよい。モバイルコンピューティングデバイス102はまた、ターゲットアプリケーション250が機密情報を漏洩するための異なるタイプのネットワーク接続性またはRAT(たとえば、Wi-Fi)を探していることを予測し得る。

【００５６】

これらの予測に少なくとも部分的に基づいて、モバイルコンピューティングデバイス102は、説明したように動的リソース選択モジュール148および動的リソース供給モジュール150などを介して、ターゲットアプリケーション250にしか認識可能であり得ない仮想Wi-Fiネットワーク接続またはインターフェースを供給し得る。仮想Wi-Fiネットワーク接続は、強固に監視されてよく、限定されたネットワーク接続性を有し得る。モバイルコンピューティングデバイス102は、説明したようにハニーポットシステム監視モジュール152などを介して、新たなWi-Fiネットワーク接続を経由して送られる(または、送られるように要求される)任意の通信を検出することが可能であり得る。

【００５７】

図3は、この例の挙動解析アルゴリズムの第2の反復および仮想Wi-Fiネットワーク接続の供給の後、モバイルコンピューティングデバイス102によって記憶された動的データ200を示す。リソースデータセグメント202bは、モバイルコンピューティングデバイス102が、図2に示すようなセルラーネットワーク接続を置き換えるためにWi-Fiネットワーク接続を供給したことを示す。ターゲットアプリケーション250にとって利用可能なネットワーキング接続のタイプを変更することに応答して、動的データ200は、ここで、ターゲットアプリケーション250が機密データ(たとえば、パスワードファイル、連絡先リストなど)にアクセスし、次いで、仮想Wi-Fiネットワーク接続を経由した外部データ転送を実施するための動作を実行したことを示す、活動データセグメント206bを含み得る。モバイルコンピューティングデバイス102は、説明したように悪意活動検出モジュール154などを介して、ターゲットアプリケーション250のそのようなアクションが潜在的に悪意があると決定し得る。反復挙動解析アルゴリズムを使用して、モバイルコンピューティングデバイス102は、少なくともターゲットアプリケーション250が機密データを盗用/配布するという悪意のある活動を実行するためにWi-Fiネットワーク接続のみを使用する(たとえば、セルラーネットワークを使用しない)ように設計されている可能性が高いと決定していてよい

。

【００５８】

場合によっては、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250の悪意のある活動をトリガするために、挙動解析アルゴリズムの追加の反復を実行してよい。たとえば、ターゲットアプリケーション250が、いくつかの条件が満たされるときしか悪意のある活動を実行しないように構成されている場合、モバイルコンピューティングデバイス102は、悪意のある活動を引き起こすための要因の正確な組合せが提示されるまで、解析、予測、および供給動作を繰り返し実行してよい。

【００５９】

図4は、セルラーネットワーク接続からWi-Fiネットワーク接続への変更に応答してターゲットアプリケーション250が悪意のあるアクションの実行を開始しない、例示的なシナリオを示す。詳細には、図4は、挙動解析アルゴリズムの第2の反復およびリソースデータセグメント202cによって示されるような仮想Wi-Fiネットワーク接続の供給の後、記憶された動的データ200を示す。この例では、活動データセグメント206cは、新たに供給されたWi-Fiネットワーク接続に応答してターゲットアプリケーション250が潜在的に悪意のあるアクションを実行したことを示さない。

【００６０】

挙動解析アルゴリズムの第2の反復の後、悪意のある活動が検出されないので、モバイルコンピューティングデバイス102は、動的データ200の中のデータの任意の組合せを使用して、ターゲットアプリケーション250に対するトリガ条件を予測するための挙動解析アルゴリズムの第3の反復を実行し得る。モバイルコンピューティングデバイス102は、ターゲットアプリケーション250にとって利用可能にされた現在のリソース(たとえば、Wi-Fiネットワーク接続)と組み合わせて、ターゲットアプリケーション250のパーミッション(たとえば、ネットワークおよびストレージ/メモリアクセス)を評価し得る。モバイルコンピューティングデバイス102は、次いで、悪意のあるアクションを実行する前にターゲットアプリケーション250が待っていることがある条件および/またはリソースを予測し得る。

【００６１】

たとえば、挙動解析アルゴリズムを介して、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250が、異なるタイプのネットワークアクセスに加えていくつかの機密データアクセスを有していたが、良性活動しか実行しなかったことを観測し得る。それに応答して、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250が、モバイルコンピューティングデバイス102が機密データにアクセスし得るがいかなるデータもローカルに記憶していないという情報を盗用する高い確率を有し得ると結論付けてよい。この状況において、モバイルコンピューティングデバイス102は、ターゲットアプリケーション250が、ターゲットアプリケーション250が盗用するように設計されている特定のタイプのデータを含む新たなデータソースを待っていることがあることを予測し得る。その予測に少なくとも部分的に基づいて、モバイルコンピューティングデバイス102は、ワイヤレスまたは有線の接続(たとえば、Bluetooth(登録商標)、NFC、ケーブルなど)を経由して接続されたハードドライブ、またはユニバーサルシリアルバス(USB)接続などを経由して接続されたサムドライブなどの、偽の外部データソース(または、ドライブ)への仮想接続を作成し得る。モバイルコンピューティングデバイス102は、新たな偽の外部データソースへの任意のデータアクセス(たとえば、コピー、書込み、読取りなど)を検出することが可能であり得る。

【００６２】

図5は、挙動解析アルゴリズムの第3の反復および偽の外部データソースへの接続の供給の後、モバイルコンピューティングデバイス102によって記憶された動的データ200を示す。リソースデータセグメント202dは、モバイルコンピューティングデバイス102が、以前に供給されたWi-Fiネットワーク接続に加えて、外部データソース(または、ドライブ)への接続を供給したことを示す。供給されるリソースの変更に応答して、動的データ200は

、ここで、ターゲットアプリケーション250が、外部ドライブにアクセスし(たとえば、データをコピーするなど)、次いで、Wi-Fiネットワーク接続を介した外部データ転送を実施するための動作、すなわち、悪意があり得る活動を始めたことを示す活動データセグメント206dを含む。言い換えれば、反復挙動解析アルゴリズムを使用して、この例におけるモバイルコンピューティングデバイス102は、ターゲットアプリケーション250が、モバイルコンピューティングデバイス102の外部のデータソースからデータを盗用および配布するという悪意のある活動を実行するために、少なくともWi-Fiネットワーク接続を使用するように設計されていると決定した。

【００６３】

図6は、様々な実装形態による、アプリケーションによる悪意のある活動をトリガするために挙動解析および動的リソース供給を使用するモバイルコンピューティングデバイスのための方法600を示す。いくつかの実装形態では、方法600の様々な動作は、各々がモバイルコンピューティングデバイスのプロセッサ(たとえば、モバイルコンピューティングデバイス102のプロセッサ121)を介して実行する、ハニーポットシステム制御モジュール140および様々なモジュール(たとえば、モジュール144～154)によって実行され得る。

【００６４】

ブロック602において、モバイルコンピューティングデバイスのプロセッサは、アプリケーションが悪意があり得る確率を査定するために、ストレージ上にインストールされた、かつ/またはモバイルコンピューティングデバイスのプロセッサ上で実行中の、1つまたは複数のアプリケーションを解析し得る。たとえば、モバイルコンピューティングデバイスは、アプリケーションによってアクセスされ得る、モバイルコンピューティングデバイスの可能性のあるサブシステムおよび/または他の機能性を識別するために、プロセッサ上で動作中のアプリケーションごとにパーミッションを評価し得る。モバイルコンピューティングデバイスは、各アプリケーションの以前に観測および記憶されたデータ(たとえば、アプリケーションの履歴的活動、現在のパーミッションなど)に少なくとも部分的に基づいて、1つまたは複数のアプリケーションの各々が潜在的に悪意がある確率を計算し得る。いくつかの実装形態では、いくつかのパーミッション、以前のアクション、またはそれらの任意の組合せは、マルウェアであることのより高い確率をアプリケーションが有することを示し得る。たとえば、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスの特定の構成要素(たとえば、ネットワークインターフェース)および/または機密データにアクセスするための、アプリケーションの機能に起因して、アプリケーションが悪意のあるデータ漏洩動作を実行することが可能である高い確率を計算し得る。別の例として、モバイルコンピューティングデバイスは、悪意のあるアプリケーションの既知の挙動を、モバイルコンピューティングデバイス上で実行中に観測されたアプリケーションの現在の(または、最近の)挙動と照合することに基づいて、アプリケーションが悪意のあるデータ漏洩動作を実行することが可能である高い確率を計算し得る。

【００６５】

決定ブロック604において、モバイルコンピューティングデバイスのプロセッサは、現在ストレージ上にインストールされた、かつ/またはモバイルコンピューティングデバイスのプロセッサ上で実行中の、1つまたは複数のアプリケーションのいずれかが、潜在的に悪意があるか否かを決定し得る。たとえば、モバイルコンピューティングデバイスは、アプリケーションが潜在的に悪意があるものとして分類されるべきかどうかを決定するために、アプリケーションが悪意があるという計算された確率をしきい値と比較し得る。いくつかの実装形態では、ブロック602～604の動作は、図1を参照しながら説明したように挙動観測および解析モジュール144を使用して実行され得る。

【００６６】

モバイルコンピューティングデバイスのプロセッサ上で現在実行中の1つまたは複数のアプリケーションのいずれも潜在的に悪意がないという決定に応答して(すなわち、決定ブロック604=「No」)、モバイルコンピューティングデバイスは、ブロック602において解析動作を継続してよく、またはすべてのアプリケーションが解析されており良性である可

能性が最も高いと見出されている場合、終了してよい。

【００６７】

モバイルコンピューティングデバイスのプロセッサ上で現在実行中のアプリケーションのうちの1つまたは複数が潜在的に悪意があるという決定に応答して(すなわち、決定ブロック604=「Yes」)、モバイルコンピューティングデバイスのプロセッサは、ブロック606において、潜在的に悪意のあるターゲットアプリケーションを選択し得る。たとえば、選択されるターゲットアプリケーションは、複数の識別された潜在的に悪意のあるアプリケーションの中の、単に次のものであってよい。いくつかの実装形態では、モバイルコンピューティングデバイスは、ブロック606～622の動作を用いて評価するための複数のターゲットアプリケーション(または、その組合せ)を選択し得る。言い換えれば、モバイルコンピューティングデバイスによるブロック606の選択は、1つのターゲットアプリケーションのみに限定されなくてよく、代わりに、ハニーポットシステムは、類似(または、同一)のトリガパラメータを有し得るアプリケーションのグループに対して動作し得る。

【００６８】

ブロック608において、モバイルコンピューティングデバイスのプロセッサは、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)による悪意のある活動を刺激またはトリガし得るトリガ条件(たとえば、利用可能なリソース、システム状態など)を予測し得る。たとえば、モバイルコンピューティングデバイスは、Wi-Fiネットワーク接続が実際に利用可能でなくても、ターゲットアプリケーションが悪意のあるアクションを開始するためにWi-Fiネットワーク接続を必要とすることを予測し得る。いくつかの実装形態では、モバイルコンピューティングデバイスは、悪意をもって挙動し始める前にターゲットアプリケーションが待っていることがある状況を識別するために、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)のパーミッション、ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、およびターゲットアプリケーションの以前の活動を示す記憶された活動データを評価することによって、トリガ条件のそのような予測を行い得る。いくつかの実装形態では、ブロック608の動作は、図1を参照しながら説明したようにアプリケーション挙動予測モジュール146を使用して実行され得る。たとえば、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスのBluetooth(登録商標)構成要素の存在またはステータスを求めて照会することなどの、ターゲットアプリケーション実行において現在時刻までに観測された関連するアクションに基づいて、将来においてターゲットアプリケーションによってアクセスされる可能性が高いアクションまたはリソース(たとえば、Bluetooth(登録商標)通信)についての予測を行い得る。

【００６９】

ブロック610において、モバイルコンピューティングデバイスのプロセッサは、予測されたトリガ条件を満足し得る供給すべきリソース(たとえば、デバイス構成要素、システム状態データ)を識別し得る。たとえば、ターゲットアプリケーションが悪意のあるアクションを開始するためにWi-Fiネットワーク接続を必要とすることを示す予測されたトリガ条件に少なくとも部分的に基づいて、モバイルコンピューティングデバイスは、偽のWi-Fiネットワークインターフェースがエミュレートまたは別の方法でターゲットアプリケーションにとって認識可能にされるべきと識別し得る。場合によっては、モバイルコンピューティングデバイスは、すでに利用可能なリソースが、予測されたトリガ条件を満足するように調整または再構成されるべきと識別し得る。たとえば、信号強度読取値が、人為的に増大または低減される必要があり得る。いくつかの実装形態では、モバイルコンピューティングデバイスは、悪意のある追加の挙動をトリガし得るコーナーケースをターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に提示するために、利用可能なリソースを強制して例外条件にしてよい。

【００７０】

説明したように、供給するために識別され得るリソースは、デバイス構成要素およびデータ(たとえば、システム変数、OSレベルデータ、レジスタデータなど)のうちの1つまた

は複数を含み得る。たとえば、デバイス構成要素は、インストール済みのアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサを含み得る。別の例として、リソースデータは、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータを含み得る。

【００７１】

悪意のある特に精巧なアプリケーションをトリガするために、リソースを動的に提供することおよび/またはリソースの調整は、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)にできるだけ現実的に見えるべきである。たとえば、ターゲットアプリケーションは、偽のまたはエミュレートされたネットワーキング状態を、モバイルコンピューティングデバイスのネットワークにおいて実際に存在する現実のネットワーキング状態から区別することが可能であるべきでない。別の例として、現実的な電話連絡先リストは、2つ以上の市外局番を有する電話番号を含んでよい。別の例として、メッセージログは、モバイルコンピューティングデバイスが、連絡先リストの中のいくつかの、ただしすべてではない連絡先と、複数のショートメッセージサービス(SMS)メッセージを交換していることを示してよい。さらに、動的リソースは、現実のリソースに一致するレベルのランダム性を伴って、出現、変化、および消失すべきである。たとえば、Wi-Fiネットワーク接続は典型的なWi-Fi送信レンジの外部で維持され得ないので、モバイルコンピューティングデバイスが典型的なWi-Fiアクセスポイントの届く範囲を越えた距離にあることを他のデータが示すとき、単一のWi-Fiアクセスポイントは、アクティブであるものとして報告されるべきでない。

【００７２】

したがって、ブロック610において、モバイルコンピューティングデバイスは、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対して予測されたトリガ条件に直接かつ/または間接的に関連するリソースを識別し得る。たとえば、マルウェアアプリがハニーポットシステム環境の存在を検出することを回避するために、モバイルコンピューティングデバイスは、移動情報(たとえば、センサ、またはGPSデータを変化させること)と、接続された異なるアクセスポイントの供給(たとえば、SSID、メディアアクセス制御(MAC)アドレス、RSSI)の両方を、提示またはシミュレートしてよい。別の例として、ターゲットアプリケーションによってアクセスされ得るもっと現実的な偽の連絡先リストを提供するために、モバイルコンピューティングデバイスは、もっと多様な連絡先が偽の連絡先リスト(たとえば、異なる市外局番からの電話番号、様々な数のSMSメッセージの異なる受信者/送信者など)に追加されることを必要とすると決定してよい。いくつかの実装形態では、ブロック610の動作は、図1を参照しながら説明したように動的リソース選択モジュール148を使用して実行され得る。

【００７３】

ブロック612において、モバイルコンピューティングデバイスのプロセッサは、識別されたリソースを供給し得る。場合によっては、供給することは、デバイス構成要素の動作特性(たとえば、スループット、処理速度、温度読取値など)を変更するなどによって、予測されたトリガ条件に少なくとも部分的に基づいて、すでに利用可能(または、認識可能)なリソースを調整すること、および/またはターゲットアプリケーションによってポーリングされ得るシステムデータの値を調整することを含み得る。たとえば、モバイルコンピューティングデバイスは、ターゲットアプリケーションが要求し得るネットワーク接続性ステータスデータを、特定の信号強度、アクセスポイント名、アクセスネットワークなどを示すように調整してよい。別の例として、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスが新たな都市に再配置されたことを示すように、GPSデータを変更してよい。供給することはまた、そのようなリソースがモバイルコンピューティングデバイス上に普通は存在しないときでも、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)にとって認識可能となるようにリソースを構成

することを含み得る。たとえば、モバイルコンピューティングデバイスは、ターゲットアプリケーションによる可能性のある使用のために、特定のネットワークインターフェースおよび/またはセンサを活動化させてよい。別の例として、モバイルコンピューティングデバイスは、予測されたトリガ条件に少なくとも部分的に基づいて、以前にターゲットアプリケーションにとって認識可能であったリソースを調整(たとえば、動作パラメータまたは構成を調整)してよい。別の例として、モバイルコンピューティングデバイスは、以前にターゲットアプリケーションにとって認識可能でなかったリソースを、ターゲットアプリケーションにとってリソースが認識可能または別の方法でアクセス可能になるように構成してよい。

【００７４】

いくつかの実装形態では、供給することは、予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを作成することを含み得る。そのような仮想リソースは、モバイルコンピューティングデバイス内に実際には存在しないかまたはモバイルコンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素および/またはデータを表してよい。たとえば、モバイルコンピューティングデバイスは、ターゲットアプリケーションにとって認識可能かつアクセス可能である、仮想的な(または、偽の)Wi-Fiネットワークインターフェース、偽のBluetooth(登録商標)無線、偽のSIMカード、結合された外部デバイス(たとえば、USBサムドライブなど)、および/または偽のDSPを生成し得る。いくつかの実装形態では、ブロック612の動作は、図1を参照しながら説明したように動的リソース供給モジュール150を使用して実行され得る。

【００７５】

ブロック614において、モバイルコンピューティングデバイスのプロセッサは、新たに供給されたリソースに対応する、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)の活動(たとえば、供給されたリソースのアクセス)を監視し得る。たとえば、モバイルコンピューティングデバイスは、ターゲットアプリケーションによって起動されるすべてのアプリケーションプログラミングインターフェース(API)呼出し、割込み、メッセージ、および/または他のシグナリングを傍受および/または検出し得る。監視された活動は、OSレベルサービスを要求すること、メモリまたは他のストレージへの読取り/書込み、より多くのパワーおよび/またはプロセッサ時間を使用すること、システム変数またはデータの照会または変更、ネットワークインターフェースを経由した通信を起動すること、デバイス構成要素(たとえば、センサ)をポーリングすること、ならびに/あるいはモバイルコンピューティングデバイスのリソースのうちの1つまたは複数を使用する任意の他の動作を実行することなどの、アクションを含み得る。

【００７６】

ブロック616において、モバイルコンピューティングデバイスのプロセッサは、ブロック614の監視動作に少なくとも部分的に基づいて、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対して記憶された活動データを更新し得る。いくつかの実装形態では、モバイルコンピューティングデバイスは、ある時間期間にわたって評価されたすべてのアプリケーションの履歴および状態を維持し得る。そのような履歴的活動データは、アプリケーションプロファイルなどの、個々のターゲットアプリケーションに関連する様々なデータ構造の中に保持されてよい。たとえば、モバイルコンピューティングデバイスは、様々な供給動作に応答してターゲットアプリケーションによって起動される任意のAPI呼出し、メモリアクセス、および/または他のアクションを示すように、ターゲットアプリケーションに関連するプロファイルデータを更新し得る。いくつかの実装形態では、モバイルコンピューティングデバイスは、ターゲットアプリケーションの組合せに関連する様々なデータ構造またはプロファイルの中に履歴的活動データを記憶し得る。いくつかの実装形態では、ブロック614～616の動作は、図1を参照しながら説明したようにハニーポットシステム監視モジュール152を使用して実行され得る。

【００７７】

決定ブロック618において、モバイルコンピューティングデバイスのプロセッサは、タ

ーゲットアプリケーション(または、ターゲットアプリケーションの組合せ)による悪意のある任意の活動が検出されたか否かを決定し得る。この決定は、リソースを利用可能にさせることまたは調整することに応答して行われる、ターゲットアプリケーションの監視された活動を評価することを含み得る。たとえば、ターゲットアプリケーションによるアクセスのために利用可能な偽の連絡先リストの生成に応答して、モバイルコンピューティングデバイスは、ターゲットアプリケーションにとってアクセス可能なアウトバウンド接続(たとえば、Wi-Fi接続、セルラーネットワーク接続など)を経由した送信のために連絡先リストが配信されるときに悪意のある活動が行われたと決定し得る。いくつかの実装形態では、この決定はまた、ターゲットアプリケーションの以前の活動を示す記憶された活動データを評価することを含み得る。たとえば、ターゲットアプリケーションが、以前に機密データをコピーし利用可能なWi-Fi接続に対して繰り返しチェックしたが、コピーされたデータを送信しようと試みなかったとき、モバイルコンピューティングデバイスは、後でターゲットアプリケーションがリモートデータソースとの接続の確立を要求していると観測されるときに、悪意のある活動が行われていると決定し得る。様々な実装形態では、モバイルコンピューティングデバイスは、ブロック612の供給動作に応答して解析器に転送される観測された活動データ(たとえば、ターゲットアプリケーションによって生成または別の方法で起動される、傍受されたAPI呼出し、割込み、および/または他の信号)に少なくとも部分的に基づいて、悪意のある活動を識別し得る。いくつかの実装形態では、決定ブロック618の動作は、図1を参照しながら説明したように悪意活動検出モジュール154を使用して実行され得る。

【００７８】

ターゲットアプリケーションに対応する悪意のある活動が検出されないという決定に応答して(すなわち、決定ブロック618=「No」)、モバイルコンピューティングデバイスは、ブロック608において予測動作を継続してよい。言い換えれば、モバイルコンピューティングデバイスは、ターゲットアプリケーションが応答するまで、リソースをどのように供給すべきかを反復的に決定してよく、それに応じてリソースを再供給してよい。たとえば、ターゲットアプリケーションの新たに観測された挙動に少なくとも部分的に基づいて、モバイルコンピューティングデバイスは、挙動予測を更新してよく、ターゲットアプリケーションをトリガするようにエミュレートまたは別の方法で調整されるべき新たなリソースを識別し得る。異なるリソースおよび/またはシステム状態データは、ターゲットアプリケーションに提供される、以前に利用可能なリソースおよび/またはシステム状態データを置き換えてよく、かつ/あるいはそれに追加されてよい。

【００７９】

いくつかの実装形態では、モバイルコンピューティングデバイスは、ブロック602においてターゲットアプリケーションによる悪意のある活動の確率を更新するために、ハニーポットシステム観測を使用し得、その結果、ターゲットアプリケーションがおそらく悪意がないと決定し得る。たとえば、ブロック608～618の動作のいくつかの反復の後、モバイルコンピューティングデバイスは、ターゲットアプリケーションがマルウェアである確率がしきい値未満であるものと決定し得、潜在的に悪意のあるアプリケーションのリストからターゲットアプリケーションを除去し得る。このことが起こると、モバイルコンピューティングデバイスは、ブロック606において次のターゲットアプリケーションを選択してよく、そのターゲットアプリケーションに注目された方法600の動作を継続してよい。

【００８０】

悪意のある活動がターゲットアプリケーションにおいて検出されるという決定に応答して(すなわち、決定ブロック618=「Yes」)、モバイルコンピューティングデバイスのプロセッサは、予測されたトリガ条件が正確であったと決定してよく、または現在供給されるリソースに注目してよく、ブロック620においてターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対するトリガ条件を満足するものとして、現在供給されるリソースに関する情報を記憶し得る。

【００８１】

いくつかの実装形態では、モバイルコンピューティングデバイスは、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)による悪意のある活動の検出に応答して様々な動作を実行し得る。たとえば、検出された悪意のある挙動に基づいて、モバイルコンピューティングデバイスは、いくつかのリソースへのターゲットアプリケーションアクセスを阻止してよく、かつ/またはターゲットアプリケーションを無効化してよい。悪意のある活動の検出に応答して実行される動作の別の非限定的な例として、モバイルコンピューティングデバイスは報告動作を実行し得る。したがって、随意のブロック622において、モバイルコンピューティングデバイスのプロセッサは、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対するトリガ条件を示す報告メッセージを送信し得る。たとえば、モバイルコンピューティングデバイスは、悪意のある挙動を提示するようにターゲットアプリケーションを刺激した、モバイルコンピューティングデバイス上で供給される配備されたリソースに関するマルウェアデータ、ならびに観測された悪意のある挙動のタイプ(たとえば、アプリケーション漏洩機密データ)を、カタログ化するように構成されたサーバと通信し得る。別の例として、モバイルコンピューティングデバイスは、配備されたリソースおよび対応する悪意のある挙動について、他のモバイルコンピューティングデバイス(たとえば、モバイルコンピューティングデバイスの近傍内の、または通信媒体を介して別の方法で到達可能なデバイスなど)に警告し得る。そのような他のデバイスは、そのような類似の設定に対してそれぞれのローカルアプリケーションを監視することを選んでよい。

【００８２】

決定ブロック624において、モバイルコンピューティングデバイスのプロセッサは、潜在的に悪意のある監視すべき任意の他のアプリケーションがあるか否かを決定し得る。潜在的に悪意のある監視すべき他のアプリケーションがあるという決定に応答して(すなわち、決定ブロック624=「Yes」)、モバイルコンピューティングデバイスは、ブロック606において監視するための別のターゲットアプリケーションを選択してよく、そのアプリケーションに注目された方法600の動作を継続してよい。潜在的に悪意のある監視すべき他のアプリケーションがないという決定に応答して(すなわち、決定ブロック624=「No」)、モバイルコンピューティングデバイスは方法600を終了してよい。

【００８３】

パーソナルコンピュータおよびラップトップコンピュータを含む様々な形態のモバイルコンピューティングデバイスが、様々な実装形態を実施するために使用され得る。そのようなコンピューティングデバイスは、通常、図7に示す構成要素を含み、図7は例示的なスマートフォンモバイルコンピューティングデバイス700を示す。

【００８４】

様々な実装形態では、モバイルコンピューティングデバイス700は、タッチスクリーンコントローラ704および内部メモリ702に結合されたプロセッサ701を含み得る。プロセッサ701は、一般または特定の処理タスクのために指定された1つまたは複数のマルチコアICであり得る。内部メモリ702は、揮発性メモリおよび/または不揮発性メモリであってよく、セキュアメモリおよび/もしくは暗号化メモリ、または非セキュアメモリおよび/もしくは非暗号化メモリ、あるいはそれらの任意の組合せであってもよい。タッチスクリーンコントローラ704およびプロセッサ701はまた、抵抗性感知タッチスクリーン、静電容量性感知タッチスクリーン、赤外線感知タッチスクリーンなどの、タッチスクリーンパネル712に結合され得る。

【００８５】

モバイルコンピューティングデバイス700は、互いにかつ/またはプロセッサ701に結合された、送信および受信するための1つまたは複数の無線信号トランシーバ708(たとえば、Bluetooth(登録商標)、ZigBee(登録商標)、Wi-Fi、無線周波数(RF)トランシーバ)およびアンテナ710を有し得る。トランシーバ708およびアンテナ710は、様々なワイヤレス送信プロトコルスタックおよびインターフェースを実施するために、上述の回路構成とともに使用され得る。モバイルコンピューティングデバイス700は、セルラーネットワークを

経由した通信を可能にするとともにプロセッサに結合されているセルラーネットワークワイヤレスモデムチップ716を含み得る。

【００８６】

モバイルコンピューティングデバイス700は、プロセッサ701に結合された周辺デバイス接続インターフェース718を含み得る。周辺デバイス接続インターフェース718は、1つのタイプの接続を受け入れるように単独で構成されてよく、あるいはUSB、FireWire、Thunderbolt、またはPCIeなどの一般のまたはプロプライエタリな様々なタイプの物理接続および通信接続を受け入れるように、複合的に構成されてもよい。周辺デバイス接続インターフェース718はまた、同様に構成された周辺デバイス接続ポート(図示せず)に結合され得る。

【００８７】

モバイルコンピューティングデバイス700はまた、オーディオ出力を提供するためのスピーカ714を含み得る。モバイルコンピューティングデバイス700はまた、本明細書で説明する構成要素の全部または一部を収容するための、プラスチック、金属、または材料の組合せから構成されたハウジング720を含み得る。モバイルコンピューティングデバイス700は、使い捨てバッテリーまたは充電式バッテリーなどの、プロセッサ701に結合された電源722を含み得る。充電式バッテリーはまた、モバイルコンピューティングデバイス700の外部のソースから充電電流を受けるために、周辺デバイス接続ポートに結合され得る。

【００８８】

図示および説明した様々な実装形態は、特許請求の範囲の様々な特徴を示すための例として提供されるにすぎない。しかしながら、任意の所与の実装形態に関して図示および説明される特徴は、必ずしも関連する実装形態に限定されるとは限らず、図示および説明される他の実装形態とともに使用されてよく、またはそれらと組み合わせられてよい。さらに、特許請求の範囲は、いかなる例示的な一実装形態によっても限定されるものではない。

【００８９】

本明細書で説明した様々なプロセッサは、本明細書で説明した様々な実装形態の機能を含む、様々な機能を実行するようにソフトウェア命令(アプリケーション)によって構成され得る、任意のプログラマブルマイクロプロセッサ、マイクロコンピュータ、または1つもしくは複数の多重プロセッサチップであり得る。様々なデバイスでは、ワイヤレス通信機能に専用の1つのプロセッサおよび他のアプリケーションを動作させるのに専用の1つのプロセッサなどの、複数のプロセッサが設けられ得る。通常、ソフトウェアアプリケーションは、アクセスされプロセッサの中にロードされる前に、内部メモリに記憶され得る。プロセッサは、アプリケーションソフトウェア命令を記憶するのに十分な内部メモリを含んでよい。多くのデバイスでは、内部メモリは、揮発性メモリ、もしくはフラッシュメモリなどの不揮発性メモリ、または両方の組合せであってよい。この説明では、メモリへの一般的な言及は、内部メモリ、または様々なデバイスの中に差し込まれるリムーバブルメモリ、およびプロセッサ内のメモリを含む、プロセッサによってアクセス可能なメモリを指す。

【００９０】

上記の方法の説明およびプロセスフロー図は、単に例示的な例として提供され、様々な実装形態の動作が、提示された順序で実行されなければならないことを要求または暗示することは意図されていない。当業者によって諒解されるように、上記の実装形態における動作の順序は、任意の順序で実行されてよい。「その後」、「次いで」、「次に」などの単語は、動作の順序を限定するものではなく、これらの単語は単に、方法の説明を通じて読者を導くために使用される。さらに、たとえば、冠詞「a」、「an」、または「the」を使用する、単数形での請求項の要素へのいかなる言及も、その要素を単数形に限定するものとして解釈されるべきではない。

【００９１】

本明細書で開示する実装形態に関して説明した様々な例示的な論理ブロック、モジュー

ル、回路、およびアルゴリズム動作は、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得る。ハードウェアとソフトウェアとのこの交換可能性を明瞭に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、および動作が、全般的にそれぞれの機能性に関して上記で説明された。そのような機能性が、ハードウェアとして実装されるのか、それともソフトウェアとして実装されるのかは、特定の適用例および全体的なシステムに課された設計制約によって決まる。当業者は、説明した機能性を特定のアプリケーションごとに様々な方法で実装してよいが、そのような実装決定は、本特許請求の範囲からの逸脱を引き起こすものとして解釈されるべきではない。

【００９２】

本明細書で開示する実装形態に関して説明した様々な例示的な論理、論理ブロック、モジュール、および回路を実装するために使用されるハードウェアは、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明した機能を実行するように設計されたそれらの任意の組合せを用いて実施または実行されてよい。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってよい。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装されてよい。代替として、いくつかの動作または方法は、所与の機能に特定の回路構成によって実行されてよい。

【００９３】

方法600を含む様々な実装形態では、説明した機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装されてよい。ソフトウェアで実装される場合、機能は、1つまたは複数の命令またはコードとして、非一時的プロセッサ可読、コンピュータ可読、もしくはサーバ可読媒体、または非一時的プロセッサ可読記憶媒体上に記憶されてよく、あるいはそれらを介して送信されてよい。本明細書で開示する方法またはアルゴリズムの動作は、非一時的コンピュータ可読記憶媒体、非一時的サーバ可読記憶媒体、および/または非一時的プロセッサ可読記憶媒体上に存在し得る、プロセッサ実行可能ソフトウェアモジュールまたはプロセッサ実行可能ソフトウェア命令において具現化され得る。様々な実装形態では、そのような命令は、記憶されたプロセッサ実行可能命令または記憶されたプロセッサ実行可能ソフトウェア命令であってよい。有形の非一時的コンピュータ可読記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのような非一時的コンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気記憶デバイス、または命令もしくはデータ構造の形態で所望のプログラムコードを記憶するために使用され得るとともにコンピュータによってアクセスされ得る任意の他の媒体を備え得る。ディスク(disk)およびディスク(disc)は、本明細書で使用されるとき、コンパクトディスク(disc)(CD)、レーザーディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー(登録商標)ディスク(disk)、およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、レーザーを用いてデータを光学的に再生する。上記の組合せも、非一時的コンピュータ可読媒体の範囲内に含まれるべきである。追加として、方法またはアルゴリズムの動作は、コンピュータプログラム製品の中に組み込まれ得る、有形の非一時的プロセッサ可読記憶媒体および/またはコンピュータ可読媒体上のコードおよび/または命令のうちの1つまたは任意の組合せまたはセットとして存在してよい。

【００９４】

開示する実装形態の前述の説明は、任意の当業者が特許請求の範囲の実装形態の技法を製作または使用することを可能にするために提供される。これらの実装形態への様々な修

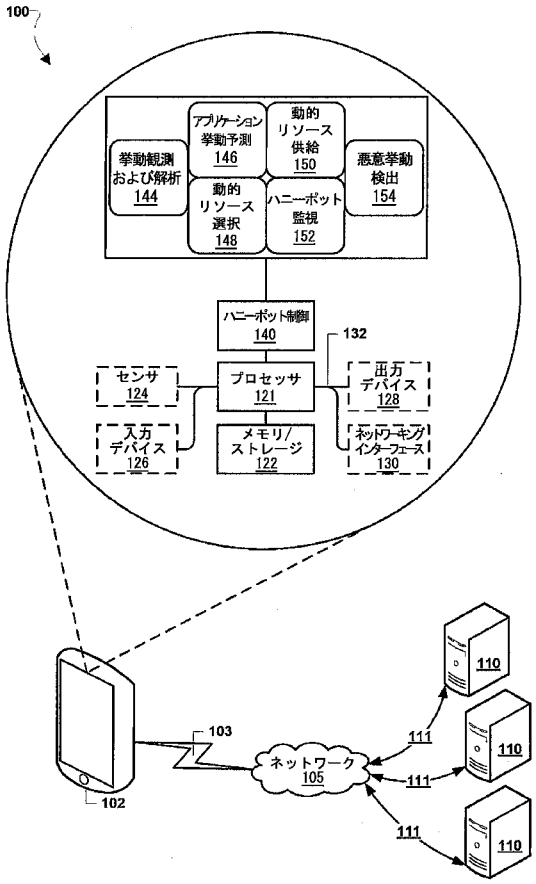
正が当業者には容易に明らかになり、本明細書で定義する一般原理は、特許請求の範囲の趣旨または範囲から逸脱することなく他の実装形態に適用され得る。したがって、本開示は、本明細書で示される実装形態に限定されるものではなく、以下の特許請求の範囲ならびに本明細書で開示する原理および新規の特徴に一致する最も広い範囲を与えられるものである。

【符号の説明】

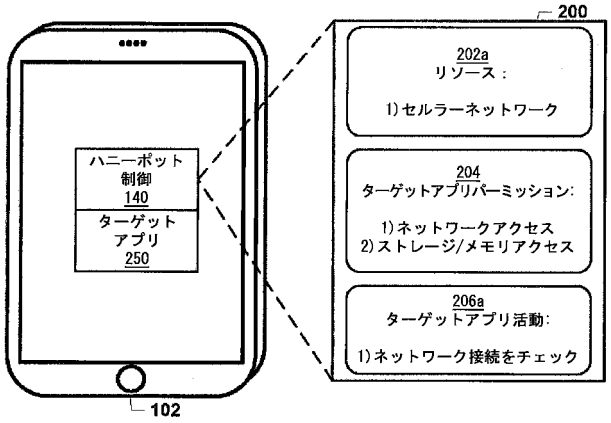
【００９５】

100 通信システム
102 モバイルコンピューティングデバイス
103 有線またはワイヤレスの接続
105 ネットワーク
110 リモートサーバ
111 有線またはワイヤレスの接続
121 プロセッサ
122 メモリ/データ記憶ユニット
124 センサ
126 入力デバイス
128 出力デバイス
130 ネットワーキングインターフェース
132 バス
140 ハニーポットシステム制御モジュール
144 挙動観測および解析モジュール
146 アプリケーション挙動予測モジュール
148 動的リソース選択モジュール
150 動的リソース供給モジュール
152 ハニーポットシステム監視モジュール
154 悪意活動検出モジュール
200 動的データ
202 リソースデータセグメント
204 パーミッションデータセグメント
206 活動データセグメント
250 ターゲットアプリケーション
700 スマートフォンモバイルコンピューティングデバイス
701 プロセッサ
702 内部メモリ
704 タッチスクリーンコントローラ
708 無線信号トランシーバ
710 アンテナ
712 タッチスクリーンパネル
714 スピーカ
716 セルラーネットワークワイヤレスモデムチップ
718 周辺デバイス接続インターフェース
720 ハウジング
722 電源

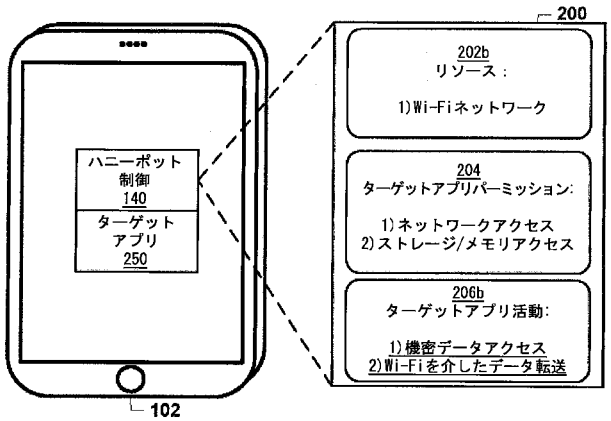
【図１】


100
アプリケーション挙動予測 146
動的リソース供給 150
挙動観測および解析 144
悪意挙動検出 154
動的リソース選択 148
ハニーポット監視 152
ハニーポット制御 140
132
センサ 124
プロセッサ 121
出力デバイス 128
入力デバイス 126
メモリ/ストレージ 122
ネットワーキングインターフェース 130
103
ネットワーク 105
111
110
102

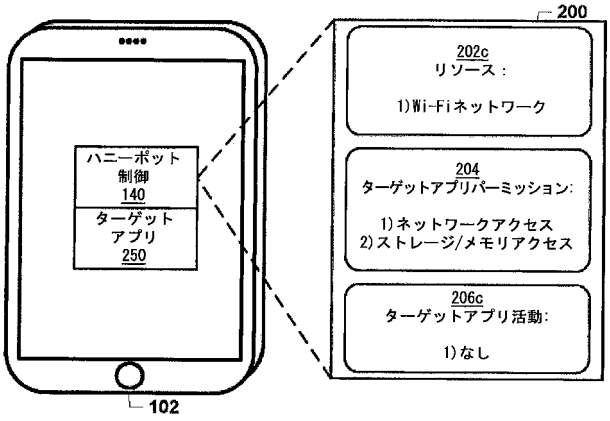
【図２】


200
ハニーポット制御 140
ターゲットアプリ 250
202a
リソース：
1)セルラーネットワーク
204
ターゲットアプリパーミッション:
1)ネットワークアクセス
2)ストレージ/メモリアクセス
206a
ターゲットアプリ活動:
1)ネットワーク接続をチェック
102

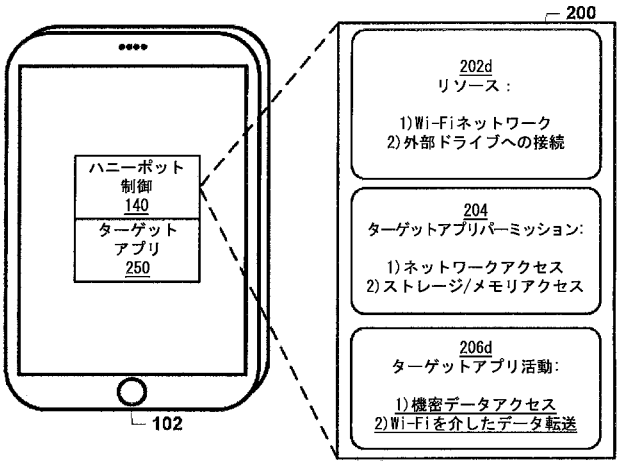
【図３】


200
ハニーポット制御 140
ターゲットアプリ 250
202b
リソース：
1)Wi-Fiネットワーク
204
ターゲットアプリパーミッション:
1)ネットワークアクセス
2)ストレージ/メモリアクセス
206b
ターゲットアプリ活動:
1)機密データアクセス
2)Wi-Fiを介したデータ転送
102

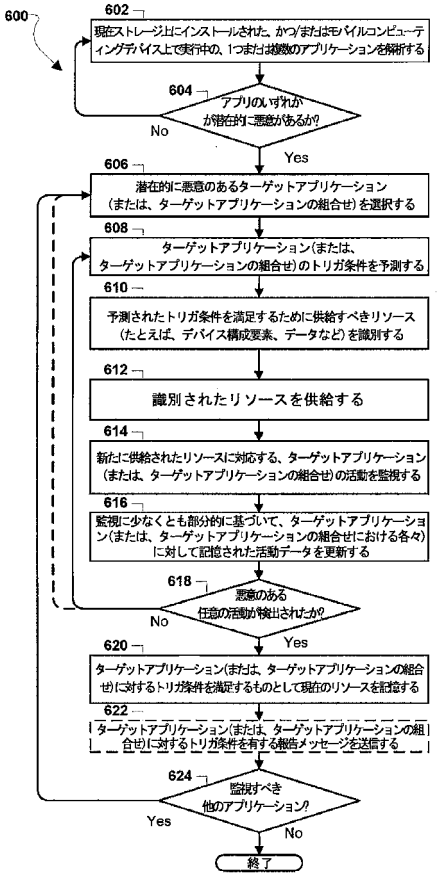
【図４】


200
ハニーポット制御 140
ターゲットアプリ 250
202c
リソース：
1)Wi-Fiネットワーク
204
ターゲットアプリパーミッション:
1)ネットワークアクセス
2)ストレージ/メモリアクセス
206c
ターゲットアプリ活動:
1)なし
102

【図５】


200
ハニーポット
制御
140
ターゲット
アプリ
250
102
202d
リソース：
1)Wi-Fiネットワーク
2)外部ドライブへの接続
204
ターゲットアプリパーミッション:
1)ネットワークアクセス
2)ストレージ/メモリアクセス
206d
ターゲットアプリ活動:
1)機密データアクセス
2)Wi-Fiを介したデータ転送

【図６】


600
602
現在ストレージ上にインストールされた、かつ/またはモバイルコンピューティングデバイス上で実行中の、1つまたは複数のアプリケーションを解析する
604
アプリのいずれかが潜在的に悪意があるか?
No
Yes
606
潜在的に悪意のあるターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)を選択する
608
ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)のトリガ条件を予測する
610
予測されたトリガ条件を満足するために供給すべきリソース(たとえば、デバイス構成要素、データなど)を識別する
612
識別されたリソースを供給する
614
新たに供給されたリソースに対応する、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)の活動を監視する
616
監視に少なくとも部分的に基づいて、ターゲットアプリケーション(または、ターゲットアプリケーションの組合せにおける各々)に対して記憶された活動データを更新する
618
悪意のある任意の活動が検出されたか?
No
Yes
620
ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対するトリガ条件を満足するものとして現在のリソースを記憶する
622
ターゲットアプリケーション(または、ターゲットアプリケーションの組合せ)に対するトリガ条件を有する報告メッセージを送信する
624
監視すべき他のアプリケーション?
Yes
No
終了

【図７】

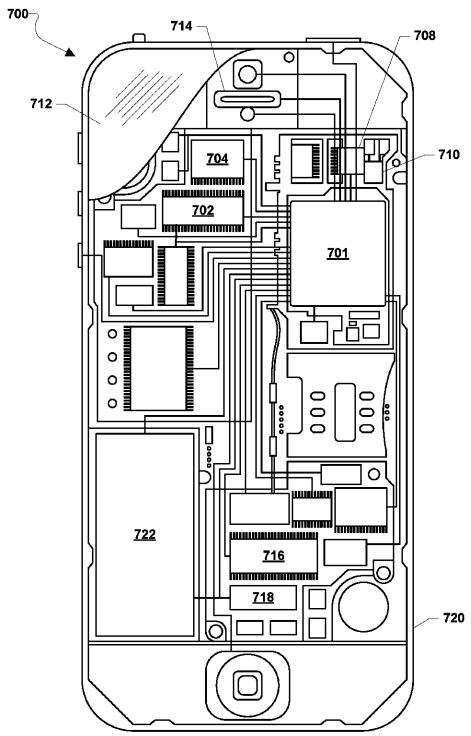

700
714
708
712
710
704
702
701
722
716
718
720

FIG. 7

【手続補正書】
【提出日】平成30年5月10日(2018.5.10)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
アプリケーションによる悪意のある活動をトリガするためにハニーポットシステムにおいて実施される方法であって、
コンピューティングデバイス上で実行中のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させるトリガ条件を、前記コンピューティングデバイスのプロセッサを介して予測するステップと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記コンピューティングデバイスの1つまたは複数のリソースを前記プロセッサを介して供給するステップと、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップと、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるかどうかを、前記プロセッサを介して決定するステップと
を備える、方法。
【請求項２】
前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、同じトリガ条件を有し得るアプリケーションのグループを監視するステップを備える、請求項1に記載の方法。
【請求項３】
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを、前記プロセッサを介して決定するステップと、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションを前記ターゲットアプリケーションとして指定するステップと
をさらに備える、請求項1に記載の方法。
【請求項４】
前記コンピューティングデバイス上で現在実行中の前記アプリケーションが潜在的に悪意があるかどうかを、前記プロセッサを介して決定するステップが、
前記コンピューティングデバイスのリソースにアクセスすることに対応する、前記アプリケーションのパーミッション、および前記アプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して解析するステップ
を備える、請求項3に記載の方法。
【請求項５】
前記1つまたは複数のリソースが、デバイス構成要素およびデータのうちの少なくとも1つを備える、請求項1に記載の方法。
【請求項６】
前記デバイス構成要素が、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサのうちの少なくとも1つを備える、請求項5に記載の方法。
【請求項７】
前記データが、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態

データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータのうちの少なくとも1つを備える、請求項5に記載の方法。
【請求項８】
前記コンピューティングデバイス上で実行中の前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させる前記トリガ条件を、前記プロセッサを介して予測するステップが、
前記ターゲットアプリケーションのパーミッション、前記ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項９】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを、前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記ターゲットアプリケーションにとって以前に認識可能であったリソースを、前記プロセッサを介して調整するステップ、および
前記ターゲットアプリケーションにとって以前に認識可能でなかったリソースを、前記ターゲットアプリケーションにとって前記リソースが認識可能になるように、前記プロセッサを介して構成するステップ
のうちの少なくとも1つを備える、請求項1に記載の方法。
【請求項１０】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを、前記プロセッサを介して作成するステップを備え、前記仮想リソースが、前記コンピューティングデバイス内に実際には存在しないかまたは前記コンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す、
請求項1に記載の方法。
【請求項１１】
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、
前記ターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを、前記プロセッサを介して検出するステップ
を備える、請求項1に記載の方法。
【請求項１２】
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるかどうかを前記プロセッサを介して決定するステップが、
前記監視された活動、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項１３】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して供給されたリソースに関する情報を含む、前記ターゲットアプリケーションに対して記憶された活動データを、前記プロセッサを介して更新するステップをさらに備える、請求項1に記載の方法。
【請求項１４】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して、前記ターゲットアプリケーションに対する前記トリガ条件を示す報告メッセージ

を送信するステップをさらに備える、請求項1に記載の方法。
【請求項１５】
コンピューティングデバイスであって、
前記コンピューティングデバイス上で実行中のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させるトリガ条件を予測することと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記コンピューティングデバイスの1つまたは複数のリソースを供給することと、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を監視することと、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意があるかどうかを決定することと
を行うように構成されたプロセッサ
を備えるコンピューティングデバイス。
【請求項１６】
同じトリガ条件を有し得るアプリケーションのグループを監視することによって、前記ターゲットアプリケーションの活動を監視するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項１７】
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定することと、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションを前記ターゲットアプリケーションとして指定することと
を行うように前記プロセッサがさらに構成される、請求項15に記載のコンピューティングデバイス。
【請求項１８】
前記コンピューティングデバイスのリソースにアクセスすることに対応する、前記1つまたは複数のターゲットアプリケーションのパーミッション、および前記1つまたは複数のターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを解析することによって、
前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定するように前記プロセッサが構成される、請求項17に記載のコンピューティングデバイス。
【請求項１９】
前記1つまたは複数のリソースが、デバイス構成要素およびデータのうちの少なくとも1つを備える、請求項15に記載のコンピューティングデバイス。
【請求項２０】
前記デバイス構成要素が、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサのうちの少なくとも1つを備える、請求項19に記載のコンピューティングデバイス。
【請求項２１】
コンピューティングデバイスがモバイルコンピューティングデバイスであり、前記データが、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータのうちの少なくとも1つを備える、請求項19に記載のコンピューティングデバイス。
【請求項２２】
前記ターゲットアプリケーションのパーミッション、前記ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを評価すること

によって、
前記コンピューティングデバイス上で実行中の前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させる前記トリガ条件を予測するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２３】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記ターゲットアプリケーションにとって以前に認識可能であったリソースを調整すること、および
前記ターゲットアプリケーションにとって以前に認識可能でなかったリソースを、前記ターゲットアプリケーションにとって前記リソースが認識可能になるように構成することのうちの少なくとも1つによって、前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを供給するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２４】
前記予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを作成することによって、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを供給するように前記プロセッサが構成され、前記仮想リソースが、前記コンピューティングデバイス内に実際には存在しないかまたは前記コンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す、
請求項15に記載のコンピューティングデバイス。
【請求項２５】
前記ターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを検出することによって、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を監視するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２６】
前記監視された活動、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データを評価することによって、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意があるかどうかを決定するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２７】
前記ターゲットアプリケーションが悪意があるという決定に応答して供給されたリソースに関する情報を含む、前記ターゲットアプリケーションに対して記憶された活動データを更新するように前記プロセッサがさらに構成される、請求項15に記載のコンピューティングデバイス。
【請求項２８】
前記ターゲットアプリケーションが悪意があるという決定に応答して、前記ターゲットアプリケーションに対する前記トリガ条件を示す報告メッセージを送信するように前記プロセッサが構成される、請求項15に記載のコンピューティングデバイス。
【請求項２９】
コンピューティングデバイスのプロセッサに動作を実行させるように構成されたプロセッサ実行可能命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作が、
前記コンピューティングデバイス上で実行中のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させるトリガ条件を予測することと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記コンピューティングデバイスの1つまたは複数のリソースを供給することと、

前記供給された1つまたは複数のリソースに対応する、前記1つまたは複数のターゲットアプリケーションの活動を監視することと、
前記監視された活動に少なくとも部分的に基づいて、前記1つまたは複数のターゲットアプリケーションのいずれかが悪意があるかどうかを決定することと
を備える、非一時的プロセッサ可読記憶媒体。
【請求項３０】
コンピューティングデバイスであって、
前記コンピューティングデバイス上で実行中のターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションに悪意のある挙動を提示させるトリガ条件を予測するための手段と、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記コンピューティングデバイスの1つまたは複数のリソースを供給するための手段と、
前記供給された1つまたは複数のリソースに対応する、前記1つまたは複数のターゲットアプリケーションの活動を監視するための手段と、
前記監視された活動に少なくとも部分的に基づいて、前記1つまたは複数のターゲットアプリケーションのいずれかが悪意があるかどうかを決定するための手段と
を備える、コンピューティングデバイス。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/056438

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/56 G06F21/55
ADD. G06F21/57

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)
G06F H04L

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/166072 A1 (CONVERSE VIKKI K [US] ET AL) 28 July 2005 (2005-07-28) paragraphs [0045] - [0065] figures 4,5A,7A	1-30
A	EP 2 610 776 A2 (VERACODE INC [US]) 3 July 2013 (2013-07-03) paragraph [0162] claims 1,3,6	11,25
A	US 2013/145465 A1 (WANG WEI [US] ET AL) 6 June 2013 (2013-06-06) the whole document	1-30

☐ 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 but 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	Date of mailing of the international search report
12 January 2017	23/01/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	De la Hera, Germán

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/056438

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005166072 A1	28-07-2005	NONE	
EP 2610776 A2	03-07-2013	EP 2610776 A2	03-07-2013
		US 2013097706 A1	18-04-2013
US 2013145465 A1	06-06-2013	US 2013145465 A1	06-06-2013
		US 2014259172 A1	11-09-2014

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA

（特許庁注：以下のものは登録商標）
１．ＡＮＤＲＯＩＤ
２．ＷＩＮＤＯＷＳ
３．ＦＩＲＥＷＩＲＥ
４．ＴＨＵＮＤＥＲＢＯＬＴ

(72)発明者 ナイーム・イスラム
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 ミハイ・クリストオドレスク
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 ラジャルシ・グプタ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者 サウミトラ・モハン・ダス
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

【要約の続き】
センサなど)および/またはデータ(たとえば、ファイルなど)であり得る。