Symantec™
Security Response

人気モバイルデバイスのセキュリティ比較

概要

Carey Nachenberg、VP、フェロー

目次

はじめに

現在、非常に多くのコンシューマデバイスが企業に進出している結果、CIO や CISO は非常に厳しい局面を迎えています。特に、モバイルデバイスを使用して企業のネットワークにアクセスし、さまざまな企業のデータを閲覧、業務を行うユーザーが増え続けています。その反面、こうしたデバイスの多くは管理者の制御下にありません。つまり、機密性の高い企業データが企業内のコンプライアンス、セキュリティ、および情報漏えい防止（DLP）ポリシーの適用外になっているのが現状です。

さらに、事態を複雑にしているのは、現在のモバイルデバイスがスタンドアロンではないことです。必ず、モバイルデバイスは、対応しているクラウドや PC ベースのサービスからなるエコシステム全体につながっています。一般的なスマートフォンは、最低 1 つの管理者の制御が及ばないパブリックなクラウドベースサービスに同期しています。さらに、ユーザーの多くは、各自のモバイルデバイスを自宅のコンピュータに同期させて、重要なデバイス設定やデータをバックアップしています。そのため、企業ガバナンスが直接及ばない企業から見て安全でない場所に、重要な企業資産が保管されていることになります。

今回、現在世界中で使用されている最も人気の高い 2 つのモバイルプラットフォーム、Google Android と Apple iOS のセキュリティモデルについて概説し、今後、企業内での採用が増えた場合に、これらのデバイスがセキュリティに与える影響を検証してみます。

この資料のフルバージョンの URL:
http://www.symantec.com/ja/jp/business/threatreport/special_report.jsp

モバイルセキュリティの目標

セキュリティに関して、この主要な 2 つのモバイルプラットフォームは、従来のデスクトップやサーバーのオペレーティングシステム類との共通性がほとんどありません。どちらのプラットフォームも既存のオペレーティングシステム（iOS は Apple の OSX オペレーティングシステム、Android は Linux がベース）が元になっていますが、いずれもコアの実装に組み込まれた、より精巧なセキュリティモデルを使用しています。他社のセキュリティソフトウェアに頼るのではなく、モバイルプラットフォームそのものが本質的に安全になるようにすることが目標だったようです。

では、安全なプラットフォームを作り上げようとする Apple と Google の狙いは成功したのでしょうか？ この問いに答えるためには、各プラットフォームのセキュリティモデルを分析し、さらにそれぞれの実装を分析して、次のような主要な脅威に対する有効性を判断してみます。

- **Web ベース攻撃とネットワークベース攻撃 :** この攻撃は通常、悪質な Web サイトまたは侵害された正当な Web サイトから開始されます。
- **マルウェア :** マルウェアは従来のコンピュータウイルス、コンピュータワーム、トロイの木馬のプログラムという 3 つの大きなカテゴリに分けることができます。
- **ソーシャルエンジニアリング攻撃 :** フィッシングなどの攻撃はソーシャルエンジニアリングを利用してユーザーを欺き、機密情報を開示させたり、コンピュータにマルウェアをインストールさせたりします。
- **リソースおよびサービス可用性の悪用 :** 攻撃の多くは不正な目的で、ネットワーク、コンピューティング、またはデバイスの ID リソースを悪用することを狙っています。
- **悪質または偶発的な情報漏えい :** 情報漏えいが発生するのは、従業員またはハッカーにより、保護されたデバイスまたはネットワークからこっそり機密情報を引き出された場合です。
- **デバイスのデータの整合性に対する攻撃 :** データの整合性に対する攻撃において、攻撃者はデータ所有者の許可を得ることなく、データの破損または改変を企てます。

Apple iOS

iPod、iPhone、および iPad デバイスを駆動する Apple の iOS オペレーティングシステム（OS）は、Apple OS X Mac オペレーティングシステムのスリム化バージョンです。

脆弱性

本書の作成時点で、セキュリティの研究者は iOS オペレーティングシステムの初期リリース以降、各種バージョンでおよそ 200 種類の脆弱性を突き止めています。こうした脆弱性の大半は重要度の低いもので、攻撃者は Safari プロセスなど、単独プロセスの制御を奪うことはできても、管理者レベルでデバイスを制御することはできません。しかし、それ以外の脆弱性は重要度が高であり、悪用した場合、攻撃者は管理者レベルでデバイスを制御することができるため、事実上、デバイスのあらゆるデータとサービスを利用できるようになります。このように重要度の高い脆弱性は、攻撃者が各自の権限を拡大してデバイスの支配権を獲得するため、権限拡大の脆弱性として分類されます。

シマンテックのデータによると、本書の作成時点では、Apple は各脆弱性の発見からパッチの適用までに平均 12 日を要しています。

iOS セキュリティの概要

iOS のセキュリティモデルは適切に設計されており、概ね攻撃に耐えられると実証されています。まとめると、次のようになります。

- **iOS の暗号化システム**はメールとメールの添付ファイルに対して強力な保護を提供し、デバイスワイプが可能ですが、断固とした攻撃者による物理的なデバイスの危殆化に対する保護はほとんど得られません。
- **iOS のプロベナンス手法**により、Apple は一般に流通している個々のアプリケーションを事前に確実に検証できます。この入念な手法は絶対確実ではありません。断固とした攻撃者であれば、ほぼ確実に回避することができます。しかしながら、マルウェア攻撃、情報漏えい攻撃、データの整合性に対する攻撃、サービス拒否攻撃の抑

止力としては十分に実績があります。

- **iOS の分離モデル**が従来型のコンピュータウイルスとワームを完全に防ぎ、スパイウェアがアクセスできるデータを制限します。また、バッファがデバイスのコントロールを奪うなど、ほとんどのネットワークベース攻撃も制限します。しかしながら、あらゆる種類の情報漏えい攻撃、リソース悪用攻撃、またはデータの整合性に対する攻撃を必ずしも防御するわけではありません。
- **iOS のパーミッションモデル**では、所有者の許可なく、アプリケーションによってデバイスの場所の取得、SMS メッセージの送信、電話をかけることができないように保証しています。
- iOS の保護技術はいずれも、フィッシング、スパムといったソーシャルエンジニアリング攻撃には対応しません。

Android

Android は、Linux オペレーティングシステムと Dalvik という人気の高い Java プラットフォームから派生した Java ベースプラットフォームとの融合です。各 Android アプリケーションはそれぞれ専用の仮想マシン内で動作し、各仮想マシンはそれぞれ専用の Linux プロセスで隔離されています。このモデルにより、デバイスをジェイルブレイク（脱獄）しないかぎり、どのプロセスも他のプロセスのリソースにまったくアクセスできません。Java の仮想マシンは安全なサンドボックスとして設計されていますが、悪質なプログラムが潜在的に含まれる恐れがあります。一方、Android はセキュリティの実施を仮想マシンに依存していません。代わりに、Linux ベースの Android オペレーティングシステムが直接、すべての保護を実行します。

脆弱性

本書の作成時点で、セキュリティの研究者は Android オペレーティングシステムの初期リリース以降、各種バージョンで合計 18 種類の脆弱性を突き止めています。そのほとんどは重要度が低く、攻撃者は Web ブラウザプロセスなど、単独プロセスの制御を奪うことはできても、管理者レベルでデバイスを制御することはできません。しかし、それ以外のいくつかの脆弱性は重要度が高であり、悪用した場合、攻撃者はルートレベルでデバイスを制御することができるようになり、事実上、デバイスのあらゆるデータを利用できるようになります。

18 の脆弱性のうち、4 つを除くすべてに対して、これまでに Google がパッチを適用しています。4 つの未対応の脆弱性の 1 つは、さらに深刻な権限拡大タイプです。この脆弱性は、Android 2.3 のリリースで対応される予定ですが、旧バージョンのオペレーティングシステムではまだ修正されていません。大部分のキャリアが顧客のデバイスを Android 2.2 から 2.3 にまだ更新していないことを考えると、事実上、既存のあらゆる Android 携帯が現在（本書の作成時点では）、攻撃を受けやすいということになります。この脆弱性はあらゆる他社製アプリケーションで悪用できるため、攻撃者がデバイスに物理的にアクセスする必要はありません。シマンテックのデータによると、本書の作成時点で、Google は各脆弱性の発見からパッチの適用までに平均 8 日を要しています。

Android セキュリティの概要

Android のセキュリティモデルは全体として、従来のデスクトップやサーバーベースのオペレーティングシステムで用いられているモデルより大幅に改善されていますが、重大な問題が 2 つあります。1 つめは、Android のプロベナンスシステムによって、攻撃者は匿名でマルウェアを作成し、配布できる点です。2 つめは、Android のパーミッションシステムは非常に強力ではありますが、セキュリティに関する重要な意思決定は最終的にユーザーに依存している点です。残念ながら、ほとんどのユーザーは技術的にこのような判断を下すことはできないため、すでにソーシャルエンジニアリング攻撃につながっています。まとめると、次のようになります。

- **Android のプロベナンス手法**により、電子署名のあるアプリケーションのみが Android デバイスにインストール可能です。しかし、攻撃者は匿名の電子証明書を用いて、それぞれの脅威に署名し、Google による証明書なしで、インターネットを介して各自の脅威を配布できます。そのため、攻撃者は正当なアプリケーションに「トロイの木馬」を仕込んだり、悪質なコードを挿入することが容易にできます。また、新しい匿名の証明書を使って署名し、インターネットを介して容易に再配布できます。プラス面を挙げると、Google はアプリケーションの配布を希望するアプリケーション作成者に対して、料金の支払いや Google への登録（開発者の電子署名を Google と共有するため）を、公式の Android App Marketplace を利用して実行するように求めています。Apple の登録方式と同様、これは組織的攻撃者を減らす抑止力として働きます。

- **Android のデフォルト分離ポリシー**がアプリケーションを相互に、また、Android オペレーティングシステムカーネルを含めたデバイスの大部分のシステムから効率的に分離しますが、いくつか特筆すべき例外があります（アプリケーションは SD カードの全データを自由に読み取ることができます）。
- **Android のパーミッションモデル**によって、アプリケーションが主要なデバイスシステムへのアクセスを明示的に要求した場合を除き、事実上あらゆる主要デバイスシステムからアプリケーションが隔離されることが保証されます。Android は残念ながら、 アプリケーションに許可を与えるかどうかの決定を最終的にユーザーに依存しているため、ソーシャルエンジニアリング攻撃を受けやすくなります。ほとんどのユーザーはこのようなセキュリティの決定を下すもとになる技術知識がないため、マルウェアおよびマルウェアが開始する可能性のあるあらゆる二次攻撃（DoS 攻撃、情報漏えい攻撃など）に対して無防備なままです。
- Android は現在、デフォルトレベルの暗号化を内蔵していません。その代わりに、分離と許可に依存してデータを保護します。したがって、Android 携帯の単純なジェイルブレイク（脱獄）やデバイス SD カードの盗難が大量の情報漏えいにつながる可能性があります。
- Android は、iOS の場合と同様、フィッシング攻撃、その他の（オフデバイス）Web 策略などのソーシャルエンジニアリング攻撃を防ぐメカニズムを備えていません。

iOS と Android の比較: セキュリティの概要

次の表に、iOS モバイルプラットフォームと Android モバイルプラットフォームの長所と短所に関するシマンテックの結論をまとめます。

表 1
対抗する攻撃のタイプ

対抗する対象	Apple iOS	Google Android
Web ベース攻撃		
マルウェア攻撃		
ソーシャルエンジニアリング攻撃		
リソースの悪用/サービスへの攻撃		
情報漏えい（悪質または偶発的）		
データの整合性に対する攻撃		

表 2
セキュリティ機能の実装

セキュリティの中心	Apple iOS	Google Android
アクセス制御		
アプリケーションプロベナンス		
暗号化		
分離		
パーミッションベースのアクセス制御		

凡例

 完全に保護される
 かなり保護される
 だいたい保護される
 あまり保護されない
 ほとんどまたはまったく保護されない

結論

現在のモバイルデバイスは、セキュリティの観点から見るといろいろな側面を持っています。これらのプラットフォームはセキュリティを高めるためにゼロから設計されましたが、コンシューマ用として設計されたため、セキュリティ面で妥協し、使い勝手を優先している場合が見受けられます。このようなトレードオフによってこれらのプラットフォームは幅広い支持を集めていますが、同時に、企業でこれらのデバイスを利用する場合のリスクも大きくなります。

このリスクの増大は、多くの従業員が自分のモバイルデバイスを会社に持ち込み、管理されないまま、それらのデバイスを使ってカレンダー、連絡先リスト、会社の書類、電子メールといった企業リソースにアクセスしていることから生じます。さらに、従業員がこの企業データを他社のクラウドサービスや自宅の PC と同期させることもよくあります。その結果、これらの行為が企業におけるバックドアになり、会社の直接の制御下にない他社のシステムを介して、機密性の高い企業データが「流出」する結果を引き起こす可能性があります。

最後に、モバイルデバイスは大きな生産性の向上を約束していますが、企業が管理しなければならない多数の新たなリスクも作りだしているのも事実です。今後、企業でモバイルデバイスを導入する際には、これらのリスクを理解し、適切に管理できるソリューションの導入は必要不可欠になるでしょう。各プラットフォームを支えるセキュリティモデルと、デバイスが関与するエコシステムについてご説明しました。これらのデバイスをより効果的に利用し、デバイスがもたらすリスクに適切に対処するための知識を、皆様に提供することができれば幸いです。

この資料のフルバージョンの URL:
http://www.symantec.com/ja/jp/business/threatreport/special_report.jsp

筆者について
Carey Nachenberg はシマンテックのセキュリティ、テクノロジ、およびレスポンス部門のバイスプレジデントであり、シマンテックのフェローです。

株式会社シマンテック
〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ
www.symantec.com/jp

E1108WP1-IN-iOSAndid