Man in the Browser in Androidの可能性

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver 2.00.01

Androidの普及とMan in the Browser

- 現在スマートフォンセキュリティの関心が高まっている
- 一方で従来からのWindows PCでもマルウェアの攻撃手法が高度化してきており、その一つの例が最近ニュースでも取り上げれているオンラインバンクを狙ったMan in the Browser (MITB)である
- スマートフォンユーザーが増えるにつれて、スマートフォン上でオンラインバンクを利用する人も増えると予測される

スマートフォン上で、これまでWindowsで起きていたMITB攻撃が成立するのか、対策方法があるのかを考える必要がある

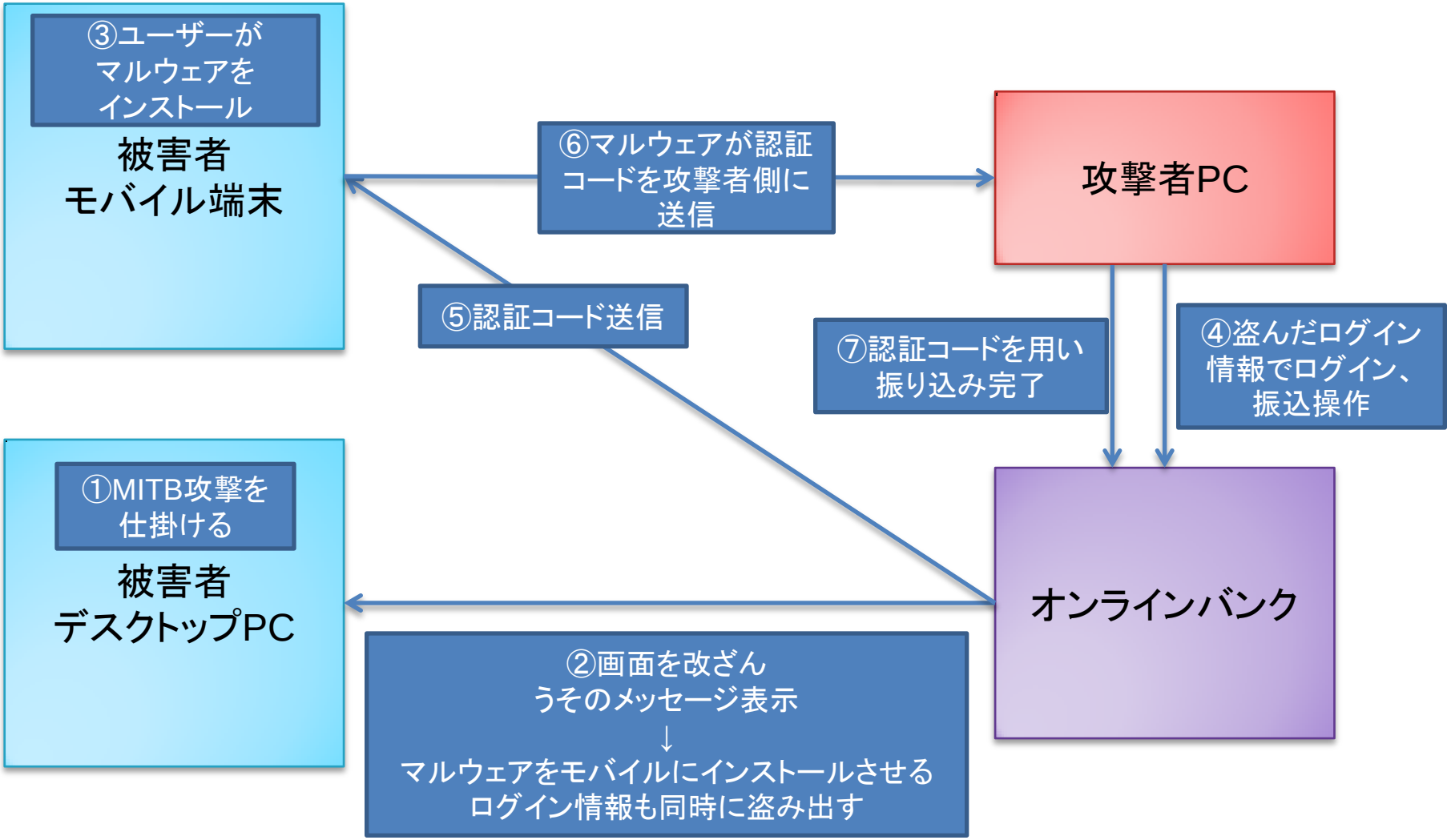
Man in the Browser (MITB)とは

- ブラウザ内に侵入して、画面を書き換える、送信されるデータを書き換える、パスワードを盗むなどを行う攻撃手法
- 主にオンラインバンクへのアクセスを監視、ユーザーの入力の搾取、改ざんを行う
- 二要素認証を用いても、正規のセッション、パスワードを攻撃時に用いることもできるため防げない
- 具体的な攻撃例については以下を参照
  - http://www.fourteenforty.jp/assets/files/monthly_research/MR201207_browser_treat.pdf

Man in the Mobile (MITMO)とMITB

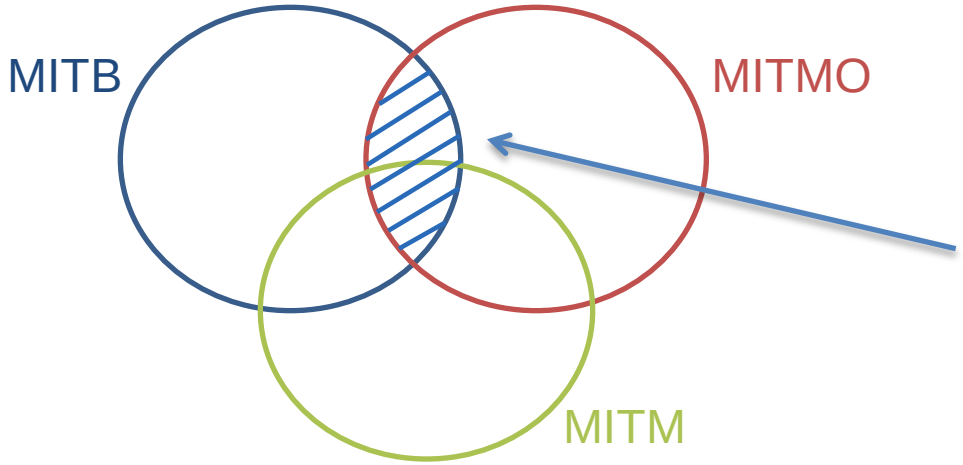
- MITBと似た用語としてMITMOがあるが、別の概念である
- モバイル端末にアプリをインストールさせることで、SMSメッセージを利用した認証を回避して攻撃を成功させるための方法
- MITBと組み合わせて攻撃に利用される
- 典型的なシナリオは以下のようなもの
  - デスクトップPCなどをMITBを用い攻撃し、「セキュリティ上必要」などのうその理由を表示させることで、利用者のモバイル端末にマルウェアをインストールさせる。同時にログイン情報も盗む。
  - 攻撃者は盗んだログイン情報を用いて、振り込み操作を行う。振り込みを完了させるにはSMSで送られてくる認証コードが必要だが、モバイル端末上のマルウェアがそれを攻撃者側に転送する。
  - 攻撃者は取得した認証コードを用いて振り込みを完了する。
- MITMO ≠ MITB

Man in the Mobile (MITMO)の流れ



MITB, MITMO, MITM(Man in the Middle)の関係

- MITBやMITMOは攻撃コードやデータが存在する場所に着目した分類
  - ブラウザ内：MITB
  - モバイル端末内：MITMO
- MITMは攻撃の形態の一つ。MITBやMITMOと組み合わせて利用されることもあるが、それ以外のものも存在する。
- それぞれ独立した概念であり、組み合わされる場合もあれば、そうでない場合もある



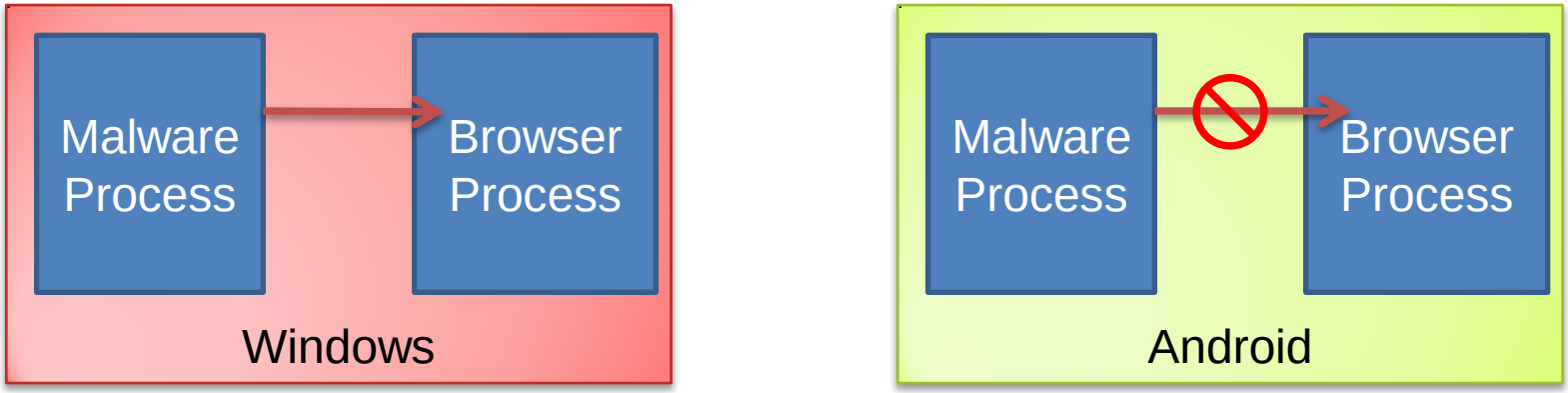
今回は、この領域の可能性について考える

MITB in Android

- MITBと言った場合、デスクトップPCのブラウザ内部に侵入しページの改ざんを行うものを指すことが多い
- これまで、モバイルのブラウザに侵入するような脅威は報告例がない
- 今回は、モバイル端末として普及しているAndroidのブラウザに侵入する攻撃方法があるのか、あるとすれば対策はあるのかを検証する

AndroidとPC(Windows)との大きな違い

- Windowsで起きるMITBがそのままAndroidで起きるか？
  - Windowsでは、マルウェアを実行してしまうと、同じユーザーで動作させている他のプロセスのメモリを変更可能
  - MITBの基本的な手法として利用される
- Androidでは各プロセス（アプリ）が別ユーザーとして動いており、他のプロセスにアクセスできないように設計されている
- Androidマルウェアをインストールしてしまってもブラウザそのものへの影響は原則ない



Androidではマルウェアが直接ブラウザに介入することができない

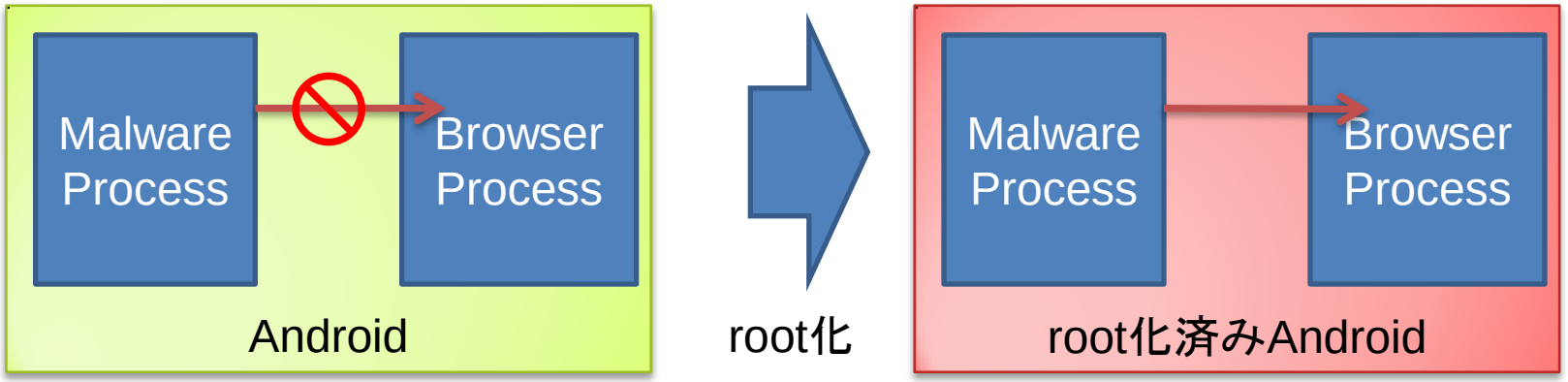
Man in the Browser in Androidの可能性

- Androidにおいて、ブラウザに介入できるとすれば、以下の4つの可能性が考えられる
  - root化端末への侵入
  - Androidシステム自体の脆弱性
  - Browser Extension
  - Class Loading Hijacking脆弱性

root化端末への侵入

- root化端末では、他のプロセスへの介入が可能となる
- root権限を持つプロセスからはメモリの書き換えやファイルの置き換えなどが自由に可能　→　無防備な状態
- プロセスのメモリの直接の書き換えのほか、アプリケーションの置き換えや、Dalvik-Cacheの置き換えなど、さまざまな手法でMITBを実現できる
- root化をした状態でAndroidを利用しないことが対策となる

root化端末への侵入



root化によりマルウェアがブラウザに介入できるようになる

LSMの効果

root化されていても、Android端末ではLSM（Linux Secure Modules)によって、root権限でできること（他のプロセスへの介入など）が制限されていることがある。ただし、LSMが有効であっても、他のプロセスへの介入が可能になる例も報告されており(*1)、root化した端末ではMITBに対するリスクは相対的にはかなり高くなるといえる。

*1 http://www.fourteenforty.jp/assets/files/research/research_papers/yet-another-android-rootkit.pdf

Androidシステム自体の脆弱性

- Androidシステム自体に脆弱性がある場合、root化される、ブラウザプロセスを乗っ取られるといった可能性がある
- ブラウザが読み込むライブラリに脆弱性があり、任意のコードが実行可能であった場合、MITBは可能となる
  - ただし、ASLRやDEPなどの実装により最近のAndroidではこのタイプの攻撃は困難になってきている
- 対策としてはアップデートを適切に行うことが挙げられる

Version	-2.2	2.3-,3.0-	4.0-	4.1-
DEP(スタック)	×	○	○	○
DEP(その他)	×	○	○	○
ASLR(スタック)	○	○	○	○
ASLR(ヒープ)	×	×	△	○
ALSR(モジュール)	×	×	△	○

AndroidのDEP, ASLRへの対応状況
http://www.fourteenforty.jp/assets/files/research/research_papers/InternetWeek2011_s10-02.pdf
より一部修正、追記して転載

Browser Extension

- Android版Firefoxはブラウザアドオンをサポート
- 悪意あるアドオンを導入してしまった場合、画面等を書き換えられる可能性がある
- アドオンが安全かどうか判定する明確な方法はない
- AMO(addons.mozilla.org)には、審査を通ったもののみが登録されている
- 対策としては、ウェブページなどで促されるままにAMO以外からアドオンを導入しないこと

Class Loading Hijacking脆弱性の利用

- AndroidにはClass Loadingという外部のDEXコードを読み込む機能があり、ネットワーク上のファイルなどをコードとして取り込める
- Class Loadingの仕方を間違えると、WindowsのDLL Hijackingと同様の脆弱性を作りこんでしまう
- ただし、Android APIのドキュメントにも注意書きが存在しており、主要ブラウザでこのような問題を作りこんでしまう可能性は低い
- Android Class Loading Hijackingについては以下を参照
  - http://www.symantec.com/connect/blogs/android-class-loading-hijacking

(参考)Browser以外での脅威

- MITBではないが、多くのMITBを利用した攻撃が最終目標とするオンラインバンクのデータ通信の搾取、改ざんという攻撃を行うために使われる可能性のある方法として、ブラウザ以外の銀行専用アプリへの攻撃が考えられる
- これらにClass Loading Hijacking脆弱性がある場合、それらのアプリの改ざんによりMITB同様の攻撃が可能となる
- また、専用アプリに似せた偽アプリを利用してしまうことで攻撃される可能性がある。

MITB in Androidの可能性と対策

ユーザーが行える対策をまとめると、以下のようになる

可能性	対策
root化端末への侵入	root化を故意に行わない root化した端末を利用しない
Androidシステムの脆弱性	システムのアップデート
Browser Extension	AMO以外からのアドオンのインストールを控える
Class Loading Hijacking	ブラウザのアップデート

まとめ

- AndroidのブラウザのMITBによる攻撃はWindowsなどに比べるとハードルが高い
- ただし、root化によってそのリスクは上がる
- root化されてない場合、システムの脆弱性やブラウザプラグインの利用といった可能性が残る
- root化端末を利用しないことが第一の対策となる
- MITBに関して言えば、マルウェアを実行してしまうだけで、MITBが可能となってしまうWindows PCを利用するよりも、Androidを利用したほうが安全
- MITB以外の、フィッシングや、偽アプリにはWindows PC同様注意が必要