VMMを用いた2段階認証の支援

石井智也[†] 忠鉢洋輔[†] 表祐志[†]
品川高廣[††] 加藤和彦[†]

1. はじめに

近年, なりすましによる不正ログインへの対策として, 携帯端末を用いた2段階認証[1)]の導入を行うWebサービスが増加している.2段階認証とは, セキュリティの強化を目的として, 2つの要素を用いて行う認証のことである. 例えば, Google社が提供しているWebサービスの1つであるGmailでは, ログイン時にユーザー名とパスワードの入力に加えて, ユーザーの携帯端末の操作によって得られるワンタイムパスワードの入力を用いる認証方法を提供している. これはパスワードと携帯端末という2つの要素を用いた2段階認証となっている. ログイン時に携帯端末を用いた2段階認証を利用していれば, 第三者による不正ログインが試行された場合でも2つ目の認証手段である携帯端末を用いた認証を通ることができないため, 不正ログインを防止することができる.

しかし, 携帯端末を用いた2段階認証の場合, ユーザーはログインを行うPC等に加えて携帯端末の操作を行い, 認証用コード (ワンタイムパスワード等) の取得をしなければならない. これにより, 認証時の手間が増加するという問題がある. また, 2段階認証を行うためには携帯端末をあらかじめ用意する必要があり, 2段階認証に使用できる携帯端末を所持していないユーザーは2段階認証を用いることができない. また, 認証時に紛失や故障等で携帯端末が使用不能となっていた場合には認証できないという問題点もある[2)].

ログイン時の認証方法に2段階認証を用いた場合の利点である, なりすましに対する有効性を損なわずに2段階認証の問題点を解決するために, 本研究ではログインを行うユーザーのPCに仮想マシンモニタ (VMM) であるBitVisor[4)]を導入し, VMM内部で2段階認証時における携帯端末の処理を代替する手法を提案する. 提案手法により, 携帯端末を所持していないユーザーでも2段階認証を行うことを可能にし, 加えて, 認証時の手間を増やさずに2段階認証を用いる事を可能にする. また, 携帯端末の処理をVMM内部で行ったとしても, 第三者が2つ目の認証を通ることができないという点は変わらないため, なりすましによる不正ログインに対する有効性も保っている.

† 筑波大学システム情報工学研究科
†† 東京大学情報基盤センター情報メディア教育研究部門

2. 提案手法の概要

本研究では, 2段階認証時の携帯端末が行う認証をVMM内で行う手法を提案する. ここでの2段階認証は、パスワードの入力と携帯端末から得る認証用コードの入力を行う. 認証の初めにユーザーはゲストOSからVMMに対して認証用コードの取得を要求する (図1中 (1)).VMMはユーザーからの要求に応じて認証用サーバと通信を行い, 認証用コードを取得する (図1中 (2)). その後, VMMは取得した認証用コードをユーザーに渡し (図1中 (3)), ユーザーはパスワードとVMMから渡された認証用コードを入力して認証を完了する (図1中 (4)). この手法では携帯端末を用いた認証の手続きをVMM内部で行い, ログインに必要な認証用コードをユーザーとやり取りすることで, ログインを行うPCを操作するだけで2段階認証を行うことを可能にする. また, ゲストOSが悪意ある第三者によって乗っ取られた場合を想定し, ユーザーとVMMの間でやり取りされる情報はゲストOS上のプログラムからは自由に取得出来ないようにする. なお, 本研究では脅威としてPCの物理的な盗難は想定していない.

提案手法によって, ユーザーは2段階認証時に携帯端末を操作する必要がなくなる. また, 第三者にユーザー名とパスワードが知られた場合でもなりすましによるログインに対する有効性を失わないので, ユーザーの手間を増加させること無く2段階認証を行うことを可能とする.

3. 現在の状況と今後の予定

現在, Gmailでの2段階認証に用いるGoogle-

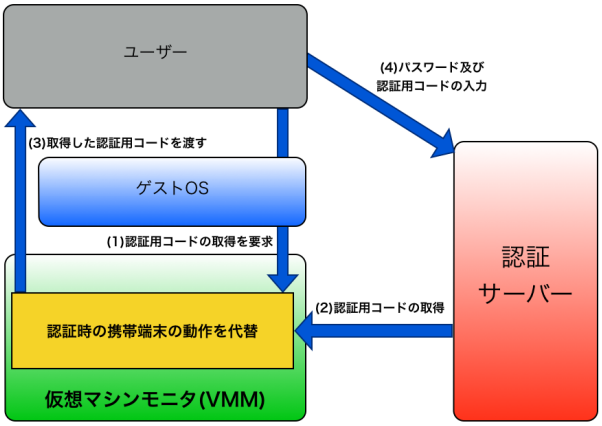

図 1 提案手法の概要

Authenticator[3] と呼ばれるトークンソフトウェアによるワンタイムパスワードの生成を BitVisor 内で行う為の実装を行い, 正しく動作することを確認した. 今後は Gmail 以外のサービスで用いる 2 段階認証でも対応できるように BitVisor の機能を拡張していく予定である.

参 考 文 献

1) F Aloul, S Zahidi, W El-Hajj. Two factor authentication using mobile phones. Computer Systems and Applications, IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp. 641-644, 2009.
2) A Czeskis, M Dietz, T Kohno, D Wallach, D Balfanz. Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions. In the Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS), 2012.
3) Google-Authenticator. https://code.google.com/p/google-authenticator
4) T Shinagawa, H Eiraku, K Tanimoto, K Omote, S Hasegawa, T Horie, M Hirano, K Kourai, Y Oyama, E Kawai, K Kono, S Chiba, Y Shinjo, K Kato. BitVisor : A Thin Hypervisor for Enforcing I/O Device Security. ACM SIGPLAN/SIGOPS international conference on Virtual execution environments(VEE), 2009.