

シングルサインオン認証に関する研究

堀井 信吾[†]

[†]東京電機大学大学院 情報環境学研究科

1. はじめに

インターネットの幅広い普及とサービスの多様化に伴い、認証情報が増大している。これにより利用者はID・パスワードの管理が大きな負担になり、さらにはなりすましや不正アクセスなどによる情報漏洩が問題となっている。この問題を解決する手段としてシングルサインオン認証が挙げられる。本研究ではこのシングルサインオン認証に、リバースプロキシ方式を軸としてKerberos認証とワンタイムパスワード認証を組み合わせた新しいモデルを提案・研究していく。

2. シングルサインオン認証とは

一度の認証手続きで権限内の複数のサービスやシステムを利用できるようにすることである。[1] ID・パスワードを一つにすることにより利用者のストレスを低減し、不正アクセスやなりすましのリスクの低減する。管理者は利用者のパスワード忘却・紛失などによる再発行などの手間の低減やID・パスワード管理の手間の低減する。シングルサインオン認証の代表的な方式に、エージェント方式とリバースプロキシ方式が挙げられるが今回はリバースプロキシ方式を採用した。採用した理由は後述する。

2. 1 リバースプロキシ方式

リバースプロキシ方式はWebサーバへのアクセス全てを一台のシングルサインオンサーバが管理する方式であり、シングルサインオンサーバが利用者とWebサーバと認証サーバを中継するシステムである。[2]リバースプロキシ方式のメリットとしては、使用するWebサーバが限定されることはなく、Webサーバに手を加える必要も無い。デメリットとしては、シングルサインオン用のサーバが全てを中継しているため、シングルサインオン用のサーバ負荷が高くなる。今回はWebサーバが限定されることがなく、Webサーバに手を加える必要も無いというメリットに注目し、リバースプロキシ方式を採用した。

3. 組み合わせる認証技術

3. 1 Kerberos 認証 (Ver5)

Kerberos とは利用者と Web サーバの相互認証を KDC (Key Distribution Center) と呼ばれる信頼できる第三者機関によって行われている。今回は Ver5 で提案をする。Ver5 では、KDC には、認証サーバとチケット交付サーバが入っている。利用者は KDC と認証のやり取りを行い、利用したいサーバチケットを手に入れ、サーバにチケットを提出して利用する形である。なお、Ver3 までは KDC が一つだったためにリプレイアタックの問題があったが、Ver4 からは今の形になりチケットにタイムスタンプが押されるためリプレイアタック対策、さらにはなりすまし対策に対応した。

3. 2 ワンタイムパスワード認証

ワンタイムパスワード認証とは、認証のために一度しか使うことができない使い捨てのパスワードのことである。代表的にはタイムスタンプ方式とチャレンジ・レスポンス方式が挙げられる。今回はチャレンジ・レスポンス方式を採用した。チャレンジ・レスポンス方式でのチャレンジとは認証サーバから意味のない数値列を送ることで、この数値はランダムに変化する。レスポンスとは利用者がその数値を入力し認証要求することである。Web サーバ側が最初に送るチャレンジを毎回変えているので、レスポンスも毎回変化する。このことによりワンタイムパスワードを満たしている。

4. 提案モデル

これまで挙げてきた Kerberos 認証とワンタイムパスワード認証の二つの認証技術をリバースプロキシ方式に組み合わせることにより図 1. のようなシングルサインオン認証の新しいモデルを提案する。図 1. はイメージ図である。

- [1] シングルサインオンサーバに認証要求をする。ここでの認証要求でワンタイムパスワードを利用する。
- [2] KDC と認証処理を行う。
- [3] 認証が成功すると権限内の Web サーバの利用が出来るモデルである。

Research on Single Sign-On Attestation
Shingo Horii[†]

[†]Tokyo Denki University

Graduate School of Information Environment

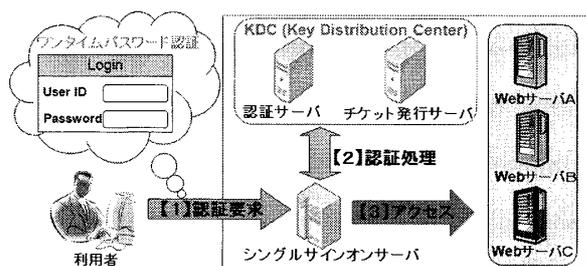


図 1. 提案モデルのイメージ図

4. 1 認証過程

図 2. を使い認証過程を説明する。

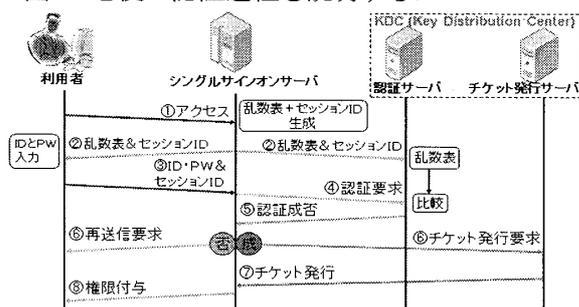


図 2. 提案モデルの認証過程

- ① 利用者はシングルサインオンサーバにアクセス要求をする。
- ② シングルサインオンサーバは要求を受けた時点で乱数表と利用者のセッション ID を生成し、利用者と認証サーバの双方へそれぞれ情報を送信する。
- ③ 利用者は受信した乱数表からパスワードを入力し、ID とセッション ID を共にシングルサインオンサーバに送信する。
- ④ シングルサインオンサーバは受け取った ID・パスワードとセッション ID を認証サーバに認証要求という形で送信する。
- ⑤ 認証サーバは事前に②で受信していたセッション ID から利用者情報を取り出し乱数表から利用者のパスワードを生成し、送信されてきたパスワードと比較する。この認証部分の詳細は 4. 2 に後述する。認証サーバは認証の成否をシングルサインオンサーバに送信する。
- ⑥ 認証が否認された場合は利用者に再送信要求をし、成功した場合はチケット発行サーバにチケット発行要求する。
- ⑦ チケット発行サーバは、利用者の権限に合ったチケットをシングルサインオンサーバに送信し、チケットを受け取り保持する。
- ⑧ チケットはシングルサインオンサーバが保持しているため、利用者は権限を付与してもらうことにより、Web サーバが利用できる。

4. 2 ワンタイムパスワード認証部分

今回提案するワンタイムパスワード認証では、利用者は図 3 のように乱数表の場所を記憶するという位置情報を取り入れた提案をする。

～乱数表～

～情報入力～

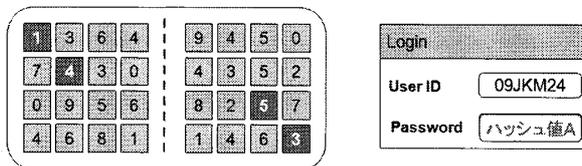


図 3. 位置情報を利用した認証

図 3 の乱数表の場所を利用者は自分で設定し、記憶しておく。パスワードには乱数表から設定した数値を入力する。但し、そのまま情報を送信しては危険なため、パスワードに ID を付加してハッシュ化したハッシュ値 A を送信する。認証サーバ側でも同じことを行い、ハッシュ値を比較して認証を行う。こうすることで、データの改竄が行われているかを確認することができ、安全に認証できる。

5. 考察

今回の提案モデルにより、シングルサインオン認証の特徴をさらに強化されると考察する。Kerberos 認証の導入によりチケット制になり、不正アクセスのリスクを低減できる。しかし、Kerberos 認証には弱点がある。最初の認証段階で盗聴されることでなりすましが可能となる。そこで、パスワードが毎回変わるワンタイムパスワード認証の導入により、弱点を解決できる。さらには、利用者は数値ではなく任意の位置を記憶することによりストレスの低減につながると考察する。このことにより、管理者はパスワード紛失時の再発行等の労力を低減することができる。

6. 今後の予定

今後は、シングルサインオンサーバの高負荷をどのように解決するかを検討し、権限付与に関して検討を行う。現在ワンタイムパスワード認証部分の実装途中であり、その後提案モデルへの拡張を行う予定である。

参考文献

- [1] http://www.exa-corp.co.jp/techinfo/review08/11_nakatani.pdf
- [2] http://www.nec.co.jp/solution/security/attestation_base/access_control.html