Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)

フィッシングを防止する HTTP 相互認証プロトコルの設計と IETF への提案

Yutaka Oiwa, Hajime Watanabe, Hiromitsu Takagi – RCIS, AIST

フィッシング詐欺とWeb認証

- フィッシング：偽のWebページによりユーザの秘密情報を盗む攻撃
  - いわゆる「Social Attack」の1つ
- 最近のWeb の利用形態の変化により脅威はますます増大している
  - 「他サイトから誘導されるページ」での認証要求の増加
    - サイト共通の認証基盤 (OpenID)
    - サイト間での権限委譲 (OAuth)
    - * 誘導された先のサイトでページが正当なものかどうかを判別するのは困難

現状のWeb認証の問題

HTTP (通信層)での認証 (RFC 2617)
• Basic 認証
•Digest 認証

⇔

HTML (アプリ層)でのフォーム＋Cookie認証
商用サイトでは主流

フォーム＋Cookie認証の問題点：

- パスワードが相手に直接送られる
  - フィッシングに非常に脆弱
- 標準プラットホームの欠如
  - バグの原因になりやすい

現行のHTTP認証の問題点：

- 現代的Webアプリに求められる**機能の欠如**
  - 時代遅れのUIダイアログ
  - ログアウト・サーバ側での認証管理
  - 認証の有無の選択
    - » 同じURIで双方を提供するのが困難
- 暗号的セキュリティ強度の不足
  - Basic 認証: パスワードを直接送信
  - Digest 認証: セキュリティ的にはまだ不十分
    - » オフラインでパスワード解読可能
    - » 認証結果の偽装が可能
    - (1方向認証なのでユーザはサーバが正しいことを確認できない)
    - » 現在の実装の互換性にも問題あり

我々の提案の概要

PAKE プロトコルをHTTPに導入

- パスワードだけを用いる強力な認証プロトコル
- 通信相手が認証情報を保持していることを**相互に認証**する
  - ユーザも、サーバが正しいサイトであることを確認できる
  - (ユーザ登録していない)サイト相手には認証が必ず不成立
    → フィッシング対策になる
- 盗聴・偽サイト等で入手した通信データからはパスワードが暗号的に解析できない

HTTP認証向けのPAKEの拡張

- 中継攻撃の直接的な検知
- 繰り返しアクセス向けの計算コスト最適化 等

同時に、HTTP認証の様々な問題点を解決

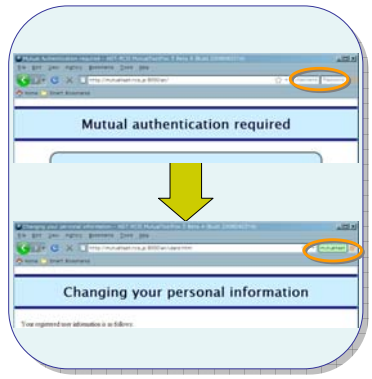
- 現代的な(ダイアログを使わない)UI
- サーバからのログアウト制御
- Optional 認証(ゲストユーザのサポート)
- 認証専用ページなどの詳細な制御

安全な UI の検討

安全性確保のための新たな認証UIの提案

- 偽サイトにパスワードが盗まれないこと
- 相互認証結果を確実にユーザが確認できること

[PC でのデモ有り]



現在の状況

Internet-Draft として IETF に標準化提案

- “draft-oiwa-http-mutualauth-06.txt”
- WG へ向け apparea で現在活動中

複数のオープンソース実装の作成と公開

- サーバ側: Apache, Webrick
- クライアント側: Mozilla, Ruby module

実証実験

- RCIS プロジェクトWebページ上
- Yahoo! Japan お試しオークション(in 2008)

Project URL: https://www.rcis.aist.go.jp/special/MutualAuth/