フィッシング対策のための HTTP 相互認証プロトコル
HTTP Mutual Access Authentication

大岩 寛, 高木 浩光, 渡辺 創　　ーヤフー株式会社オークション事業部との共同研究 ー

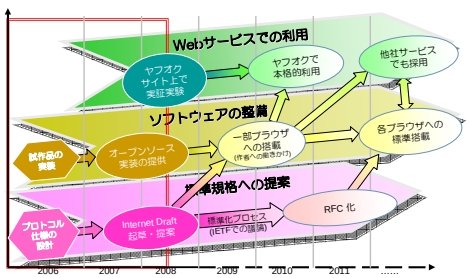
Web に適した新パスワード相互認証プロトコルの提案

- 高い安全性
  - 偽サイトを確実に検出
    - ユーザ、サーバを相互に認証することで実現
  - 偽サイトへのパスワード漏えいを防止
    - オフライン辞書攻撃にも対処
      (↔DIGEST 認証, pwd_hash:
      パスワードを安全に保つには20文字以上が必要)
- 利用の容易性
  - 人間が記憶可能なパスワードのみを使用
  - ユーザによる秘密情報の保持が不要
    (↔TLS クライアント認証, パスワードリマインダ)
- 高い汎用性
  - ホワイトリストが不要 (↔EV SSL)
  - ブラックリストが不要 (↔IE/Firefox での警告)
  - どのサイトでも利用可能 (↔専用ツールバー)
- ★ *長期的な視点からの解決を目指して：*
  - *将来のフォームによる認証の置き換え*

フィッシングの形態による分類：
1. ユーザパスワードの詐取
2. サーバの「ログイン成功」動作の模倣
   その後に個人情報を盗むため
3. パスワードの正当性チェック
   そのまま正当なサイトへ転送することで実現
   （中間者攻撃）

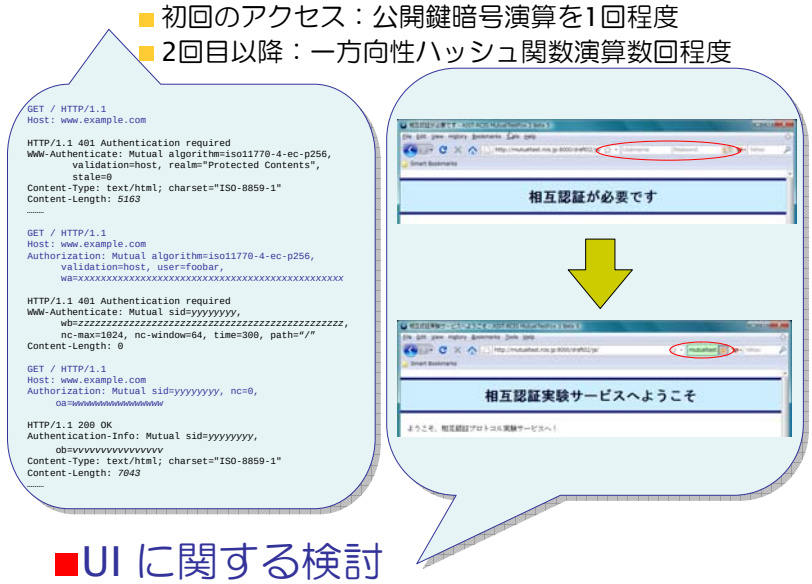
提案手法の技術的な特徴

- PAKE を Web の認証に適用
  - 弱い秘密情報（パスワード）による相互認証
  - パスワード情報漏えいを防止
    - オフライン辞書攻撃にも対処
  - RFC2617 の自然な拡張として認証法を設計
  - BASIC/DIGEST 認証の置き換え
  - フォームによる認証の置き換え
  - ペイロード部分の秘匿は TLS との組み合わせで実現
- ホスト名を利用したフィッシングの検出
  - 中間者攻撃の回避



プロトコル詳細

- ISO/IEC 標準となっている PAKE を利用
  (ISO/IEC 11770-4 KAM3)
  - パスワードとホスト名を「弱い秘密情報」として使用
  - 中間者攻撃を回避
    π = H (password, host)
- サーバ/クライアントでの計算量は TLS 並
  - 初回のアクセス：公開鍵暗号演算を1回程度
  - 2回目以降：一方向性ハッシュ関数演算数回程度



UI に関する検討

- 入力フィールドの画像による偽造への対処
  - ポップアップダイアログの不採用 (↔BASIC/DIGEST 認証)
  - 例：ブラウザのクロム領域の利用 (上のブラウザ画像参照)
- ユーザによる認証状態確認容易性の実現
  - 偽サーバによる「認証成功の振り」の防止

プロジェクトの現状

- Apache HTTP サーバの認証モジュール実装の公開
- ブラウザ試験実装 (MutualTestFox) の公開
- Internet-draft 提出 & IETF での標準化活動開始

今後の予定

- ヤフーオークションサイトでの実証実験
- オープンソースコミュニティへの働きかけ

関連研究

- EV-SSL … 皆が信頼すべき機関が必要
- passpet … 秘密鍵の保持が必要
- pwd_hash
  - 同様のホスト名を用いた偽サイト検知を採用
  - オフライン辞書攻撃には脆弱