Visolve – Open Source Solutions

Customized Solutions for Your Business Enrichment
Visolve – Securing Digital Assets

Contents

- Security Overview
  - Security Concerns
  - Security Needs

- Technical Overview
  - Two – Factor Authentication System
  - OTP – One Time Password Solutions
  - OATH – Open Standards for OTP
Security Layers - Challenges

- Authentication
  - Ability to Validate
  - Proving Identity

- Authorization
  - Access to Network
  - Allowing to Transact

- Accounting
  - Management
  - Auditing

- Users
  - Profiling

- Security Policy
  - User Rights
  - Access Levels

- Security Platform
  - Applications Interface

- Security Device
Security Threats & Business Needs

- **Vulnerabilities**
  - Cyber Crime – Identity theft and Fraud
  - Phishing & Pharming attacks becoming more sophisticated and malicious

- **Business needs**
  - Enhanced Security: Stronger user authentication
    - Two Factor authentication System
  - Cost effective Password & Identity Management
  - Delivery Mechanism – Convenience of carrying security devices and ease of use
Power of One-Time Password (OTP)

- OTP deployment makes full life-cycle management easy & cost effective
- Flexibility and availability of various OTP methods – time synchronized, event synchronized or challenge response
- Password generated valid for single use
- Enhanced security environment for users to authenticate and transact on web
- Centralized repository of User profiles and credentials
Visolve – Open Standards for OTP

- Today, with the exception of RADIUS, integration of OTPs can be achieved only through costly proprietary interfaces & protocols
- Can leverage on existing VPN/Wireless LAN infrastructure
- Low cost/no vendor lock alternative to proprietary solutions
- Easily added to existing web server password validation infrastructure
- Token based solution now inexpensive for wider B2C deployments
Technology Overview

HP – UX AAA Server and OATH:
Standard Based Two – Factor Authentication
Technology - Framework

- **Two - Factor Authentication**
  - Authentication using two independent method – typically something you have (device) and something you know (password)

- **One - Time Password**
  - Password valid for single use
  - Two-Party Model: Client and Server use OTP software or hardware to generate and validate password
  - Two-Channel Model: High value transaction can be authenticated by requiring an OTP being delivered through secondary channel vis email or SMS

- **OATH**
  - Open standards for OTP generation
    - [http://openauthentication.org](http://openauthentication.org) sequence based algorithm
  - Supported by all of the token device vendors
Advantages of OATH vs. Proprietary OTP

- **Low Cost**
  - Sequence based algorithm allows low manufacturing cost for token device
  - No Royalty Programs
  - Leverage in both price-points and form-factors

- **Wide variety of user deployment models**
  - Standalone token device can be built into consumer electronics
  - Secondary channel solutions – SMS

- **No Vendor Lock**
  - Client, Server, user management components can be purchased separately
  - Multiple OTP clients can be concurrently supported from the same authentication server
OATH/OTP Authentication Opportunities

- **User Tokens**
  - Low priced tokens from multiple vendors
  - Soft-tokens that can run on java enabled device-mobile phones
  - SMS delivery of OTP for non java enabled devices

- **Mobile makes ideal OTP device**
  - Ubiquitous
  - Leverage applications provisioning to manage OTP soft-token
  - Addressing Consumer issue of handling multiple hard tokens

- **Opportunity for OTP authentication as telecom service**
  - Consumer authenticates to bank/retailer
  - Retailer authenticates password locally
  - Forward OTP to Service Provider
## OATH/OTP Vs. Other Major Authentication Technologies

<table>
<thead>
<tr>
<th>Method</th>
<th>Password</th>
<th>OTP + Password</th>
<th>Digital Certificates/PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td>Widely used and supported by the largest number of applications</td>
<td>Two-factor authentication compatible with password based infrastructure: zero client footprint option</td>
<td>Bi-directional authentication</td>
</tr>
<tr>
<td></td>
<td>Technology easily understood by users</td>
<td></td>
<td>Can provide two-factor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Non-repudiation</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td>Relies on human protection and management of the secret.</td>
<td>Requires possession of OTP generation software/hardware or access to a secondary channel for OTP transmission</td>
<td>Certificate management cost can be prohibitive for large user base.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Heavy footprint to manage on client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not compatible with small devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Requires distribution of certificate/smart card to client.</td>
</tr>
<tr>
<td><strong>Key Vulnerabilities</strong></td>
<td>Brute force</td>
<td>Man-in-the-middle/client insertion</td>
<td>User override of warnings</td>
</tr>
<tr>
<td></td>
<td>Man-in-the-middle/client insertion</td>
<td>Phishing (reduced to one time action)</td>
<td>Client insertion (reduced)</td>
</tr>
<tr>
<td></td>
<td>Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Over the shoulder</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Keystroke loggers</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Applicability</strong></td>
<td>Lower risk environments</td>
<td>B2C Commerce</td>
<td>Highly secure environments</td>
</tr>
<tr>
<td></td>
<td>Legacy environments</td>
<td>Enterprise Security (VPN)</td>
<td>Monetary or legal transactions where non-repudiation is a required feature</td>
</tr>
<tr>
<td></td>
<td>No network usage or protected network usage</td>
<td>Environments not suited for PKI (e.g. password based application infrastructure)</td>
<td>Environments where mutual authentication is required.</td>
</tr>
</tbody>
</table>

Customer slide presentation from HP
**OATH Soft Tokens: Three Tier-Service Provider Model**

1. **Provisioning**
   - User Key and sequence number are generated by service provider.
   - Key and OATH Applet are delivered to user device by client provisioning service.

2. **Local Authentication**
   - User connects to web retail presence via browser.
   - Password verified locally.

3. **OTP Authentication**
   - User provides OTP from cell phone. Passed to Service provider for verification.

4. **Multiple Retailers**
   - Multiple retailers share the same OTP service, while locally maintaining password authentication.

Customer slide presentation from HP
**OATH: Provisioning Life Cycle: Token Cards**

1. **New Installation**
   - Supplier delivers tokens and key file. Admin tool imports serial number/key pairs into secure storage.

2. **New User**
   - Serial number key and sequence number assigned to user entry. Token device is delivered to user.

3. **Help Desk**
   - User entry can be resynchronized with user’s token device if needed.

4. **Deactivate User**
   - User entry locked. Token device may be assigned to another user.
Basic Password Authentication Sequence
Adding Two Factor Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>User name/password entered on client device&lt;br&gt;Oncally appended to password field (separate prompt or combined with existing password input)</td>
</tr>
<tr>
<td>2.</td>
<td>Protocol&lt;br&gt;VPN: L2TP/IPSec&lt;br&gt;C: 802.1x&lt;br&gt;Web: HTTPS&lt;br&gt;\ldots Etc.</td>
</tr>
<tr>
<td>3.</td>
<td>Web Server, VPN Gateway, Firewall, WLAN Access Point, Unix (login/SSH,\ldots) etc&lt;br&gt;Authenticate password locally or forward to AAA</td>
</tr>
<tr>
<td>4.</td>
<td>Protocol&lt;br&gt;RADIUS</td>
</tr>
<tr>
<td>5.</td>
<td>AAA Server&lt;br&gt;Authenticates password&lt;br&gt;Tracks and logs user session&lt;br&gt;OTP validated, token sequence number updated in database</td>
</tr>
</tbody>
</table>

Existing password based single factor authentication infrastructure.

Two factor authentication can be added with minimal disruption. Zero client software changes possible.

Customer slide presentation from HP
HP-UX AAA Server Overview

**Purpose:**
- Centralized service to provide authentication and recording of user access to network resources
- Control access to wireless LANs, VPN gateways, HTTP servers, and other RADIUS enabled devices or applications
- Provides access and accounting control for greater security and compliance

**Advantages:**
- Based on widely supported RADIUS and Extensible Authentication Protocol standards
- High performance/high availability features for enterprise and service provide deployments
- Supports a wide variety of authentication methods including password, token cards and digital certificates
- Highly customizable, supports ODBC compliant databases and LDAP compliant directories
- Included with HP-UX11i

Customer slide presentation from HP
OATH: Higher level HMAC-based One Time Password Algorithm (HOTP)

**Generate OTP**

1. Shared Secret (20 bytes)
2. Sequence Counter (8 bytes)
3. HMAC-SHA1
4. Truncate
5. OTP (6 or 8 Digits)

**Validate OTP**

1. Password + OTP
2. Authenticator
3. AAA Server
4. Shared Secret Sequence Counter +1
Visolve – Fortune 100 Clients

- SMB’s

- DTS - Largest ISP in Madagascar
- Several K-12 School Districts
- ISPs in US and Canada
- City of St.Paul, MN
- Blueprint Data, FL
- Fanshawe College, London
- Genesis Technology, Taiwan
- Axseed – Japan
THANK YOU