Security Awareness for User Authentication: Passwords and Beyond

Host:
Rodney Petersen, EDUCAUSE

Speakers:
Cathy Hubbs, American University
Tom Davis, Indiana University
Bob Hillhouse, University of Tennessee
IAM Online
Security Awareness for User Authentication: Passwords and Beyond

Cathy Hubbs, CISO
Password Best Practices and User Awareness
October 9, 2013
Activities & Resources

• Available for distribution: Winning entries of the 5th Annual Information Security Awareness Video and Poster Contest

• The Security Guide “Toolkits”
  – “NCSAM Toolkit”

• 10% of the 2013 activities focus on passwords
  – Passwords are still being used...
People who can't log in to my account because of my ultra high security password
PROTECT YOUR PERSONAL DATA – CHANGE YOUR PASSWORD OFTEN

Make it strong – use a long mix of letters, numbers and symbols.
Use different passwords for important accounts.
You can name her whatever you like but be sure it’s something you can remember. You’ll be using it as a security question answer for the rest of your life.
"Sorry, your password must contain a capital letter, two numbers, a symbol, an inspiring message, a spell, a gang sign, a hieroglyph and the blood of a virgin"
CASE STUDY  American University

• Survey of Student, Faculty & Staff

• Issues
  – Frequency of Password Change (90 days)
  – Experience during change (Multiple Devices)

• We surveyed our peers about passphrase use

• We ran our ideas by our auditors

• We landed with giving customers the option…
Password Options

Original Policy
- 8 character limit
  - Start with a letter
  - Mixed Case
  - Number or Symbol
  - 90 day expiration
- Unique within the year

New Policy
- 16 character minimum length + upper and lower case
- 365 day expiration
- Unique from last 2 passwords
Wrap Up & Next Actions

• Implemented a new notification system to send email reminders prior to users’ password expiration
• Finished before students came back
• October 3rd requested feedback on changes
  – Positive results thus far
• Next
  – Pilot Project two-factor for privileged accounts
Security Awareness for User Authentication: Passwords and Beyond

Tom Davis, Chief Security Officer, Indiana University

Passphrase Vaulting
Best Practice?

• Choose complex passwords or long passphrases.
• Use different passwords for each service or class of service.
• Do NOT write passwords down.
Password Management is Hard Work!

• Generating easy to remember but difficult to guess and crack passwords.
• Remembering multiple complex passwords and passphrases.
Password Vault?

- Securely stores passwords (or more generally secrets) within the vault.
- “Key” is a very strong password/passphrase.
Why use a Vault?

• Users only need to remember one password – the “key” to the vault.
• Generates and stores complex passwords.
• Facilitates future use of passwords.
• Allows user to maintain unique passwords across all services.
Common Vault Features

• Integrates with common browsers.
• Auto-fills passwords on web sites.
• Provides defense against phishing.
• Generates complex passwords.
Common Vault Features

• Supports multiple operating systems.
• Provides sync-ing between devices.
• ... and more (credit cards, shipping addresses, secure notes, etc.)
Vaulting in(to) Action!
Central Authentication Service

Username:

Passphrase:

Login

Trouble signing in? We can help.

For security reasons, you will need to close your web browser when you finish using services that require authentication.
Central Authentication Service

You have been logged in successfully.

For security reasons, quit your web browser when you are done accessing services that require authentication.
Vault Best Practices

• Use a strong passphrase to lock the vault.
• Ensure passphrase used to lock the vault is different than any of those stored in the vault.
• Protect the vault file (and resist cloud sync-ing).
Vault Best Practices

• Clear the clipboard.
• Never leave computer logged in and unattended.
• Don’t lose vault passphrase or file.
For more information:

• http://go.iu.edu/8uz
A Case for Multi-factor Authentication

You’ve got 30 minutes until the meeting.

Bob Hillhouse
Associate Chief Information Officer,
University of Tennessee
Cast

- The University of Tennessee, Knoxville
- 57 merchants across campus
- The UT Office of the Treasurer
- The Office of Information Technology (OIT)
Act I - Prelude

- PCI-DSS Requirement 8.3
  - Incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties...

- 100 devices in the PCI-Subnet require Remote Desktop Services (RDP)
Act II – The Timeline

- 8:00 AM
- 8:15 AM
- 8:30 AM
- 9:00 AM
Act III – Prologue

- 2013 – The end of strong password-only security.
  - [http://bcove.me/29pw0pz5](http://bcove.me/29pw0pz5)

- Are Smartphones Killing Passwords?
Evaluation
Please complete the evaluation of today’s IAM Online:
http://www.surveymonkey.com/s/IAMOnline_October_2013
<table>
<thead>
<tr>
<th>Day</th>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>Nov. 11</td>
<td>REFEDS – Global R&amp;E Federation Operators</td>
</tr>
<tr>
<td>Tuesday</td>
<td>Nov. 12</td>
<td>Advance CAMP Identity Services Summit</td>
</tr>
<tr>
<td>Wednesday</td>
<td>Nov. 13</td>
<td>Advance CAMP Identity Services Summit (through noon)</td>
</tr>
<tr>
<td>Thursday</td>
<td>Nov. 14</td>
<td>CAMP: Managing Identity and Access in an Era of Distributed Services</td>
</tr>
<tr>
<td>Friday</td>
<td>Nov. 15</td>
<td>CAMP: Managing Identity and Access in an Era of Distributed Services</td>
</tr>
</tbody>
</table>

**Registration Still Open**

- **Thursday, Nov. 14**
  - CAMP: Managing Identity and Access in an Era of Distributed Services

**SOLD OUT**

- **Monday, Nov. 11**
- **Tuesday, Nov. 12**
- **Wednesday, Nov. 13**
- **CAMP Pre-Conference: Getting Started with Federated Identity Management (afternoon)**
InCommon Shibboleth Workshop Series

Installation Training for Shibboleth
Single Sign-on and Federating Software

October 21-22 – University of Nebraska Omaha – Omaha, NE
Details and registration at www.incommon.org/shibtraining
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by Internet2’s InCommon, in cooperation with the EDUCAUSE Identity and Access Management Working Group