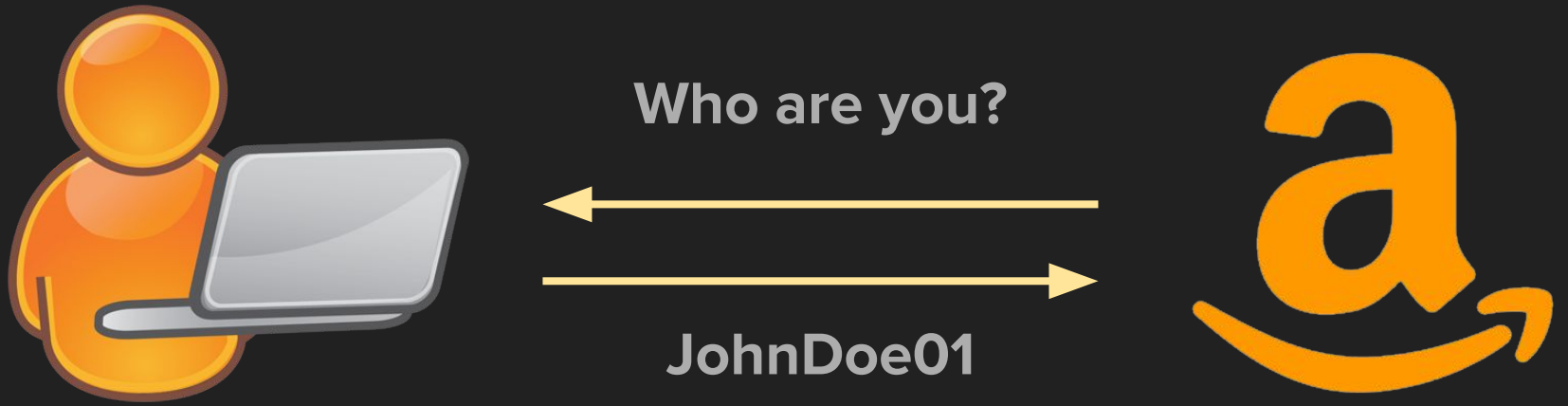
Augmenting Centralized Password Management with Application-Specific Passwords

Trevor Smith
Brigham Young University
tsmith@isrl.byu.edu

Scott Ruoti
MIT Lincoln Laboratory
scott@ruoti.org

Kent Seamons
Brigham Young University
seamons@cs.byu.edu

Remote User Authentication



Passwords

- Easy for developers
- Familiar to users
- Cost effective

- Difficult to remember
- Weak passwords
- Password reuse

Centralized Authentication Management

- Improved security
- Improved convenience

- Single point of failure
- Requires absolute trust
- Additional software

Password Managers

- Generates random passwords
- Stores encrypted passwords
- Protected by a master password

Single Sign-On Systems

- User authenticates to an identity provider
- User requests access to the web application
- Web application contacts the identity provider
- Identity provider authenticates to the web application

Our Proposal

Combine central authentication management with application specific passwords.

- Mitigate the single point of failure
- Reduce the required trust

Application-Specific Passwords

- Relatively low-entropy secret
- Can be unique for every application
- Combined with centralized authenticators

Threat Model

There are three major threats we consider:

1. Phishing a user’s master password
2. Stealing the centralized authentication manager’s password database
3. Stealing a web application’s password database

Evaluation Metrics

Deployability

Requires no changes to the:

- ❏ Web Application
- ❏ Password Manager
- ❏ SSO System

Security

Protects against:

- ❏ Stolen Master Password
- ❏ Central Party Compromise
- ❏ Web Application Compromise

Proposed Systems

1. Password Manager + User Addition
2. Password Manager + Hashing
3. Single Sign-On + Application Request
4. Single Sign-On + Protocol Modification
5. Single Sign-On + Challenge

Augmenting PM - User Addition

	Password Manager Supplied		User Supplied
Password:	zGJ9H?jVdkaQ!iBHD!b6aHTJ	+	itsme192

Deployability

Requires no changes to the:

- ☑ Web Application
- ☑ Password Manager

Security

Protects against:

- ☑ Stolen Master Password
- ☑ Central Party Compromise
- ❑ Web Application Compromise

Augmenting PM - Hashing

Password Manager Supplied User Supplied

Password: h(zGJ9H?jVdkaQ!iBHD!b6aHTJ + itsme192)

Deployability

Requires no changes to the:

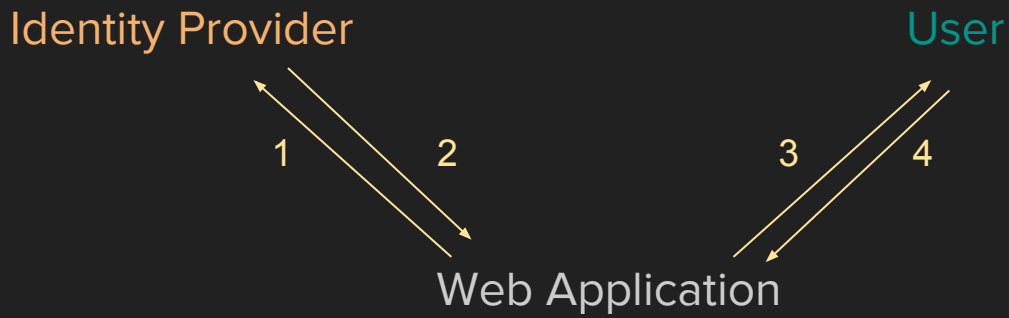
- ☑ Web Application
- ❑ Password Manager

Security

Protects against:

- ☑ Stolen Master Password
- ☑ Central Party Compromise
- ❑ Web Application Compromise

Augmenting SSO - Application Request



Deployability

Requires no changes to the:

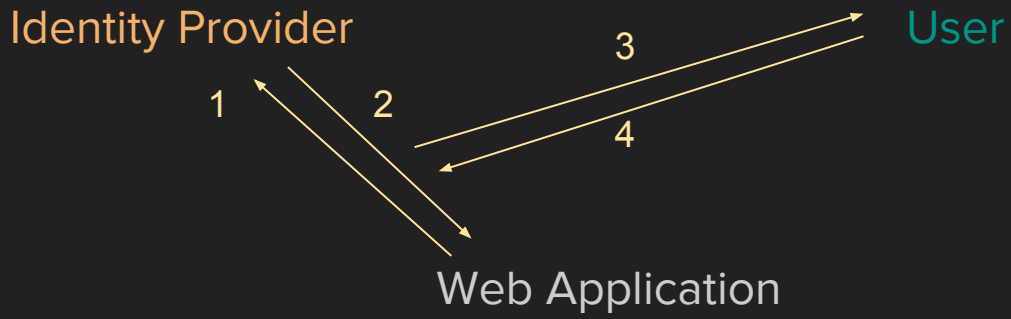
- ❑ Web Application
- ☑ SSO System

Security

Protects against:

- ☑ Stolen Master Password
- ☑ Central Party Compromise
- ☑ Web Application Compromise

Augmenting SSO - Modified Protocol



Deployability

Requires no changes to the:

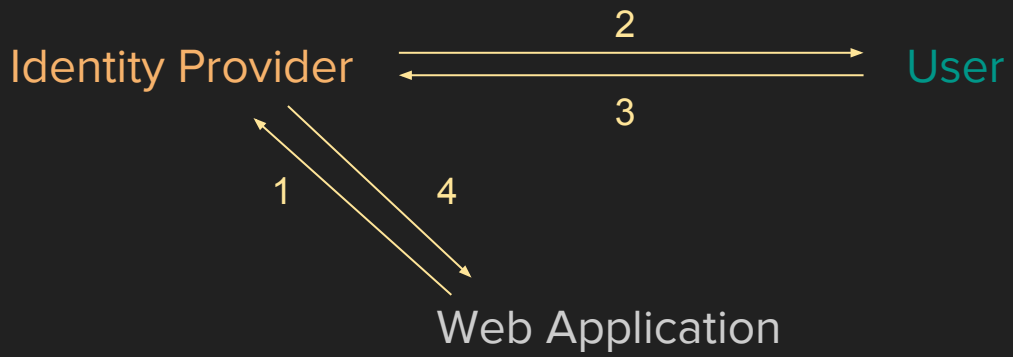
- ❑ Web Application
- ❑ SSO System

Security

Protects against:

- ☑ Stolen Master Password
- ☑ Central Party Compromise
- ☑ Web Application Compromise

Augmenting SSO - SSO Challenge



Deployability

Requires no changes to the:

- ☑ Web Application
- ❑ SSO System

Security

Protects against:

- ☑ Stolen Master Password
- ❑ Central Party Compromise
- ☑ Web Application Compromise

Next Steps

Evaluating Usability

- Attitude and Acceptability
- Laboratory Usability Studies
- Longitudinal Studies

Discussion

- How do we decide which system is best?
- How should we measure difficulty of deployment?
- How does these systems compare to Two-Factor Authentication?
- Are there benefits gained from a single point of entry?
- How does not adhering to best practices affect security?
- How should these systems handle recovery?