Class Notes Thursday

September 23rd 2021

Tuesday 1PM: @CakeLab Zoom

Trent Jaeger – Security Writer/Expert from Penn State University

Will be giving a 45 minute

Be on the look out for the intellectual nugget of the talk, will be part of question 1.

Send a message on slack to show that your in the meeting.

**Single Sign On Continued**

**Identity Provider (ID-P):**

The company or organization that is responsible for authentication the user

**Relying Party (RP)**

The website that is relying on the IDP for SSO

**User**

The person using SSO

**Steps to use SSO:**

1.) User: Hey RP, can I log in?

2.) RP: Sure, but you need to go to this authorization endpoint (HTTP 302)

3.) User: Hey auth endpoint, I want to log in, and I was told to go here

4.) IDP: Sure, let’s auth (Via session cookie)

5.) IDP: Credentials check out. RP Access?

6.) User: Yep

7.) IDP: Here’s a URL to access the RP. RP, Parameter: token

8.) User: RP here you go

9.) RP->IDP: Is this token valid?

10.) IDP-RP: Yes

11. )RP: Sends a session cookie to the user

**Attacker**:

Has IDP-Auth Token

* Session cookies for RPs that allow IDP-A Login
* Could pose as an RP and get an IDP-B token which would give it access to all other trusted RPs

**Two-Factor Authentication**

**First Factor:** Passwords

**Second Factor:** OTP or One Time Passcode which are sent over SMS, within an app, or an RSA key fob

**Types of Factors:**

1.) Something you know (Password)

2.) Something you have (Device)

3.) Something you are (Biometrics)

* Value does not change over time
* Convenience