# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

**Thursday, Oct. 5, 2017**, at 2 pm Eastern, 11 am Pacific

- video: https://bluejeans.com/678543210/browser

To join via Phone:

1) Dial one of these numbers or see all numbers - http://bluejeans.com/numbers

+1.408.740.7256

+1.888.240.2560 (US Toll Free)

+1.408.317.9253 (Alternate number)

2) Enter Conference ID: 678543210#

Back to Study Group wiki: https://tinyurl.com/tierOauth

## Participants

Alan Crosswell - Columbia
Keith Hazelton - UW-Madison

## Agenda

- *OAuth 2 in Action,* ch. 9 “Common Authorization Server Vulnerabilities”

- Alan and Keith will attend Oct. 10 meeting of new InCommon WG on OAuth-OIDC Deployment
    - Practical, concrete, e.g., why does it have to be JWTs vs bearer tokens; too burdensome, it will fail.
    - Don’t overcomplicate solutions
    - Only OIDC for ID Tokens seem useful so far
    - A Crosswell: Put in the hands of developers; Using mulesoft, do as much as possible FOR them; see https://github.com/n2ygk/raml-snippets
    - @ Columbia, real standards choices are Json Api (no standards docs) and Json Schema (04 corresponds to wright draft 01; 1.1 is under discussion) @ columbia; not RAML or OAS; RAML parser/lib is .js or java only; competition is Hypertext Appl. Language (HAL), expired drafts (08 in 2016)
    - RFC drafts exist for json schema; schema validation, hyperdata, core (still live until Oct.17).

- ACAMP unconference session proposal around OAuth/OIDC?

- Jon Miner takeaways from Catalyst

## Next Meeting

**Thursday, Nov. 2, 2017**, at 2 pm Eastern, 11 am Pacific

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, Sept. 7, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Ethan Kromhout - UNC Chapel Hill
Keith Hazelton - UW-Madison
Ashish Pandit - UCSD
Alan Crosswell - Columbia U

## Agenda

- API Manager WSO2, supports OAuth out of the box; AuthZ code auth type is most used; auto-approval for users to access public resources; Grant type that will leverage SAML ECP; implicit grant for JavaScript; Next up is to get familiar with the vulnerabilities; Lots of QA APIs and not too many in Prod.; started w OAuth, had to also support additional mechanisms: Basic Auth, Client Certificate, Role server connections; OAuth is newer and more API-centric, lots of our integrations with legacy apps needed the older mechanisms; did an env. Scan three years ago; but need for iPasS will drive them to commercial products; Boomi, Mulesoft, Informatica, WSO2: each comes with their own API manager; Does security, but workflow for pub/sub of API;
    - Informatica as iPaaS

- There's a new API group planning meeting spinning up, Jon & Ashish planning it;

- *OAuth 2 in Action* Ch 8 "Common Protected Resource Vulnerabilities"
    - In modern practice, X-sameorigiin headers replaced with content security policy headers

- Future: Jon Miner takeaways from Catalyst

## Next Meeting

**Thursday, September 14, 2017**, at 2 pm Eastern, 11 am Pacific

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, August 24, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

José Cedeno - Oregon State
Ethan Kromhout - UNC Chapel Hill
Alan Crosswell - Columbia U
Keith Hazelton - UW-Madison

## Agenda

1. Chapter 7, “Common Client Vulnerabilities”
    - Exercise 1

2. [Keith] contact RolandH about joining one of these calls
   [Keith] talk to ITANA about having one of their book sessions with Justin Richer on OAuth2 in Action

## Next Meeting

- Thursday, September 7, 2017 at 2 pm Eastern, 11 am Pacific
    - Ch 8 “Common Protected Resource Vulnerabilities”
    - Jon Miner takeaways from Catalyst?

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, July 27, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Ethan Kromhout - UNC Chapel Hill
Keith Hazelton - UW-Madison
Alan Crosswell - Columbia
José Cedeño - Oregon State U

## Agenda

1. Chapter 6, “OAuth 2 in the Real World”

3. Grant types
    - Authorization code (“code”)
        - Preferred method when applicable
        - Suitable when you need/want ‘user permission’ on top of client’s basic auth
        - Not necessary for server-to-server (where both servers trust each other)

    - Implicit (“token”)
        - For in-browser javascript clients

    - Client credentials (“client-credentials”)
        - For client invocation of back-end APIs
        - Server-to-server
        - Oregon State U uses this token type for server-to-server but with short lifetimes
        - Scopes are the authorization filter: that’s how you could mock the
        - Canvas has an act-as capability
        - Used in non-production env. to impersonate a user for testing; NOT in production

    - Resource Owner credentials (“password”)
        - Avoid if at all possible; One step better than client passing resource owners un/pw to authZ server

4. Discussion

    - Alan Crosswell is willing to join an API call to talk about management and use of scopes; Rewriting our student system rather than buy. Approach is to replace bits of functionality with microservices over time. Using Mule primarily as a proxy to handle policy, OAuth, scopes, etc. MIT has 18 vCores--they're committed; Aug. 11

    - José: Apigee is also primarily used as a proxy for policy, OAuth, scopes, WSO2 would increase support costs because of upgrades and tinkering; Allow anyone to have an account for access to public data; jscript apps use a client id (api key) Client credentials for more sensitive APIs and data.

    - Ethan: Do services on a point-by-point basis as needed to help get students beyond screen-scraping-based apps. Un/pw up to now.

    - What about AWS API Gateway? José: We found it disappointing: Best for other things running on AWS like lambdas; Security perspective: Apigee can limit access to APIs; AWS will not provide fixed IPs for the API gateway. Will look again later in the year.

    - Azure? What's in front of their own APIs in the way of gateways? Nice management UIs for one thing.

## Next Meeting

**Thursday, August 17, 2017**, at 2 pm Eastern, 11 am Pacific

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, July 6, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

## Agenda

I sent out a cancellation notice, but I'll be on the call and *if one or both of you show up*, we'll talk about things other than the exercises in the book. Meanwhile we'll try to rouse the crowd to show up for next Thursday's call. --Keith

Alan and Ethan: I'd like us to brainstorm about a couple things.

- What might we include in our TIER API AuthN guidance doc contain?
    - Alan, would you be OK with us pulling in some of the material in your drafts?
    - Should we put together some how-to's to support Holder of Key (in the absence of final standards in some areas)?
        - Pass bearer tokens down a whole stack of resources hittint multiple resource servers for one user
        - 3-tier pattern is pushed by MuleSoft. Mobile client - browser client: w different UX
        - Shared
        - Python for backend and X.js for front end would be most useful; swagger UI js library yields a look that
        - Ethan: bringing on Informatica in role of an ESB and SOA on top of PS to create a more stable suite of APIs to consumer.
        - Aren't JWTs using asymmetric keys already? Isn't that as good for establishing identity of the Authorization Server to the client?
        - REST best practices could go a long way; id's should be called 'id', etc.
        - Grouper groups for OAuth scopes; a framework over PingFederate
    - Should we talk about what API authN approaches they will find out there in the wild?
    - I think a heavily commented set of .js files from the chapter exercises might be a help to people wanting to get their hands dirty. Each line of code seems to invoke one or more libraries to work some magic. We could explain how the magic is done.

- Ethan, we could also talk a bit about the EC2 midpoint instance and next steps.

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, June 15, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Keith Hazelton - UW-Madison
Alan Crosswell - Columbia
Ethan Kromhout - UNC Chapel Hill

## Agenda

5. HOMEWORK for Thursday, June 15: Exercises in Chapter 6 of *OAuth2 in Action,* "OAuth 2.0 in the Real World"
    - See the wiki for instructions on obtaining a copy of the code repository for the exercises

6. Alan Crosswell from Columbia U would appreciate comments and suggestions on a document and a presentation he is developing. *For our group only for now*:

    - API/Integration Overview
    - https://docs.google.com/presentation/d/1s8D-iSvREIJUUSWktT3sMnEZ9mp5TUffC6DacZV7RLk/edit?usp=sharing

    - Scope Standards: API Coarse-grained Authorization
    - https://docs.google.com/document/d/1ExWaLQdRBKE59VsctuNhBERp3Vj4FlbNgqXSk5NGWmY/edit?usp=sharing
    - Client credentials grant type: Seems made for back-end interactions of clients and services (no user or browser involved)
    - Is PKCE a viable option for 'public clients'?
    - Does Dynamic Registration (ch. 12) help address security concerns
    - Scope discussion:
        - The OAuth in Action book's eg of scopes as filtering (ch. 4);
        - The Resource Server's role in checking scopes

7. HOMEWORK for June 29: Jump ahead to Chapter 15 "Beyond Bearer Tokens" as a logical follow-on to this week's material on grant types and flows. Then back to ch. 7 for the following meeting
    - To what degree do these new approaches add complexity to the Client? To the Resource Server?

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, June 1, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Keith Hazelton - UW-Madison
José Cedeno - Oregon State
Kevin Rooney - Virginia Tech
Ethan Kromhout - UNC Chapel Hill
Ashish Pandit - UCSD
Louie Zelus - UCSD

## Agenda

8. Introduction of new attendees:
    - Ashish Pandit - UCSD, co-chair of ITANA API group; UC-level API group; 2-3 using packages, Berkeley using on acquired by JBOSS, UCSD using WSO2, UCSF uses Mule, UCLA in RFC stage; shared API
    - Louie Z. - UCSD, OAuth2 in-house expert

9. HOMEWORK for Thursday, June 1: Exercises in Chapter 5 of *OAuth2 in Action,* "Building a Simple OAuth Authorization Server"
    - LOTS of error checking even in this set of exercises
    - Gateways take on or proxy some of the OAuth2 AuthZ server, caution: lock-in possibility
    - Scopes: How do we design the packaging around the APIs? APIs bundled into subscritions, logical service chunks, scopes are another way to do that.
    - Louie: scopes are like groups or roles; authZ code grant type, the scope the client requests are presented to the user to give them a chance to approve/decline various scopes.
    - Scopes with client credential grant type: The user is not involved
    - Scopes can be mapped to/from group memberships
    - Scopes in facebook are actions
    - Client invoking a service API: client credential;
    - Name of app, proof that the app is, name of user that is behind the keyboard, and proof that the user is who they say they are; client credentials passes only the app info: app identifier and optionally proof of app identity

10. Alan would appreciate comments and suggestions on a document and a presentation he is developing. *For our group only for now*:

- API/Integration Overview
- https://docs.google.com/presentation/d/1s8D-iSvREIJUUSWktT3sMnEZ9mp5TUffC6DacZV7RLk/edit?usp=sharing

- Scope Standards: API Coarse-grained Authorization
- https://docs.google.com/document/d/1ExWaLQdRBKE59VsctuNhBERp3Vj4FlbNgqXSk5NGWmY/edit?usp=sharing

11. Check out the email thread on EDUCAUSE IdM list, “OAuth2 Server”
    - Participant scan: Which, if any, OAuth/OIDC libraries are under study or in use at your institution?

**OAuth2 Servers**

On 05/12/2017 11:58 PM, Mailvaganam, Hari wrote:
Hi List:

Has anyone here implemented OAuth2 server -- for internal API authorization?

Which technology/platform did you select?

Thanks.

Best regards,

Hari

---

**Hari Mailvaganam**
Access Application Architect, Identity and Access Management
UBC Information Technology
The University of British Columbia

Hari,

Not directly what you're asking, but you may want to check out OIDC Survey Working Group Final Report. It has a number of aggregate statistics from a recent survey of OIDC/OAuth use in higher education. More detail is available from the group's wiki space.

David Walker

Hari,

The Internet2 TIER initiative is looking at setting up an OAuth 2 Authorization Server + Resource Server host package as part of an API AuthNZ solution. If this is of interest, let me

know.

--Keith Hazelton (keith.hazelton@wisc.edu)

---
*Yes -- it is.*

*Thanks.*

*Best regards,*

*Hari*

---
Bill,

Glad to hear of your interest. Perhaps we could talk sometime this week. Would 10 am your time Thursday or Friday morning work for you? Skype? (kei2th).

Have you looked at the open MIT licensed Gluu.org OAuth/OIDC support or the Apache 2-licensed uaa package from CloudFoundry?

From https://github.com/GluuFederation/oxAuth

**"oxAuth**
oxAuth is an open source OpenID Provider that implements the OpenID Connect 1.0 stack of REST services. The project also includes OpenID Connect Client code which can be used by websites to validate tokens. It currently implements all required aspects of the OpenID Connect stack, including an OAuth 2.0 authorization server, Simple Web Discovery, Dynamic Client Registration, JSON Web Tokens, JSON Web Keys, and User Info Endpoint.
oxAuth is tightly coupled with oxTrust. oxAuth configuration is stored in LDAP, and oxTrust is needed to generate the proper configuration."

Hi Hari,

When I worked at Stanford we picked UAA ( https://github.com/cloudfoundry/uaa ) which is a general purpose, stand alone, open source OAuth2 authorization server.

- You can get users and groups from LDAP or provision it with SCIM.
- A user's groups determine what scopes they can authorize in a consent flow.
- Everything is API based (https://docs.cloudfoundry.org/api/uaa/) for
- client creation, administration, etc.
- It support SAML and OIDC for user logins (not sure if it supports
- multiple configurations)
- It is Apache2 license

- It is under active development by Cloudfoundry

- Patrick Radtke

UMich is looking at possibilities right now. Our ideal solution would integrate with the Shibboleth IDP.

Of particular interest is the work the Unicon did for U Chicago integrating MITREid Connect into v3 of the Shibboleth IDP.

We're also interested on similar work being done by GEANT, though I don't know if there are any deliverables yet.

Another possibility is MITREid Connect integration done by Surfnet / OpenConext (https://github.com/OpenConext/OpenConext-oidc), which is a maven overlay that makes MITREid Connect available as a SAML SP.

--
Liam Hoekenga
ITS Identity and Access Management
The University of Michigan
liamr@umich.edu

**REFEDS OIDC for Research and Education OIDCre WG**

Hi all,
Please find attached the slides from todays presentation on the OIDCre workgroup

https://drive.google.com/file/d/0B4FyQfoKFISKdzFnSExjaURCRTQ/view?usp=sharing

The OIDCre group has a separate list, please join oidcre@lists.refeds.org if you want to contribute.
Pointers:

- The document with the basic and advanced implementation SAML <-> OIDC recommendation here:
- 'REFEDs OIDCre - Recommendation for implementation mappings between SAML 2.0 and OpenID Connect in Higher education'
- https://docs.google.com/document/d/1TMvHEGAi4jTrOQ_fyFmBhJTZJ_jJIzB5hUXcZZHSW3E/edit?usp=sharing
- The OIDC federation RFC proposal: https://github.com/OpenIDC/fedoidc/blob/master/draft/oidcfed.hf.txt
- Information on the working group: https://wiki.refeds.org/display/GROUPS/OIDCre

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

We kindly invite you to provide feedback on the documents and participate in the discussions. If you are visiting TNC2017, you are very welcome to join the workshop on OIDC federation on Friday: https://tnc17.geant.org/core/event/26
Best,
Niels
(OIDCre Chair)

The proposal on mapping SAML to OIDC
https://docs.google.com/document/d/1TMvHEGAi4jTrOQ_fyFmBhJTZJ_jJIzB5hUXcZZHSW3E/edit?usp=sharing

OIDC implements the things that OAuth doesn't tell you how to do.

Clients to hosted experience: OAuth2, SAML2, capability provided; wanted to be an SP

AuthN w SAML, 3-legged OAuth, web app sends browser user to authN, is sent to OAuth server, also pulls all the claims out and packages to JWT sent to backend service.

## Next Meeting

**Thursday, June 15, 2017**, at 2 pm Eastern, 11 am Pacific

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, May 4, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Keith Hazelton - UW-Madison
Jon Miner - UW-Madison
Chris Hyzer - Penn
Alan Crosswell - Columbia
Ethan Kromhout - UNC Chapel Hill
José Cedeno - Oregon State

## Agenda

12. HOMEWORK for Thursday, May 4: Exercises in Chapter 4 of *OAuth2 in Action,* "Building a Simple OAuth Protected Resource"
    - NOTE: There is an error in the source code ...authorizationServer/approve.html: fix is available at https://github.com/oauthinaction/oauth-in-action-code/commit/83c3c2719208a4aec8edd6e783aafdab74b4b93c#diff-14ebd7db3d2527c41e61aebca1fe3a1f
    - Scope and descriptions of scopes must be predefined in the AuthZ Server
    - NOTE: If you don't have access to the book, send a note to hazelton@wisc.edu
    - OAuth 2 in Action book forum incl. errata: https://forums.manning.com/forums/oauth-2-in-action
    -
    - Client can get full list of scopes by asking the AuthZServer; and then use refresh to get more restricted scopes.
    - Counting on the client to be a good actor WRT scopes on resource
    - If you have an API hierarchy, system APIs, process APIs, user experience APIs at top of stack. That access token could be percolated down to lower layers…?
    - Resource server introspection call, RS has it's own credentials to AuthZServer, so authZServer can decide to only give certain scopes;
    - Links to other scope patterns
    - Look at Alan Crosswell
    - Protections are all in the AuthServer which tends to be an institutionally-run service so that's ok
    - Hierarchy of scopes and relation to tokens as an area to investigate
        - At authZ code grant time, Use grouper to define groups to control who has 'read' scope;
        - Social media:
            - end user is in charge of what gets shared
            - Institution has a role too
    - Create directory and download code for above book: https://github.com/oauthinaction/oauth-in-action-code
    - Prerequisites for running the examples:

- Node: https://nodejs.org
- NPM: https://www.npmjs.com/ (Bundled with Node)
- Express: http://expressjs.com

13. Google Docs phishing URL (lines split up for readability):

```
https://accounts.google.com/o/oauth2/auth
?client_id=623002641392-km6voeicvso16uuk7pvc8mvbqheobnft.apps.googleusercontent.com
&scope=https://mail.google.com/+https://www.googleapis.com/auth/contacts
&immediate=false
&include_granted_scopes=true
&response_type=token
&redirect_uri=https://googledocs.docscloud.win/g.php&customparam=customparam
```

The above grants ability to “Read, send, delete, and manage your email” (https://mail.google.com) and “Manage your contacts” (https://www.googleapis.com/auth/contacts).

So this guy was able to register his app with Google with the given redirect_uri and the exposure was imply that he named his app Google Docs and Google’s scope permissions UI just shows the app name without clearly indicating where it comes from.

**Examples of Scopes in the Wild**
https://developers.google.com/identity/protocols/googlescopes
https://blogs.oracle.com/OracleIDM/entry/securing_access_with_oauth2_how’
https://developer.github.com/v3/oauth/#scopes
https://brandur.org/oauth-scope
https://api.slack.com/docs/oauth-scopes
http://wso2.com/library/articles/2015/12/article-role-based-access-control-for-apis-exposed-via-wso2-api-manager-using-oauth-2.0-scopes/

## Next Meeting

**Thursday, May 18, 2017**, at 2 pm Eastern, 11 am Pacific

14. HOMEWORK: Exercises in Chapter 5 and 6 of *OAuth2 in Action*

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, April 20, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Alan Crosswell - Columbia
José Cedeño - Oregon State (I'll have to leave after the first 30 min)
Jon Miner - UW-Madison
Nick Roy - InCommon
Sumner Warren - Brown U
Keith Hazelton - UW-Madison
Kevin Rooney - Virginia Tech

## Agenda

1. HOMEWORK for Thursday, April 20: Exercises in Chapter 3 of *OAuth2 in Action,* "Building a Simple OAuth Client"
    a. Create directory and download code for above book: https://github.com/oauthinaction/oauth-in-action-code
    b. Start with the first exercise in Chapter 3
    c. DON'T try to read through all the code, each example includes a whole suite of OAuth2 services, and they should be treated as scaffolding, or black boxes.
    d. The examples mostly consist of partial code for the component under study (in Chapter 3, it's the 'client' component), and the solution involves filling in the missing bits, following the leads in the textual notes within the code. Hints: "Read the RFC" or do a diff between client.js and completed/client.js

## Next Meeting

**Thursday, May 4, 2017**, at 2 pm Eastern, 11 am Pacific

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

---

**Thursday, April 6, 2017**, at 2 pm Eastern, 11 am Pacific

## Participants

Keith Hazelton - UW-Madison
Gabor Eszes - Old Dominion Univ
Alan Crosswell - Columbia CTO
Ethan Kromhout - UNC Chapel Hill
Chris Keith - Brown
José Cedeño - Oregon State
Ethan Disabb - UFlorida
Kevin Rooney - Virginia Tech
Bill Kaufman - Internet2
Jon Miner - UW-Madison

## Regrets:

Jim Jokl - U Virginia
Nick Roy - Internet2
Steven Carmody - Brown

## Agenda

1. Round Robin Introductions,
    a. Name, institution, role
    b. Prior exposure to OAuth2/OIDC
    c. When course is done, what do you hope to have achieved?
    d. GaborE: Brush up on technical details and the exact ramifications of each grant type; have us be on the same page
    e. Alan Crosswell, CTO, Col. U. bought Mulesoft: API portal/gateway; also had to buy 1 of 2 OAuth servers (Ping Federate or OpenIdM) OAuth ‘federation’ auth code flow hooked into Shib IdP and external (social) IdPs ; ‘Scope magic’ tells PingFederate which OP to use. Read websites, started with OIDC, should have started with RFCs; has python/flask authz code flow. Submitted errata already; Hope to achieve understanding of what they’ve already done. Mulesoft uses proprietary; Ask API gateway for client credential (before dynamic registration RFC was published); Do want to look at OIDC, too. ID ALL the relevant RFCs:
    f. RFCs:
        i. https://tools.ietf.org/html/rfc6749 OAuth 2.0 framework
        ii. https://tools.ietf.org/html/rfc7591 OAuth 2.0 Dynamic Client Registration

iii. https://tools.ietf.org/html/rfc7662 OAuth 2.0 Token Introspection
iv. https://tools.ietf.org/html/rfc6750 Bearer Token Usage
v. https://tools.ietf.org/html/rfc7009 Token Revocation
vi. https://tools.ietf.org/html/rfc7521 Assertion Framework for Client Authentication and Authorization Grants
    1. https://tools.ietf.org/html/rfc7522 SAML 2.0 Profile for …
    2. https://tools.ietf.org/html/rfc7523 JSON Web Token (JWT) Profile for …
vii. https://tools.ietf.org/html/rfc6819 Threat Model and Security Considerations
viii. https://tools.ietf.org/html/rfc7636 Proof Key for Code Exchange by OAuth Public Clients
ix. https://tools.ietf.org/html/rfc6755 An IETF URN Sub-Namespace for OAuth
x. (maybe some of these are not so relevant)

g. EthanK: run some m'ware groups at UNC; looking for a better understanding; want better security over APIs; integration selection group now looking: Boomi, Mule, Informatica.
h. Chris Keith: oversee web, IdM and integration: both consumer side view plus IAM; consumer of OAuth2 APIs more than a developer; running Mule, building an API service layer; most services today are basic auth over SSL; want to move into current software, better security
i. José Cedeño: Oregon State: Implementing APIs, consuming others.; know less about OIDC; Community Building as a goal
j. Ethan DIsabb: U FI, identity infrastructure; Warren wants him to learn more about all this. Better understanding of how they work. Will lead to local development and use.
k. Kevin Rooney, Virginia Tech; ID Architect; have used OpenID IdPs for password reset; Google moved, all the identifiers changed, forced migration underway, got Google to extend support for old identifiers to May 2017; Learn from others, steal open source code.
l. Bill Kaufman, Internet2, Sr Proj Mgr for TIER, onboard about a year, new to IAM, newer to OAuth re security/authorization for APIs; 30 yrs comm. protocol...Here to learn, help propagate this into TIER
m. Jon Miner UW-Madison; authNZ since stone age. Re OAuth/OIDC, nothing official in way of services yet, some instances scattered across campus. TIER stuff is interested; Msn data governance is still primitive, but is changing; Was a big push for open data in state government

2. Group Wiki page

3. To subscribe to mailing list: tier-oauth@internet2.edu

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

4. How should we proceed? Suggestions?
    a. One possibility: Work with each of the code exercises in chapters 3 and beyond of OAuth2 in Action
        i. Chapter 1 is free for download
        ii. Create directory and download code for above book: https://github.com/oauthinaction/oauth-in-action-code
        iii. https://forums.manning.com/forums/oauth-2-in-action
        iv. Prerequisites for running the examples:
            1. Node: https://nodejs.org
            2. NPM: https://www.npmjs.com/ (Bundled with Node)
            3. Express: http://expressjs.com

    b. Have more advanced participants introduce topic and lead discussions
    c. HIgher level Applications using APIs securely
        i. Mulesoft will gradually increase support for Swagger/OpenAPI
            1. See under 'Product Tour' at https://www.mulesoft.com/platform/api/anypoint-designer
        ii. José: could discuss OAuth2 grant types
        iii. Alan: Look at validation with introspection of JWTs "jots"
        iv. Gabor: JOSE standards;
        v. The published writings are horrible (except the RFC)
        vi. OAuth Bible is an exception
            1. http://oauthbible.com/
    d. OAuth 1 (admittedly dated) had many, many grant types, so developers found it too complicated but most sources now claim that OAuth 2 is complicated and enterprisey instead.
    e. Try to learn a bit about OAuth2 scopes for controlling access to enterprise info.

5. Homework for two weeks from now, Thursday, April 20
    a. Start with the first exercise in Chapter 3 (in your clone of the code repository)
    b. Read the RFCs =) (see above)
    c. Or just read through the textual notes in the code, and look at the completed code if you get lost
    d. DON'T try to read through all the code, each example includes a whole suite of OAuth2 services, and they should be treated as scaffolding, or black boxes.
    e. The examples mostly consist of partial code for the component under study (in Chapter 3, it's the 'client' component), and the solution involves filling in the missing bits, following the leads in the textual notes within the code.

# TIER OAuth/OIDC Study Group Meeting Agenda and Notes

*OAUTH2 IN ACTION, Justin Richer, Antonio Sanso*



## Next Meeting

**Thursday, 20 April 2017, at 2 pm Eastern Daylight, 11 am Pacific**