Book of Proceedings

www.internetidentityworkshop.com

Compiled by
HEIDI NOBANTU SAUL, LISA HORWITCH AND EMMA GROSS

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_18_Notes

May 6 -8, 2014
Computer History Museum
Mountain View, CA

IIW founded by Kaliya Hamlin, Phil Windley and Doc Searls
Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul

Contents

About IIW – the Internet Identity Workshop

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Hamlin. IIW is a working group of Identity Commons. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity. The event is now in its 10th year and is Co-produced by Kaliya Hamlin, Phil Windley and Heidi Nobantu Saul.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format – the agenda is created live each day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast paced arena.

For additional information about IIW: http://www.internetidentityworkshop.com

To read the Values of IIW as articulated by attendees of the 11th event held in November of 2010, you can go here: http://www.internetidentityworkshop.com/iiw-values/

To read descriptions of 'what IIW is' as articulated by attendees of the 11th event held in November 2010, you can go here: http://www.internetidentityworkshop.com/what-is-iiw/

IW #19 will be October 28 - 30 2014 in Mountain View, California at the Computer History Museum. Registration is now open at: https://iiw19.eventbrite.com

IIW Events would not be possible without the community that gathers or the sponsors that make the gathering feasible. Sponsors of IIW #18 were:

Microsoft ~ Google ~ Gigya ~ Neustar ~ Yubico ~ SalesForce

Nexus ~ Respect Network ~ ForgeRock ~ IOPT Consulting

If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at eventbrite@windley.org for event and sponsorship information or reply to this mail with your query.

Upcoming IIW Events in Mountain View California:

IIWXIX #19 October 28, 29 and 30, 2014
IIWXX #20 April 7, 8 and 9, 2015

Agenda Creation

IIW 18 Session Topics

Tuesday May 6, 2014

Session 1

- Respect Network LAUNCH – Drummond Reed & Les Chasen
- Social ID's in Enterprise – Dedra Chamberlin
- Indie BOX – Let's Bring Our Data Home – Johannes Ernst
- Covert Redirect – What It Is/What It Ain't – John & Pam & Hannes & John B
- Improving the Mobile Federation Sign-In Experience – George Fletcher
- Phishing Blend Authentication and Authorization – Mark Stiegler

Session 2

- JOSE Can You See – A Technical Overview of JWT – Brian Campbel
- Collaboration For Collective Impact – Gabriel Scheer
- Me Depot – Serving Billions – Lionel Wolberger
- Intentions vs Identity – Edi Immonen
- I o T = Identity of Things – Jeff Stollman
- Customer Support for Personal Data Stores – Adrian Gropper
- An Introducing to IndieWeb – Ben Werdmuller
- "SCIM" Next Steps – Planning Ahead, Domain ID Management – Bill Mills
- New OAuth 2-wg – Multi-Party Federation – Mike Schwartz

Session 3

- OpenID Connect – Interop Testing Details – Mike Jones & Roland Hedberg
- It's NAPPS – Enabling SSO for Native APPS – Paul Madsen
- Engaging End Users – How Do We Get Consumers to Participate in Identity – Eno Jackson
- "Privacy Lens" A New Open-Source Active End-User Privacy Manager w/Informed Consent, Available for Many Attribute Flows Including: SAML & soon Open ID Connect and… - Kenneth Klingenstein
- Ethical Data Handling : What Is It? What are the Obstacles? What is Success – Robin Wilton
- Platform Deep-Dive of: Qredo – Hugh Pyle
- Open ID Connect 101 – How it Works/What is it for – Pam Dingle
- Join the Indieweb! Practical Session to Make Your Own Idieweb – Kevin Marks
- Silicon Valley "Culture of Youth": Experiences; Lessons & Effects; Predictors & Steps – Randy Farmer
- Your Digital Traits for STRONG Auth – Bert Spencer & Chris Canfield

Session 4

- OpenID Connect – Logout/Session Mgmt (Part 1) – Mike Jones, John Bradley & Naveen Agarwal
- How Do We Preserve and Protect Identity / Identity Theft – Kris Alman
- CAN'T BE EVIL – John Light
- NSTIC – Update from NIST & Roundtable – John Sheire
- FUSE Architecture – PICOS & Connected Cars – Phil Windley
- IndieAuth – Turn Your Personal Domain Into An OAUTH Provider – Aaron Parecki
- Practice Session for Investor Panel – Nathan Schor

Session 5

- OpenID Connect – Logout/Session Mgmt (Part 2) - Mike Jones, John Bradley & Naveen Agarwal
- Personal Sovereign Design (#VRM; #Sovereign Source Authority) – Devon Loffretto
- 4th Parties – Use Cases for Others Besides the User, IDP and Relying Party – Matt Berry
- DOXING as Vigilante Justice – Sarah Davies
- Respect Network + XDI – Markus Sabadello
- Aging + Caregivers + Post Death Identity Management IoT Assisted Living – David Howell
- NSTIC/IDESG A Listening Session to Hear From You: What do you think it is? What could/should it b? What would be valuable – Kaliya Hamlin

Wednesday May 7, 2014

Session 1

- VRM (Vendor Relationship Management) Progress Report – Doc Searls
- OAuth Security – Proof of Possession Hannes Tschofenig
- Privacy Metrics – What Could They Be? What Should They Measure? Should They Exist? – Sean Brooks
- Home Owner Personal Data – Lionel Wolberger
- "We Are the Last Generation of Free People. There Are Only About 10yrs Left." Discuss: What Are We Doing to Ensure We Are Free 100 Years From Now? – Kaliya Hamlin

Session 2

- VRM Adoption Case Study – MYDEX – William Heath
- HTTPSY – Leave the Certificate Authority Behind – Mark Stiegler & Alan Karp
- SAFEnet – John Light
- Data Inequality $ = $ Income Inequaliy – Kris Alman
- Channel Binding for Open ID Connect – Mike Jones & Breno
- ADHOC: UMA Interop Testing Session Thing – Mark Dobrinic

Session 3

- Mozilla Listens to IIW – Sean Bohan & Brian
- Real Estate Use Cases – Bill Wendel
- Shopping for Identity Providers – What do I Need To Know Before I Put My Identity in Your Provider – Matt Berry
- Functional Model Elements from NSTIC – Personal Cloud Review – Kaliya Hamlin
- Self ID: What Technical Problems or Incentives do we need to Make Hosting Your Own IDP Really a Viable Thing? – Bryant Cutler
- Mobile Connect: What Would You as an Rp/IoP/Attribute Broker Want from the Carriers? – Mike Eagan
- Clarify & Learn About Web Payments & Identity – Brent Shambaugh

Session 4

- New Book – Extreme Relevancy – John McKean
- IoT and Open Standards – Oauth2, UMA… - George Fletcher
- Gettign WC3 People to come to IIW19 – Brent Shambaugh
- Mobile SSO – How We Did It/USIMG/OAuth, Open ID Connect – Sascha Preibisch

- OAuth SASL (OAuth for non-web apps, ep.IMAP) – Bill & Hannes Tschofenig
- Post Life Identity Privacy – Akiko Orits
- Root of Trust – Bryant Cutler
- Investor Pitch Practice w/Special Guest Jerry Weissman – Nathan Schor

Session 5
- Be Ready for the AUTHpocalypse – Lightweight/Dynamic Client Registration for IMAP/SASL – John Bradley, Breno & Naveen
- Identity Ecosystems + the IDESG – Kaliya Hamlin
- Google – Recent Update & Input on OAuth DevX – Adam, Jack, Naveen, Bruno
- I0 Things You Can Do With A "FREEDOM BOX" – Markus Sabadello
- The ID – Library/Film Fest & Anthology – 'this Community Cannon' – Kaliya Hamlin
- Help us Do Social Media Marketing for the Respect Network Launch – Drummond Reed
- How To Deal With The Case When The Intended Audience Is Not The Releasing Party – Roland Hedberg
- Lost Dog! User Centric ID Management (FIDO & Other Opts…) – Chris Edwards
- Bitcoin & Identity – Pat Reilly
- NAAPS Working Group – John Bradley

Thursday May 8, 2014

Session 1
- In 5min or less – Tell Me a Happy Future Story About "IDENITY" – Sarah Davies
- Let's create some -Partinent Art – That Speaks to Our Condition & Brainstorming Ides About Topics for Books for Children and Management – (like SCADA & ME) – Kaliya Hamlin & William Heath
- Reputation – Dave Sanford
- DNSSEC 101 – Intro How It Works/My War Stories – Jim Fenton

Session 2
- DARASHA XDI app – Music Library – Really Cool Working Code – William Marin & Jack Senechal
- AWS Q&A: Questions About AWS Identity, Federation, or Access Control Policy? Come Ask Us!! – Bryant Cutler & Matt Berry
- ACE = Authentication & Authorization for Constrained Environments – Hannes Tschofenig
- Help Doc prep for the VC Panel – Doc Searls
- The Maker Economy & Identity – Brent Shambaugh

Session 3
- What's it Take to get a Customer-Centric Startup to Win Funding? (VC Panel Discussion) – Nathan Schor
- Kitties are Fluffy!! – Justin Richer
- Icons for Privacy – Akiko Orita
- Where Are the RP's? – Peter Cattaneo
- HOW CSP's (cloud service providers) and Authentication Providers Fit Together on the RESPECT NETWORK – Drummond Reed

Session 4

- Start-Up's Pitching – Nathan Schor
- Free People Beyond the Next 10 Years – (Continuation from Wed Session/Manifesto Writing) – Kaliya Hamlin

Session 5

- Start-Up's Pitching – Nathan Schor
- Murder via Google Maps – Justin Richer
- CAMBRIAN – A User-Centric de-centralized platform for entrepreneurs – John Light

Tuesday May 7

Respect Network Launch

Tuesday 1A

Convener: Drummond Reed & Les Chasen
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to Respect Network Launch and Lunch Events Schedule
World's First Global Private Network:

http://finance.yahoo.com/news/privacy-revolution-starts-now-130000306.html

Privacy Revolution Starts Now!

Indie Box: Let's Bring our Data Home!

Tuesday 1D
Convener: Johannes Ernst
Notes-taker: Kevin Marks & Ben Werdmuller & Aaron Parecki

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Find notes from this session here:
http://indiewebcamp.com/2014-05-06-iiw-indiebox

Further Notes:
Johannes Ernst: indiebox is a home server for your family to use that connects to the net crowd funding for Indie Box has started today: https://www.indiegogo.com/projects/indie-box-let-s-bring-our-data-home #indieweb

Ben Werdmüller: is taking great notes at https://etherpad.mozilla.org/iiw on the @indieboxproject

Johannes Ernst: the internet has become a centralised system. Indiebox is mean to turn that back so you can have your own server
Aaron Parecki: philips hue lightbulbs also have a server in your house that you can access without their cloud service
Johannes Ernst: I'd like to run an app against all the devices in my house we don't have an app that is an IDP app @aaronpk: hey, I have one @johannes_ernst: great lets use it

Received from Ben Werdmuller:

Notes by Ben Werdmuller and Aaron Parecki
These are permanently hosted at: http://indiewebcamp.com/2014-05-06-iiw-indiebox

Realized that we all made a big mistake back in the day - we let other people use our data.

Indie Box is an effort that allows us to control our data.

Where's our data? Not in the hands of the people - in Facebook, Flickr, Google, YouTube, Dropbox, plus various governments. We need to take our data back home!
Indie Box One is a personal cloud server that you place in your home.

Crowdfunding is live as of a few minutes ago. There will be lots of different kinds of hardware, but this is the first one - you take your own server and put your own personal data on that. If your data is your own, you control it. You unplug the server, nobody can access it at all!

Indie Box One (so, there will be many different kinds) has an energy efficient process. Designed to be the first box in from the web - it sits on the wire between your home network and the outside world. It can see everything that happens. In most cases, that would be a privacy violation - except, it's your box! You could run ad blockers on it, Tor if you were so inclined, site blocking for your kids, prevent your IoT devices from phoning home ...

What does it actually do?

- Runs a firewall, NAT, DHCP, and runs web apps internally and/or externally
- Auto-administration
- All code on Indie Box One is FOSS - free and open source software

An actual screenshot. Indie Box includes WordPress, Known, Mailpile, Mediagoblin, Owncloud, Selfoss, Shaarli

Johannes has found himself bookmarking more stuff on the web now that he does it in his private space on his own server, rather than, eg, Delicious

Indie Box also comes with an app store, so you install and get new applications on it

Automatic software upgrades

- OS, middleware, apps
- all configuration, db migrations, etc
- Scheduled offsite backups
- Hardware monitoring

Audience didn't like that it was online & the first box in from the Internet. Johannes pointing out that it doesn't _have_ to sit there - it's also a DHCP client.

Because the box is a DNS server itself, it works, but if you get your DNS from somewhere else, configuration is a little more complicated. But it can do both.
There are two hard drives in Indie Box One. They're mirrored, to help mitigate against hard drive failure.

Johannes looked at operating systems for a long time. In the Linux world, there are two "free" distros left: Debian and Arch. Johannes didn't want to tie it to some other company's strategy that wasn't necessarily entirely transparent. Chosen also because it has excellent ARM support - while Indie Box One is x86 based, the software platform works well on ARM, and probably in a year or two Indie Box will be based on ARM.

Audience is worried that automatic updates are a vector for hackers. Johannes points out that, essentially, you're damned if you do and damned if you don't: you'll be hacked if you don't update, too.

Audience asking if the concept is to create a warehouse for your data that bypasses many of the security issues in the wild - "is this just a small cloud for our data? Is that it?" Johannes explaining that, eg, for intra-family communications, there is added security by ensuring that communications never leave your home. You're almost always going via a large siloed provider. If you have your own server, you have this possibility.

Johannes: "what we're trying to do here is turn the Internet inside out. We're trying to put the Internet the way it was, where everyone has their own server."
This is particularly interesting wrt the Internet of Things: Johannes has a number of sensor devices in his own home, that right now go via, eg, Heroku. He has a front door sensor that goes via Heroku to let him know that his front door is opening. This makes no sense. Indie Box could fill that role.

Aaron Parecki pointing out that Philips also does this for their connected lightbulbs, ensuring that you have a connected architecture in your home. However, Johannes points out that you end up with multiple base-stations for different providers (although, the audience points out that they are using an open standard to communicate). Indie Box provides a central point in the home.

Audience asking if there's anything about this product that would enhance the user's relationship with third-party services. eg, discussing Spambox, which provides proactive email filtering via IMAP. It'd be cool to run something like that in Indie Box, to intercept IMAP communications and filter out spam.

Johannes says that WordPress and Known will be preconfigured "the indieweb way" - so your content is syndicated to third-party services. This is one way in which your relationship with third-party services is enhanced.

Audience asking about where this relates to the PATRIOT Act! Apparently the laws are very strong about possession of data, where possession is defined as on your body or in your home. The cloud doesn't count. Therefore you have stronger data ownership / privacy protections

against the PATRIOT Act with Indie Box than with a cloud service. Johannes would like people to check on the platform and audit it for security & privacy.

Audience asking, if you have 10,000 Indie Boxes, who pays for the electricity? What's the business model? Johannes discusses the app store, and the possibilities to act as a marketplace for third-party apps.

Johannes says that more integrations need to be done. He still needs to port much of his store code from Cloudstore, taking into account things like changing IP addresses (that are less likely to occur on servers in the cloud).

Johannes is keen to ensure that there is no lock-in, because otherwise you don't have full control & ownership. But on the other hand, lock-in is sort of required to run a business (ish). So Johannes is giving a percentage:

A percentage of the purchase price of the box goes towards the operating costs of the infrastructure that keeps the box running (updates, etc)

App store model - indiebox runs the marketplace, handles the billing, software authors get paid and removes hassle from the users.

Audience question - concerned with apps, what privacy agreement you sign, what is stopping apps running on the box from selling data? Do we end up in a sitaution where old data is stuck in the box like old LPs? Are there any protections from malicious apps shipping data elsewhere?

Johannes: if there are 100,000 apps on the app store then there's bound to be mailcious apps, there's no magic. What happens if indiebox implodes and you want to migrate off? Already exists software to migrate one indiebox to another. Even if indiebox goes away, all the open source projects still exist and you can run them elsewhere.

It's not up to any single entity to make this successful. This can be a barn-raising effort.

The Indie Computing Corporation is going to be an uncorporation: no management, none of the trappings of a typical corporation. It's intended to be a vessel for projects like this. It's open entry; if you want to participate, come in and help. If there's money, you can get paid. You have code? Put it on! You want to help make dynamic DNS better? Come talk to me.

Audience worry: Heartbleed was from open source so open source must be bad. There's nothing we can do at indiebox that would have stopped heartbleed. "Open source coders even with their good intentions don't have the resources...."
Audience answer: Heartbleed is a success story. There was a problem, it was fixed.
j12t: One reason we have an app store ecosystem is to provide money back into the ecosystem for open source apps.

"No more Big-Sites-With-Lots-Of-Secrets-For-Sale - This is how we unbreak the Internet." - Brian Behlendorf

Johannes: "If you have an IDP app, we can include it." Aaron: "I have one!" Johannes: "Of course you do! I want it! -- This is how it works."

https://www.indiegogo.com/projects/indie-box-let-s-bring-our-data-home < Johannes encouraging donations.

Audience question about using Indie Box One in medical IT. Pointing out that it's probably more secure than many places for data. (Same audience member asked about using the apps with smartphones. Potential for interesting use cases involving hospital-hosted data accessed by staff on handheld devices throughout an institution.)

Audience concern about app security, and how you ensure that apps on the box are secure and aren't bad actors with your data. Johannes says it's too early to comprehensively tackle this - it's important to get something running first. Hinted at some sort of signing/app store verified thing. But he also points out that Linux namespaces may offer some interesting possibilities.

Johannes: '"We cannot put all of our eggs in one basket, unless we can watch that basket really well," as Mark Twain said. I am much more comfortable with a Linux box that is mine than anyone else's system.' Intends to seed the ecosystem with technical early adopters, and will work up to an easy-to-use device that is suitable for very non-technical users.

If everything the organization does is transparent, it's very difficult to defraud the public. Johannes is making the Indie Computing Corporation open and uncorporation-ey in order to help people feel secure with the product.

Johannes: email is difficult (he agrees that it's irredeemably broken). But there are possibilities when more people are running boxes that use the same open protocols as Indie Box. You don't have to use email protocols when you know that something else is available and usable. You can eliminate third parties from communications loops, enhancing security and adding new features in the process.

Improving the Mobile Federation Sign-In Experience

Tuesday 1G
Convener: George Fletcher
Notes-taker: George Fletcher

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

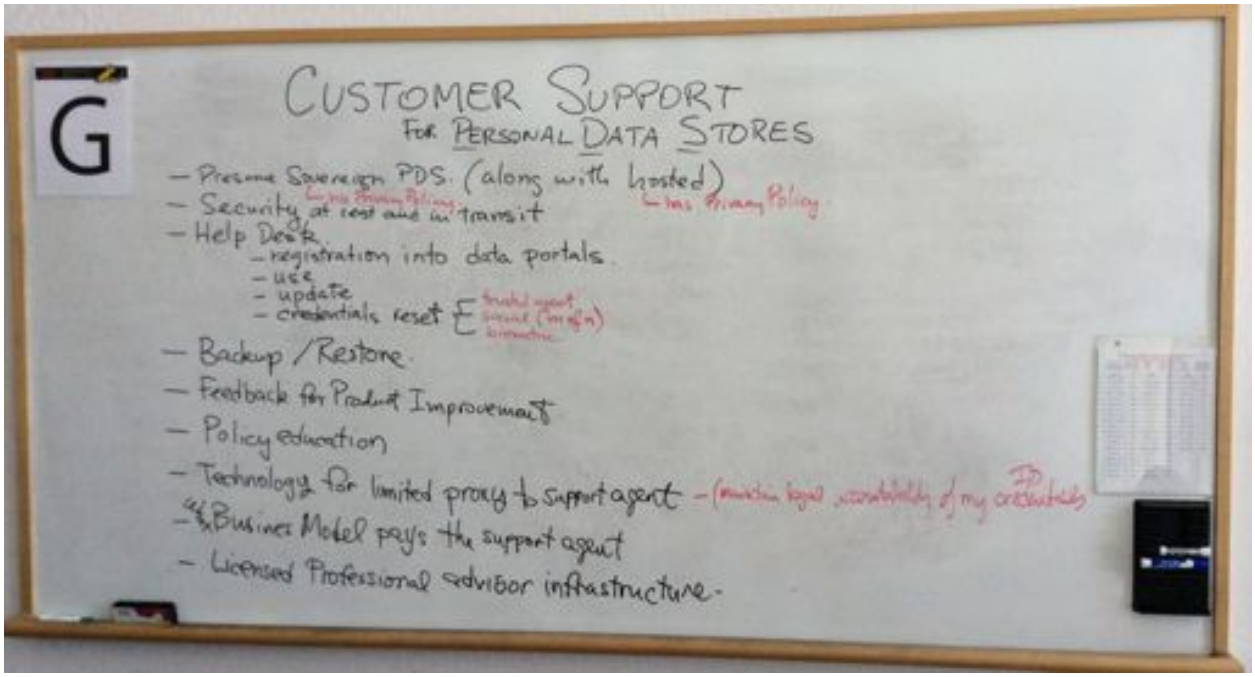
How to improve the mobile sign-in experience where the mobile app wants to allow users to login with Facebook or Google, but doesn't want to use the webkit mechanism because it forces the user to re-enter their login-id and password even if they already have the corresponding apps on their mobile device. Basically, we talked about how to use the locally authenticated apps as a mechanism to get a token (already part of the Facebook mobile SDK) and then exchange that token with the mobile app's OAuth2 Authorization Server to get the

app an OAuth2 token to use with the Apps resource servers.

Maybe a more concrete example will help. ACME has built a mobile finance app with portfolios and other financial management capabilities. ACME provides a set of APIs protected by OAuth2 that the app users to provide it's features. ACME wants to allow users from Facebook and Google to use their existing identities to use the app.

In this example, if the ACME mobile app gets a token from the local mobile Facebook app, then the mobile app will need to exchange that FB token for an ACME token to use with the ACME OAuth2 protected APIs.

Conclusions:
1. Many people are dealing with this issue
2. All are dealing with it differently with different levels of security
3. Basic flow is to pass the social token obtained on the device to the OAuth2 AS using a "token exchange" flow



Phishing Blend Authentication & Authorization

Tuesday 1J
Convener: Marc Stiegler
Notes-taker: Rory Ford

Tags for the session - technology discussed/ideas considered:

#Phishing

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

2 Factor Access Control - Delivering on the promise made by 2 Factor Authentication

Every year, a Fortune 500 sends out an email out to employees that links to a Log on screen. Phishing tricks the user into revealing credentials at the wrong site.

2 Factor Authentication doesn't make any difference to Phishing. Phishing workflow still humanly indistinguishable from legit workflow. The problem is credentials are still unbundled from valid site.

One way to solving this problem is via an unguessable random Webkey
Eg https://verysimplewebsite.com/demo/#0vib39n3dimwicm
Google Docs, Youtube, Craigslist and HP rooms use this.
Objections include: shoulder surfing, social engineering, user unfamiliarity.

2 Factor Access Control (2FAcc)
Can combine the password with the private login page

A web key can be used everywhere.
This fixes 75% of enterprise breaches at this stage.

An alternative:
Use an unguessable link for access. No username or password.

Claim: URL's aren't meant to contain secrets.
Server can be fully secure
Routing fabric: can be full secure.
Browser: breach of history/bookmarks

Comments:
This is fine internally.

As the application developer you are hoping people don't walk away.
With this people have to have walk away to then come back and access.

Challenge and response is stronger.

JOSE Can you see: technical overview of JWT and its JOSE underpinnings, which are poised to be the next generation identity token, and a look at using one open source implementation

Tuesday 2A
Convener: Brian Campbell
Notes-taker(s): Brian Campbell

Tags for the session - technology discussed/ideas considered:
JOSE, JWT, JWS, JWE, JWK, JWA, JW-STEAK, JW*, JSON Web Token, JSON Web Signature, JSON Web Encryption, JSON Web Key

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

It was more of an informational/educational type session rather than an interactive one and the slides from the session are available at http://www.slideshare.net/briandavidcampbell/jose-can-you-see-34360871

The open source jose4j software discussed is available at https://bitbucket.org/b_c/jose4j

ME Depot: Serving Billions

Tuesday 2C
Convener: Lionel Wolberger
Notes-Taker: Bill Wendel

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Me Depot
Lionel kick-off session with overview
Lots of people here for different reasons, all arguably under the umbrella of Personal Identify
One way to think of that is a market, as a thought exercise one way to think about that is as a market. So let's think about a place we can call Me Depot.
Driving by in car, see Home Depot but not interested in Home Debot, but not interested in stopping because "we don't need anything for our car."
Come to Me Depot, and say, Oh, my personal sovereignty has been bothering me… let's pull in."
"I'm uncomfortable about using gmail, now that we have kids."
Walk into Me Depot, greeted by MEgreater, who asks How can I help?
Walk-in and can we think of the departments in Me Depot
Exercise is designed to get people thinking
What isle would your product go into?

Me Depot = Personal Empowerment Store

De-Silo'ed
Everything flows to your personal cloud
Home Depot:
Anything you buy can interconnect now
But IoT = too silo'ed
What do you want to export to your OWN cloud?
Walk into
Find ready made stuff

Geeks are first adopters so need to - Read the news and suddenly we realize we have a need
We've arrived

We Depot = Common Good store?
What data am I willing to share with 4th Party?
Family package
Five Personal ID Respect Network package sold at auction for $185 ($150 retail value)

Discussion of need have alternatives to internet of things that connect to the enterprise
Eg. Fitbit = own silo'ed
Digifit

Respect Network is trying to create a market for personal data that we keep in the cloud
Do people know enough about cloud to know what we're talking about?

DEPARTMENTS
B2B
Office supply
Auto
Horizontal departments
Security
Passwords
Respect Connect
Identity aisle
Should be in the store
Browser
Mozilla
IntentCasting
Cloud service provider (CSP)
Cloud network isle
Empowerment
Sovereignty
Mobile
Personal.com
Desktop
Personal.com
Wearables / personal
Verticals departments

Put intangible stuff in a box, because that is the only thing people understand
Intangible Me departments
Wellness
Capacity bot
Demonstrate what I can do
Document what I have done
Tangible Me departments
Financial
MeeCo
Garden
Sprinklers
Appliances
Home Cloud Appliance
Drummond "beginning to think more that people are going to be keeping more and more of these boxes at home. Some are really sexy like
Proto.net

Home improvement
ZiggBee Light Link
Clothing
Optical

Intentions vs Identity

Tuesday 2D
Convener: Edi Immonen
Notes-taker(s): Edi Immonen

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The talk was around Glome and what the concept is about - intentions not identity. The basic idea is to separate static data (who you are, where you live) with dynamic data (what you want).

Static data is your identity: it does not change and with it comes registrations and strong crypto => focus on making sure it is you.

Dynamic data are your intentions: they constantly change as we human are irrational animals => focus on serving without friction or forced authentications.

The talks were about value proving and fitting how to fit into existing businesses AND how to get value to all parties. Here is a link to a video: https://vimeo.com/91443707

Here are the slides: http://www.slideshare.net/GlomeInc/anonymous-loyalty-card

IoT: Internet of Things Unintended & Unexpected Consequences

Tuesday 2F
Convener: Jeff Stollman
Notes-taker: Dave Sanford

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation by Jeff, IoT components:
1) sensors
2) processors
3) actuators
4) combinations of above

Lots of use cases described, with associated abuse cases

Starting to include Scada
Includes home appliances, Nest,
Irrigation and flood control
Limited ensuring data integrity - not always clear whose responsibility.

Dave Sanford - for any new use case, one or more new abuse cases.

Lots of discussion about gaming systems (e.g. fitbit users sending apparent physical exercise to health insurance company)

Who owns the data you collect?

Phil Windley - power of distributed systems to create robustness in book 'Honeybee Democracy' bee swarming and finding a new place - may be somewhat like 'unit of work' in bit coin.

Who is controlling your vehicle? Phil - V2V (vehicle to vehicle), collision avoidance systems for cars, may allow governmental entities (or hackers) to shutdown multiple cars at the same time.

Lots of discussion about security and usability.

Smart packaging - tell you what drugs to take.

Physical security devices - home surveillance cameras

Electric grid - security and liability

So issues raised include security, privacy, ownership and liability

Blue boxes that tell lights that emergency vehicle is coming through. Originally easy to clone and use.

Lots of talk about Arduino and approaches for IoT design.

Received from Jeff Stollman – Link to Power Point:
http://www.secureidentityconsulting.com/unanticipated-consequences-in-the-internet-of-things-iot/

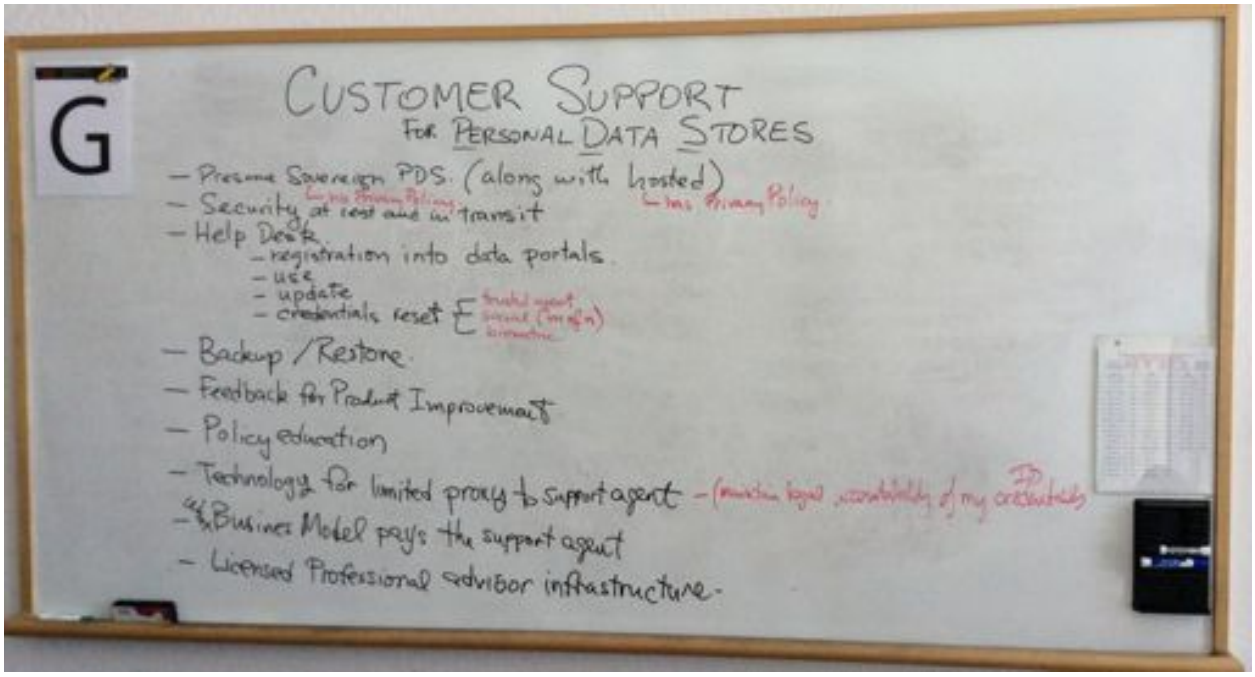
Customer Support for Personal Data Stores

Tuesday 2G
Convener: Adrian Gropper
Notes-taker(s): Kris Alman

Tags for the session - technology discussed/ideas considered:

Personal Data Stores
Sovereign Personal Data Stores
Sovereign Identity
Accountable Identity

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Reasons to have:

- Presume sovereign PDS: no privacy policy (along with hosted which assumes a privacy policy)
- Security at rest and in transit
- Help desk essential
    - Registration
    - Use
    - Update
    - Credential reset (could be biometric, proxy—such as trusted agent)

- Backup/Restore
- Feedback for product improvement
- Policy education about external connections
- Technology of limited proxy to support agent (i.e. don't want to share passwords with tech support; this is intended to maintain legal accountability of ID credentials)
- What is business model to pay support agent?
- Infrastructure for access by licensed professionals

An Introduction to the INDIEWEB

Tuesday 2H
Convener: Ben Werdmuller
Notes-taker: Kevin Marks & Ben Werdmuller

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Find notes from this session here:
http://indiewebcamp.com/2014-05-06-iiw-intro-indieweb

Further Notes:

Ben Werdmüller: we talk a lot in #indieweb about "silos" - dropbox, facebook etc who make money by locking up our data

facebook is a fantastic proof of concept of a social network, but they take control away from you

#indieweb is about having your own space on the web - your own domain as your primary identity

the #indieweb goal is for you not to lose anything by not being in the silos, by connecting to them

I haven't posted directly to facebook or twitter for a year, I post to my site and share to them instead

the #indieweb community practices what we preach - we build for our own sites not making standards for other people

there are lots of small building blocks that we use to build the #indieweb - microformats are how we add meaning to web pages

another building block is webmentions http://indiewebcamp.com/webmention that tell sites when you have linked to them

by using these building blocks we can have likes, retweets, replies, and RSVPs on our own #indieweb sites currently this is mostly about publicly visible data, but we add authentication with indieauth.com we are not trying to establish a huge standards organisation, but instead a community of people who implement and discuss how many people have their own websites? [most] how many post regularly [fewer]

Stefan Magdalinski: does posting once a year count as regularly?
Aaron Parecki: twitter can be almost to easy - you need an interface that is as easy to us as twitter for your own site

there is an opportunity for "twitter apps" for your own site - use other people's apps to post to your own #indieweb site

Kevin Marks: shows off noterlive, which is a way to post these kind of live tweets and keep them for posting on my own site
Ben Werdmüller:

@aaronpk has posted a photo on his site - I can reply to that using idno's firefox plugin and it shows on my site

I can also reply to @kevinmarks's tweet using the Firefox plugin, and it posts on my site and shares it to twitter too

There's an event tomorrow night in SF called Homebrew Website Club - I can RSVP to that on my site + share to Facebook

creating the twitter and facebook integrations for idno too about an hour and a half each

I'd love to create a way to upload HTML5 games and post them to your site and send highscores by webmentions

it's an open community - there's an IRC channel: http://indiewebcamp.com/IRC and a wikihttp://indiewebcamp.com- all are welcome

other sites could shut down apis, but at least you don't lose your own posts when that happens

with silo'd sites there is na ethnocentric design as they're all made here in SF - indieweb is less SV dominated

Stefan Magdalinski: this is interesting from a hacker perspective, but how big can it go? this blogging will never catch on
Aaron Parecki: there is a page on the wiki for wider adoption: http://indiewebcamp.com/generations (there's a page for everything)
Ben Werdmüller: we're more likely to get to mainstream by iterating on working code and consensus
Stefan Magdalinski: I've run lots of my servers at home (and fax machines) -what happens when they're all botnets?
Kevin Marks: not necessarily hoem servers, can be in cloud, or even static sites that can be synced
Aaron Parecki: there are ways that we can do this with a wholly static site and services that build the communication parts
Steve Williams:
the other way is to run an unhosted app that posts to a static server and have the data locally in the browser

Ben Werdmüller: one advantage of making this web-centric is that we don't have to impose any architecture on anyone else to communicate
how to get started? one list is at indiewebify.me

Aaron Parecki: first get your own domain and put up a page that links to your existing profiles elsewhere, so you have your own space

Tantek Çelik: also look at http://indiewebcamp.com/Getting_Started to see where to go

Erin Jo Richey: we're hoping by the end of the summer to have idno be a one-click install http://idno.co/

the idno code is all on github at https://github.com/idno/idno tomorrow it will be called "known"

Ben Werdmüller: we're going to switch to MySQL from mongo on idno to make it run where wordpress runs

we're not quite there yet to be able to deploy a dynamic site anywhere

do come to Homebrew Website Club meetings on wednesdays in SF, Portland, Chichago + sunnyvalehttp://indiewebcamp.com/events/2014-05-07-homebrew-website-club

Received from Ben Werdmuller:
Notes by Aaron Parecki
These are permanently hosted at:
http://indiewebcamp.com/2014-05-06-iiw-intro-indieweb

the real promise of the web is that we can all connect and learn from each other and you're not giving up control of your data and identity selfdogfooding - get something up and running for yourself and live it. if you expect people to live by a standard or principle, live it yourself first

building blocks - make it easy to get started quickly

- microformats - encode machine-readable data into HTML, rather than trying to create huge backend system for things
- webmention - has become one of the key building blocks of the indieweb - people are using this today and forgetting about the technology and actually having real site-to-site conversations

Because each of the building blocks are so small, people can pick up one of them and experiment and build something that works in a day.
how many people have their own domain name? all but 2 raised their hand [nice! -t]
how many people post regularly? most - does annual count?
"i used to" - 'why did you stop?' - twitter, it's faster
benwerd: I get to choose to syndicate to twitter and other silos
aaronpk: one of the challenges is to have a user interface to post to your own site that is as easy as Twitter. Some folks have built user interfaces on their own sites as simple as Twitter.
aaronpk: not everyone wants to build their own user interface. micropub lets apps post to indieweb sites.
kevinmarks demonstrating noterlive

- put in a hashtag and speaker name
- posting to twitter, but also collecting HTML into the page
- when he finishes, copies the HTML to his site
- wants to add micropub to automatically post the HTML to his site instead of manual copy/pate
- this interface is *more useful* than twitter for tweeting

benwerd demoing his site

- showing aaron's photo of this session
- clicking reply button in firefox plugin for Known
- typing a reply, hit save
- posted it first as a comment on his own site
- automatically shows up at the bottom of my photo as a comment
- url: http://aaronparecki.com/notes/2014/05/06/4/iiw-indieweb
- http://werd.io/2014/great-to-see-so-many-people-here
- demoing RSVPing to tomorrow's homebrew website club indie event
- these plugins took about an hour to build each

would love to find a way to post HTML5 games so indie game developers could quickly host games. high scores could be received back with webmentions.
There's the IndieWebCamp wiki and IRC channel. Everyone is welcome.

- http://indiewebcamp.com/
- http://indiewebcamp.com/IRC

There is no mailing list: http://indiewebcamp.com/FAQ#Is_there_an_IndieWeb_mailing_list
Q: can the "big guys" withdraw the APIs? A: of course! but it's not like they can disable an API key and the whole indieweb goes down. but it's also useful to note that we don't necessarily need them to have indieweb conversations. also they can't turn off their own HTML.

Q: if Google+ doesn't have an API, do they even really exist?
... Freedom box ... from Austria ... just got back from ouishare in Paris following indieweb on the sidelines ever since FSWS one of the powerful ideas of the indieweb is that it's loosely defined, so it's easy to get going and start using building blocks
Q: this is really interesting from a hacker perspective, but how mainstream can it go?
A: aaronpk, pretty much every question has an answer on the wiki. E.g. for this, see https://indiewebcamp.com/generations - right now we're mostly a hacker community. We saw the internet go from a hacker community and go completely mainstream. This is how it starts.
A: benwerd: 10 years ago, social web, people would say what? it's not mainstream. ... We're more likely to get there by iterating on working code.
KevinMarks: one of the arguments is, how much can you push statically? a bunch of us are doing this.
Aaronpk: when your website is a pile of HTML files and you can put it on any FTP server and still communicate with other sites? You end up with using a webmention service.
[12:37] <bretttt> its key to eventually get that service data INTO the html file itself. working on that now
KevinMarks: part of the point here is to NOT just build a monoculture.
https://indiewebcamp.com/monoculture
because we started with 6 people writing their sites in 6 different programming languages, it made monoculture way less likely to happen
Getting Started:

- buy a domain
- find space to host it
- put up a simple home page with an h-card with your name and links to other profiles

Known - currently PHP + MongoDB. going to be PHP+MySQL.
known / withknown.com (sp?)
benwerd: As Kevin said, monocultures are bad. This only going to work if there are a number of platforms out there. Idno is one. p3k is another. Interesting things with WordPress plugins. Taproot. See https://indiewebcamp.com/projects
If anyone is here in this area, or Portland, or Chicago, there's a Homebrew Website Club every two weeks.
SF one is 18:30 on Wednesday:

- http://indiewebcamp.com/events/2014-05-07-homebrew-website-club

Portland one is usually hosted by ESRIPDX or MozPDX but not this week.
Chicago one is usually at Intelligentsia.
KevinMarks: Do we want a satellite one here in MV?
Benwerd: not looking forward to driving back in rush hour
KevinMarks: we can grab a table at the Firehouse and make that the MV HWC

"SCIM" Next Steps – Planning Ahead: x Domain ID Management

Tuesday 2I
Convener: Bill Mills
Notes-taker: Phil Hunt

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Three proposed topics:
* authentication - "oauth 2.0 is more wrong than other choices"
* P2P instead of client server model
* more capabilities - per user feedback
Signaling
Bill Mills has desire to do signaling on account actions via SCIM - think shared signals. Yahoo Mail observes Eric's mail account is compromised and is now sending Spam from multiples ip/locations. In federated scenario, how can the email provider notify the IDP of suspicious activity?

Phil brings up Tony and his lightweight authentication protocol
* a problem emerges as to who is responsible for what. Do RPs have right to tell IDPs what to do?

If so, what *should* RPs be telling IDPs if anything?

Ian suggests looking at Andrew Nash's shared signals work

Phil. Would a token approach work where Yahoo issues session tokens for emails based on an authentication from an IDP. That way Yahoo can revoke rights for an abuser without need of alerting IDP.

However it still doesn't solve the problem of Yahoo playing nice and informating the IDP of a suspicion about a Nigerian spammer.

Another case is Yahoo acting as IDP to Google Apps.

PubSub seems to be an interesting way to deliver these events.

Is there a liability issue in sending these messages. E.g. biz partners that separate.

We discussed a number of issues SCIM has started exploring regarding ASYNC operations: workflows, bulk requests, event notifications.
Ian raises issue about situation in which SCIM server is bombarding SCIM client. Can the client tell the server to throttle its requests? A too busy state/code in HTML?

Bill was thinking about being able to enable a server to write to a subset of a user object but he recognizes that isn't ideal - this is a p2p approach

* he isn't sure that pubsub model

Phil raises point he and @cmort looking at PubSubHubbub for event model

talk on token approach for mail accounts

the general case of the conversation - I need to tell you about one of your accounts and I want you to do something about it, but I cannot touch it because you own it.

Bulk and large scale transactions
Instead of bulk what about SPDY?

Authentication
We can use OAuth2 but that isn't a requirement
Some other bearer token?
Or just have an agreement that it's a JSON token with a specified format

should we sign the payload?
* we could a JSON signing token profile for SCIM

New OAuth2-WG: Multi-Party Federation!

Tuesday 2J
Convener: Mike Schwartz
Notes-taker: Mike Schwartz

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

A multi-party federation enables a group of autonomous entities to drive down the cost of security by agreeing to a common set of business policies, technical schema and protocols. An example of a federation is InCommon, which has over 400 university participants, and over 150 websites. The list of InCommon participants can be found at http://www.incommon.org/participants, the Agreements for a participant to join can be found onhttp://www.incommon.org/join.html , and an example of mulit-party federation metatdata in SAML can be found at :https://spaces.internet2.edu/display/InCFederation/Metadata+Aggregates

Given the success of federations using SAML, it seems only natural that existing and new federations could benefit from using the same strategy to drive down the cost of OAuth2 based applications. Originally, Gluu had proposed such an approach for OpenID Connect: http://ox.gluu.org/doku.php?id=oxauth:federation&s[]=federations

However, on further consideration, it became apparent that other profiles of OAuth2, especially UMA, could be incorporated. At the InCommon Advanced Camp held last year, it was suggested that instead of the OpenID Foundation, that perhaps such an effort would be better suited as a working group of OAuth2.

OAuth2 brings new schema that needs to defined, including OpenID Connect scopes and UMA scopes. Some of the requirements are being uncovered by Gluu as a result of one of its involvement in the formation of the first OAuth2 based federation for a K12 project in Texas. The schema for that federation has already been published at :https://idp.texaspass.org/tech-info

In addition to schema and metadata, endpoints would need to be defined to publish federation metadata and to enable entities to join federations. An idea of these are alos proposed on the above mentioned OX Wiki page on the "Design for OpenID Connect Multi-Party Federations" mentioned above.

While much work on this topic is being done by Gluu, Mike pointed out that he really needs help to move this forward. It would be a great chance for someone who wants to get involved in standards development to get involved (hint - hint).

This work is critically needed by many ecosystems. If OpenID Connect becomes a ubiquitous federation protocol, better trust models will be needed. The federation provides an efficient way to distribute public certificates. If a Heartbleed-like vulnerability were to afflict OpenID Connect or UMA AS's, re-keying would be a nightmare. In addition to the cost savings associated with federations, they would reduce the impact of such a nightmare.

Open ID Connect Interop Testing Details

Tuesday 3A
Convener: Mike Jones & Roland Hedberg
Notes-taker(s): Mike Jones

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Add tests for third-party initiated login
Form post response mode
Registration specifying keys using "jwks_uri"
Registration specifying keys using "jwks"
WebFinger tests
Verify that issuer in discovery doc matches "iss" in ID Token
Key rotation tests
Do OP, RP support standard MTI algorithms
Support for request and request_uri parameters
Test for require_request_uri_registration
Test for default_max_age
Test for require_auth_time
Test for request_uris
Tests using ui_locales and claims_locales
Review acr tests
Test that server certificate validates

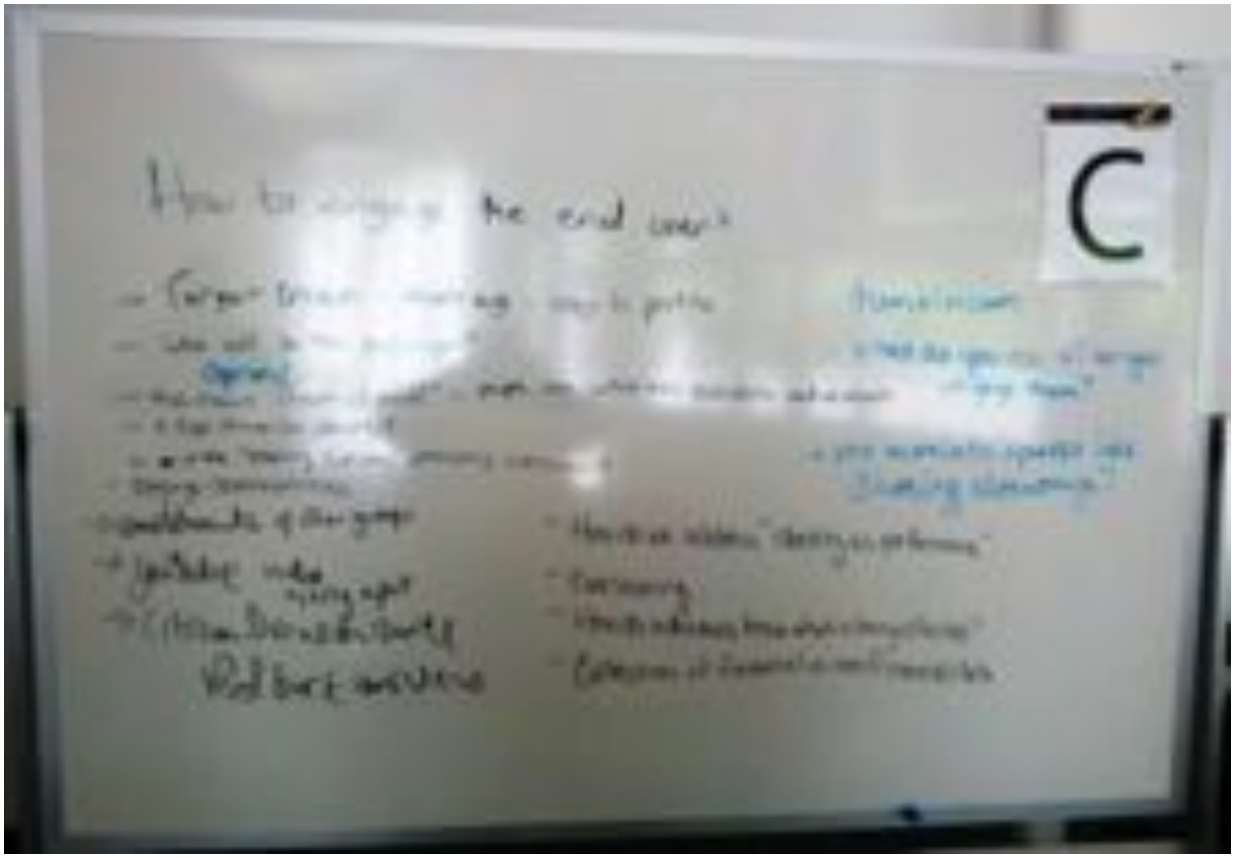
Update names in the existing tests:

logo_uri instead of logo_url
policy_uri instead of policy_url
*_url -> *_uri
user_id -> sub

Engaging End Users: How Do We Get Consumers to Participate in Identity Discussion?

Tuesday 3C
Convener: Eno Jackson
Notes-taker(s): Eno Jackson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Ethical Data Handling: What is it? What are the obstacles? What is success?

Tuesday 3E
Convener: Robin Wilton
Notes-taker(s): Robin Wilton

Tags for the session - technology discussed/ideas considered:

Personal data, ethics, privacy, harm

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We used four topics relating to personal data processing, as a framework for the discussion:

- The principle of "no surprises" (if users found out what you were doing with their data, would they be unpleasantly surprised?)
- The idea of "ethical dilution" (that the more data passes from one controller to another, the less responsible any of them feels towards the data subject)
- Ethical issues in multi-stakeholder cases
- Ethical issues in multi-context cases

Some ethical factors appeared across several topics – for instance,

- User expectations, and informedness
- Predictability and determinism, and their role as a trust factor
- Power imbalances (including economic imbalances)
- Cost/risk assessment, harm as a privacy metric

Platform Deep-Dive of QREDO - ID•PRIV•AUTH

Tuesday 3F
Convener: Hugh Pyle
Notes-taker: Dave Sanford

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Hugh's slide show (link here):
http://www.slideshare.net/qredo/qredo-internet-identity-workshop

Doc gave an intro - could have been written by Project VRM, founders came from Visa Europe which is a non-profit. IIW has ability to support and vet.

Qredo provides end-to-end crypto and a framework for other stuff.

Hugh - Everyday stuff is broken. Applying for a service where you don't have an existing relationship:
- progressive disclosure

- hard to negotiate as an individual
General-purpose platform architecture for authentic communications:

- Lightweight
- Secure
- Anonymous

Will provide value to app developers, first on cell phone delivery stuff.

Zero id. Establish trust by having a conversation, but if I come to the conversation with credentials that make me trusted in some context (old enough to have a drink - but not leaving other information).

Doc - trying to make the digital world more like the ordinary world, in the physical world I can interact without leaving persistent knowledge beyond what is needed for the transaction.

Need to be able to:

- send a message securely
- apply for a loan - don't need to disclose who I am, but may need to disclose the value of my assets in a way that is verifiable
- sell a guitar - don't want them to hold my 'reputation', beginning to look like intent casting
- prove that I'm over 21 at the bar - single transaction from me and the bar staff to validate my age
- split a cab fare (cash scenarios without using cash or credit cards), how do I leave a tip, or deal with folks I don't inherently trust, strangers

Rendezvous - I can make up a string, one time only 'rendezvous' tag. Public tag can have $5 (for example), at the same time an ephemeral key is created and only known by the two parties (shared secret) and an anonymous conversation - that is available from the tag.

Secure interpersonal cloud:
- Messages
- Documents
- Authenticated personal data
- Cash

Conversations can start without me sharing identity and only the context needed other than what is required for the conversation. Doesn't imply any context even for future conversations from the same entities.

Lots of discussion about when keys become compromised does that compromise previous transactions.

Cash is just one kind of high valued conversation.

Identity and authenticity

Enforce using crypto what other people enforce using policy.

Very little of this is new technology.

All of this is programmable. Application developer uses Qredo SDK for:
` iOS, Android, Linux, Windows, OSX
App builds user interface and behavior

Uses all the full Certificate Authority technology, the new piece is the 'rendezvous' and the ability to discover using the 'skyhook'

Qredo does not have a direct relationship with the end user. The app developer and the service provider do have relationships with Qredo.

Discovery of rendezvous names looks a lot like intent casting.

Having different identity types allows you to add identity into the conversation - you don't start with identity but you can add it in as it provides value.

How to Join the IndieWeb

Tuesday 3H
Convener: Kevin Marks
Notes-taker: Kevin Marks & Tantek Celik et al

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Find notes from this session here:
http://indiewebcamp.com/2014-05-06-iiw-join-indieweb

Further Notes
Kaliya-IdentityWoman: lets see if we can introduce ourselves with one word this time
Ben Werdmüller: I'm one of the indie posse here today - I'm doing an Introduction to the #indieweb
Aaron Parecki: I'm doing a session on indieauth, making your own site an identity provider #indieweb
Kevin Marks: I have a practical session "Join the #indieweb" - get your personal indie website set up

Received from Ben Werdmuller:
Notes by Tantek Çelik et al in the #indiewebcamp IRC channel, based on an audio feed
These notes are permanently hosted at: http://indiewebcamp.com/2014-05-06-iiw-join-indieweb

Kevin is starting with a short 5 minute intro to the IndieWeb to get those that missed earlier sessions caught up.
Describes the basics of IndieAuth but defers to the later session on the subject.
Brief description of POSSE.
Directing people to getting started link.
Audience is hosting their own sites in a number of places (in their basement, on a hosted server, etc)
Q: Just as a general user, I don't have a static IP, does it make sense for me to run this at home if I really want to own it?
A: What you really OWN is the URL, hosting can be anywhere, but it is the URL that is what verifies you.
Q: If I have an IndieBox can I run this?
A: You would need some sort of dynamic DNS, but that is an implementation detail.

- cannot hear clearly, but there are a number of questions between audience specifically around IndieBox (Sounds like Johannes is there fielding questions)*

If you are on your own domain, you are on the same level as silo's not underneath them. You can still go down, but you are able to back that all up yourself.
This isn't the app for everyone. We realize this. Only now are getting to points where there are bits of this that can be made easy for the people who aren't hackers.
The point is to have a lot of different implementations. Most attempts to replace sites like Facebook have always just made the assumption that they are a monolith as well. The point is to go back to the open standards and interoperability of the early web.
j12t: bridgy was kind of magical, I set it up on my site and forgot about it, then found a bunch of comments from people and realized they were from Facebook!
"I just logged into the wiki already, and it pointed out a few helpful problems with my rel-me links, so that's great!" (Steve Williams, sbw.org)
aaronpk: Step 1 try to sign-into the wiki
you need to add rel=me to the link to your other profiles, e.g. Twitter, Github
"speaking of Salmon - hahaha" (Kaliya)
Kaliya introduced Gabriel Scheer
"what's your domain name?" "futureoffish.org" "no, yours" "mine? gabrielscheer.com, but it hasn't been updated in months"
Why not about.me?

- the URL is http://about.me/kevinmarks
- they decided they don't want visible links, by that I mean links that are hidden to anything except a browser with javascript
- if you try to fetch about.me/kevinmarks with curl you get HTTP 418 error

Note: people that were able to sign into the wiki from IIW for the first time! (times are likely UTC, thus 7 hours later than PDT would indicate)

- Sbw.org (Created on 2014-05-06 at 21:21:43)
- Scottylogan.com (Created on 2014-05-06 at 21:51:25)
- Aheadrobot.com (Created on 2014-05-06 at 22:04:42)

per
http://indiewebcamp.com/wiki/index.php?title=Special%3AListUsers&username=&group=&creationSort=1&limit=500

Silicon Valley "Cult~~ure~~ of Youth" :Experiences; Lessons & Effects; Predicotrs & Steps

Tuesday 3I
Convener: Randy Farmer
Notes-taker(s): Randy Farmer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The conversation on the "Cult of Youth" was personal and confidential. There are no notes - only this:

There is a problem with what to do with all the no-longer-young former programmers that are now overqualified for the number of level-appropriate positions available.
Dick Hardt suggested that anecdotally, many of his 50+ friends are now in enterprise software positions.

Digital Traits for Strong Authentication

Tuesday 3J
Convener: Herbert Spencer & Chris Canfield (Traitware)
Notes-taker(s): Herbert Spencer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The slides at the following link were shown and discussed by Herbert Spencer and Chris Canfield from Traitware:
http://traitware.com/wp-content/uploads/2014/05/Digital-Traits-for-Strong-Authentication-5-6-14.pdf

The following link is to a white paper on the material discussed:
http://traitware.com/wp-content/uploads/2013/11/Digital-Uniqueness-in-the-Use-of-Smart-Phones-and-Tablets-11-09-13.pdf

Following the presentation some question were addressed:

1. Q: Can the process be used across multiple platforms? A: This is an area under development. As along as a uniform salt is used in the hashing process of the user traits across multiple platforms, such as for a phone or tablet, the traits can be compared across platforms.

2. Are traits independent enough that probabilities computed for traits belonging to the same individual can be combined to get an overall higher identification probability? This needs further investigation but the difference seen in individual traits shows the traits are relatively

independent. For example it is unlikely that a song list and contact list will be of the same length.

There were then some discussions of the app based on using traits.

Open ID Connect: Session Management / Logout Discussion (Part 1 & Part 2)

Tuesday 4A & 5A
Convener: Mike Jones; John Bradley; Naveen Agarwal
Notes-taker(s): Mike Jones

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Participants also included:

Torsten Lodderstedt
Chuck Mortimore
Brian Campbell
Alan Karp
Breno de Medeiros
John Pinter
Bill Mills

Back channel logout

Multiple RP sessions might be logged in at once
OP doesn't have session identifiers
Torsten - back channel logout has been shown to cause problems
Chuck - the session-based SAML logout doesn't work well and isn't supported
Brian - requiring JavaScript on every page a non-starter in enterprise contexts
Alan Karp - Better UI could help users better understand what's actually going on
John - one requirement can be extending session lifetimes across sessions
Chuck - The only session state typically present is the session cookie
Brian - SAML has fragile redirect chain
    Another means is for the IdP to do a GET to each RP endpoint
    Ping is currently implementing something like that
Naveen - Unless the browser tab is active, the JavaScript logout doesn't work
Naveen - Yahoo had a variant where they stored state for all sessions in a single cookie
Brian - Doing GETs to single-pixel images, which trigger logouts
John - The RP could check the referer if it wants to secure the logout
    But in general, not protectable against XSRF
Chuck - Browsers are getting better about preventing cookie state manipulation in iframes
Torsten - Will check what DT is doing
John - ID Token "exp" claim doesn't trigger logout in practice
Naveen - We could just document both front channel mechanisms as optional
    Enterprises might choose one method, the Web might choose another
    We should document both as a next step

Mike - If we support multiple mechanisms, the RPs would get to decide
John - Back channel notification is yet a third mechanism
David Pinter - The front channel won't always be available
Bill Mills - Security policy may require ability to kill all sessions
John - A compromise back channel mechanism is notifying RPs on the back channel of a state change

Mechanisms:
- postMessage:
  - Pro: RPs get notifications, minimal web traffic
  - Con: Requires RP JavaScript
    - Doesn't work when RP tab not active
- image/iframe GETs:
  - Pro: Doesn't require JavaScript
    - Still uses session cookies
  - Con: IdP needs to track active RP sessions
    - Ugly logout page
    - All RPs might not be notified before the browser is closed
- backchannel notifications:
  - Pro: Works even when RP tab not active
  - Con: Requires RP logic to identify and communicate with session to logout
    - IdP scaling issues

Chuck - Current spec doesn't work for enterprise use cases because of JavaScript requirement and because the RP must be active for the logout to work
Chuck - We didn't put "jti" in the ID Token - we could for enabling logout
- That would enable correlating back channel notifications received to active sessions
- Open questions about whether to use the same ID in multiple responses to same RP
- Probably use a separate session identifier that is not "jti"

Dale - Back channel notification is effectively ID Token revocation
Chuck - The OP wants to be authoritative for the session ID
Chuck - Revoking a session could be done like an OAuth revocation
- OAuth revocation supports CORS and JSONP

Actions:
- Add image/iframe description to Session Management
- Also describe back channel mechanism
- Then we decide what to do after that

Naveen, Breno - Google is planning to build a token caching layer
- It would get tokens at login time and clear them at logout
- It would send notifications when things change
- It would communicate internally with postMessage
- postMessage requires a security layer

George - How is this like the Trusted Agent in the Native Applications work?
Naveen - It's a lot like that

Identify Theft: How do we preserve & protect identity (medical, financial, social) in era of big data – where algorithms to detect fraud/surveillance aren't working.

Tuesday 4B
Convener: Kris Alman
Notes-taker(s): Kris Alman

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Identity theft & big data: how to protect and preserve through policy and technology

Whether taxpayer related/ credit card / medical, identity theft is financially motivated.

This same problem exists in Europe where the SSN is used as an ID and not for authentication.

Overarching problem that our identity is overused in transactions; authorization-based access control (such as that used for bit coin) subtracts the person's identity out of the equation. Cached data should not be bound to individual. That said, de-identified data can be re-identified (Latanya Sweeney);

2-factor authentication: through phone/postal/email an identifier is sent and necessary for the process. Using postal service is most expensive. A random sequence generator creates passwords that are temporary.

Algorithms to detect fraud are population-based; they never work well for the individual.

There should be uniformity across states to protect against identity theft.

There will always be potential for fraud; if this occurs through the postal system (mail is stolen), this is a federal offense (the penalty)

Discussed using third parties who authenticate identity for new password authentication using public information. Potential promise, but prevailing concern was that attackers who know your history, know your data better than you. This contrasts with proving who you are through shared secrets.

Discussion whether we are better off with policy vs tech solution; concerns about regulatory capture.

Can't Be Evil!

Tuesday 4C
Convener: John Light
Notes-taker: Jack Senechal

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Zero Knowledge
  - of content on the system
  - of user's ID, IP, browser fingerprint, etc

- Open Source
  - you can't just state intent, you must be able to prove it
  - audit
  - identity exploits
  - validate claims

- Client Side Crypto
  - if the server can decrypt your stuff, the whole system falls apart

- Zero Trusted Entities

- Distributed
  - preferably p2p

Good crypto is not about trusting people, it's about trusting math. In math we trust.

Bitcoin is the first system to solve the Byzantine Generals problem.

Tahoe LAFS (least authority file system) is a Can't Be Evil system

There's some zero-knowledge Etherpad out there, maybe called PiratePad?

Bitcoin, NXT are good examples of CBE

Ripple is totally based on trust all around, so it may not fit.

Respect Network + XDI
==========

Q. If I have a cloud name, how do I find the service that's providing data for it?

XDI discovery. You get your cloud, register it with a cloud service provider that you choose, they register it with a name registry
service. You look at the registry service for =markus, and they tell you where to find the cloud.

XDI is open and distributed, doesn't have to be only one registry.

Q. How do you avoid duplication across registries?

Right now you don't. Within the Respect Network there is one registry. The cloud service providers are decentralized.

If you run discovery on =markus, you get the location of the cloud, and the cloud number. Cloud name can change, the cloud number is
a UUID that doesn't change.

The cloud number is not issued by a central registry, you generate it yourself. You can choose to register it with some registry. The
registry will ensure that the number persists and give you a mechanism to change the name.

Can have multiple cloud names pointing to one number. Called synonyms.

Q. How much does a cloud name cost?

Neustar: CSBs pay $19 per registered user, up to 1m users. After that there will be a different price negotiated. We're not there yet.

NSTIC: Update from NIST & Roundtable

Tuesday 4E
Convener: James Sheire
Notes-taker(s): Kaliya Hamlin

Tags for the session - technology discussed/ideas considered:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NSTIC = National Strategy for Trusted Identities in Cyberspace

It is the National Strategy to form an Ecosystem ~ where people can voluntarily choose and ID and login.

Privacy, Interoperability, User-Friendly, More Secure ---> User have to create dozens of account.

Problems it seeks to address - Re-Use over and over of passwords.

They (the NPO) is facilitating a private sector lead group.
The purpose is to create the policies, rules and standards and framework that governs the interactions in the ecosystem.

Getting Federal Government Programs to get being early adopters and use 3rd party credentials.
Access to government services, file a medicare claim.

FCCX (pronounced F6) service users login approved credentials. Choose from IDP's that are approved.

Q: Do any of them let them control their ID.
A: At higher level of assurances must have it be bound.
Vouch for Individual

What about allowing users vouch self where the individual holds externally vouched for attributes?

Dialogues will emerge on different efforts.
LOA - 1, 2, 3, 4

Digital Certificates of Proof

The hardest part is the business process - record keeping etc.

Robin: HIS model where brokering system where credentials themselves come from bank.

Update: become independent entity with its own capabilities. 501(c)3
-comment from crowd - "so it is a charity"

IDESG will have funding through Grants

FCCX (USPS) (Contract with Secure key) to build the HUB - processes for ID and for departments who will pulg in.
It has better privacy capabilities.

It will have a consistent experience for citizens. <---starts new behavior

What is the business model for FCCX
Cost reduction
Agencies will/do subscribe

Tired of paying for proofing vs. authentication again and again.
Payment for Authentication.

Question: States? get involved?
Legislation to expand

Struggling with attempts to integrate access via single ID
Citizen authentication strategy

Virginia DMV
others HHS (Health and Human Services)

Hurdle 1 - create place for 1 credential
Then 2 - accepting third party

requirements - verify eligibility.

Ken K. 700 Credential service providers
not approached about getting $

Jims comment Agencies want Identity proofing - wants to be stateless

Tensions and Challenges - ID Resolution - Do I have right dataset?

As CSP (credential service provider)

They don't have all the attributes they need - even if we had moving them in back.

The way NSTIC coordinate ONC
see potential

TrustedID = better proofing of ID better security + privacy options

How same patient @one place is another place.

Inora Healthcare 3rd party private access - Google, MSFT.
Personal Health Records

"Tools"
What does that mean?
* Standards?
* how you do it?

Direct Protocol - well established
Digitally signed email
RESTful health exchange

Feature Speaker ONC
Awarded 12 pilots to catalyze 2 states 10 innovations
NSTIC.gov
great way to meet pilots
Round 3 is being announced in early fall.

Might have a 4th round.

Question to facilitate.

Market 2011 - when issue, where now?

Mobile Device
OpenID Connect is the answer
of course privacy a lot of attention.

Real marketplace competition
Wanted to stimulate broad spectrum of identities to choose from. greater level of offering

In coming year - write framework requirments
* work
* intention
* resources

Its a "round table" always looking for feedback.

2 schools of thought - credit agency, VRM Proofs
look at Scandinavian model

The truth about NSTIC - what is a trusted (verified) ID
Financial services - IDProofing/Authentication

Three aspects
* Session
* Authentication
* ID

They are different

Pilot in NY with Broadridge
IdP -> KYC
* attribute
* exchange
* networks

timeframework 2010-2011 IdP "do" everything

My thought while listening - what to do to create a real learning community

Power / Info Asymmetry
with IdP / AP / Relying Party

Why FB make change, fine grain
Indepth privacy assessment
one for internal / one for external

they are now enabling anonymous login - sell in aggregate form to the later

NSTIC language "unobtrusively" IdP

FCCX - double blind unobservability

still a lot to be done have consumers fully participate. In value of data
Privacy enhancing workshop series at NIST

Full value exchange
How to leverage against include services
changing user expectations

Fuse Architecture Picos & Connected Cars

Tuesday 4F
Convener: Phil Windley
Notes-taker: Phil Windley

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to presentation notes
http://www.slideshare.net/windley/fuse-2

IndieAuth: Turn Your Personal Domain Into An OAuth Provider

Tuesday 4H
Convener: Aaron Parecki
Notes-taker: Kevin Marks & Ben Werdmuller

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Find notes from this session here: http://indiewebcamp.com/2014-05-06-iiw-indieauth

Further Notes:
Steve Williams: is indieauth what I used to log into the wiki? @aaronpk: yes @sbw: I have a bug report
Aaron Parecki: if you have signed into indiewebcamp.com you have used indieauth already

If you link from your site to and form a silo with rel="me" that is relMeAuth -you delegate authentication to a silo - this lets you use your own domain as the identifier, but other sites as authentication

indieauth.com is a little confusing as it is doing two things

indieauth.com came from wanting to add relMeAuth to mediawiki on indiewebcamp.com

instead of getting down in mediawiki code to add auth, I made indieauth.com do to auth as service

by making indieauth.com a service, I could add a small plugin to mediawiki to talk to indieauth

I initially didn't expect anyone else to use indieauth.com originally one of the things that OAuth2 did different from OAuth1 was separating auth as an internal service

after I made it work with the wiki, I made it work with my own site hosting p3k

we need to find an OAuth2 provider agreed on between indieauth and the user

I had the same problem with posting to my own site - I needed authZ to post to my own site

http://ownyourgram.com/ is a way to post to your micropub endpoint when you send photos to instagram

as OAuth2 doesn't specify discovery, we have OpenID Connect, and no other spec.

I used rel=authorization-endpoint and rel=token-endpoint from existing specs and made up rel=micropub

one of my goals is to avoid crypto and rely on TLS like OAuth2 did (it seemed like a good idea at the time)

Kevin Marks: well, the SSL code has had a lot of people look at it closely recently
Justin Richer: @aaronpk should look up token introspection as an OAuth spec (which I wrote) - similar to IndieAuth token factoring
Aaron Parecki: indieuath can be an internal part of the wiki, or it can be service that the user's micropub site uses
Justin Richer: UMA is a protocol built on OAuth2 and OpenID connect to introduce the client to the auth services there's a lot of potential synergy between UMA and what the Indieauth delegation is trying to do

there is a profile of OpenID Connect that lets you defer verifying the signature, but implementations do it anyway

what if you don't have an HTML parser?

Kevin Marks: we have an HTML parser service in the cloud that will make it into JSON for you #indieweb

Received from Ben Werdmuller:
Notes by Ben Werdmuller - These are permanently hosted at: http://indiewebcamp.com/2014-05-06-iiw-indieauth

If you have signed into the indiewebcamp.com wiki, then you've already used IndieAuth. In this session, Aaron will get into the guts of it.
RelMeAuth: Your site <----> Multiple silos
Your domain is the identifier for the thing you're logging into; you're delegating the actual authentication to a third-party service (e.g. a service)
E.g., aaronparecki.com logs in using RelMeAuth using Aaron's GitHub account (github.com/aaronpk) to actually do the authentication.
Aaron apologizes for a slightly confusing indieauth.com site.
Initially, he wanted to write authentication for the indiewebcamp.com wiki. MediaWiki has a very convoluted codebase, and he was dreading diving into it. He knew that for every new authentication method he had to add, he'd have to do it all again. So instead he decided to write the integration code once, using indieauth.com as an integration point, and write all of the other authentication integrations for indieauth.com, which had a much cleaner codebase (as he was starting from scratch).

The integration mechanism is OAuth-like.
There is some discussion between Justin Richer at MITRE and Aaron Parecki about whether the indiewebcamp.com authentication mechanism is effectively siloed authentication. Aaron defended on the basis that OAuth 2.0 explicitly featured the ability to separate the auth service from identity. (It's a tactical decision to have a proprietary link between indiewebcamp.com and indieauth.com, although it's a little more exposed because the communication happens over HTTP. Justin notes that it would be better to use existing authentication protocols that are designed for security.)

Aaron discusses using IndieAuth with micropub, an API for using third-party apps to post to indieweb sites. The micropub-compatible app needs to be able to log into your personal site.
OwnYourGram.com: you log in via IndieAuth, authorize the app, and it reads your Instagram feed and autoposts it to your indieweb site using micropub.

- [me] -> (rel) -> [authorization endpoint]
- [me] -> (rel) -> [token endpoint]
- [me] -> (rel) -> [resource server, micropub]

Aaron took authorization & token endpoints from OAuth / OpenID connect; micropub is new.

A question came up about why this uses HTML vs using a .well-known address. The answer is that it's easier to code on a wider variety of platforms.
A further issue was brought up re: OAuth separating authorization and token endpoints, which is not something that is actually supported in OAuth. Aaron points out that you _can_ have them on separate servers, as long as they are tightly coupled - as is the case here.

Aaron: "avoid crypto". He likes the idea of signed tokens, but nobody can agree on the signing mechanism. Conversations tend to disappear down unproductive rabbitholes .....

Aaron discussed the OAuth workflow and how it relates to IndieAuth. IndieAuth assumes clients that have a web presence. It can be an internal part of the indieweb site, or it can be an adjacent service that the site delegates to.

Personal Sovereign Design

Tuesday 5B
Convener: Devon Loffreto @NZN
Notes-taker(s): Devon Loffreto

Tags for the session - technology discussed/ideas considered:

#VRM #SovereignSourceAuthority

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

http://www.moxytongue.com/2014/05/iiw18-personal-sovereign-design.html

Abstract: A discussion on the nature of personal Sovereign data structures and identity structures useful for the expression of information of relative value to Individual people and organizations of people.

Reference: "What is Sovereign Source Authority?" and associated information conveyed here.

Society is administered, Administration is Society. Access to and control of participatory context is an administered Sovereign event that we exercise upon Human babies. This administrative context defines the tools we use to transact authority in Society.

So long as Individual people must register 'within a system' in order to receive legal authority to represent oneself in subsequent legal transactions, administrative precedence defines the nature of this data relationship between asset managers and data-subjects structured as social liabilities with increasing costs/debts leveraged against their respective Rights of life, liberty and pursuits of happiness.

"Personal Sovereign Design" begins with risk management considerations. The foundation of integrity within Society is the Individual people that stand up freedom and security in every context required. "We the People" can not be contrived by an administered process, nor managed by administrative methods alone successfully... for every natural or man made emergency that threatens the lives of people in our communities requires Individual people to act with integrity and courage to produce opportunities for both survival and continued prosperity. We celebrate entrepreneurs of all types... social and commercial heroes that act.

Personal Sovereignty is the structure of the United States of America by 'Declaration' (ref: John Hancock), and the lack of a recursive signatory part to the US Constitution allowing for generational stewardship of the Rights that make our Union strong represents an "error of omission" causing structural concerns highlighted by an Internet-based administrative framework of Society.

Can an Individual self-provision identity? Can a family self-provision asset structures? When? Birth Registration, Kindergarten Registration, Voting Registration, Health Care Enrollment, Genetic Profiling, every transaction...?

Human -vs- Systems (context considerations)
Meatspace realities versus Virtual aspirations
Ebay repuation system - absolute control of context value
Local reputation has much more dynamic and subtle means of evaluating context values within Human relationships. Freedom itself requires absolute local control... local to the Individual. The 1st and 2nd Amendment were constructed so that a Government "of and by the People" would always contrive authority accurately. Individuals administer our governed Rights. Individuals standing Free, Individuals standing Brave.

A story was told of the character 'Rabbit" from the book Rainbows End by Vernor Vinge describing a character that was ultimately controllable by "Revocation of Certificate Authority" and an analogy was drawn to the current nature of freedom from within an "Administered State", where the structure of personal Sovereignty is not implied by design, and requires central administration.

Additional conversation pointed to subsequent introduction of **httpsy**://algorithm:fingerprint@domain:port/path1/!redactedPath2/..... protocol by MStiegler.

Later Session Title: Self ID - Provoked related conversation around self provisioning identity by Individuals serving role of IDP. Self-authorization methods considered against backdrop of risk management considerations (LOA 1, 2, 3...)

Enterprise requirements and security requirements exist in context.

Individual requirements exist in context.

Can a risk management regime change the administrative precedence of the IDP role to enable self-provisioning identity with capabilities of increasing levels of assurance being exchanged as needed?

Very lively and engaging conversation with many capable and interesting people in room.

Doxing as Vigilante Justice

Tuesday 5E
Convener: Sarah Davies
Notes-taker: Sara Davies

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Respect Network & XDI

Tuesday 5F
Convener: Markus Sabadello
Notes-taker: Brent Shambaugh

Tags for the session - technology discussed/ideas considered: #respectnetwork, #XDI

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1 minute intro:

- cloud name in personal cloud
- fancy name for getting cloud stuff
- www.respectnetwork.com
- Personal cloud fancy name for XDI data store
- Get an XDI identifier and XDI graph

- XDI graph model with nodes and arcs
- Cloud name is the XDI identifier

write applications that can put data in your graph

- what does a graph look like?
- How would you store certain data?
- How do you communicate

Cloud name, how to find
→ use data service discovery
How to find the cloud.

Register with cloud service provider
→ get in register
→ look for = variations cloud and registry service will tell you where it is

→ run registry – XDI discovery process
→ open and distributed XDI itself
...one repository

Avoid duplication across multiple registries
Respect network as one registry
==> cloud service providers completely decentralized...

- Respect network as one registry
- cloud service providers completely decentralized
- find where is the cloud & the cloud #
- cloud name human readable identifier (UUID)

more can change later

- Transit more into number
- OpenID … log w/ domain name ...but don't remember domain...
- XDI ….more and number in case... you do not have domain name
- Random identifier for cloud
- Registry changes name… line persistent and uniqe with URI
- You can have names, roles, and functionality
- Can have multiple cloud names pointing to cloud #s
- Also planning mechanism called pseudonyms

→ one cloud references the other …

- expose yourself with different

→ like personas
UUID … what resources for XDI

XDI in Java ….run own XDI server.
Can do XDI discovery
Interoperate with Markus e-mail and then transverse.
Iterogate ,,,, find the cloud and then find data
--XDI .. multiple utilities...tools deployed here...

Tool for XDI discovery
Type cloud name and do discovery
UUID with extra info … then get address of cloud..

XDI response that I get out of it...
1st step finding cloud
2nd step find stuff within cloud?

Every cloud comes with key pairs
we call that peer-k-i
each person has more than one key pair within the cloud

-validate … b/c discover the public key
-cryptograpic signatures with the network

what is the authority?
Authority ….technical name for my cloud.

– Cloud name...host that personal cloud anywhere.
– Discovery Public Discovery
2nd class..

- Anyone discover
- Then certain fields discover

→ with a group of cloud network

- w/policy within cloud
- all on access to that group

→ discovery tool smart enough

- Message .. who is sending the message

Questions?
then talk about...

- Look at actual data
- Get into XDI syntax...

what is in my cloud
XDI tutorials...Explains XDI from scratch

Step 1. Graph Model

- graph nodes and arc

empty graph has a common root node...
Markus' data
in 1 point encryption? (as in a very small font)

→ API driver question
programmatically create
→ send an XDI request and get an XDI response

2 different serialization formats of the graph
SQL..interrogate
the union set is small query w/ XDI format

- 2 different serialization formats

1 is JSON

- what does an XDI graph look like?

- Tool for displaying XDI graphs
- finding adapter...peak of duct tapes adapters that are hard to find
- XDI graph editor , create tool displaying graphs

- common root for graphs
- load a graph...it would be faster
- Here is a graph – a force directed graph

- change the sample graph
- change the plus sign into something else...

- was dictionary space...shift opp

- XDI …
  - I can see cloud name and cloud #
  - Alice name, e-mail...Alice e-mail, Bob's cloud # … 2222

  - not best practice b/c none are rassignable

→ node is a persistent address

- Linking is something that is fundamentally reassignable
- Pattern … Link to something that you want it to point to
- difference between a name in brackets and the ampresand
- create a triple … the predicate is always an ampresand
- all relation statements show up in the graph as arks

identiy \ ampresand that represents a value

- indentity at a value and indentity of the reference to a value
- what would an xdi graph do … all of a sudden 111.
- How would you change your cloud network on lionote
- put a ref from the 1st cloud # to another

but these are the same

→ fundamental is control of the cloud #

- Put an account into suspense

→ what a state between dead an alive

→ run through mat

XDI arch … can model every option...

reference … explicit

reference is opaque

Add personal cloud?

→ standardization of personal cloud

End of day circle time..

Aging & Caregivers & Post Death Identity Management IoT Assisted Living

Tuesday 5G
Convener: David Howell
Notes-taker(s): Akiko ORITA

Tags for the session - technology discussed/ideas considered:

IoT #Aging #Post-Life

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

After brief introductions of attendees, we discussed both "Aging in Place" and "Post-Life Identity".

<Aging in Place>
- seniors stay at home
- service vendor network (**Financial (day to day, estate) / **Medical Vendor)
  vender management system
- medical coordination
  - power of attorney
  - electronic monitoring of medication
  - Family DNA
- house system control
  - motion detection
  - cloud
- entertainment
  - even known technology can become harder : More complicated TV controller
- Telephone Interface
  -usability,change is very difficult
  - (son or daughter must know how to deal with it)
  - does the senior need to know?

- personal history / legacy
  The personal stories
  Take their stories from physical artifact (from printed photos to digital data and in the future??)
- ** personal information estate planning
  Medical / Memories

- Creating hooks back to older memories
- Control with the voice
- Safety boundary
- The model of delegation

Delegation problem -- health record, medical record, information coordination

<Post-Life>

- Maintain the Identity, identity still persist
  after certain inactive period, the account will be removed
|
lightweight vault - identity systems are not aware of this state
- social media monuments
|
How to transfer ownership -- things we own as individuals exist only digitally

Wednesday May 8

OAuth Security: Proof of Possession

Wednesday 1B
Convener: Hannes Tschofenig
Notes-taker(s): Roshni Chandrashekha

Tags for the session - technology discussed/ideas considered:

#OAuth2 #PoP

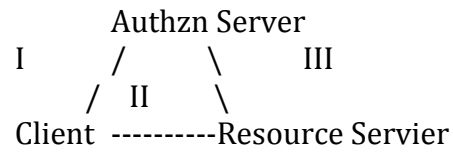
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to PowerPoint: http://www.tschofenig.priv.at/oauth/IETF-OAuth-PoP.pptx

Presented status of various specs for provided security better than bearer token security.

JWT - uses JSON based encoding to describe claims
- "security token" but may also be used as an access token

Two cases:
1. Asymmetric Key
2. Symmetric Key (JWK encrypted in JWE)



Motivation:
1. Desire to have E2E security at the application level.
2. To disallow a resource server from reusing an access token in other services. (single use tokens)

Q. PoP almost a factor of client authentication
Discussed methods of binding the secret:
1. secret bound to token
2. secret bound to client
3. secret bound to client instance

I. Client - Authzn server interaction
Reference:
Key distribution at client registration (draft-jones)
Key distribution at access token issuance (draft-bradley)

Followed up with an example of the symmetric key case:

(i) The client sends a request for an access token along with some indication that says "I support PoP tokens".
(ii) AS then creates a PoP enabled access token
(iii) AS sends access token to client along with the key. The key is also included in the token.

Discussion:
The symmetric key is produced by the AS.
For the asymmetric key case, the client generates public private key pairs.

What is the motivation for letting the client *ask* for PoP enabled tokens?
"I can handle PoP" is different from explicitly asking for a PoP enabled token. The server must have some way of knowing that the client can handle these tokens. Should therefore not be a runtime request (some ambiguity about runtime requests spec'd in the reference draft)
-- reason for question: limit giving more options to potential attackers.

Does this work if the access token is not in a JWT?
Yes, but this example made 4 assumptions:
i. symmetric key
ii. JWT
iii. No token introspection between AS and RS
iv. Long term key shared between AS and RS.

Repeat:
PoP key should not be tied to JWT.
ACK. Need to follow up.

For asymmetric keys, the draft currently supports both key creation at the client and by the AS.

II. Client-RS interaction
- i) Proof of possession of PoP key
- ii) Message integrity + channel binding
- iii) RS to client authentication

The authenticator is a keyed message type computed over the request (contains access token and channel binding). Client generates JOSE object (JWS) - covers access token + some secret component --> access token identifier, and then submits the whole structure with the HTTP message, does the above (i), (ii), (iii).

There are problems with not signing everything. There was some discussion about mobility of headers and ordering. If the ordering of the headers matters for the API, then the app needs to be aware of that.
Suggestion: use existing RFCs for canonicalization of requests affected by mutability under HTTP and proxies.

Or -- use channel binding (more to follow in the next talk).

The RS then uses the shared long term key (with the AS) to unwrap / decrypt the access token and verify the authenticator.

Channel Bindings:
Ways to get the application layer security into the transport layer security
Options include using a public key in the TLS or use tls-unique and tls-server-end-point.
Warning: new attacks identified with the TLS based channel binding.

III. RS-AS interaction
Token introspection -- get claims and keying material from the AS to verify the authenticator, but the RS needs to identify itself first.

Next steps:
slides to be shared on the OAuth mailing list.

"We Are The Last Generation of Free People"

Wednesday 1G & Thursday 4G
Convener: Kaliya Hamlin
Notes-taker(s): Kaliya Hamlin

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session was called by Kaliya Hamlin to discuss the statement Julian Assange made in Dec 2013 at CCC in Germany. He said paraphasing - *we are the last generation of free people and there is about 10 years left to resist the trends that are proceeding and to make sure we don't loose our freedom.*

We began the session by articulating the things we were afraid of (these were subsequently clustered into 8 broad categories. Each post-it note was written by one person and the read first set of bullets under each is are the text of those.

The next set of of bullets in blue were the solutions (which subsequently were clustered to with the 8 problem categories, but clearly some of the solutions are applicable to more then one problem cluster).

Inbetween articluating the problem and articulating the solution we also discussed how things were different now with technology.

Syping on Snail Mail happened - but was costly and more time consuming + potentially obvious that it was happening.
We had tyrany - lack of freedom and the Divine right of Monarchy.
Can law adapt to extreme power of technology?
New: Economics - beyond reasonable - open field. GPS v. Police
Anonymity is related to cost of de-anonymizing

ILLUMINATI - elite control

- American Dominance / Imperialism
- State controlled narrative of what is right/wrong, current events
- Lack of randomness in the world
- Invisible ubiquitous control of the powers of state by the monied elite
- Breakaway civilization in space of elites lead by Musk and Theil
- Centralized actors control decision making. This results in portions of society being increasingly marginalized - violence continues to be the primary regulatory tool.
- What does unfreedom look like? what are we most concerned about? Loss of individual rights of choice to exist or function in a society you have to X or there will be Y punishment.
- Elyseum, Hunger Games, Small ruling elite have total control over the vast majority of people.
- Total subjugation to an arbitrary / involuntary collective.

    - No Money in Politics
    - More local connectivity and empowerment
    - Community Rights Movement Ordinances
    - More Local Connectivity and Empowerment
    - No Money in Politics
    - Consumer Co-Ops as Tech Platforms
    - Deliberative Democratic Processes for all levels of government in systems
    - Transform Culture through institutional structures and processes
    - Disruption of Current Electorate Habits
    - Figure out how to "clear" issues triggering of collective shame and vulnerability
    - Insist that state systems be simply explained to regular citizens
    - Invest in "schools early" stage engagement in tech vs. lawsuits later
    - Stop Policy Laundering
    - Atoms are different then Bits
    - Bounties for whistle blower info
    - Producer Consumer healing - relational capitalism?
    - Sharing Economy - supporting it digitally in real way
    - Better democracy - measurable feedback systems - quantifiable plurality
    - Wealth / power transparency

Online Tracking -> Offline Oppression

- UN-Freedom "online" more and more affecting the "real world.
- Organizing....collective action is practically inhibited to prevent change and social dissent.

Violence / Accountability

- Widespread unaccountable market for violence
- Violent suppression of nonviolent dissent
    - Police / Military Accountability and Regulation
    - Empathy / Peaceful parenting

Hivemind/Lack of Discourse

- No divers and critical thinking
- Total loss of individual autonomy
- No disagreement = no diversity =no resilience
- Death of Political Dissent
- Hivemind by Radio Telepathy
- Censored Content based on Political/Religious Ideology
- Sock Puppetry + Astroturf-auto-matic detection mechanisms.

Apathy

- Indifference (People Accepting Surveillance, Censorship, etc as Normal).
  - Agorism
  - P2P Economy - crypto currencies, distributed exchange, local and personal production.

Computer - Control

- Algorithmic enforcement of societal norms.
  - Build respectful software for the world we want.
  - Distributed, Anonymous, Encrypted Mesh Cloud Networks and Storage
  - Search and seizure laws catch up with technology
  - Web protocols and application that empower individuals both in their access to synthesized information and in their control over distribution of information. Goal: Self-Balance

Government Opacity

- Lack of government transparency / punishment of whistleblowers
  - Government Transparency
  - Open Data is Not Enough - Citizen Tools public tools to sense make address challenges
  - MayOne SuperPAC

Privacy

- Privacy for the powerful, transparency for the weak

- No Privacy.
  = no safe space
  = no places/times where we can make ourselves vulnerable
  = no diversity of ideas/behaviors ways of living.
  = no resilience

- Privacy goes away completely. Government knows everything.
  Oops! It's happened already!

- Unfreedom - There is no longer a safe space anywhere (on your person, in your home, in the cloud, etc) where individuals can store their personal info and data without the reis of it being seized, searched and compromised by an authoritative body.

- Ubiquitous Surveillance - by government & of each other.

- The Details of our lives are wholly-owned assets of third party entities.

    - Data is recognized as property owned by the individual.
    - Work on technologies that improve privacy and security on the internet.
    - Other forms of violence - economic, psychological are acknowledged
    - Resistance the government systems of surveillance via local political bodies - city, county and state.
    - Breakdown Tight Hierarchy towards Decentralized.

????

- On facebook no one will hear me scream
    - Buy a Microphone
    - I don't know the solution, but it has to be social, technical, political, economic legal etc. all in one.

VRM Adoptions Case Study: MYDEX cic (How we tell it; where we are; what Mydex looks like including: peek at UK IDAP)

Wednesday 2A
Convener: William Heath
Notes-taker(s): William Heath

Tags for this session – Technology discussed/ideas considered:

#PDS #Personal clouds #trust frameworks #VRM

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Mydex CIC is a social-enterprise VRM platform, live at pds.mydex.org and with contracts in UK market including UK government ID assurance provider. Having a national government agreeing to contract with individuals based on credentials held by the individual is potentially a significant VRM breakthrough.

First we heard how Mydex presents the big VRM picture to the uninitiated (which is still the majority). "Personal control over personal data" does not much resonate with consumers but there is a real political consensus about the fact there is a problem and personal control over personal data is a policy each British political party is committed to.

All the pols agree on that. But what they don't get is how to implement personal control over personal data, and what the implications of it be. Aim is to set this out and to explain why it is a win-win for all parties: it's a global problem, which affects organisations and individuals.

What Mydex does

Mydex offers personal data stores and connections, wrapped in a legal & technical trust framework.

The community needs diversity and interoperability in PDS providers. Key differentiating determinants of trust will be

1. governance & legal form: Mydex takes the legal form of Community Interest Company, limited by shares, highly transparent, asset locked and regulated in the returns it can offer shareholders.
2. Commercial (or business) model: Mydex is free in perpetuity to individuals, making a small micropayment charge to connecting organisations and apps
3. Legal basis: Mydex uses contract law and places the individual in the role of "data controller" in data protection law
4. Technical: Mydex has turned away from esoteric and untested tech and moved pretty much entirely to open course tech and standard tools, supporting multiple ID protocols (OpenID, Mozilla Persona, SAML, Shibboleth)

Market adoption has started with contracts in finance, media, local government and housing; also a potentially very significant contract for UK government ID assurance services. The proposition to individuals is convenence, control, trust and value. To organisations it's cost savings, reduced regulatory overhead and opening the path to new services.

What Mydex does

We did a live walkthrough of the sandbox site (which replicates the live service) populate with dummy data. This showed data entry, management, connections, visualisations of the data and account management including "download my data" to enable switching to a different service.

The live sites are:

- sbx.mydex.org: the Mydex sandbox where you can use dummy data
- dev.mydex.org - developer resources eg data schema, new data schema requests, API resources
- pds.mydex.org where people can get a personal data store.

Place in the market
The contracted connections are still in the process of implementation. For this reason user numbers are still only in the hundreds (ie people curious to see what Mydex looks like, even though they are not yet able to use it to connect). We also saw an outline of the UK government ID assurance service user journey, based on a mixed information set keyed in by the user. The UK government ID assurance programme rolls out in the course of 2014.

HTTPSY: Leave the Certificate Authority Behind.

Wednesday 2C
Convener: Marc Stiegler/Alan Karp
Notes-taker(s): Marc Stiegler

Tags for the session - technology discussed/ideas considered:

HTTPSY: a proposal for a protocol that eliminates the need for certificate authorities in many cases and enables placing sensitive information in a bookmarkable link. Also enables the creation of secure bookmarkable OAuth bearer tokens.

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Draft format of the new httpsy protocol proposal:

httpsy://algorithm:fingerprint@domain:port/path1/!redactedPath2/ ...

the protocol is httpsy. The algorithm is used to interpret the fingerprint, for example, "sha-256". The fingerprint of the public key is used to challenge the server to prove that he is the holder of the public key, to foil DNS cache poisoning and similar attacks. Any part of the path prefixed with a bang "!" is redacted when the url is displayed in the window by the browser, in the referrer header, and in server logs.

Controversy over whether this improves the user's situation with respect to phishing or makes it worse: on the one hand, the domain that people look at to see where they are is buried in a long string of gibberish, on the other hand, it can be claimed that the use of the domain to determine your location, in a world with millions of sites, necessarily not humanly distinguishable, is the source of the problem, not the solution.

System eliminates need for certificate authorities in many circumstances, the self-signed cert is adequate to prove that, if someone you trust gives you a link, you are guaranteed when you click the link to arrive at the place the trusted party intended for you to go.

Concern raised about untrustworthy parties sending you to untrustworthy places, but they can do that today anyway.

Often requires a "trust on first use" pattern similar to what you do with ssh.

Does not solve the problem with reliably going to a place that you saw on a billboard, since the billboard must be completely memorable.

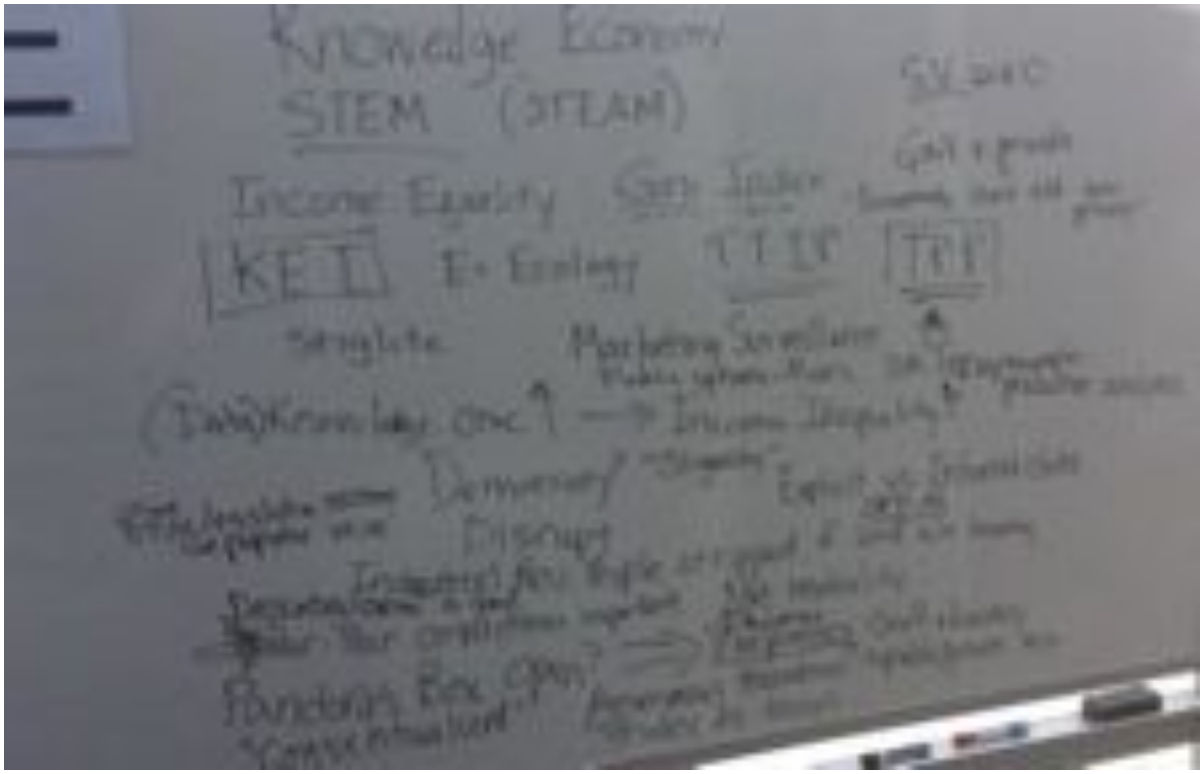
The redacted parts prefaced with a bang can hold credentials, turning these links into unguessable self-authorizing links, suitable for use both as bookmarkable webkeys and as oauth bearer tokens.

Alan Karp and Marc Stiegler are leading a group that meets on Friday mornings, with people from HP, Google, PayPal, and others, to develop an RFC spec for httpsy.

Data Inequality / Income Inequality

Wednesday 2E
Convener: Kris Alman
Notes-taker(s): Kris Alman & Matt Berry

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Income inequality/ Data inequality

If data is concentrated in fewer hands, will income inequality grow?
And will this further tilt power structures?
Can we measure data inequality, like Gini coefficient does to measure income inequality?

21st century post-industrial economy called knowledge or information economy.
Influence on education: STEM careers (STEAM acknowledges art—creativity/innovation—as important.) Compared to industrial revolution where people were stripped of land and were unaware what happened & how livelihoods changed. Will middle class "knowledge workers" (doctors, teachers, IT, musicians, etc.) become devalued as data is gleaned and monetized by big corporations?

"Privacy is a nonrenewable resource. Once it gets consumed, it is gone." Frank McSherry of Microsoft Research Silicon Valley in Mountain View, Calif.

http://www.simonsfoundation.org/quanta/20121210-privacy-by-the-numbers-a-new-approach-to-safeguarding-data/
http://www.scientificamerican.com/article/privacy-by-the-numbers-a-new-approach-to-safeguarding-data/

Controversial concept. With each birth, privacy is a renewable resource!

Pandora's Box is open and data collected without our ability to opt-in or out.

- **Decentralization with Peer to Peer connections important.**

- **Demand education and transparency of data collected by both business & government.** We should not have different standards for government and private sector as they have merged.
- **Consentualized data** can occur through:
    - Anonymous transactions (using public/private keys)
    - Privacy by design

Transparency is limited by bad laws. E.g. transparency of prices in health care and trade secret laws that prevent disclosure of negotiated rates for services.

There is a difference between **explicit and inferred data.**
Marketing surveillance comes from explicit info shared on sites like facebook.

Example of inferred data. Defense Intelligence Agency took photographs of and analyzed protests with Topsy. Determined that adding food carts decreased violence.
http://topsy.com/

Predictive analytics with data collected over which we have no control (or know exists) is concerning.

Trade agreements like TPP and TTIP impact data inequality (such as who controls data for international companies; how might net neutrality be impacted). Secret trade agreements (corporations writing them) are writing them without transparency to public. Could this impact net neutrality or data ownership/access?
How does this impact governance? Acknowledgement that we are an oligarchy. Recent Huff Post article that demonstrates 83% of legislation is contrary to public opinion.

Good resource:
Knowledge Ecology International, Attending and mending the knowledge ecosystem (KEI): http://keionline.org/about
"a not for profit non governmental organization that searches for better outcomes, including new solutions, to the management of knowledge resources. KEI is focused on social justice, particularly for the most vulnerable populations, including low-income persons and marginalized groups. There are probably 5 billion people who live in the margins of the global economy, and an entire planet that depends upon knowledge for economic and personal development, education and health, political power and freedom, culture and fun."

Joseph Stiglitz, economist and a professor at Columbia University, is an advisor. He won Nobel Prize in Economics for his analyses of **markets with asymmetric information**.http://keionline.org/node/18

Recommended book: **Who Owns the Future?**http://www.amazon.com/Who-Owns-Future-Jaron-Lanier/dp/1451654960

Channel Binding for Open ID Connect

Wednesday 2G
Convener: Mike Jones/Breno
Notes-taker(s): Roshni Chandrashekhar

Tags for the session - technology discussed/ideas considered:
OpenID Connect, Channel ID, Channel Binding

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

TLS
Mutual authentication
- end-user auth technology
- certificate for user identity
- no relationship to server user authentication
- should involve user content

Because of these assumptions, it is not practical for user-facing actions, but is now used in server-server communication -- this works well in a closed environment where you control large parts of the stack.

TLS Channel Binding
Authenticate device (context) rather than the user
- public keys / no trust chain requirement
- no steps by the user for provisioning since your machine can now autogenerate a binding.
- isolation of which keys are used to communicate with each server based on same-origin policy

The same privacy model that browsers currently have in place for cookies will work well for keys/TLS Channel IDs

Side-note:
TLS Raw Public Keys
- public keys / not bound to the same origin
- bound to access token or some other oauth construct
- uses same container TLS uses for certificates (certificate pay-load container)
(No need to define a separate field in TLS)
- but doesn't solve the problem of certificate hinting

Back to TLS Channel Binding:
TLS Session Resumption
another feature of TLS Channel IDs.
- server recognizes when it sees the device again
- provides the ability to manage sessions ~ cookie memcache infrastructure

TLS Channel ID
- automatically managed by TLS infrastructure
(if we rekey the same cert, this breaks - requires reauth, WAI)
You can now bind artifacts to this context.

Application layer code on both sides of the connection are able to inspect Channel ID and use it in protocol messages (signed or encrypted) - the recipient pulls out the channel ID and ties application layer state to a particular channel setup so that if the message arrives on the wrong channel, it can be tossed (example, capture and replay)

The channel ID can be used in application/protocol state - the server could create an integrity protected cookie with channel ID in it. If the cookie leaks, this context cannot be reused.

Q. Can you clear cookies and keys separately?
Yes, but you'll need new cookies if you reset keys.

You can use channel binding without protocol support if UA supports Channel IDs and the client and Authzn server have the same origin. If they do not, we need protocol support.

IETF Cross Certifying Channels
secure and ID token E2E from an OpenID provider or Oauth server.
Refer to diagram:

Naive method:
Put channel ID available to browser and the server in the ID token. Won't work. Client compares channel ID received to the one used and they don't match.

However, there is an authoritative party that knows both channel IDs - the browser, where the communication is moving through, typically by a redirect, is in possession of the private key material for both channels.

So, we create a message containing each channel ID signed using the other channel ID. Having both signatures is the cryptographic proof that the same party holds the information for both channels.
If the 302 redirect to the client had a flag that said "please emit channel pari proof as a param, possibly in an HTTP header to the client", the client would then look in the ID token, see the channel ID (ch1) and look in the header -- "do I have proof that ch1 is paired with ch2 (my channel ID)?" and accepts the ID token as coming from 2 channels transiting the same device.

The TLS channel binding is not aware of user consent to give information to the server, since channel binding should be independent of the application. The browser also does not need to know what is being protected by the channel ID, therefore, we can't use raw public keys alone.

Q. Is it sufficient to include Channel ID (ch2) in the request to the server?
A. This still allows MITM attacks, diminishing the value of the channel binding. It also does not provide E2E proof.

Q. What about browsers talking to an app on a phone?

Open Q with room for discussion:
How do we extend this exercise to the code flow?
There'd be a 3rd channel ID. Handling the client-browser-server issue is harder to solve and the expectation is that the code flow won't be as hard.

Note about the 302 redirect and cross-certification:
The 302 redirect is one of 3 mechanisms in modern browsers that cause cross-domain communication in a controlled manner
- location reference from one origin causes a message to be sent to a different origin
- there are limited ways to do this, and at the same time as the cross-origin communication is occurring, with the consent of the parties involved, you can cross-certify the channel IDs.

However, there are two other mechanisms: POST message and CORS. If we have a cross-certification mechanism, both W3C and the browser community will want it to be applicable to all 3 cross-domain communication mechanisms.

Ad-hoc UMA Interop Testing Session

Wednesday 2J
Convener: Mark Dobrinic
Notes-taker(s): Mark Dobrinic

Tags for the session - technology discussed/ideas considered:

UMA #interop

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Session should make first attempts at introducing one UMA-role with another.
Interop specifications are being written, and can be found at http://tinyurl.com/uma1iop

The purpose is to see what to do to setup an interop test for an UMA Resource Server. For this, relations with an UMA AS and a UMA Client must be setup. The configuration of those roles must be identified first.

Next an explanation of the big UMA picture took place, to zoom in on the actual context of testing an UMA RS.

Based on the UMA big picture, discussion took place of different problems that can be covered by an UMA infrastructure.

One problem of interop testing with UMA, is that the API that the RS provides to a Client, is NOT standardized by UMA. This is recognized by UMA group though, so testing there is done not based on an API, but should be done by other validation rules.

In the discussion, it also came up that the concept of a Resource Scope in UMA is not the same as the concept of a Scope in OAuth or OpenID Connect.

To bootstrap: RS needs info about the AS, and AS needs info about the RS (either statically, or using Dynamic Client Registration).

Next steps for RS testing are to fork Roland's OAuth Authorization Server and make the tweaks (meaning: support the predefined PAT-scope) for UMA compliance.
Build as much on top of existing OAuth specification.

We'll be taking it from there!

Mozilla Listens to IIW

Wednesday 3A
Convener: Sean Bohan & Brian Warner
Notes-taker(s): Sean Bohan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Agenda: Mozilla has been to IIW before, but this is Sean and Brian's first time. We want to engage the community and start discussions around what Mozilla is doing in Privacy/Identity and what the community needs. Brian had deck slides and they will be posted.
Notes:

- Mozilla is an Ecosystem of multiple platforms (desktop, android browser, $25 smartphone OS)
- We are working on Persona, Accounts, Sync
- Marketplace for apps and small-scale storage are also a part of that and critical needs
- Mozilla is using symmetric encryption keys
- Not an not an Identity Provider for 3rd party services, our work right now is aimed at mozilla services
- We need to know browser has rights to modify or read and the auth mechanisms as well
- sync/storage accept browser id insertions
- Client creating data -using KeyB because server should not see it
- Use case - Firefox marketplace to buy html applications
- run from any desktop browser
- receipts tied to Firefox account
- greet you by name

Crowd:

- Have we looked at UMA?
- UMA on top of OAuth

Mozilla:

- We dont know much about UMA - and will look into it
- User Managed Access - more for user controlling policies for access to the data
- We are thinking of whitelisting specific apps and the marketplace can learn without asking
- 3rd parties have to get permission

Crowd:

- UMA for the person to control
- good opportunity - who wouldn't want to use PDS for some requirement
- wonderful opportunity
- mechanisms like that - share specific data - separate keys
- share keys with diff recipients

Adrian -

- MIT has 2 camps looking at oAuth
- one camp - pds users must use it as part of the big data thing
- second camp -make sure the server, encrypt, so server can't be controlled and keys to the server are handed out specific to the query
- service based system - payment serv or shipping serv
- legal recourse if it's required

Crowd: doing purpose built value add vert integrated verison of YAS?

Mozilla:

- Firefox accounts - our intention right now is to solve the needs that we have, to solve for issues we have - also to get to be a bigger player in this space by bringing more to the space
- Right now the only rps supported would be mozilla services
- The Profile stuff we are working on is new
- User Personalization is related

Drummond:

- Gen question - whole ecosystem, interop, doesn't it make sense for that what we are building be an interoperable personal cloud
- These questions are the questions for all uses of personal clouds: encryption, how to encrypt? etc.
- If best pract/interop are developed and Firefox is a user agent - then it seems we cross into new space

Brian:

- what features you want in the browser to support it?
- things we thought of - before Accounts was "profile int he cloud" - should be retrievable from any device - interesting ways to combine 2 factor stuff, kiosks, flight, etc.
- "pickle" - get browser profile to be cloud and not local drive
- extend from that - other things kept in synch with other cloud services
- bookmarks synch with other cloud services

bookmark synch - provide better framework - synch server one choice

Adrian:

- Wants to see on the slide is a cert authotity –
- agrees with asa and drummond - if moz would use it's leverage to put the 3 things together - demand issues desire to evolve consistent steppingstone and the splice point into the reality of pki with all of it's faults
- wants mozilla to solve user experience prob for PKI

Drummond:

- adoption of pclouds and user recogntion of clouds
- mozilla listening - big deal

Asa:

- Uses chrome - because it has users he can switch from and testing
- If Firefox were not conflating concepts of accounts and who I am that would be great
- Better: there would be a hard and fast - this cand that can learn and see how behavior models diff personalities that would be grt
- ideal - go to banking site and not worry cookies or connections would be needed
- don't need a plugin or ridiculous chrome profiles

Brian:

- Big thing to fix and nail down the UI for that
- Thinks we need to have aspects of Firefox Accounts that afect the behavior of the browser - ties to Sync
- website signing into with other identities
- remembers set of emails you have control over
- remembers last email - defaults to that
- set of addresses persona knows about
- mapping rp to address
- ID given to a given website - enables within that profile

Ping Identity person:

- killer feature to be secure discovery service
- introduce to the right services (federation or somethign else) pds - if we can be central place that stores pointers but gives usability and ability to plug things in
- not just an ask for PDS integration - ask for this to be a theme and a system others can plug into
- BETTER IF browser delivered privacy exp they want

Drummond:

- Early features - ironic "what can browser do for me"
- from his perspective - privacy prob
- private browsing modes one aspect
- new aspect control over info and releasing - lot picking up on it
- html 5 meta referrer none

Brian thinks it's great

Sean says Mozilla is definitely coming back to IIW

Real Estate Use Cases: Problems, Solutions, Opportunities

Wednesday 3C
Convener: Bill Wendel
Notes-taker: Doc Searls

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Setting the stage:
* The home is the major component of the built environment where we spend our time
* It has appliances that can track their life cycle information: refrigerator, heater, hot water heater, air conditioner, microwave, refrigerator, washing machine, dryer
* It has communication and mains infrastructure: electricity, phone, internet, television
* it has a very rare ownership transfer cycle, and a very long "own" cycle
* Omie, a table being developed by Customer Commons, has no "silo" and is individual-centered. We can consider the Omie as the table for the home
* If Omie was the "GUI for the connected home", imagine it set in the wall near the door

Registering devices in the home:
* Science fiction, a possible gestural language for registering devices
* Square tag could do registration via QR code
* Read write near field
* Scott Jensen (http://jenson.org/): the connected home is not just, lights to go on when I get home. Because the logic is mind boggling--is someone sleeping? who is in the bed? The permutations are mind boggling. The programming languages are currently way too simple.
* See Zada, a silo that is solving these problems
* the "aging in Place" movement, 125 4th parties or villages, who help operate the home on behalf of elderly people
* Angie's list--advertising home services

Discussion
* Appliances have a class code (barcode) not an instance code
* Bigger appliances may have the serial number expressed in a bar code
* Stealth connectivity--two stories, the Samsung TV story and the GE dishwasher story. Calling out, the Samsung TV reported all behavior by default, just because that function was built-in--Samsung was not even collecting the data.
* How do we make this less scary (that everything is connected)?
* Perhaps the data could be sent via the electric network. Electricity is great because it is daily, active.
* It could be a diagnostic tool
* User as the point of integration--the user has to put all the pieces together
* Community group could get this going--we could gamify an entire block. But community means mutual trust, there might be issues with that.
* In real estate there is an essential issue, who owns the data behind the listing? A power and manuals device could allow intent casting of a for sale offer, could even intentcast for-sale intentions years in advance. If this is under control fo the owner, it would be a game changer.

Comparing Home device with Fuse (device for a car)
* Fuse gathers all the data of your car in one place
* Edmunds.com chariman told Phil: if you have all the data on how the car was maintained, that would cause a differential in the price
* Each fuse has a unique UUID, this could be mapped to an XDI name (=windley*fleet_ford_truck)

Proposals for 'a beginning'
* At the end of the real estate transaction, you get a house gift: a tablet with everything on it that relates to the home
* Like the drawer with all the manuals
* Replace the "drawer"
* Include the financials, the escrow, the mortgage documentation
* Low hanging fruit: power consumption of each device in real time
* Compare with Make a training course, on how to do a
* each house could have an =10.main.street address in the cloud; terra.gov is a related effort by the builders, a response to failures in the MLS
* inman.com runs the most digitally advanced real estate firm, they have an annual convention

Why a device and not hosted, in the cloud?
* Dropbox could do this!
* Physical device is more concrete
* Alzheimers/elderly, more concrete and discoverable

Appliances
* GE had to re-flash a rinse cycle SW, and it required a truck visit. So now, GE dish washers have a GSM card in them. It could be sending back user information.

Applications
* Visualization of power consumption
* Possible machine learning based on the electric consumption
* Static stuff: the user manual of every device in the home

Aging at home list: they offer
* acupuncture at home
* airpot transportation
* ambulance service
* appliance sales and repair
* assisted living
* audio/visual repair
* auto repair/maintenance
* baby gear rentals
* bicycle repair/sales
* bill pay/bookkeeping
* book/record disposal
* carpenter
* carpet cleaning

* catering
* cell phone tutor
* chimney repair
* chimney sweep
* computer repair
* contractor
* dentist
* doctor
* dog walking
* downsizing
* driver
* driveway repair
* driving evaluation
* driving instruction
* dry cleaning
* elder service organizations
* electrician
* emergency response system
* event planner
* florist
* food preparation
* food/meal delivery
* gardener
* funeral information
* furniture repair
* geriatric care consultant
* grocery shopping service
* hair salon
* etc...

Shopping for an Identity Providers: What do I need to know before I put my identity in your provider?

Wednesday 3E
Convener: Matt Berry
Notes-taker(s): Dan Sanford

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Things to consider
nsio
strong authentication
privacy policy
protocols
guarantees
operational security
scopes and types of information
relevancy
information required for identity proofing

How do I measure it?

Could certify operational security and privacy policy

Lots of discussion - what is an IDP (e.g.)
- abiility to export data
- ability to provide data to a third party'

how (when and why) will privacy policy change? Lots of discussions about who measures, what and how much IdP describes this information? Are we willing to pay for it?

Government or others can monitor changes and/or validating that entities do what they intend to, or possibly even meet some standard (e.g. w3c recommended policy standards for website - has gone nowhere)

Lots of discussion of standards for these things to consider that we would want that don't exist right now - which is something that we would want to consider if they were available.

Self ID: What technical problems or incentives do we need to make hosting your own IDP really a viable thing?

Wednesday 3G
Convener: Bryant Cutler
Notes-taker(s): Matthew Schutte

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Topic Altered during session to Self-Authentication, then to Distributed-Authentication

GOAL: What can we do to make sure that RPs begin to accept authentication from more than just the big monoliths (Google, FB, Twitter etc.)

Why do relying parties feel tentative about accepting Self ID

1) User Experience
    a. Liability / Risk (perceived by the management)
    b. Nascar > empty text input
    c. Quality of Authentication experience (if you use twitter or FB, they don't mess up the flow) if you are letting everybody choose how to authorize, the diversity of quality in their auth processes may result in greater friction.
    d. Patch / Security
        i. Customer who fails to adequately maintain their blog – do you go after them because their negligence led to the fraud (that they were a victim of)?
    e. Resourcing
    f. DNS ponage
        i. Belief that connecting to arbitrary sites opens us up to DNS spoofing etc..
    g. Size / Trustworthiness of provider
    h. Assurance levels provided by IDP

Question:
Why do we think Self ID is important?
Personal sovereignty v. corporate serfdom
As we see new authentication mechanisms emerge – support for (not necessarily personal ID provider) but arbitrary identity provider. Wants to open up the market to encourage the innovation in the authentication / security space.

How do you prevent the assertion of false identity?

objection: authentication is different from identity. What is a false identity?

Separating Authentication and Identity.

There is disagreement about where authentication occurs. Some in room contend that it occurs at the beginning of sign up. Others argue that it only occurs after enrollment.

Authentication deals with an identifier that we use for both enrollment and authentication.

What we are trying to talk about:
Enrollment and authentication

What we are not trying to talk about:
How we handle payment etc.

The vast majority of people choose to use

We are ok with allowing people to host their own email server or their own dns server (RP's end up interacting with them freely despite the potential problems that could occur there). Why are RPs not OK with us using our own authentication server.

There was a bit of a discussion

Why can't I show up with a Bank as my authentication service.

With and ID
Can authenticate with AWS
Can browse otherwise public info
May be able to bookmark for use later
i.e. you will only use that ID to make use of a service in ways that

you enable pseudonomous use – it would be better if we started from that place. We don't want it bound to an identity up front. L

we are breaking the person away from those moments of administration.

Why do I need to enter into an administrative relationship until I chose to. At those moments where an administrative relationship is required, then I can up the ante.

Ex: browsing anonymously, for posting, we may require some authentication, for purchase we would go beyond that – going into identity etc.

Q: What is the difference between AWS SAML and OpenID processes.
Step 1: open account
Step 2:

Enrollment happens before there is value. As a result, trust is not a problem at that point.

Assurance of the IDP vs Assurance of the accounts that the IDP gives you.

Level of Assurance – even with Google, you are at best at LOA 1, not LOA 2, because they are not verifying their identity with physical
https://www.cio.wisc.edu/security-initiatives-levels.aspx

Indieweb guys want to let people log into a wiki.

IndieAuth
They ask you to put rel:me link in your website that points to your twitter id. They go through your domain name to discover who you are willing to use to log in with. By doing that, they allow you to repudiate FB or Google if you decide you don't trust them.

It doesn't boil the ocean, does make use of those existing services.

One participant's goal:
To be able to repudiate a service

How do you get developers to adopt any API's?

The reason developers are using social authentication rather than SAML – Google and other auth providers did a very good job of listening to developer concerns and created something that was useful to developers.

OpenId Connect is useful is because it is the API is useful

The issue is that "The business model affects the nature of interaction."

I'm a credit union that is highly respected for their protection of users.

Banks need a high level of assurance – they have ten different ways of authenticating – are not going to outsource that to anyone.

Needs to be user friendly both for developers AND for end users.
====
NASCAR remains a better user experience than an empty text input

Account Chooser – local storage that will enable us to show up at a page, have the auth providers populate on the page
====

I get better security because I'm not storing account credentials

Loss of control of account reset is problematic for the RP.

No consequences

We need a ZERO additional effort w/ implementation, demonstrate customer benefit,

Fix account chooser, lower the cost of the implementation.

Mobile Connect: What would you as an Rp/IoP attribute broker want from the carriers?

Wednesday 3H
Convener: Michael Engan (T-Mobile)
Notes-taker(s): Michael Engan

Tags for the session - technology discussed/ideas considered:

mobile connect, GSMA, one api, multiple user agents

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The group was gathered to discuss and review the Mobile connect work that the GSMA is currently working on. The Mobile Connect suite will be a likely extension of OpenID connect that supports the use cases and mobile network provider data models.

An Open ID foundation working group is being stood up to work on the common profile and claims that may exist with mobile connect, and the possible OpenID extensions.

GSMA is a member of OIX and vice versa.

The group discussed what data the MNO (mobile network operators) might have. This included but was not limited to

Phone number
Other phone numbers on the account
Location (billing address, mailing address, e911 address, and current location)
Credit class
Billable support
Device identifiers or details (phone type, version, os…)

Proof of life (has this user been in this fixed location or moving around like a real person does, making calls).

Some various use cases were discussed, but most seemed to focus on the MNO's as second factor authentication providers. Perhaps to elevate the LoA of the initial IDP.

Some other examples talked about the out of band connection and multi use agent options.

For instance a user on a pc authenticates with an IDP… the IDP makes a request to the MNO for a second layer (higher loA) the MNO reaches directly to the users device (not their pc browser.) the user approves the transaction on their phone, and then sees the pc now logged in.

Other uses were around the combination of location and the user. With user proofing. For instance the user is in a store, the MNO can prove that it is that user/device currently in the store.

Side conversations also covered MNO exposure of SIM and sim authenticators. And the relevance of an existing One API that GSMA already provides as a point to point query protocol with no user consents.

Clarify & Learn About: Web Payments & Identity

Wednesday 3J
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

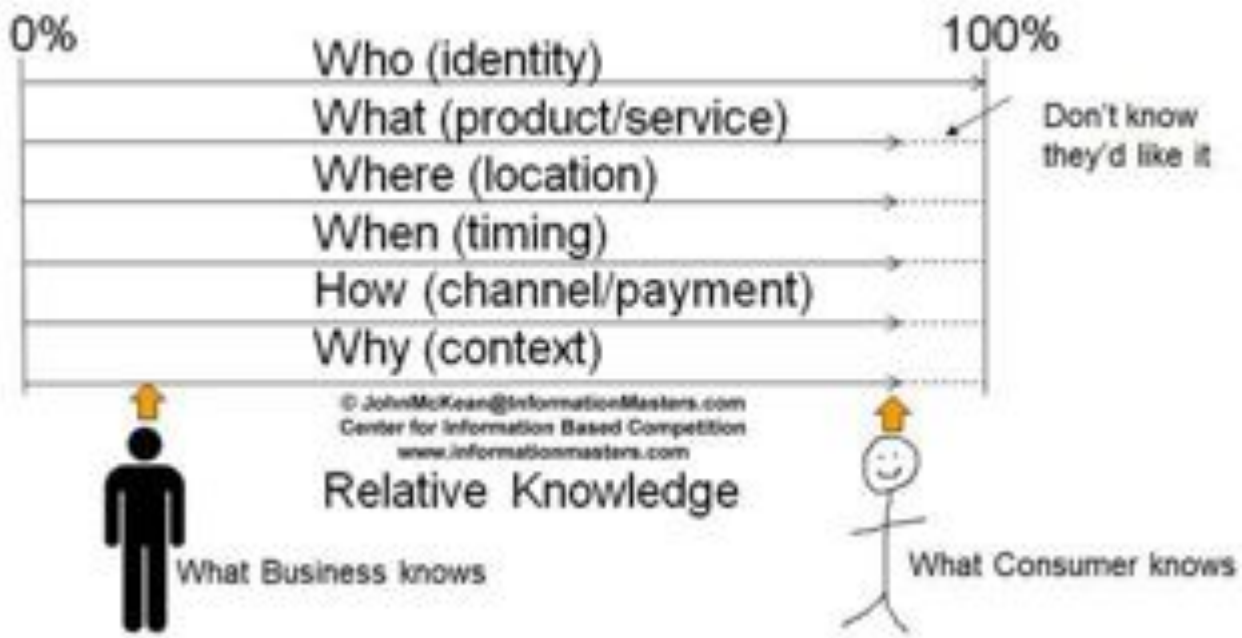
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation slides found at:
http://bshambaugh.org/presentations/payments_identity_iiw18.pdf

New Book: Extreme Relevancy

Wednesday 4A
Convener: John McKean
Notes-taker(s): John McKean

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

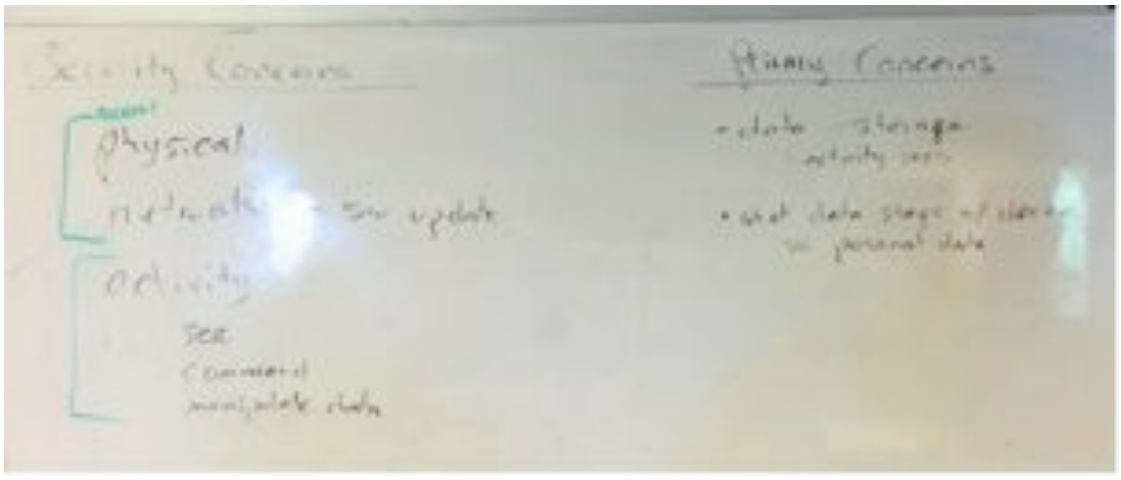


IoT and Open Standards (OAuth2, UMA…)

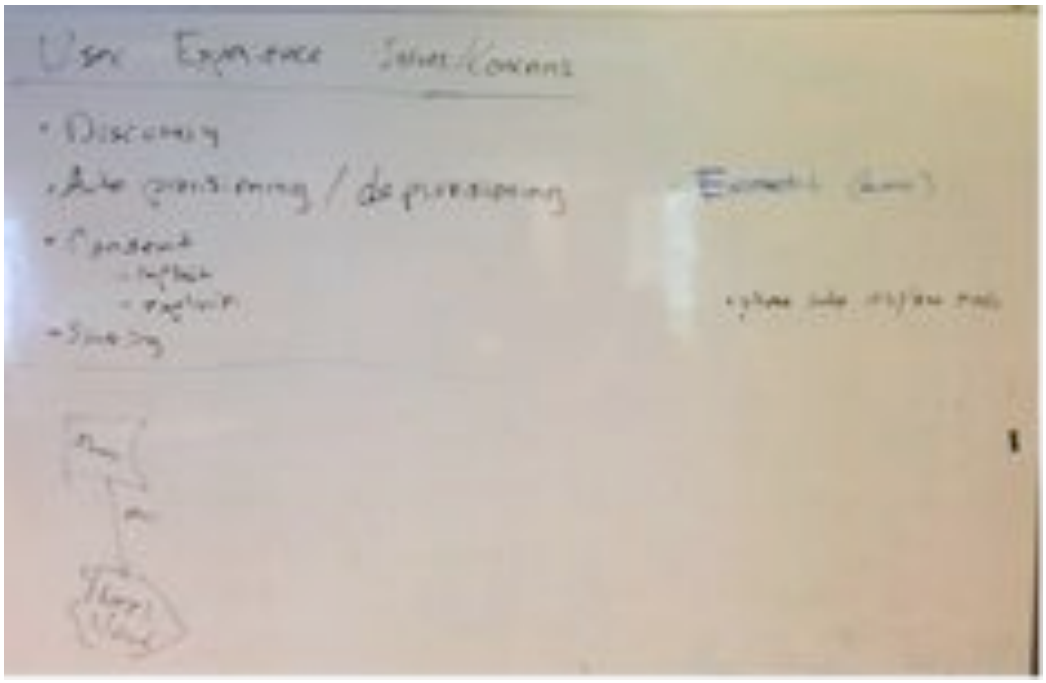
Wednesday 4B
Convener: George Fletcher
Notes-taker(s): George Fletcher

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was a lively discussion where we talked about a lot of things that relate to the Internet of Things space: Taxonomy of "things" ~ Security Concerns ~ Privacy Concerns Discovery and Provisioning Flows ~ User Experience




B
"connector"
VRM


User Experience
Discovery
Provisioning

Timbl on UI offered by WebID: Getting WC3 People to come to IIW19

Wednesday 4D
Convener: Brent Shambaugh
Notes-taker(s): Paul Trevithick

Tags for the session - technology discussed/ideas considered:

WebID, Authentication, User Experience

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

For background: A WebID is a URI that points to a WebID Profile document.

For example if a user Bob controls https://bob.example.org/profile then his WebID would be https://bob.example.org/profile#me . A profile document is an RDF file with some information about the agent.

We discussed the UI as implemented in browsers for WebID.

OAuth SASL (OAuth for Non-Web Apps, ep.IMAP)

Wednesday 4F
Convener: Hannes Tschofenig
Notes-taker(s): Roshni Chan

Tags for the session - technology discussed/ideas considered:

OAuth, SASL

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to PowerPoint:
http://www.tschofenig.priv.at/oauth/IETF-SASL-Kitten.pptx

OAuth SASL
Presented work done by the IETF KITTEN WG.
SASL (Simple Authentication and Security Layer - RFC 4422)
- middleware
- generic security services (GSS API)
- SASL and GSSAPI sort of merged, but the mechanisms in the RFC only specify SASL mechanisms.

Typical challenge - authentication mechanisms chosen by some may not be appropriate for some other people, therefore SASL provides a container within which to run an authentication framework. SASL messages need to be dumped in an application layer protocol to be useful -

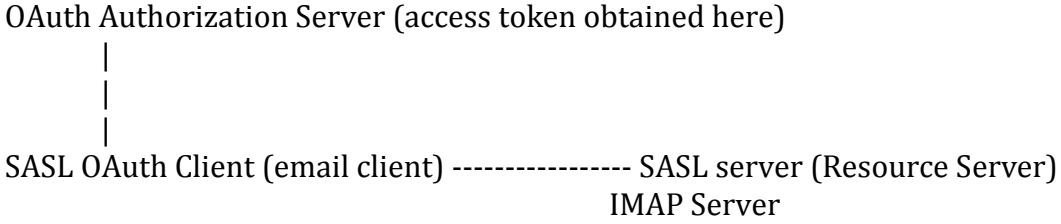
these protocols are called SASL profiles. Email based examples provided in the slides from spec.

High Level SASL Exchange
Client requests authentication exchange. The server initiates a challenge and then initiates the actual exchange with the authentication protocol specified and eventually responds with an outcome. The outcome depends on the SASL mechanism used.

In the IMAP example from the presentation, the keywords used were AUTHENTICATE=OAUTHBEARER where the client uses the AUTHENTICATE keyword to specify what mechanism it wishes to use, and the server can list what mechanisms it supports using the AUTH keyword. The client and server exchange blobs till success or failure.

TLS: The server/client can request TLS. The problem with using TLS is that the security mechanisms are now in the underlying layer and not known to SASL.

Standard OAuth SASL architecture:



Different from popular OAuth in that the client is not pre-provisioned with any information. Some bootstrapping is required for the server to learn about the client ID and metadata, and the client doesn't know which Authz server to use.

Actual Client-Resource Server interaction
Two OAuth SASL Mechanisms
- bearer tokens RFC 6750
- OAuth1.0a RFC 5849

Q. OAuth1.0 has a list of vulnerabilities listed in the appendix as unaddressed flaws, so why are we still using it?
OAuth1.0a is being used to show how we would use this for a signed profile. OAuth2 doesn't mention signed messages, but supports PoP.

Q. Why not use TLS and then recommend relying on something else later.
A. GSS API requires mutual authentication and TLS is outside the GSS layer.

Discovery
-- missing in the spec.
- manual config needed, which isn't the best user experience.
Possible Options
- in-band discovery (the IMAP server provides some data to bootstrap with)
- Webfinger, and then retrieve a JSON based doc to get config parameters
- Dynamic Client Registration

Implementations of SASL in email clients
- Google has SASL with OAuth2 (server-side)
- Amazon Kindle clients, Blackberry clients and the Microsoft Nokia phones use Gmail IMAP

Next steps
- spec discussion in the KITTEN WG
- issues like Discovery
- error messages for revoked/expired tokens
    use simple error messages and require a second call to check whether token was revoked/expired (deterministic behavior by client).

Some discussion about the GSS Header.

Tunneling an HTTP-like mechanism to use it within SASL seems like we're forcing an HTTP convention instead of using a JSON Convention - should be discussed further.

SASL-SAML does discovery by getting the client to talk to the IMAP server to get the IDP from the username. (email address -> IMAP server address. IMAP server -> authz server address)
- in-band discovery in SASL (by separating out discovery of IMAP server and authz server)
- authz server ID (URL) + attach a trusted component -- hit discovery endpoint and download config param document.
-- Type OAUTHBEARER + 1 URL -- if for authz server
-- add a trusted pth, fetch the doc with endpoint info
-- OR send the username and the actual discovery doc is a f(username).

Reference: draft-ietf-kitten-sasl-oauth-14

Be Ready for the Authpocalypse: Lightweight/Dynamic Client Registration for ImAP/SASL

Wednesday 5A
Convener: John Bradley/Breno/Naveen
Notes-taker(s): Roshni Chandrashekhar

Tags for the session - technology discussed/ideas considered:

Dynamic Client Registration

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Dynamic Client Registration

Issues tabled for later:
-- discovery

Consider the example of ThunderBird (TB):
A user downloads TB and it uses OAuth2, but it doesn't know which authz server to use. OAuth2 requires a client ID, and when the user enters X@gmail.com, there needs to be some way to send a client ID to the authz server.

Disadvantage of WebFinger --
not every enterprise has a web server with a TLS cert that it can put WebFinger info on.

Segue:
Assume you have the oauth token. You want to access 4 different services with the same token
-- IMAP, SMTP, Address Book HTTP, Calendar HTTP
-- use one downscoped token for the difference security contexts of the different protocols?

We cannot assume that all the endpoints for these 4 services are in the same location, because we know this to not be the case in several cases. However, it is trivial for the client to find that the issuer is not the same for all these services and handle that. If the issuer is the same, then the client should combine and ask for multiple scope consent.

Scenario:
IMAP ----------> AUTH ----------> CLIENT REG

Options:
1. Any public client gets a fixed client ID and everybody supports it. For example clientID=IMAP.
-- branding issues on the approval page
+ avoids each client making a registration request and then an OAuth call.

2. JWT from vendor (containing client info and PoP)
3. Public key for instance.
    -- prevents intercepted code in response
    -- protects code but not refresh token

1&2 identifies client. 3 authenticates client.

4. Dynamic Client Registration
5. Stateless dynamic client registration where client ID is the server assertion.

Q. AS, do you have a client that redirects to this URL? Give me that client ID.
A. Not secure, susceptible to interception.

Goal: to keep the code from being used if intercepted, which is what client ID is used for.

We can recognize that the assertion in (2 -- Vendor JWT) is the same across a range of clients.

"Software Statement" -- a statement signed by the software developer with some parameters that helps to identify the software through which the request is made.

Use assertion flow only and a public key -- makes discussions about statelessness simpler.
    -- client generates its own public/private key pair
    -- no security implications of encryption
    -- use JWT assertion for client authentication

Q. Does every instance of installed client end up with its own client ID and secret?
A. Yes. But the server doesn't store it. Use public keys to give each instance its own client ID.

Confidential clients
-- you don't need to protect the request if you have a confidential client.
-- the software statement as client ID for all authz flows implies you need to give up the option of making clients confidential and use PoP for code instead.

The current dynamic client registration spec supports both public and confidential clients. Using the software statement implies you can now track installed clients as separate instances.
Class differentiation is made easier to handle. (For Example: A loses laptop, we should allow A to disable access through the laptop but not ask for re-auth on a phone and other devices)

If the authz server has to support only one kind of dynamic client registration, it reduces the pain for the implementation of an IMAP client.

Summary:
Current spec of dynamic client registration
+ add software statement so authz server knows what software is making the request
+ authz server choice of stateless/stateful
+ make it mandatory to implement specific authz mechanism by IMAP client

10 Things you can do with a Freedom Box

Wednesday 5D
Convener: Markus Sabadello
Notes-taker(s): Brent Shambaugh

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- UI is written in Python
- Chat is an XMPP server
- store and share photos
- This user interface is called. This is how you manage a FreedomBox

---

- Build PGP … criticize certificate authorities …

small linked number of companies

- PGP Web of Trust ...
- Sign each others key pair

--Monkey sphere....take this an apply it to the web

- Domain name system....

HTTP does not really
– is the monkey sphere pretty complete...
communications box...makes communications secure …
Markus – Project Danube
Through P2P network … & VPN they can find each other...

---

single sign on … openID …
one identity provider... one provider...log into many website
– same as Mozilla Persona...

Know Diaspora...
The idea is clear...
Send message and photo … one box to another...
Do you have XDI running on this ...earlier did XDI on it
Put VRM ...a buying intent … say I want to buy something with certain properties …
use RDF linked data

Earlier at OuiShare conference …

- How can I have a kind of marketplace....
- * How can I publish this kind of info

Semantic web relies with linked data

---> OuiShare
** Philosophy behind sharing.
2nd part hackathon
→ hack on some of these ideas

IIW _ create connection to each other
Have mesh network between box

- Some applications make sense w/o net community

How easy to make it portable

- random people logged in and published to his box.

Distributed filesystem w/o internet connectivity

Figure out freedom box …
→ market could exit with
Adding software … Freedom Box
Some related to identity

Apps category … New Addition
of things to add …
No need for command line …
Johannes … Greek … and moral wov
Community wifi – Networks in europe

→ use mesh network for internet connections sharing
→ the box can do a mesh network
Work in a Mesh network....work with connectivity

Active mesh network in Athens Greece
Have their own twitter and news site

You have an average mom in America … use mesh network
** Mesh network in China
Networking Pakage(?) happen to have Mesh network

MIT w/ Mesh network
+ Scratch teaches kids to create Mesh networks
– Who is the Freedom Box for?

- Have simple UI like indie Box – VM have in expert mode – complicated things – have wireless built in
- Freedom Box is actively looking for hardware partners

→ It all needs to come together

- Paranoid Chinese dissident

On Arch Linux … well respected...secure … Packts built ...Freedom Box chose Debian

- What to pick form a market perspective
- Main attaction … effective way of doing something on the internet differently
- Put this … communicate … not just for computer scientists

- Use TOR to hide the IP address as a client
- Configure to be a TOR exit mode
- Chat talks to g …

--- Purpose of you ...TOR hides you as a

- Run a Blocka wiki … TOR enabled...

- IS there a Freedom Box

Shopping list (things you can Bug)
→ You can buy the Freedom Box online

Can you also use Raspberri Pi
→ Yes, but more limited ….
---> I tried with the Raspberri Pi...
it is not easy

TOR Browser What kind of Mesh Hardware…

OIDC & SAML2: Dealing w/the case when the intended audience is not the relying party

Wednesday 5G
Convener: Roland Hedberg
Notes-taker(s): Roland Hedberg & Mike Schwartz

Tags for the session - technology discussed/ideas considered:

How to make an IdP (SAML2) or an OP (OpenID Connect (OIDC)) set the correct audience in an assertion or an id_token. That is when the SP/RP knows it is not the ultimate receiver and also knows who the correct one is.

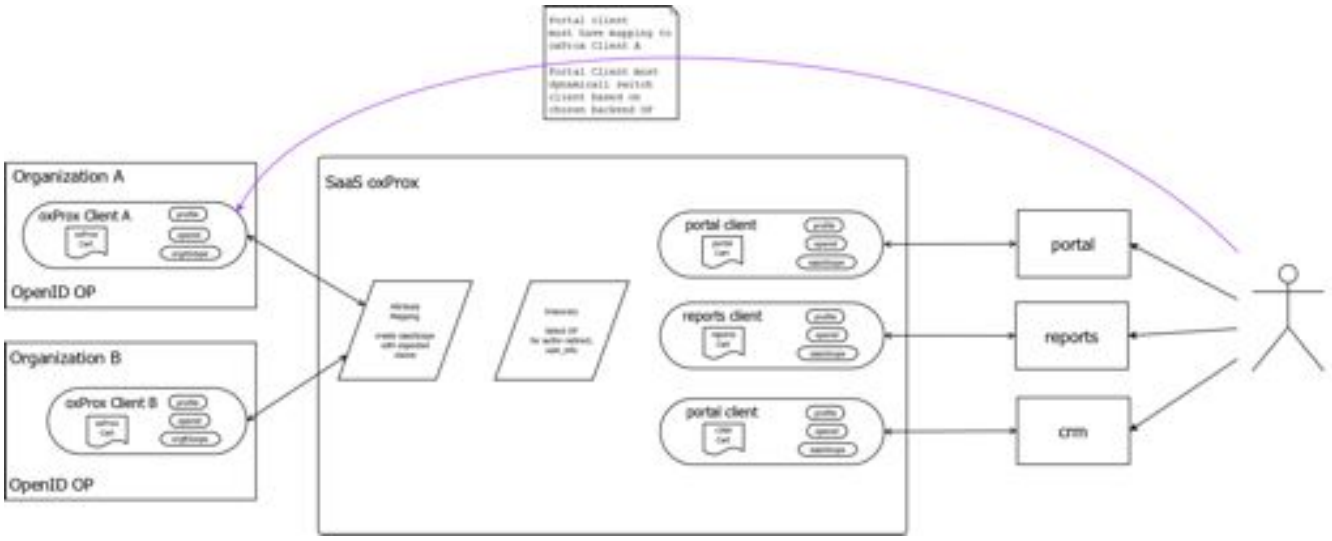
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Three examples of the problem:
UMA: where an Authorization Server needs extra information about the requestor from the client. The client will act as the SP/RP against an IdP/OP to gather the necessary information but the client is not the intended audience the AS is.
Token exchange: There are cases where a issued id_token must be exchanged for a SAAS token. Again the receiver of the id_token is not the intended audience the SAAS token exchange service is.
Proxys: An effect of the design. A proxy exists in two environments and wants to transmit information received in one to the other.

There is no way either in SAML2 or in OIDC for the RP/SP to signal the OP/IdP who the intended audience is. To change this in SAML2 is probably very hard, to change it in OIDC is probably doable so we took that as an action item.

Notes from Mike Schwartz
RP's have a problem when they try to pass an id_token to a backend API. If you pass the id_token directly to a 2nd back-end RP,
the aud specifies the client id of the original RP. And while it may work because (id token may not be encrypted), it violates the policy that an RP would should not use a token which was not intended for it to consume. Perhaps it exposes the RP to potential liability.

Shon and Matt from Amazon and Roland were completed perplexed how to solve this problem. Mike Schwartz walked in with five minutes left in the session, and solved it. He drew a crude diagram of oxProx, Gluu's open source OpenID Connect proxy. It explained how in this case, oxProx would be the RP to client1, and would be OP to client2. and then would issue the correct aud to the backend RPs. Not only this, but oxProx would enable claims mapping, and allow for normalization of OpenID Connect scopes.



Lost Dog! Usercentric ID Management

Wednesday 5H
Convener: Chris Edwards, Intercede
Notes-taker(s): Peter Cattaneo, Intercede

Tags for the session - technology discussed/ideas considered:

User-Centric ID, FIDO, credential lifecycle management, lost/stolen devices, device migration, improved user experience

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Brief history of credential management. Smart Cards, HSPD-12: Enrollment, lifecycle management. Existing solutions based on centralized issuance and management model. Support lifecycle events such as lost/stolen devices, credential updates, device migration, user termination.
Secure credentials migrating into mobile devices; multiple secure elements available. Works today with existing centralized ID systems.

User centric ID needs a different approach. Brief FIDO overview
.
What happens when you lose a device? How do you migrate to a new device after you've registered lots of sites? How can you provision multiple devices with authenticators for the same set of RPs.

FIDO does not specify these user management features. Risks:

1) Bad user experience
2) Recovery process is lower security than FIDO PK credentials creating at soft point of attack

Possible solutions:

1) enhance the device to enable management on a mobile device;
2) cloud service;

MePin.com has implemented a cloud service with similar functionality; does not yet support FIDO.

Follow up:

Need to make sure that FIDO specs do not contain anything that would preclude implementing this functionality.

Work to standardize functions to:

revoke existing authenticator;
add second authenticator; using the first authenticator for authentication.

Thursday May 9

Let's Create Some Pertinent Art ~ That Speaks to Our Condition & Brainstorming Ideas About Topics for Books for Children and Management - *(like SCADA & ME)*

Thursday 1D
Convener: Kaliya Hamlin & William Heath
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Open Reputation Framework

Thursday 1G
Convener: Dave Sanford
Notes-taker(s): Dave Sanford

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Dave started by giving an architectural overview of a proposed Open Reputation system that would allow individuals to assert reputations to individuals, their knowledge and possibly lots of other things (e.g. products, etc.). Mostly this is not self-assertion of their own reputation, while that should probably be allowed - it has very little weight outside itself.

Dave also suggested that to be decentralized this should be build on top of a decentralized consensus algorithms like block chain or ripple.

The model includes an individual's ability to define their preferences for their own use in curating and weighting the value of information sources, etc. so that they can filter information coming in. By feeding these weighted preferences to:

Aggregate reputation modes - which use various weighting algorithms (pagerank?, Bayesian) to create weightings of reputations which are available to individuals.

Individuals and reputation nodes will have reputations that are created about the quality of the reputations that they produce, which change over time.

There were various discussions about how reputation information is defined and communicated - that included discussions about comments and context. This led to the discussion of information being communicated via graphs and XDI.

? asserted that this becomes communicated like X has a reputation for Y among Z.

Lots more discussion - common protocol is clearly required. Is a common reputation algorithm required for individual and/or aggregate reputation nodes?

DNSSEC 101 (Intro: How it works? My War Stories!)

Thursday 1J
Convener: Jim Fenton
Notes-taker(s): Jim Fenton

Tags:

DNSSEC, DNS, Security, Certificates

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

DNSSEC is a mechanism for cryptographically signing records in DNS to certify that they are authentic. Jim Fenton related his recent experience deploying DNSSEC, starting with verification of DNSSEC signatures and on to signing a domain using DNSSEC.
One of the issues with DNSSEC is that it's largely transparent to the user, so its benefit is not evident. One way to check the use of DNSSEC is to use a browser plug-in such as DNSSEC Validator.
DNSSEC doesn't directly replace certificates, etc. in certifying identity, but can be used with new technologies like DANE to secure other information that might be stored in DNS.
Resources:
DNSSEC Validator: http://www.dnssec-validator.cz
Internet Society Deploy360: http://www.internetsociety.org/deploy360/dnssec/
Jim's war stories:
https://altmode.wordpress.com/2014/04/09/adventures-with-dnssec-part-1-checking-signatures/
https://altmode.wordpress.com/2014/04/17/adventures-with-dnssec-part-2-signing-my-domain/
OnTheMedia story about signing the root the domain:
http://www.onthemedia.org/story/so-many-keys/
http://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web

ACE: Authentication & Authorization for Constrained Environments

Thursday 2D
Convener: Hannes Tschofenig
Notes-taker(s): Hannes

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to PowerPoint presentation:
http://www.tschofenig.priv.at/oauth/ACE-Summary.ppt

The Maker Economy & Identity

Thursday 2I
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

Tags for the session - technology discussed/ideas considered:

#Biometrics #arduino #objectandartifactidentity #identityawaredevices

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Maker – Chris Anderson
- Open Source Hardware

3: Aspects
- Scruffy Hackerism

"If you can't open it, you don't own it"
* Element of Artistic Self-Expression ==> Long Tail Art
- Revolutionary Manufacturing ==> Most interesting
- Value Youth

Refrigerator Art ==> Kids make drawings ==> long tail
- inefficient autos

* important as anything else

Maker movement and 3D Printing lots

New Tech 3D Systems
- linked

Physics dance in desktop publishing

(talking about the indie song movement)
Easy library from Groups
Word processing – Make it interesting to write
---> Decent production Low
Do not need different
Not flooded with quality music low? (paraphrase: but is indie music really that bad, it appeals to someone?)
So much....hard to find quality …
+ People I know (Social Recommendation)

So much … hard to find quality …
- People I know (Social Recommendation)
- Like Reputation ...(Good Enough) …. Established Social Network

Reputation as Maker … Wireless Device Controlling
EC were (?)...
Get indentity layer …
Where to add identity?

Reputation Systems can and will be gamed

- Robot had version of someone elses router (?)
- 1000's of reviews
- Routing i-bay(?) transaction
- Reddit – Investigative Journalism

How do [you] aggregate based on similar tastes

Model … Master Running Raspberri Pi

Kickstarter and Indiegogo …
Do everything where able …
Brain states … IQ … Skeptics
Why ...Reputation Systems
Never Gained … Upside & Downside...
Respect Network as an example

Implementation System
Different Respect Network

Somehow Art is Aware of them
It knows me in some way I think
Identity … Does FB recognition

Are there platforms and standards
Lot of Mercury[?] to get out of phone

GAP in Maker Space ….
No Shield … identity iterator shield …
std[?] way … broad costs … very [?] … open standard...

Think other way around … identity in the cloud

Your device can interact ...extrapolate to borrowing car

some other attribute ...on his key start … his car

Zip car Dcerive [?]

Not [?]

Going to MakerBot

Fungible [?] … Put on Arduino

What UI to use … Plyn[?] Identity
OAuth … it does not exist

- A lot of preses there …
- Sheild … Oauth Presentation Layer
- not in Arduino ...Sheild … Oauth Presentation[?] layer
- not in Arduino … Do not have screen to show transaction

- Display list devices … SMS challenge...

Bridge to trusted device

Hard to Identifier

Same to send to Oauth server

Web Browser … in Done 4 Years …. [?]
Oauth … Hard to Launch Business to Platform

Open Browser w/ HTTP stuff...
See more elegant ways w/ Oauth 3 & 4

Standard Biometric Data … a lotd[?] phone up to

your eye … Did investment in company...
worst bad stays connection [?] .. Per Auth using ECG

ECG must give permission …

20 second record ...take awhile … (writers comment: to hack right?) … skin elevation …

Not as accurate yet … Interesting application

- Tesla App
- Mastercard use 4 Payment Authentication

Arythmia[?] … stay[?] w/Name of Company
Biomen

Identity … Sovereignty of data … do I[?] own it?
Take pictures …

Identity problem

Bother … makes treat us as user names and not passwords...however anything … not a big deal

If some are sterling[?] ..do I need a new heart … 9 password resets to fill out? 19?

As username … totally fair …

stole from … take credit …

Start 4 Username + Presenting[?] ...DII[?] ...you want...notion of username...like...notion of username … something real...still get participate[?] as opposed to steal signatures...

All security lead pipe

Can You create audiences...

Facilitate...A lot of stuff..

Built 4 its own sake...

Chuck off in

About creating connection

writter's annotation main topics:

-Make device identity ware

-use identity to connect objects and artifacts
---
7 Bit Hero … Show up … MIDI is a 7 Bit Protocol ...Show up at concert...Scan at beginning of concert … Everyone[?]

Proximity...You could add virtual participants into concerts … get Kinetic sculpture...

fascinating possibilities … beginning needs to be explored...

- Participants generate wate...
- This is a co-creation – structure and Artist

The Artists Makes to Rules
Theote[?] component changes

Another thing is … what happens if 15 or 150 interacting...visual representation...Good thing calle
dranondage[?] other play in to
How musical transitions

Some sets the wise...

A good D.J. ….sets up the
some ...D.J. Will change it up

Definition … any[?] the tranditional--

Identity is very personal –

Identity may be a bundle of attributes … stages[?] of heart beats … Good performance Art...
Eyes Beating ….lighting[?] build by w/Art piece

Have Biometric Reading Glasses...

Trippy to watch interaction...
What happens..do people synchronize

Switch to another person's heartbeat

Ocular...break open an egg...
several different latencies...

show...latencies(?) of the[?] internet work

Throws you off on a cell phone conversation

Have to increase...

What It Takes to Get a Customer-Centric Startup to Win Funding?

Thursday 3A
Convener: Nathan Schor
Notes-taker(s): Panel Discussion Video

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

An accomplished group of investors were invited to discuss challenges to funding startups building privacy, identity and customer-empowerment solutions, as well as to hear founders pitching specific business model.

To the best of our knowledge, this is the first ever investor event focused exclusively on funding user-centric business models.

Here is who participated:
• Noah Doyle - javelinvp.com
• Keith Teare - archimedeslabs.com/
• Derek Anderson - startupgrind.com
• Kayvan Baroumand - nestgsv.com
• Dan Gordon - valhallapartners.com/
• Amit Shah - Aritman Ventures artiman.com/
• Anandan Jayaraman

Here is a link to video of the Panel Discussion:
https://vimeo.com/channels/iiw18investorpanels

Kitties are Fluffy!

Thursday 3B
Convener: Justin Richer
Notes-taker: David Pinter

Tags for the session - technology discussed/ideas considered:

multiple personas, corporate identity, personal identity, anonymity, outing,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

BYOD is evolving into BYO Id

How does a corporate interest get impacted by action made from within a personal context?

Aggregate reputation/impact of employees _is_ the company reputation: The higher up the employee in the org, the greater the impact

Corporations (as employers) are NOT managing ID. Employees are bringing their IDs into the enterprise (ex: Forwarding corporate email to personal Gmail b/c that's where the employee's email lives, and where they "do" email).

Posts/comments are a reflection of personal State when made by individuals using company-provided IDs.

Comments made under a Company provided ID have a greater weight than a personal ID
Employees are at risk posting under company ID

Is there a safe harbor on the Net for Real Personas?

To what extend does an IDP stand behind the individual? It's different when the individual is an Agent of the IDP (employee) or customer.

Young people today have always HAD the internet, and are used to the concept of multiple identities/personas and can manage them natively (like children who grow up speaking multiple languages)

Tools, comfort, and calluses develop over time.

The Internet lacks a richness of context; sometimes the wrong persona is used on line. But when in Grandma's living room, it's not possible to switch out of the "grandma context" (vs. the school or friend or parent context)

The Internet doesn't forget or integrate. Transcripts are available for replay, but overall impressions formed in personal interactions (facial expression and body language, etc) add to human to human conversations that ultimately make the experience something greater than the recorded transcript.

Systems can now correlate contributions and recognize individuals using multiple personas, have the ability to "out" posters using different IDs.

We use different pathways when we speak than when we write.

Some individuals are better able to manage separate personas than others, kids in particular are inherently better at this.

Startups Pitching to VC Panel

Thursday 4A & 5A
Convener: Nathan Schor
Notes-taker(s): Nathan Schor & Video

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Here is a link to video of these pitches: **https://vimeo.com/channels/iiw18investorpanels**

Panelists

- Noah Doyle noah@javelinvp.comhttp://www.javelinvp.com
- Keith Teare keith@teare.comhttp://www.archimedeslabs.com/
- Derek Anderson derek@startupgrind.comwww.startupgrind.com
- Kayvan Baroumandkayvan@nestgsv.comwww.nestgsv.com
- Dan Gordon,dan@valhallapartners.com, http://www.valhallapartners.com/
- Amit Shah, Aritman Ventures, amit@artiman.comhttp://www.artiman.com/
- Anandan Jayaraman anandan.jayaraman@gmail.com

Companies Pitching

Respect Network Founding Partners

Respect Network ~ Emmett Global ~ URQUi ~ inWebo

Independent

Glome ~ HIE of One ~ MePIN /Meontrust ~ Pomcor ~ Tozny ~ Traitware ~ Welcomer

Respect Network Founding Partners

Company: Respect Network **Website:** http://respectnetwork.com/ **Location:** Seattle
Management Team:

- Drummond Reed, Co-Founder and CEO
- Gary Rowe, Executive Chairman
- Katherine Singson, CMO
- Andy Dale, CTO
- Matthew Sutton, VP Products
- Mark Timbrell, Head of Respect Network EU

Bios and links are all listed at http://respectnetwork.com/executive-team/

Business Model:

Respect Network is the world's first global private network of personal and business clouds. Respect Network is based on an award-winning trust framework developed over 3 years by leading Internet architects and 50 Founding Partner companies from around the world. As a decentralized, multi-provider network similar to the global banking or email networks, the Respect Network will enable members anywhere in the world to share sensitive private data with strong assurance that their privacy will always be respected. In fact, Respect Network is the only global data sharing network engineered from the ground up around *Privacy by Design*.

Traction: 50 founding partners who have already signed up.

Amount funds seeking: Respect Network Corporation is currently raising a $3M Series A round. On Friday April 25 we held a first closing for $1.325M. We anticipate the second closing will be the first week of June.

------ ------ ------ ------ ------ ------- ------ ------ ------

Company: Emmett Global **Website:**www.EmmettGlobal.com **Location:** New York /Israel

Management Team:

- Kenneth J Lefkowitz, CEO
- Lionel A Wolberger, Architect
- Joshua Zieman, CMO

Business Model:

Emmett Global distributes best of class open source solutions that enable true Personal Data management. Three included solutions are;

1) Cloud service provider on the Respect Network

2) Browser extension bundle for Chrome and

3) Mobile tablet device.

Amount funds seeking: $950,000 to complete our seed funding

------ ------ ------ ------ ------ ------- ------ ------ ------

Company: URQUi **Website:** www.urqui.com **Location:** BCCanada

Management Team:

Jonathan Bell, President, Computer Consultant – Ambassador of Privacy by Design

Ken Jennings, kjennings@urqui.com @kwjennings, https://www.linkedin.com/pub/ken-jennings/0/7a2/602 Board of Directors Skkynet Cloud Systems Inc. Skky OTC.bb - **Ambassador of Privacy by Design**

Dr. Jose M. Fernandez P.Eng, Ph.D., Assistant Professor of Computer and Software Engineering, Polytechnique MontrealFrequent Speaker on IT Security & Cryptography - Ambassador of Privacy by Design

Business Model: URQUi"Your Key" is a secure, patent-pending, network or SaaS password alternative. URQUi One Time Passwords eliminate the need to store static passwords on servers. Users need not remember passwords. Using URQUi, a FREE app, individuals control their privacy, secure their online presence and protect themselves from identity theft. User-centric URQUi embodies Privacy by Design. The Heartbleed bug could not have breached accounts using URQUi! ~ URQUi's Business model is disruptive. URQUi is a multi-sided recurring revenue SaaS business. URQUi is free for individuals; free SaaS for government and non-profit servers; billable recurring revenue SaaS for commercial servers. URQUI's pricing to commercial SaaS customers will be disruptive at 15% of comparable services (RSA SecureID). Distribution to individuals is done through iTunes et al. Distribution to server owners is done through resellers and vertical market partners. URQUi expects processing margins in the area of 50% - 60%

Traction: URQUi has not yet achieved traction in the market, however URQUi has developed significant partnerships. Ambassador of Privacy by DesignFounding Partner of the Respect NetworkCTA@Boston, Fall 2014 Cohort

Amount funds seeking:$1,750,000 **https://angel.co/urqui**

------ ------ ------ ------ ------ ------- ------ ------ ------

Company: inWebo **Website:**http://www.inwebo.com **Location:**

Management Team:

Didier Perrot, CEO and founder, didier.perrot@inwebo.com

http://www.linkedin.com/pub/didier-perrot/0/72/b9/
Bruno Abramatic, CTO and co-founder
Olivier Perroquin, SVP Sales and co-founder, http://fr.linkedin.com/pub/olivier-perroquin/0/424/240

Business Model: inWebo provides a Cloud-based authentication platform and a password management service to help enterprises, businesses and service providers protect users' online access and transactions in a highly secure yet non-intrusive way.

Traction:

Amount funds seeking: 3M$ https://angel.co/inwebo

Independent Startups

Company: Glome **Website:** www.glome.me **Location:** Finland
Management Team:
Edi Immonen – Co-founder & CEO edi@glome.me https://www.linkedin.com/in/jemiweb
Ferenc Szekely – Co-founder & CTO https://www.linkedin.com/in/ferencszekely

Business Model: Glome has created an anonymous personalisation platform (an API) for businesses where individuals own, control and benefit from their digital footprint with full anonymity.
Traction: Glome had a soft launch in Finland and we targeted a few key players with great success. Now we have partnered with:

1) A top-10 media in Finland with close to 1M unique weekly users
2) A leading Scandinavian web shop company
3) A leading Finnish consultancy & big data company

Amount funds seeking: A total of 1.8m€ in steps in year 2014 so that: 300k€ for finishing the product-market-fit phase (Q3&Q4 / 2014) ~~~ 1.5m€ for launching and expanding (Q4/2014 ->)

Company:HIE of One **Website: N/A** **Location:**Boston
Management Team:
Adrian Gropper, MD –agropper@healthurl.comhttps://www.linkedin.com/pub/adrian gropper/1/665/691
Josh Mandel, MD –https://www.linkedin.com/pub/joshua-mandel/35/472/883
Adam Powell, PhD –https://www.linkedin.com/in/adamcpowell
Business Model:HIE of Onewill sell a personal data store (hardware or cloud) and live support to consumers to enable the coordination of family care teams for the elderly and seriously ill. Our service uses open source software to create a platform for patient-directed health information exchange that will be preferred by app and services developers because it is verifiably privacy-preserving, verifiably secure, free to the developers, and, as a community open source project, carries no risk of vendor lock-in. HIE of One is a public benefits for-profit corporation designed to appeal to both financial and strategic investors.
Traction:HIE of One has limited traction. We won one of the major prizes at an MIT health hackathon a a short time ago and we have a commitment from Smart911 to participate provide an API and participate in a demo this summer. We've also got three separate collaborating groups in the San Diego and San Francisco areas.
Amount funds seeking: $2 M

Company: MePIN /Meontrust **Website:**https://www.mepin.com **Location:**Finland
Management Team: Markku Mehtala, CEO,
markku.mehtala@meontrust.com http://fi.linkedin.com/in/markkum/
Business Model: MePIN provides smart security for consumer online services, protecting the services and their users against password phishing, account hijacking, transaction fraud and privacy problems.
Amount funds seeking: We just raised a round, so looking for contacts for future rounds.

Company: Pomcor **Website:**www.**pomcor.com** **Location:**Boston
Management Team: Karen Pomian Lewison,
CEO, kplewison@pomcor.com, http://www.linkedin.com/profile/view?id=28011537
Francisco Corella, CTO
fcorella@pomcor.com, http://www.linkedin.com/profile/view?id=78440530
Business Model: Pomcor is developing an Enterprise Mobility Management (EMM) solution to help an enterprise protect data stored in a mobile device with a patent-pending technique that prevents an adversary who steals the device from mounting an offline attack against an activation PIN.
Traction: We don't have a product, so we don' have traction yet. We do have a no.1 position in Google for one of the market segments, even without a product.
Amount funds seeking: We are looking for a letter of interest to support an NSF SBIR Phase I grant application, followed by an investment of $60,000, conditional on our getting the SBIR Phase I grant of $150,000. The $60,000 investment would be matched by a Phase IB grant of up to $30,000. Successful phases I and IB would give us a very good chance of getting a Phase II grant of up to $750,000, which in turn would allow us to get a Phase IIB grant of up to $500,000 matching an additional investment of $1,000,000.

Company: Tozny **Website:** http://tozny.com **Location:**
Management Team:
Isaac Potoczny-Jones, President
ijones@tozny.com@SyntaxPolice http://www.linkedin.com/pub/isaac-potoczny-jones/4/b64/23b
Leah Daniels, VP Business Development http://www.linkedin.com/in/leahcdaniels
Business Model: Digital authentication - proving who we are - is a constant necessity on modern networks. Users are buried under the weight of too many passwords, and are faced with a conundrum: good passwords are impossible to remember, and bad passwords are easy to guess.
Tozny replaces passwords with a cryptographic app on your smart phone, making login both easier and more secure than passwords. Alternately, use Tozny to augment passwords with multi-factor authentication. Tozny helps enterprises and web sites stay secure and gives users an easier way to log in.
Traction: We have a customer in the government who is funding our work under a small business innovation program, and we have strong leads with a few large consumer-facing organizations in banking, health care, and telecommunications.
Amount funds seeking: $500K

Company: Welcomer **Website:** http://www.welcomer.me **Location:**Australia
Management Team:
Kevin Cox - kevin@welcomer.meau.linkedin.com/in/kevinrosscox Kevin is an Identity domain expert who has deep understanding of how organisations can benefit from giving people access to their own information. Kevin previously founded identity verification company Edentiti which was acquired in late 2013.
Paul Marando - paul@welcomer.meau.linkedin.com/pub/paul-marando/4/111/486 Paul comes across from Edentiti bringing with him a deep understanding of identity technology

and a track record developing scalable architecture. Paul looks after the technology as well as leading the engineering team.
Rory Ford - rory@welcomer.meau.linkedin.com/in/roryford/ Rory brings a background in online marketing and product management. Previously he established a portfolio of websites bringing in online sales across more than 120 countries. Rory also worked within Edentiti, looking at new product opportunities that have formed the basis for Welcomer.
Business Model: Welcomer provides an identity verification solution to small and medium organizations by utilizing a person's access to their own information. Based on proven Enterprise technology, already used by banks, Welcomer makes money from each successful verification.
Traction: Company has raised ~$450K seed funding.
Amount funds seeking: $300,000

Company: Traitware **Website:**www.traitware.com **Location:** San Francisco
Management Team: Harlan HutsonPresident - Mr. Hutson is a serial entrepreneur now on his third start-up. Harlan has been fascinated with online transactions and security since the creation of his second start-up, an online event ticketing company that was sold in 2010
Dr. Herbert w. SpencerCTO Dr. Spencer has been a developer of new technologies since building a computer from pinball machine parts in junior high school. He received a Ph.D. in plasma physics from Auburn University and started EC&C Technologies, Inc.
Business Model: TraitWare™ delivers 2-factor authentication making mobile and web computing more secure and enjoyable. Our patent pending process authenticates both user and device, binding them together to create a secure signature. When combined with PhotoAuth™, TraitWareID™ eliminates the need to enter a PIN, OTP or "out-of-band" SMS codes for authentication.
Traction: TraitWare is fully operational is now being used in pilot tests by companies that have been signed as partners. TraitWare is bundling its authentication with software to solve customer needs in the areas of finance, payments, and health care.

Thank You to All the Fabulous Notes-takers!

There were 93 sessions called and held ~ we received notes, white board shots or video for 66 of these sessions thanks to those of you who submitted notes and information!

IIW Women's Wednesday Breakfast

We had many new faces at this IIW including quite a few women - at the close of Tuesday's circle Kaliya invited the women to connect over breakfast Wednesday morning. We filled a whole table and thus began a new tradition at IIW.

We shared who we were, what we did, where we came from in the world, along with a bit about what inspired our work. We talked about the topics we had heard discussed on the first day of IIW and the ones we hoped to discuss in the coming days.

We hope you will reach out and invite women colleagues you know in the field who would enjoy and contribute to IIW. We can't wait to meet them.



1. **Indie Box One:** Johannes Ernst
   URL: http://indieboxproject.org/
   Bring your data home when you have control over it.

2. **The Internet Society:** Asa Hardcastle
   URL: none at this time
   TOSBack2 backwards compatibility project with TOSBack and a terms of service browser plugin

3. **Respect Network Global Private Network:** Drummond Reed & Matthew Sutton
   URL: http://respectnetwork.com/
   We'll be showing the private invitation process for the world's first global private network of personal and business clouds, including registration of a lifetime cloud name and a preview of the first Respect Network apps.

4. **Welcomer Dashboard:** Rory Ford
   URL: http://www.welcomer.me
   Demo Description: The Welcomer Dashboard gives individuals access to their personal information. This could be as a customer, employee or user. The Dashboard enables new personal data applications to be developed.

5. **Glome:** Cashbackcatalog.com and the Glome anonymous authentication and personalization platform in action: Edi Immonen
   URL: www.glome.me (the platform / API) - www.cashbackcatalog.com (service using the Glome API)
   How Glome's anonymous human driven personalisation platform is used by Cashbackcatalog.com to remove forced sign-up and sign-in. Frictionless shopping, sharing and earning cash back with full control of own digital footprint.

6. **3-factor seamless authentication by inWebo:** Didier Perrot
   URL: http://inwebo.com/videos/inWebo-3factor-authentication-mobile-push.mp4
   This demo features a truly secure, yet really frictionless 3-factor authentication. It's now a commercial product, which requires hardly any integration

7. **Idno:** Ben Werdmuller and Erin Richey
   URL: http://idno.co
   Idno is a way for groups and individuals to create and publish a site they truly own. Open source and easy to use, it supports indieweb technologies.

8. **MePIN / Meontrust Inc:** Markku Mehtala
   URL: https://www.mepin.com
   MePIN is a smart consumer grade 2-factor authentication and transaction authorization solution. The privacy protecting PKI -based service allows users to confirm logins and transactions with a simple tap in an app.

9. **Tozny:** Isaac Potoczny-Jones
   URL: http://tozny.com
   Good passwords are hard to remember, and bad passwords are easy to guess. With Tozny, your phone is the key. Tozny replaces passwords with a cryptographic app on your smart phone, making login both easier and more secure.

10. **Yubico and YubiKey NEO U2F Device:** Nishant Jadhav & Klas Lindfors
    URL: http://yubico.com and product specific site: http://www.yubico.com/products/yubikey-hardware/yubikey-neo/yubikey-neo-u2f/
    Yubico will demonstrate the YubiKey NEO fido-ready U2F for seamless authentication across desktop and mobile platforms.

11. **No Phishing, No Hardware, No Browser Mods:** 2 Factor Access Control: Marc Stiegler/Hewlett Packard
    URL: Link to 2FAcc: http://skyhunter.com/marcs/noPhishing.pdf
    75% of enterprise breaches start with phishing. 2 Factor Authentication does not stop it. Unguessable urls render phishing inexpressible. Combining such webkeys with passwords combines virtues with low cost and little user impact.

12. **Traitware:** Bert Spencer and Chris Canfield
    URL: www.traitware.com
    Traitware Authentication simplifies and secures access to protected applications and web sites by employing the User's Mobile Device as a "login token" or "authenticator", eliminating or reducing dependence on the use of usernames, passwords, or separate hardware tokens.

13. **Authentication with PayPal and the Samsung Galaxy S® 5:** Brendon J. Wilson
    URL: http://www.noknok.com
    Marvel as I reveal to you how Nok Nok Labs enables a simpler, more secure PayPal mobile shopping experience based on the emerging FIDO standards. I'll show how mobile and web experiences can experience strong authentication using the Samsung Galaxy S5's built-in fingerprint sensor.

14. **MIT's Distributed, PDS-based Microblogging App:** Paul Trevithick
    URL: http://cimba.co
    Cimba.co is an experimental microblogging app that, unlike a traditional app, stores its data in user's personal data stores (PDSes). *Benefits*: the users's data remains within their own PDS entirely under their control, they can expose it to any app they choose, and they are free to switch app providers. *Implementation*: Linked Data Platform 1.0 (March 2014), RDF, HTTP and other open standards.

IIW XVIII #18 Photo's by Doc Searls

Here is a link to Doc's photos of IIW 18 ~

https://www.flickr.com/photos/docsearls/sets/72157644704359437/

Pictures taken and provided by:
Lisa Horwitch, Doc Searls and Heidi Nobantu Saul

Thank you to our tremendously hard working IIW #18 production/facilitation team
Alli Windley, Kas Neteler and Lisa Horwitch