Internet Identity Workshop 13

Book of Proceedings

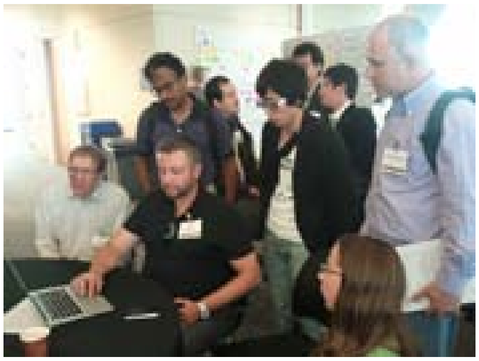
www.internetidentityworkshop.com

Compiled by
KAS NETELER, HEIDI NOBANTU SAUL AND EMMA GROSS

Notes in this book can also be found online at
http://iiw.idcommons.net/IIW_13_Notes

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

October 18-20, 2011
Computer History Museum
Mountain View, CA



Contents

OpenID Connect Intro 4
User-Managed Access Update 4
3 Screen & 4 Screen Identity Management for Online Entertainment 5
IIW 101 6
Scalable Community Trust Infrastructure 7
Low Friction Identity Proofing 7
Trust Frameworks and Other Fundamentals 8
Browser ID 9
Session Logging on to Windows 8 with Live ID 10
Layered Identity in Partnership Networks 10
Pseudonymity, Reputation, and Real Names 12
Developments in Drupal 14
Evented APIs 14
Per Site Account Chooser 15
OAUTH Web Authorization 15
SCIM 16
Per-Browser Account Chooser 18

Identifying with Your Bank 18

Killing Passwords 18

Simple Web Payments (Oauth, OpenTransact, W3C) 19

Why XDI is Needed? 20

Federated Authorization with OAuth2 22

The Role of State Government (data, policy, operations) 23

Smart OpenID, SIMcard based OpenID; what can Mobile carriers bring to OpenID? 24

OpenID Connect Client Registration 25

A Contrarian's View of Identity: Only Real Names 25

Sneaky Bastards 27

PDEC Legal Advisory Board 28

NSTIC Update 29

hQuery 34

OpenTransact Spec Session 37

XDI Link Contracts 38

Technology Solutions for User Attribute Control (W2B) 39

Impact of Devices as an Entry Point into Online Ecosystems/Data Platforms 40

CSDIP Cross Sector Digital Identity Program 42

Converging Cyber and Physical Identities for access to Facilities, Critical Infrastructure, etc 44

NSTIC Interoperability 45

Open ID Connect Flows and Levels of Assurance 49

A National ID for the US? 50

NSTIC Privacy 53

Data Portability - Wading through the BullShit 54

NSTIC and Privacy 56

Levels of Protection 56

Is There a Business Case for Click Stream 58

My Personal Event Network Waters My Lawn 60

Europe vs. Facebook 60

Strangers on the Net 61

Employment and Usability of Cryptographic Credentials 61

OpenID Connect Intro

Tuesday 1A

Convener: Mike Jones, John Bradley, Nat Sakimura

Notes-taker(s): Mike Jones

Content used to facilitate discussion:

http://openid.net/connect/

http://openid.net/wordpress-content/uploads/2011/09/OpenID_Connect_Update_September_2011.pptx

User-Managed Access Update

Tuesday 1B

Convener: Eve Maler

Notes-taker(s): Judi Clark

Data price for online services is too high. There's provisioning data by hand or by value, problems of oversharing, lying.

Another problem: meaningless consent to unfavorable terms, messy and painful management, more oversharing.
Enables you to manage sharing (host: biographical, reputation including credit scores, location, etc.; other authorized users: share selectively, protect; other requesters) and protect access from a single hub (authorization manager).

UMA gives users a true digital footprint dashboard. Unified access control under one access manager. You can test for claims like "over 18″ or reuse policies with multiple hosts. Not good for serious security concerns though. You can keep rebuilding your "sharing circles." Can't advertise your content without giving it away, can't get a global view of all sharing relationships.

UMA lets web apps easily offer "context, control, choice and respect." You can provide sophisticated protection and sharing of any user content or data that isn't meant to be public, can outsource the entire job to third party AMs, can ensure that protection of sensitive resources is stronger than the "Private URL" trick, build trust more readily with users who are "privacy fundamentalists, and can integrate these features using lightweight OAuth, JSON, HTTP, REST paradigms and a freely implementable protocol.

Glossary item: Access Control Lists (ACLs)

Demo of UMA in action with the SMART system. SMART: Student-Managed Access to Online Resources, a project at School of Computing Science, Newcastle University. They'yre planning to open-source its "UMA/j" implementation and contribute to Apache Amber. smartam.net and gallerifyme

UMA's history with OAuth: they've kept up with emerging tech. UMA pliers are really just enhanced OAuth players. Think of Authorization Manager as "authz server," think HOST as "resource server, and Authorizing User and "resource owner." Much overlap between authz server and resource server. They standardized scope enough to make this interoperable.

UMA has 3 phases: 1. protect a resource, 2) get authorization, and 3) access a resource. The process depends on the authorizing user being present, even if as shared agent or power of attorney.

Phase 1: Alice introduces host and AM using OAugh (possibly dynamic registration). The host registers sets of resources to be protected and available scopes at AM host resource set registration endpoints. Alice ensures that AM knows her policies for sharing an item. (She can set policies out of band.) Scope URIs resolve to scope descriptions (can live anywhere). Host registers resource sets and maps to available scopes using RESTful API.

Glossary item: Scope = like the object and potential verbs. What's possible to do with APIs and what happens in the access, permissions.

Between phases 1 and 2: an intermission. Requesting party learns about a resource (discovery, email, etc.), and knows how to use the API and scopes at the host (somehow).

Phase 2: Get Authorization. Requester attems to get resource but… token from AM requester token endpoint, permission for scope from AM authorization endpoint, likely claims to win permission. Host uses AM token status endpoint to check each attempt by requester, then Host uses AM permission registration endpoint to register the sought-after scope. This flow is a back-and-forth process for requesting access to something.

Language between requesting party and requester is really important. There's a fair amount of redirection to facilitate the flow of tokens and claims.

Edge case: Alice to Alice sharing! (Sharing with herself.) She only needs to list herself in the policy.

Promises: can't be made by software, must be made in person (self-asserted). UMA doesn't discriminate against claims.

Next steps: they've submitted 2nd Internet Draft. More info at later session.

3 Screen & 4 Screen Identity Management for Online Entertainment

Tuesday 1C

Convener: Wendell Baker

Notes-taker(s): Wendell Baker

Reviewed
http://www.w3.org/2011/identity-ws/papers/idbrowser2011_submission_14.pdf

The presentation focused on the diagram and the use of single sign (SSO) to affect the sharing of identity chains across the voluntary audience side and also the force-placed advertising side. The linkage between the two sides via opt in during the SSO ceremony was highlighted.

Tuesday 1F

Convener: Kaliya

Notes-taker(s): Kaliya

2004 Digital Identification World was the beginning of the process of how to build an ID for usage on the web in all situations.

Companies had for inside the enterprise but how to have for outside as well the individual

ID Commons began in early 2000's and ideas and individuals from this and Digital World were the beginning of IIW.

Reading:

7 Laws of ID by Kim Cameron

The Venn of ID by Eve Maler

At a Crossroads

Personhood in Digital Age

SIMPL – Simple Assertions Markup Language

Individuals talking to each other on different systems compatibility

Open ID – People have a URL from a blog or other application. How do they use this URL to ID themselves around the web.

INFORMATION CARDS – Good Idea, but now a dead idea.

Government wants to use this type of info, but no way to implement.

Personal Data Banks and Stores

Individual have their own info and who stores it, who do they share it with and where does it get used.

Companies today mining data, storing it and then selling it. Want to give individual control, but how.

Personal Data Ecosystem.org Consortium - How to give individuals control of their own data

OAUTH – Open Authentication

Simple management of date

User Managed Access

More sophisticated management of own data

Spectrum of ID

NSTIC – How do networks with safe credentials work together.

FICAM – Federal ID Problem!!!

Scalable Community Trust Infrastructure

Tuesday 1G

Convener: RL "Bob" Morgan

Notes-taker(s): Dave Burhop

- REFEDS.org (Research & Eval Federation) is a global consortium of organizations modeling community trust infrastructures. Located in more than 30 countries.
- Organizations are in communities, aka verticals, sectors and industries.
- Communities have existing trust relationships
- Commercial "trust" providers have inherent flaws
- SAML metadata not having expiration dates
- Protocols like max (meta data exchange) act as drivers between organizations
- All communities intersect in multiple ways
- It's all about claims/attributions
- How quickly can organizations get registered?
- Scalable aspects align with NSTIC trust model

Low Friction Identity Proofing

Tuesday 1I

Convener: Bret Tobey, Paul Donfried, Stephen

Bret Tobey – AutoIQ.co

Paul Donfried – Verizon

Stephen - Trulioo

- Lexis/Nexus

Tannis Jorge – Trulioo

Ian – Stanford, PhD candidate

Paul - Vz – Common law: user owns id, Civil Law: state says who you are, “WildWest”

Biological Identity - Deepest

Attributes –

Bret – Self-asserted attributes add validation value beyond organization centric id proofing

Stephen – Common law countries build social assertions into the breeder documents like passports

P. – before we ask too many questions, we may need to legally auth./assoc. the electronic credential about to be issued, with

S. – can we use “wisdom of crowds” logic as part of a predictive analysis of whether or not social proofing is valid

Trust Frameworks and Other Fundamentals

Tuesday 1J

Convener: Scott David

Notes-taker(s): Chad Grant

A trust framework is based on the need for voluntary agreements amongst relying parties, data subject, and an identity provider. The challenge is how to achieve this at a scale as large as the Internet. Two examples were given:
1. Scenario one included a states DMV as the IdP, a citizen as the data subject, and a bar as the relying party that authorizes an individual to drink at a certain age.
2. Scenario two was related to the credit card system with the banking industry as the IdP, the consumer as the data subject, and the retailers as the relying parties.
Both scenarios need to have a degree of accepted trust amongst participants.

It was highlighted that the goal s to make the trust framework interoperable, but it must be done incrementally by starting small. These arrangements may comprise of contracts between parties, a SLA, or other various options.

Several questions were asked during the session. Including:
What is the role of the auditor and who is watching the watchers?
How does a framework become enforceable?
These questions led to a discussion on privacy and how terms and conditions are generally in favor of the company because of the desired benefit of the service.

It was brought to the groups attention that a newly formed group, Customer Commons, is going to look at was to provide ratings for trust frameworks. This model would be based on the way Consumers Report gives industry and product analysis. The website should be up in approximately a week.

Questions left to consider from the discussion:
1. What would a trust framework look like from the perspective of the data subject (citizen, consumer, etc.)?
2. In relation to terms and conditions, are citizens competent enough to make educated decisions on

the services that collect data about them?

Quote of the session: “trust algorithms, not people”

Browser ID

Tuesday 2C

Convener: Ben Adida

Notes-taker(s): Sam Curren

The browser can help.
Developers need an email address.
Users understand email as a persona.
Devs like getting a verified email address.
Devs need to message users.

Going to impliment JSON* specs.
Js back off... Does nothing in the presence of native support.

Central dependancy disappears naturally as browsers add support.

Testing email ownership done currently by browserid.org, done later by email providers.

Eventually, ownership assertions will be short, relying upon webmail sign in to make it easier.

Browserid password is only temporary, till browsers support.

OpenIDComnect might be just as easy to build.
Convergence between these two?

Lets not kill each other for ‘not helping the main project’

Js shim for browser support is a good strategy being demonstrate.

Password antipattern, eliminating the password solution.

Recycled email addresses.

Multiple secondaries?
trying to avoid this.

What is the status of browserid browser?
Adoption of primaries is the biggest adoption issue.

Session Logging on to Windows 8 with Live ID

Tuesday 2D

Convener: Vicki Milton, Dave Hebert

Notes-taker(s): Dave Hebert

At Microsoft's BUILD conference a few weeks ago, the company announced that Windows 8 will have the ability to log a user on to Windows with a Windows Live ID.

Showed a quick demo of Windows 8 based on the BUILD conference "Developer Preview". The focus was on setting up and using user accounts on a Windows 8 PC.

- Logging onto Windows as before with domain-joined accounts
- Switching to another Windows account that uses a Windows LiveID (non-domain-joined). A consumer email account string can be used for logging into Windows account.
- This can be what Microsoft has called in the past an EASI ID, meaning you can use email accounts strings that are not ".live.com" or "hotmail.com". Account string is added as an ID in the LiveID system.
- Account credentials are not Open IDs.
- Identity is used to sync a range of settings (PC personalization, language, apps settings, app state [not app data], web account credentials and a range of device settings). These can roam across established trusted devices.
- Credentials associated with online accounts are encrypted and stored safely.
- Trusted Devices are devices the end user designates as such

For more information, look at the Windows 8 developer blog:

http://blogs.msdn.com/b/b8/archive/2011/09/26/signing-in-to-windows-8-with-a-windows-live-id.aspx

Layered Identity in Partnership Networks

Tuesday 2E

Convener: Justin Richer, (MITRE)

Notes-taker(s): Heather Flanagan

Tags for the session - technology discussed/ideas considered:

OpenID Connect; federation; collaboration

MITRE Partner Network - Justin Richer
Problem space = we have a social networking system on the DMZ where MITRE employees can log in, and external people can be invited ("handshake"), collaboration can happens; but all the external people coming need a site-specific user name and password to get in tot he site, so the question is how to get external people with their own credentials that are trusted at some level

this is something where a distributed and federated protocol fits the bill

GOAL of today's session: get the idea of this model out in to the community to encourage other companies to think about a better user experience for their collaborators and employees

Current concept is concentric rings of trust [diagram] = employees to trusted partners to invited partners to identified public; these terms are open to discussion
* employees = employees of MITRE
* trusted partners = organizations that MITRE has agreed to trust, have MoU or other legal agreements with to hold legally accountable for user actions
* Invited partners = employees have determined these people are the ones they want to collaborate with (and don't need to clear it with corporate)
* identified public = we know you are a person (probably), and (probably) the same person that came by last time with that pseudonym, and that's good enough; MITRE wants the info just to have some idea of who is using/downloading their docs

key design goals = the apps created by "shadow IT" should be equally supportable in the corporate IT world

Q: is this opensource or proprietary or both?
A: approaching it with the idea of making it as open source as possible, with the local proprietary bits being add-on's that won't be required for other sites to use it

OpenID Connect allows a very tight integration at the inner levels (employees, trusted partners), but also discovery and dynamic registration for outer levels (invited partners, identified public)

The whole enrollment process that depends on sending an email with the registration info and passwords is just a sad state of affairs, and yet it is explicitly trusted in today's systems; we must be able to do better than that and stop using email for identity provisioning

Q: why have more than 2 rings (employees/non-employees)?

A: Need a certain amount of granularity due to sensitivity of information; if you build something like this, you can build an interesting invite-gated community

Q: this model implies trust is reciprocated. At data access time is the data service responsible for obeying not only the individuals invite but also the company policy that may provide conflicting requirements?

A: the blacklist is underlying all of this, and it does not actually require reciprocation; that's the problem with SAML federations, that trust must be 2-way; MITRE doesn't want to require 2-way at all, want a model that allows the trust to just go 1-way

Q: how stable are these different rings? The outer ring looks like it can just keep growing, and proportionally the inner rings are smaller and smaller

A: NSTIC lives in the ink in the ring between trusted partner and invited partner; the diagram as it is right now is not the final answer, but it has holes and just starts the conversation

Q: this model implies that all employees have access to all the data

A: the model vastly oversimplifies the authZ model; there is a rules engine that must apply

Q: so why not just model it as groups?

A: because the venn diagram will make your head spin, an unreadable morass of endless circles; and note that access control does not need to be centralized, and arguably it would be better not to be

Q: in Handshake, do you trust domains for the trusted partners?

A: effectively, yes, but you still need a local-to-app username/password; trying to abstract out the user list from handshake so other apps can use it

Q: in terms of identity management, what happens when deprovisioning happens on the other side?

A: MITRE is thinking about that; use case of employee invites someone in, employee leaves, what should happen to the invited person? Lifecycle management is a big open question; also, what happens as employees leave, come back – what happens to their data? Their invites? Their profile? Also an interesting account linking problem

Q: this requires your partner(s) to be an OP, so what happens then?

A: yes, and right now, the partners usually say "OK, so what do I need to install, and what are your policies for access?"

If anyone is interested in participating in this effort of an OpenID Connect reference app, let Justin know

Pseudonymity, Reputation, and Real Names

Tuesday 2F

Convener: Dave Sanford, Kevin Marks

Notes-taker(s): Joe Boyle

Google+ "real" names controversy - "WASP names policy" (must "look like a name")
Kevin was involved with Portable Contacts - oops, it only had one name field. Flawed assumption because we started with address books - less true for profiles,
People want to be found => multiple names for searching connected to one identity
People want not to be found => multiple personas not publicly connected
Dave: Legal name is just one attribute - not needed for most stuff. But people need to develop reputation and therefore a persistent persona / identity, even when want it separate from legal identity.
High or low assurance - high more likely to use "real" credentials
Q: Why not one "real" identity and various pseuds linked by crypto. A: For a technical solution like that, questions like where does the linking take place, how hard is it to crack, etc. C: If linked at all then is vulnerable to govt e.g. subpoena.
@tariktech (CTO personal.com): We put a flag in the sand on some of these issues. We believe in user control and transparency to the user. Would pass a warrant on to the user.
Kevin: 3 or 4 layers of legal in US. Different in UK.
Rick Campbell: Identity can be just a public key, names just attributes attached to those via self-

signing, cert authority, etc.
Kevin: Credit databases are designed to correlate info with people who don't want to be correlated. They make DBs we create look robust.
Jay Unger: Pairwise pseudonymous IDs (PPIDs) Comment: But they haven't been adopted widely.
Bob Morgan: SPKI (Simple Public Key Infrastructure) 10 years ago, still complicated and not widely adopted.
Kevin: Currently widely adopted example is OAuth tokens, now bigger than any of the other crypto examples.
Dave: "Reputation demands linked pseudonyms"
Darius: (missed)
Phil Windley: Everyone's activity tends to link pseudonyms, making them useless
Comment: Face to face adds a degree of verification
Kaliya: People need pseuds for private life. Need something between pseudonymity and "real" identity: idea of Limited Liability Persona, that can have verifiability or reputation.
Jay Unger: A few attributes like first name, SSN, something else (place?) can identify 95% of Americans. Correlation is easy. Users have to trust system to do anything, currently don't understand system and give up privacy. Idea: Display some kind of metric on how identifying a query would be, so user can judge how privacy revealing. Change the exch mech between RP and IDP to enable this.
Kevin: When forced to fill out info, users give false info, so harvested data is often mostly garbage anyway
Sara Singlett: Even independent from need for privacy or strong pseudonymity, people have multiple reputations, reputations in different fields are fairly separate. Want persistent reputation per facet.
Dave: I am long time fan of open reputation framework linking sites in a given subject area.
Phil Windley: Glad to share Bibtech file of literature on reputation systems
?: Even when current RPs good on pseudonym portability they are not good on attribute portability
Phil Windley: "Bad reputations don't stick to cheap pseudonyms" because they're disposable. E.g. eBay doesn't want to make accounts hard to create to not drive away business => there are no active accounts with bad reputations Jay: I wouldn't buy from 100$ rep but month old. Rick: Wouldn't buy from 10y old but 3 transactions either
Kaliya: G+ is not allowing use of long-established (expensive) pseudonyms
Bob Morgan: Cites a system linking faculty members to all their publications etc. allowing easy evaluation by potential collaborators etc.
?: Cheap pseuds problem is only for mistrust. Flip focus to trust. Long-est pseuds Kaliya cited develop via natural usage not artificial tests.
Dave: for a federated reputation system, the member cites need reputations to be evaluated by too!
Kevin: Empirical answer used recently is binding to a name, statement, photo allowing other users to evaluate trust. Up to host to make sure those attributes non forgeable. Similar to real life evaluating people on face to face behavior. Purely machine system would be much more difficult / less good at evaluating.
Jay: RP convenience seems to outweigh user privacy. "I have very little sympathy for programmers"

Kaliya: Normal people give correlateable identifiers like phone numbers all the time. How can we ask services to not resell or correlate them and have some trust in that? Don't want norm to be selling everything. Tarik: Purpose binding. Rick: Seems like an impossible problem. Dave: Auditing doesn't scale. Jay Unger: Can audit at different levels - per transaction, per code version. Sammo: Need to make auditing actual behavior scale. Jay: Disagree. Kevin: Default is trust. Rich Goodwin: Also limit time data is retained. Tarik: Hard to insure over multiple systems designed for data retention, many don't use SSL. Rick: Difficult to prove you've deleted something. Rich Goodwin: Cites policies that service will delete your data on service termination. Tarik: 1/3 of Personal's codebase for is ensuring this stuff.

Developments in Drupal

Tuesday 2L

Convener: Judi Clark

Notes-taker(s): Judi Clark

General request for update on who's doing what that's compatible with Drupal.

Paul, Forge Rock, has done work with OpenSSO, OpenDS

Scotty, Stanford, uses two modules: weapon of mass destruction and a shibboleth module to deal with Drupal on campus and Drupal Gardens projects. Makes logins look like their webAuth, works with SAML 2.

Question about if drupal works with MongoDB: yes, Drupal 7 has a database module that does.

Question about presentation controls (UI) for graphic presentation of data: look to jquery for widgets and toolkits.

Isaac, Animate Login, described his drupal and android project to use QR codes on mobile phones to get away from password use.

Scotty briefly described his current mobile web project that resizes and reorients pages.

Of interest to a stealth brokering (authentication) project I'm working on, suggestions to look at these technologies:

- Microblogging APIs (including PubSubHubub) for notification of consent
- Telehash and evented APIs
- Pingback & Trackback models
- identi.ca and status.net, diaspora (host your own)

We started a Google Group to talk more about this. Join us if you speak this language!

Evented APIs

Tuesday 3A

Convener: Phil Windley, Sam Curren

Notes-taker(s): Judi Clark

From Kynetx session on Evented APIs: overview: when something happens, this function alerts or does some action. Sam's demo: new event consumer (account created), then form presented as event builder. Send (process) form as POST, JSON body or Get, then received event is displayed on a web page. Event consumer vs event generator.

So what? Phil's accounts: TripIt, FourSquare, and Expensify: how to mash up those three kinds of data sets? Open TripIt books a trip and opens an expense report, checking in with foursquare adds expenses–helps to orchestrate these events and consequences.

Semantics? Context is an important part of the picture. Event generators are going to be responsible for semantics, need consistency. Longer-term problem is, as a developer, need to map and look-up language to find mapping.

How does someone build an app around this? Anything that can receive a GET or POST can use this. Look at “If this then that” for wizard-like way of implementing. There may be reasons to encrypt return traffic or apply higher level security, can be added on top as function.

Per Site Account Chooser

Tuesday 3B

Convener: Eric Sachs

Notes-taker(s): Eric Sachs

Summary site: accountchooser.com

Main preso/notes: https://docs.google.com/present/view?skipauth=true&id=ajkhp5hpp3tt_97q7cw8xg7

More detailed notes and site for followup: https://sites.google.com/site/oidfacwg/

OAUTH Web Authorization

Tuesday 3C

Convener: Barry Leiba, Hannes

Notes-taker(s): Kent Landfield

The OAuth v2 draft has been approved by the working group is going thru final editing. RFC expected in Nov.

The working group needs to have a discussion on future work. This will require the working group to be re-chartered. It is hoped / expected that re-chartering will be complete by the end of the year.

Potential items to include in the next charter:
More token types, token revocation, token type negotiation, UMA, discovery, User interface extensions - more handshaking between OpenID and OAuth work expected.

Discussion of better documentation of OpenID Connect as it pertains to Oauth.

Bearer token request ? Standard identity token? Structured with OpenID Connect? Discussion that there is a OAuth document that may cover most of this.

Phil, Mike discussed - is another layer needed for technologies that are not OpenID Connect? OAuth would need to carry authentication information and that is something that has been resisted by OAuth in the past. The first step is a new use case document to be written. Phil - that is coming

Show of hands of the number of people not involved in IETF OAuth work. Approximately 50% raised hands. Do you want to be ? Some discussion of participation means with mailing list activity proposed as a first step. There was definitely interest in doing so.

Discussion of whether or not OAuth should take the OpenID token format work.

JOSE - Javascript Object Signing andEncryption has agreed to take some work (see list below of breakout).

OAuth will take the OpenID token format work.

Dynamic registration a topic that may need to be included in OAuth. If so, OpenID will use it.

The following table lists the agreement of OpenID needs and IETF WG support moving forward: Mike put this on the whiteboard.

JWT - JSON Web Token
OAuth
JWS – JSON Web Signature
JOSE
JWE – JSON Web Encryption
JOSE
JWK - JSON Web Key
JOSE
SWD - Simple Web Discovery
OAuth
OAuth Assertions (Token type agnostic)
OAuth
OAuth SAML profile (Use Assertions)
OAuth
Token Revocation
OAuth
OAuth JWT profile (Use Assertions)
OAuth

Token Revocation focus was on well behaving clients needing to release tokens
Response serialization format - expired draft ?

SCIM

Tuesday 3H

Convener: Morteza Ansari

Notes-taker(s): Kelly Grizzle

Tags for the session - technology discussed/ideas considered:

SCIM, Cloud, Provisioning

SCIM Overview

Discussions started around a year ago

Spec arose because most major cloud vendors have proprietary APIs for identity and group management

Currently close to 1.0 version working under OWF. Interop testing happening now.

Spec consists of a REST API, schemas for identity and group that can be extended. Core schema contains basic user and group attributes and an enterprise user extension.

Discussion of user IDs

User IDs must be globally unique within the service provider

Multi-tenancy can be handled by including tenant information in user ID or via the URLs for the REST endpoints.

Other similar schemas – OpenSocial, OpenID Connect

SCIM was based originally on PortableContacts.

There are small differences between the SCIM schema and existing specs, but the existing specs either had too much or too little.

It is alright to diverge from existing standards when use cases call for it (eg – enterprise vs. consumer, etc…)

We are open to input on how to make it better! Please join the discussion at http://www.simplecloud.info.

Who has signed on to this effort?

Salesforce.com, Cisco (Webex), Google, Ping, UnboundID, Technology Nexus, SailPoint, others

A goal was to keep it simple enough to drive adoption and achieve critical mass.

Group membership

Consider specifying information associated with a group membership (eg – your role with respect to the group – admin, etc…)

This concept makes a lot of sense with “collaboration groups”, maybe not so much with “security groups”

Mappings from SCIM to other schemas

Group is working on creating standard mappings between the SCIM user and group schemas to other schemas (eg – Active Directory, inetOrgPerson)

Next Steps

Wrap up draft 1.0 version of the spec within the next month

Not quite sure how to get this blessed by the larger community

BoF at winter/spring IETF?

Move to a standards body after 1.0 is complete.

Per-Browser Account Chooser

Tuesday 4B

Convener: Eric Sachs

Notes-taker(s): Eric Sachs

Main preso/notes: https://docs.google.com/a/google.com/present/edit?id=0AbCo72FjqHbUZGNxdGc5N3ZfMGhybng0Mmhx

Background information from previous session:

- Summary site: accountchooser.com
- Main preso/notes: https://docs.google.com/present/view?skipauth=true&id=ajkhp5hpp3tt_97q7cw8xg7
- More detailed notes and site for followup: https://sites.google.com/site/oidfacwg/

Identifying with Your Bank

Tuesday 4D

Convener: Sid Sidner

Notes-taker(s): Sid Sidner

Link to slides here:

http://www.slideshare.net/TooTallSid/iiw13-identifying-withyourbank?from=share_email

Killing Passwords

Tuesday 4G

Convener: Isaac Potoczny-Jones

Notes-taker(s): Isaac Potoczny-Jones

* Animate Login blog entry: http://corp.galois.com/blog/2011/1/5/quick-authentication-using-mobile-devices-and-qr-codes.html
* Animate Login web page: http://animate-innovations.com/content/animate-login
* Video demo: http://www.youtube.com/watch?v=omQu3KSsaPI
* Speaker: Isaac Potoczny-Jones, Galois http://www.galois.com

Passwords are past their prime. Users are buried under the weight of too many passwords, and most of us constantly struggle with these password conundrums: Simple passwords are easy to guess, but complex passwords are hard to remember. Writing passwords down means not having to remember them, but it also means they might get stolen. Sharing passwords between accounts means that if one account has a password database spill, all the accounts are compromised.

Animate Login replaces passwords with mobile phones and replaces typing passwords with scanning a barcode on that phone. The phone uses two-dimensional barcodes to make a link between the user's browser session and the physical presence of the user, then utilizes the phone's Internet connection to send a long and complex shared secret to the web site to prove the user is who he/she claims to be.

Animate Login includes three components: the protocol, the mobile app, and the server-side software. We have developed a prototype implementation of the system using Android. This approach can be deployed with minimal changes to web sites. In fact, in just a few hours, we were able to modify two popular open source content management systems to support it.

In this session, we discussed what's wrong with passwords, the Animate Login approach, the prototype, some vulnerabilities, and Isaac got advice from the room. At the end Isaac did a quick demo of the live system. Several people voiced enthusiasm and interest in the approach!

Some advice we got:
 * Consider going beyond shared keys. e.g. hash the shared key with a one-time session key
 * One of the user adoption problems will be that it needs to either be used by a lot of web sites or easily integrated with existing password management systems so that it's not a separate thing the users need to do
 * Similar to the above, consider this as a browser plugin

There will be a demo session Oct. 19, 2011.

Simple Web Payments (Oauth, OpenTransact, W3C)

Tuesday 4H

Convener: Pelle Braendgaard

Notes-taker(s): Tom Brown

Tags for the session - technology discussed/ideas considered:

Oauth, OpenTransact, OpenID Connect, W3C

acknowledged the "banking darknet"

legacy mindset is that payment is a message. In the web age, we can consider that payment is an asset instead of a message.

Even if banks don't implement opentransact, there is room for small companies to offer better services with it

OpenID Connect has all the facilities for making payments. See the standard spec.

tomorrow we intend to complete a first draft.

Why XDI is Needed?

Tuesday 4K

Convener: Mike Schwartz

Notes-taker(s): Mike Schwartz

Why XDI is needed?

It is too hard to secure data against use by the wrong people, and to share data with the right people.

It is too hard to use the Internet to make sense of data.

What new services would be possible if we had a secure, scalable framework for data sharing?

Security must also be portable / interoperable

XRI 3.0
Extensible Resource Identifier

XDI 1.0
XRI Data Interchange
Standard for connecting XRIs into meaningful graphs

XRI Summary:

Abstract identifier (not tied to network which is constantly changing)
Persistent identifiers issued by global registry under the management of non-profit: XDI.org

Example of XRI cross reference to URI: (http://www.gluu.org)

XDI Summary:

Graph data structure based on
Subject / Predicate / Object semantics:

Example: =schwartz/+age/(data:,41)

OpenXDI project: implementation of XDI 1.0 draft:

oxJava, oxRuby, oxJS : Native implementations of XDI standard

oxServer : J2EE server implementation: persistence (LDAP), messaging,

oxGraph : Visual tool for viewing, validating, and converting XDI

oxAuth : OAuth 2.0 Authorization Server using XDI graphs to persist tokens

oxTrust: UI for organizational IDP and trust network management

oxModel: REST interfaces to make it easier for app developers to build XDI enabled applications

Why XDI is a critical innovation:

1. To control data we need to be able to name it

2. Once we can name it, we need to be able to make sense of it

3. Once we can make sense of it, we need to be able to control access to

4. Level playing field / inter-operability

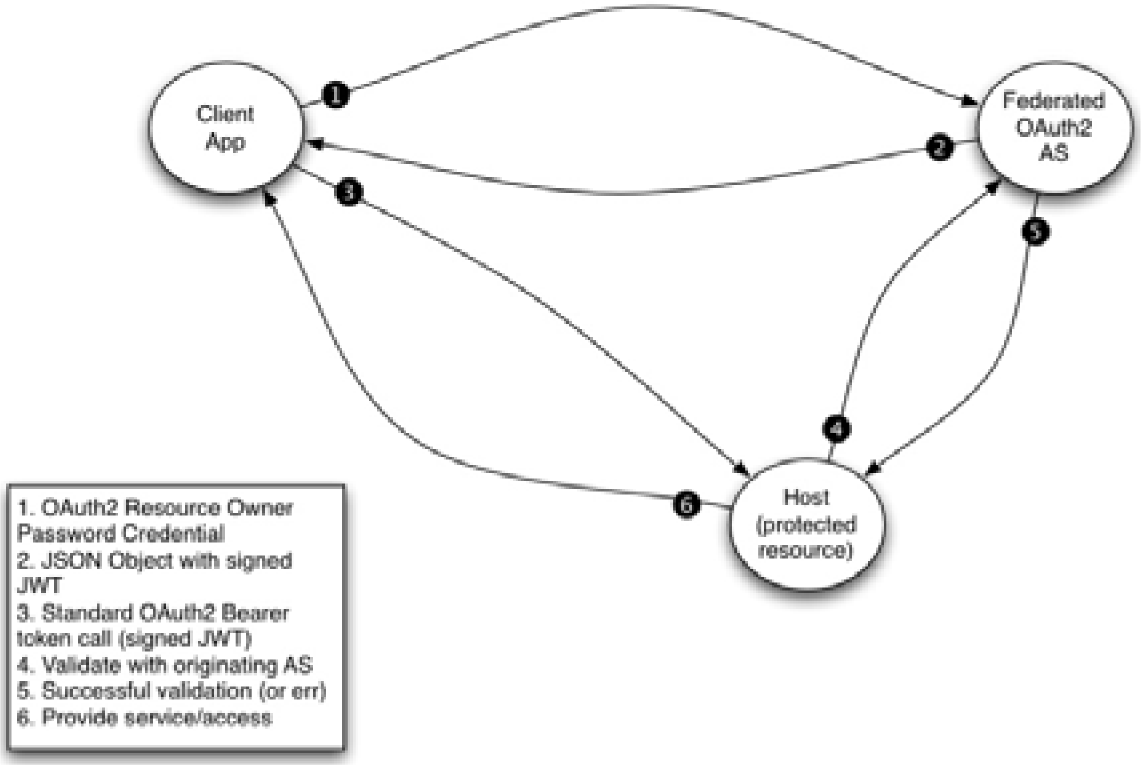
5. New service possibilities ! ! !

Federated Authorization with OAuth2

Tuesday 5A

Convener: George Fletcher

Notes-taker(s): George Fletcher


Client App
Federated OAuth2 AS
Host (protected resource)
1
2
3
4
5
6
1. OAuth2 Resource Owner Password Credential
2. JSON Object with signed JWT
3. Standard OAuth2 Bearer token call (signed JWT)
4. Validate with originating AS
5. Successful validation (or err)
6. Provide service/access

Overall flow for supporting Federated OAuth2 tokens

Enabling support of federated OAuth2 tokens comprises three main steps: 1. Get an OAuth2 token from the user's Authorization Server 2. Present the token to the federated resource server 3. Federated resource server validates the OAuth2 token with the token issuer

Step 1: Get an OAuth2 token from the user's Authorization Server (OAuth2 Resource Owner Password Credential flow)

POST /token HTTP/1.1 Host: as.oauth.example.com Content-Type: application/x-www-form-urlencoded

grant_type=password&client_id=s6BhdRkqt3& username=johndoe&password=A3ddj3w&scope="user-info"

Step 2: Receive token response from Authorization Server

HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store

{

"access_token":"ewogaXNzIDogaHR0cHM6Ly9hcy5vYXV0aC5leGFtcGxlLmNvbSwKIHVpZCA6IGJzZHNhc2RmOGFhZmhzc2Q5ZGZnaHNzZGZncywKIGFjY2Vzc190b2tlbiA6IGFzZGZhZXJnMmdkZGYzNDY1MzV0d2RmZ3c0Nndnd2V0MzQsCiB2YWxpZGF0ZVVSTCA6IGh0dHBzOi8vYXMub2F1dGguZXhh

bXBsZS5jb20vdmFsaWRhdGUKfQ”,

“token_type”:”bearer”, “expires_in”:3600, “refresh_token”:”9as23fvsdf34t”

} Step 3: Present access_token to federated protected resource (host)

GET /api/myService?params=asdfasdf&... HTTP/1.1 Host: resource.example.net

Authorization: Bearer
ewogaXNzIDogaHR0cHM6Ly9hcy5vYXV0aC5leGFtcGxlLmNvbSwKIHVpZCA6IGJzZHNhc2RmOGFhZ
mhzc2Q5ZGZnaHNzZGZncywKIGFjY2Vzc190b2tlbiA6IGFzZGZhZXJnMmdkZGYzNDY1MzV0d2RmZ3
c0Nndnd2V0MzQsCiB2YWxpZGF0ZVVSTCA6IGh0dHBzOi8vYXMub2F1dGguZXhhbXBsZS5jb20vdm
FsaWRhdGUKfQ

Content-Type: application/x-www-form-urlencoded

Step 4: Validate OAuth2 token with token issuer

POST /validate HTTP/1.1 Host: as.oauth.example.com

Authorization: Bearer
ewogaXNzIDogaHR0cHM6Ly9hcy5vYXV0aC5leGFtcGxlLmNvbSwKIHVpZCA6IGJzZHNhc2RmOGFhZ
mhzc2Q5ZGZnaHNzZGZncywKIGFjY2Vzc190b2tlbiA6IGFzZGZhZXJnMmdkZGYzNDY1MzV0d2RmZ3
c0Nndnd2V0MzQsCiB2YWxpZGF0ZVVSTCA6IGh0dHBzOi8vYXMub2F1dGguZXhhbXBsZS5jb20vdm
FsaWRhdGUKfQ

Step 5: Validation response from token issuer

HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store

{ }

“uid”: “bsdsasdf8aafhssd9dfghssdfgs”,

Step 6: Return requested resource or service. Response is resource/application defined

Possible structure of the Signed JWT returned as the OAuth2 bearer token in Step 2 {

“iss” : “https://as.oauth.example.com”, “uid” : “bsdsasdf8aafhssd9dfghssdfgs”, “access_token” : “asdfaerg2gddf346535twdfgw46wgwet34”, “validateURL” : “https://as.oauth.example.com/validate”

}

Instead of requiring the host (protected resource) to validate all federated OAuth2 tokens with the token issuer, it’s possible to use short lived signed JWTs (JWS) that can be validated locally by the host. Determining which model to use depends on the risk profile of the use case being implemented.

The Role of State Government (data, policy, operations)

Tuesday 5B

Convener: Dave Burhop

Notes-taker(s): Dave Burhop

Tags for the session - technology discussed/ideas considered:

- How involved should state government, especially DMV’s, be in identity proofing…is their mission changing?

- Should state governments design their authentication systems with a national framework in mind?
- Using what technology?
- What are the policy implications
- Economic incentives?

- DMV’s have the most relying parties for their credentials
- Identity “proofing” is currently done by many different types of organizations who can’t detect fraudulent credentials
- Aspects of the federal Real-ID act actually provides a stronger position for states to perform identity proofing
- Perhaps a central entity like the American Association of Motor Vehicle Administrators (AAMVA) could facilitate a federated model across state DMVs similar with what they do for other systems (commercial drivers)
- Virginia cited by the feds (study done on all states) as having a 16% error rate in its healthcare eligibility databases
- The Commonwealth of Virginia recognizes the value of their DMV proofed records in combination with other agency’s records that forms an enterprise data management (EDM) model. EDM can be used to ensure a person is who they say they are and can be used by all state agencies resulting in reduced fraud and identity errors.
- Virginia to be authenticating both individuals and organizations through their Commonwealth Authentication Services (CAS) system, which they’re currently developing, in preparation for general healthcare eligibility requirements and Virginia’s Health Information Exchange (HIE) program
- Virginia is trying to get other state DMVs to consider this change in their fundamental mission – the certification that a citizen can safely operate a vehicle while also certifying that the person is who they say they are

Smart OpenID, SIMcard based OpenID; what can Mobile carriers bring to OpenID?

Tuesday 5D

Convener: Andreas Leicher

Notes-taker(s): Andreas Leicher

Tags for the session - technology discussed/ideas considered:

OpenID; SIMcard based OpenID

presented a concept which allows Mobile Carriers to be attribute and identity providers by leveraging the security and authentication infrastructure they already have

Mobile carriers have some identity information that they might want to monetize, e.g. verified address etc.

Mobile carriers also have some good and secure authentication system in place, especially with the SIM card.

What if the SIM card can be used not only to authenticate the device and user but be enhanced to host an identity provider instance which allows users to create identity attributes and sets of claims, based on the verified identity information from mobile carriers?

Smart OpenID is about creating an instance of an OpenID identity provider on the SIM card on the mobile device, allowing the user to authenticate towards services and share identity attribute data with services.

The mobile network carrier is not involved in the exchange of this attribute information, so a level of privacy towards the mobile carrier is created.

slides will be made available at http://smartopenid.novalyst.de/

OpenID Connect Client Registration

Tuesday 5G

Convener: John Bradley

Notes-taker(s): Justin Richer

A change is being made to the OpenID Connect Dynamic Client Registration to make the client registration endpoint an optionally OAuth2-protected resource. With this change, there are no other anticipated changes required to support the use cases brought about by UMA's initial dynamic client registration draft.

The UMA Working Group may consider using the OpenID Connect dynamic registration proposal for generic OAuth2 client registration.

A Contrarian's View of Identity: Only Real Names

Tuesday 5H

Convener: Heather Vescent

Notes-taker(s): Heather Vescent

Blog post found at:

http://www.heathervescent.com/heathervescent/2011/10/a-contrarians-view-of-identity-only-real-names.html

A Contrarian's View of Identity: Only Real Names

When I was at IIW earlier this week, I held a session called, “A Contrarian View of Identity: Envision a World with Only Real Names.”

The ground rules of this session were:

- There is no discussion. We are starting with the assumption that real names are the only reality.
- No dystopian or negative perspectives (relieved this for last 5 minutes of info gathering)
- I then asked those in the room to close their eyes. Take a deep breath. Envision all of the identities that you use online and out in the world. See them moving to the middle and coming together, becoming one identity, and that name is your real legal name. If there is any negativity coming up with this, just put it aside for the moment. Sit with this vision of your identity as your real legal name. Take another deep breath. Pause. Now open your eyes.
- Here’s what we came up with.
- Make it easier to decide what I won’t do online, simplify decisions
- Stop doing things on line.
- I changed my name to one I like.
- Transparency: More empathy because I see you
- Easier to find connections between people and create opportunities, because you see all capabilities. E.g. not only limited to see me as someone who just does this...
- People would be nicer to each other if tied to a single ID.
- Alleviates Simplifies – don’t have to manage multiple personas don’t have to know the context of relationships.
- Better connected to the real you – See multifaceted people.
- Less Victimization, but sociopaths will always be sociopaths. There could be the chance that some people could really hurt and manipulate people.
- Sociopaths will not stop/be deterred, people will find easier victims.
- ** More protections for our privacy because we are more vulnerable. It’s an everyone problem so maybe governments act more.
- If you can tell who I a:
- easier to vote with the internet
- eliminate Fake Public Policy Groups
- literally find people easier (physically)
- You own you -> others can’t impersonate you, lie about you as easily, harder to be impersonated, defrauded, protected.
- Better connected to your history. (could be a pro or con)
- Short Term vs. Long term effects (e.g less watching porn but ok to watch porn no stigma)
- There would be fewer IIW Working Groups because Less work to do, save work.
- Reaching your full potential w/o being able to explore ID. I would not have reached my human potential if I had not been able to explore with various IDs, even though I may not have/be/use them anymore.

- Highly repressive governments would have a much easier time.

After 15 minutes of information gathering, I released the “No dystopian or negative perspectives” rule and all comments were welcome.

After the session, one person remarked that by requiring us to start with positive perspectives, we came up with some really interesting and creative responses. (That was my goal. ;)).

I highly enjoyed taking on the contrarian view of Identity. It was refreshing to put my judgements and assumptions aside and try on a new, usually discarded view. Everyone who participated found the session highly interesting and at least one person mentioned they were going to try this technique with other topics. I found it a great way to see around my blind spots.

Sneaky Bastards

Tuesday 5K

Convener: Renee Lloyd

Notes-taker(s): Judi Clark, Joseph Boyle

Judi’s Notes:

Renée Lloyd’s talk on how VRM disrupts and liberates legal practice. VRM challenges how legal practice is executed. What if new businesses had to negotiate with her? What messages are people giving us? Agreement making in a human style: sharing thoughts, contextual, ceremonies and expressions vary. Contrast: agreement corporate style (hand cuffs, “None are more hopelessly enslaved than those who falsely believe they are free.” -Goethe)

Clickwrap “agreements” are what we call Contracts of Adhesion: no negotiations, take it or leave it. Should not be assumed that we always want a fast track. Look especially in employment contracts, very restrictive. Makes sense in certain contexts but should not be a universal solution. Even if you’re the 800 pound gorilla, you don’t always have to act like one. The processes are insidious, things start small but quickly spread into areas where it’s impossible to right any wrongs.

Lawyers use existing terms from contracts to create new, limit liability. Nothing new: no innovation is allowed (social media prohibited). Caveat emptor: problematic because consumers can’t “be aware.” FTC expects that markets create innovation, expected that it will help protect. But no plain english rules, effective regulation that’s reactive (because bad things happen) produces unworkable constraints and rules. System is out of balance. “No number of legal victories, tech tools or whitepapers–however well-intended or important–are going to convince people to take ownership of agreement-making back from lawyers and companies.” It’s about people, not lawyers. We need to bring the balance back, help people to take ownership.

Time for a change of attitude! What do you do when the most economic solution is a data exploiter for the big companies? What if there was a trusted voice? For example, what if the Terms of Use on a site, instead of the pages you see now, told you this (video) [x] Cede your rights? No site has fair terms right now. Or what if you had a “sneaky bastards” prompt that took your selected text, marked it up, turned it into a visual games? (Sue for emotional distress: Amazon’s terms at 80 pages and Renée didn’t have it all, PLUS they can change those terms anytime. Outrageous.) Activities to bind parties, even if they don’t understand, includes individual initialing every page. New advice in legal community is to make it clearer that they knew. Relaxed formality standards.

ThoseSneakyBastard.org – starter site with Renée's rants, hall of shame, hall of fame, etc. Learning, doing, kicking butt, giving props, pure ferocious fun! Data on collaborative law shows less law suits in case where people/individuals are consulted about change. Innovation: minimum viable contracts, curate, track and assess new contract models, etc. Check the site for things to develop.

Joseph's Notes:

Agreement making human style has ceremony Not just writing down documents.
Agreement corporate style - pages of fine print (overlay with pic of handcuffs) "None are more hopelessly enslaved than those who falsely believe they are free" -Goethe
Clickwrap "agreements" are called "contracts of adhesion" - no negotiation, take it or leave it
Has there been any pushback from consumers? 2nd Life case where user had invested a lot in their site. Court threw out mandatory arbitration provision as unconscionable.
What happened was b2b lawyers defining the new b2c world. It's normal now but also insane and bad for business.
Scott David: "Caveat emptor" is fine when buyer population is capable and empowered, less so for atomized individuals.
No number of legal victories, tech tools or white papers are going to convince people to take ownership of agreement making back from lawyers and companies.

Idea: Addon to highlight agreement text to show provisions that are sneaky. Gamify it!

[Forgot to take notes after this point - Renee's presentation was too good - post it on the wiki!]

PDEC Legal Advisory Board

Wednesday 1A

Convener: Mary Hodder, Judi Clark

Notes-taker(s): Markus Sabadello

PDEC's mission:

There are different efforts + projects. As a consequence, there are also different local perspectives.

PDEC's desire is not to build any concrete things (trust frameworks, technology, etc), but:

- to coordinate existing efforts, and help finding each other
- to follow, track and educate about existing efforts and different views
- to facilitate dialogue between the actors
- to support new startups/initiatives to realize the vision
- to bring together sociologists, technologists, lawyers, etc. working on personal data
- to include people who are new to the circle but doing related work

Some concrete topics during the session:

- multi-jurisdiction issues

- multi-disciplinary groups with interdisciplinary focus

- defining the new business layer (not just legal layer)

- common elements of a trust framework

- technologists (want to push things forward?) + lawyers (want to push things back?) need to work together!

- how do we represent individuals?

- legal practice becomes law

- role of regulation (managing risk)

- look at existing regulator models for telecom + postal interop

- what is institutionally required for certain services + systems

- what can individuals do? where are groups + capital required and where are they not required?

- relationsip of IdPs to each other and to nation-states who set policies

Kaliya presented the "Personal Data Ecosystem Landscape" diagram explaining the conceptual relationships between different parties in the PDE.

NSTIC Update

Wednesday 1D

Convener: Jeremy Grant

Notes-taker(s): Iana Bohmer

IIW Update: National Strategy for Trusted Identities in Cyberspace (NSTIC)

Jeremy Grant

This session consisted of a presentation by Jeremy Grant and a Q&A period.

Overview of NSTIC. Focused on establishing a framework for trusted identities in cyberspace. Calls for the creation of an Identity System in accordance with the Guiding Principles established in the NSTIC Strategy.

NSTIC Governance Notice of Inquiry (NOI) Responses. Department of Commerce received 57 responses to the NOI covering areas related to NSTIC governance: initiation of governance group (Steering Group), governance structure stakeholder representation and international participation.

- Government position that the Steering Group must led by private sector, not government.
- Comment period was originally through the end of July, but was extended through August.
- Responses ran the gamut from large companies to individuals.
- One area in which the Government wanted input was as to whether an existing organization

should be leveraged to serve as the Steering Group or whether a new organization should be established. The overwhelming response was that a new one should be created.

- Another item around which questions arose was as to whether FACA would apply, however, the NSTIC National Program Office (NPO) has clarified that the Government is not requesting advice or recommendations from the private sector, but rather is looking to facilitate a partnership with the public sector in which the private sector takes the lead in developing the Identity Ecosystem Framework.
- There were many recommendations regarding the structure of the Steering Group. Common themes were that the Steering Group should have a "light touch"; that it should seek to work with existing trust frameworks (rather than re-invent); and that the Smart Grid model should be leveraged to the extent possible.
- Funding of the Steering Group was another issue on which respondents provided comments. In general, the consensus was that the Government should pay or at least partially subsidize the formation of the Steering Group.
- There were numerous comments regarding advocacy of the individual. What was gratifying was that not only advocacy groups, but also respondents from large organizations insisted that the interests of the individual must be put front and center.
- The necessity of allowing everyone to participate in the Steering Group also was a common theme – there were many recommendations regarding the use of technology tools to achieve this balance, e.g., virtual meetings, webcasts, etc.
- Finally, with regard to international coordination, the consensus is that NSTIC/NIST needs to look beyond the US border and leverage international standards bodies – the Identity Ecosystem can't be developed in US-centered vacuum.

What are We Doing Next? NSTIC NPO will be publishing a paper with recommendations and draft charter within the next couple of months. The paper must go through the government vetting process which is what takes time because it has to go through multiple government parties.

- What can be said at this point is that there are many consensus points from the NOI responses and the recommendations paper can be expected to be in line with those responses.
- There were numerous comments regarding how NSTIC should use the Smart Grid model as a starting point because of its mission to establish standards for interoperability. Nonetheless, Smart Grid is dealing with interoperability standards for the electric grid with a limited number of stakeholder groups and a narrower topic. For identity, there are many more stakeholders with the individual at the center. Therefore, NSTIC can borrow some aspects of the Smart Grid model, in particular those aspects that serve to catalyze the formation of a public private partnership.
- Much of the near-term activities of the NPO will be dependent on funding. Although the House did not include funding for NSTIC, the Senate agreed to $24 million. NSTIC expects to have the resources to move forward, but they have to wait for the formal channels to work their way through.

OMB Memo of 10/6 on Externally Issued Credentials. Recently the Federal CIO – Steve VanRoekel issued an OMB memo regarding government policy on externally-issued credentials. The memo basically says that any new government website has to give the public the option to log in with LOA 1-approved credentials. The government is also reviewing the acceptance of LOA 2-4 credentials recognizing that government websites need to be able to accept these higher levels of assurance and thus align with FICAM. OMB has a strong control mechanism related to these policies because they approve the budgets of the agencies.

- A key role for the Federal government will be to act as an early adopter. In a 10/14 White House blog post from Howard Schmidt, he says that NSTIC is helping to drive the concept of an individual having a single credential to access government areas and services.
- WhiteHouse.gov will be the next site to accept externally-approved credentials – by the end of the year.
- A problem in the private/commercial sector is that they have expended a lot of resources to comply with government identity standards and get certified and yet few agencies accept these credentials.
- In the government agencies, the most interest lies with LOA 2 and 3 credentials, especially 3. Soon GSA is expected to have an approved LOA 3 service provider.

Inception of Pilots. Of the requested $24.5 million for the budget, $17.5 million is expected to be for funding pilots. The NPO has heard from numerous organizations with ideas for pilots.

Upcoming Events:

- Dec. 8-9: meeting on Privacy-Enhancing Cryptography at NIST; already a high level of interest.
- ID Trust: March 13-14, at NIST

Questions

What is the Government looking for in pilots?

- Government wants to know whether there specific technologies that are partially done but need to be tested and work for NSTIC guiding principles. New and promising approaches.
- Government is looking for cross sector pilots that could demonstrate NSTIC – multiple credentials working with multiple relying parties.

Where does the Government see ID proofing taking place?

NSTCI doesn't prescribe business models. Although most models have ID proofing at the IDP, NSTIC is not adverse to other models as long as they align with the NSTIC guiding principles.

Are pilots meant to serve as a test bed?

Yes, but also to serve as a foundation within the Identity Ecosystem. The government will publish pilot criteria once funding becomes available.

What is the handful of killer applications for NSTIC at government agencies? Can you talk about them?

Examples:

SSA – Because of the cost, SSA wants to stop mailing out yearly benefit statements, but they need to have an online solution that is more secure than ID/passwords

VA – Need to provide benefits and access to health records and placement services but they don't have an effective and secure method of authentication.

IRS – Faces a number of challenges regarding what information can be provided on line. They have experienced identity theft related to online tax filings.

Does NSTIC have influence for speeding up the FICAM trust framework process?

In the immediate term, no, but in the long-term, maybe. The Government recognizes that there has been a great deal of frustration in this area and it looking at options to address the process.

How can we be sure that "this time it is different" – that the government won't come up with a new concept, companies will spend a lot of money to implement, and then the government won't use the solution?

This time we have the strong participation of the Executive Branch. Also, the government is going to act as Government has to be an early adopter and can't "pull the football away" again. White House involvement will ensure consistent follow through – it will bolster all the work that has been done by NIST, GSA, OMB over the last several years and put pressure on the agencies for adoption. In addition, the NPO will leverage NSTIC to encourage agencies to become early adopters.

How bi-partisan is the support for NSTIC? How about election?

Yes, there is bi-partisan support. Although the Chamber of Commerce and Administration don't always see eye to eye, on the identity issue, they do. And, there is Congressional oversight over NSTIC. The NPO has briefed the oversight committees on numerous occasions.

How many IDPs are signed up/accredited from the private sector?

There are 5 signed up and one in the queue to be accredited. The Government has seen a lot of support for the process from companies that have come to visit the NPO. The accreditation process will be an issue for the Steering Group to decide. NIST is statutorily bound to look at external standards that are developed rather than develop them in the Government.

Has there been any demonstrated interest in NSTIC on the part of Relying Parties?

Yes, but not enough and this is largely because of where we are right now and the Steering Group has not yet been established. The Chamber of Commerce has been asked to assist in reaching out to Relying Parties.

How will the Government address the asymmetry between IDPs and RPs, i.e., monetization in the private sector? What about liability allocation and rule-making for when things go wrong?

All these issues will be addressed in the Steering Group. The NIST NPO will be issuing a recommended charter to catalyze the discussion.

Will Government involvement minimize the voluntary element with all this process?

The voluntary aspect is embodied into the Guiding Principles, so no, the Government will always stress that participation is voluntary.

How is the Government going to convince the Relying Parties that there is a business case in their participation?

There is a gap between the Government's belief in the value proposition to the private sector – both IDPs and RPs – particularly when the agencies often don't end up using these services. The community needs to develop a business model and economic plan so that it is made clear exactly what is expected and what can be expected from those participating in this business. An example has been for those working on FICAM – to date most private-sector participants have realized little profit on its implementation.

Has the Government established any policies on privacy for the Identity Ecosystem? Are the privacy issues on hold until governance/Steering Group is resolved?

NIST held a workshop on privacy in Boston on June 27-28. Currently the NPO has limited resources and is working on foundational governance issues that need to be resolved before addressing privacy. There are 3 people on detail at the NPO who are looking at the privacy issue. The NPO intends to hire a chief privacy officer once funding becomes available.

What will the role of the Steering Group be vis-à-vis the Government¤s role?

The Government's role will be to establish the Steering Group both with initial funding (pending funds availability) and assisting in its launch.

Is NIST going around FACA by calling this organization a steering group?

No, the Steering Group will not be an advisory board to the Government.

Will the rules or guidelines that emerge from the Steering Group be preferable to existing laws?

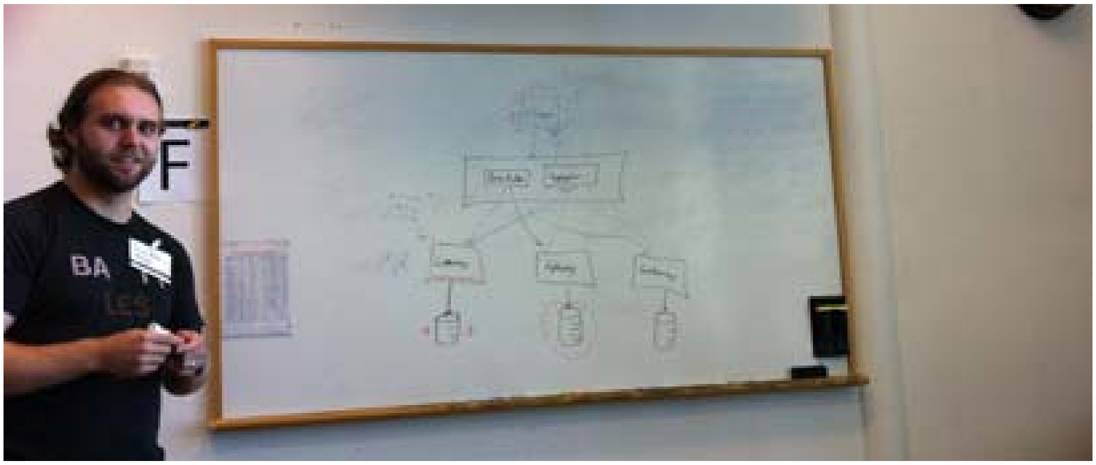
There are no real laws that exist in this area, particularly around privacy. Although the Government is not ruling out the need for new laws, the expectation is that a set of commonly agreed-to rules may alleviate the need to create new laws.

hQuery

Wednesday 1F

Convener: Justin Richer (@zer0n1ne)

Notes-taker: Eve Maler (@xmlgrrl)



Justin advertised this session as trying to “hit the problem with the OAuth hammer”! The goal is to see if OAuth provides the right access management framework for tackling this problem.

Introducing the hQuery project (http://projecthquery.org/), part of the Query Health initiative (http://wiki.siframework.org/Query+Health), run by ONC (the Office of the National Coordinator for Health Information Technology). MITRE has come up with a system that allows distributed queries across health info. There are lots of privacy concerns, data security concerns, and distributed access concerns.

The idea is that you put together a query on the client side, e.g. how many people are between the ages of x and y, how many people are taking a certain drug, etc. for epidemiological survey purposes, demographic studies, and similar. This data exists in many places, but we can’t just have people all the data everywhere, even if it’s somewhat de-identified. It can be deanonymized too easily.

You want to be able to make the query very specific and complex, across a variety of data sources. The sources need to toss their results back to an aggregator. It should be possible to keep the query results updated too. And it shouldn’t be possible to query for data about what amounts to a single known person who can be identified (like Lady Gaga or George Clooney, or even a not-famous person in a small town who’s well known, there, to have HIV). Correlation over subsequent data cuts could deanonymize pretty handily.

The demographic goal of Query Health is different from patient care systems, which do need individual patient data access. Project hData is more about electronic health care records, and it’s using things like UMA to manage access by various healthcare professionals.

For Query Health, you need to think beyond SQL. The client generates a query and sends it across a query network. Is this a map-reduce pattern? This is how they've happened to implement it, but this isn't a formal program decision at this point. The theory is that map-reduce has fewer constraints than a formal query language. The working group is likely to offer several different query paradigms. There's been discussion of rules-based forms and SQL-like forms.

The health data world likes to invent their own stuff -- off-the-shelf solutions are often spurned because "people could die". So the architecture to date is somewhat ad hoc with respect to security etc. Justin's work involves applying RESTful patterns and OAuth2 to enable better access control.

The query builders send the query out to known endpoints representing standardized RESTful gateways to data sources. The aggregator knits together all the results, even if they're very disparate in nature. Query results could come back at wildly different times; it can't be synchronous. So it's not a single HTTP transaction or socket connection. It's basically a batch system that's designed to tolerate eventual consistency. There's no blocking or crashing on lack of results from one source, though the querier is informed which sources haven't contributed. Queries can last forever or be time-limited. Eventually, the client gets a result that can be used in writing reports and so on.

The trust is managed through joining, e.g., the CDC trust network and living up to their constraints. The authorization server is some trusted party that could live at the gateway level, the query builder/aggregator level, or even a third party that's trusted. The resources are OAuth-protected at the RESTful gateways.

Who pays the cost of performing these potentially expensive queries (effectively DoS, whether malicious or accidental)? That's a simple matter of sysadmin. :-)

Likely each organization that runs a query builder/aggregator will offer its own client app.

There's the client, the local access point, the trust network association (AS), and the data/gateways/PRs. Wouldn't the gateway want to audit who gave access (which AS)? This is where the AS/PR separation becomes important. It was noted that UMA formally separates ASs and PRs, and provides a way for them to build mutual trust in the context of a particular user. Or in a purely pairwise fashion, they could use JWT keys and dynamic discovery to bootstrap trust-building.

Query Health should look at the DURSA from NHIN (http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_849891_0_0_18/DRAFT%20NHIN%20Trial%20Implementations%20Production%20DURSA-3.pdf) for trust relationship building.

Or the query builder could naturally serve as a discovery service for finding the relevant data sources. This would be a good idea to consider. Since this network is not meant to be open to the public, there are optimizations that could be applied.

Are there always four parties, or are there multiple ASs and other nested relationships? Would opaque tokens continue to work if you received an opaque token in and need to validate it but don't know which AS issued it? Perhaps the scope in the header could say which AS issued it, by agreement.

The counterproposal that has been made is to use persistent direct two-way TLS connections between TCP sockets. You could even use SSL JDBC connections! But that seems very tightly coupled. You could have possibly millions of data sources, and the gateways are likely to be run by smaller institutions.

So the AS seems to be an important role, akin to a CA in the "old world". Certificate revocation lists will tend to weight heavily on the overall cost of the system, as always.

How important is it to make the contractual relationships more flexible? The query builders/aggregators could get no permissions on their own, other than what the client allows them to have. Once there's an authorizing user who operates the client and can accept liability for the connections they're forging, this is where UMA's phase 1 potentially gets more relevant.

If each gateway had its own unique set of scopes governing its data sources, maybe the client would have to ask the query builder to go off and figure out what scopes will be needed, before actually making the query of it.

Can the client can be simply an OAuth client?

The personal health "bank account" model, like Google Health's model, is starting to gain favor with HHS. This is more like hData (for which see a potential protection model here: http://kantarainitiative.org/confluence/display/uma/hdata_scenario). If you used these as data sources, what do you do about the duplicate-record problem? Actually, you have this problem regardless. "GIGO." If you could fix this, you'd be linking data records, which violates privacy.

The health vaults are often operated as cloud services. Some of these are state-run.

It might be worth looking at Medify.com (https://www.medify.com/), which is taking something like this public-data approach, for individual people.

The gateway itself is having to be trusted to see the raw data from the data sources, so there are sandboxing requirements even at that level, and potentially even something like certification for those parties. If you accept such risk, there's a business opportunity for being paid to take on that risk. Thus, the gateway is where the business model opportunity lies.

If SWD gets used, it would be for initial bootstrapping, but then there are "semantic" aspects of discovery around finding which gateways offer which data sources that would be needed to satisfy the query.

The emphasis in this whole project is IETF-like: rough consensus and running code. There's also the NHIN Direct project. MITRE and Microsoft are both involved in the Query Health initiative, which is helpful for ensuring we don't have totally opposing approaches; likely a blend would be best. hQuery is being run as an open group, so interested parties can get involved pretty easily. There's a F2F being held in DC this week.

OpenTransact Spec Session

Wednesday 1H

Convener: Pelle Braendgaard

Notes-taker(s): Tom Brown, Nov Matake

Tags for the session - technology discussed/ideas considered:

oauth, opentransact

this was a long session for the purpose of producing a first rough draft which was completed during the day and can be found here: http://www.opentransact.org/core.html

we considered different kinds of requests, vocabulary and specifics (such as receipts).

We also discussed 3 flows:

1. transfer request (fetch payment form)
2. transfer authorization (single use oauth token)
3. transfer (post payment)

XDI Link Contracts

Wednesday 1K

Convener: Mike Schwartz

Notes-taker(s): Joe Savak

The internet is broken

- URIs are not persistent.
- XRI is an abstraction layer on top of URI. Resolving an XRI will get a URI.

Internet != Web.

Internet needs a better infrastructure for naming to secure data. It wasn't designed for security. It's hard to make sense of the data on the internet.

Security must be portable and interoperable.

XRI 3.0: extensible resource identifier. New standard

XDI 1.0: extensible data

Who maintains registry: Neustar keeps names to identifiers persistent.

IName = !gluu assigned to INumber = @!DA….

IName could be @gluu, @gluu*mike; =Schwartz.

Parentesis around URI cross references it for XRI

XDI says if we want to represent personal data, we can do it in multiple ways. Need to put data in the right way in the first place. Graph gave us the most flexible system to ask the hard questions.

XRI are the points. XDI connects these points to make a graph. Ex: =schwarts/+age/data(+41)

Semantics – allows interdomain security. Semantics delayed the spec for years.

Hardcoded security rules in social networks – previous standards not good to help people make their own rules. Working with IDQ at MIT for declarative security.

OxGraph – browser for XDI (produced through openXDI) – create memory model for XDI to prove the spec.

OpenXDI project:

- language bindings
- Server (J2EE/LDAP)
- oxGraph
- oxAuth: oauth 2.0 authZ server using XDI graphs to persist tokens;
- oxTrust: UI for org IDP;
- oxModel: ReST interfaces

XDI 1 standard; XRI 3 is ready to go. Need to get it to OASIS. Need funding to write standard.

White listing in XDI? –

When you make an XDI message from a client to a server, need to reference link contract (XRI address) and must be pre-specified (or can do discovery). The other thing it'll look for is an access token. XRI registry would return service endpoints originally – but this point we resolve to URI and can use XDI to query for authN preferences.

XDI for Mom & Pop shops?

No – initially it should be for businesses – but it really isn't that complicated.

The architectures that arise organically from XDI/XRI could become complicated. Maybe the right tools would help. Allowing someone to write rules right for them is powerful. What likelyhood near term for XDI?

MIT was interested in this project – it's a framework really right now. The current solutions are complicated themselves. Really we need to spread the word and get people more familiar with it to make it simpler. XDI/XRI isn't really that hard.

We just need to hide it from the user more.

Users aren't even using the ReST interfaces. Tools to write the rules instead of writing rules themselves. Graphs can be made, but making it easier for users to make the graphs is a harder problem. Even app developers wouldn't make the graphs. They will be using the ReST interfaces to make the graphs.

Technology Solutions for User Attribute Control (W2B)

Wednesday 2B

Convener: Naomi Lefkovitz

Notes-taker(s): Judy Spencer

Tags for the session - technology discussed/ideas considered:

Privacy Provisions in Trust Framework Evaluation; User Control; Opt-in

Current technology solutions don't allow user control of what attributes provided to a reying party □ or there is no granularity allowing users to select which go over.

Info card would permit this – but not really a player anymore.

OpenID had this at one time but found users got confused and completion rates dropped.

The market wants correlatable identifiers so producing an environment where users decide is contrary to market acceptance.

Is the application of a 'TrustE' type of certification to ensure no misuse of information pertinent?

Maybe there can be a warning when a relying party asks for unnecessary attributes.

The real problem is that the primary LOA 2 solution is SAML but SAML doesn't support user attribute control.

OpenID Connect will support user consent.

Personal Data Ecosystem Landscape (Kaliya’s slide) may offer a solution by giving user control over which attributes get released.

This may be a paradigm shift.

It is being built today. Individual owns data, sets release rules.

Infrastructure must be written in a non-proprietary way.

Another issue is the NSTIC notion that the IDP not know how data is used and by whom. This may be overcome by user/data locker contract.

OpenID Connect introduces Relying Parties to personal data lockers.

Level 1 should be separated from Levels 2 and higher – contract may not be needed at Level 1. Definitely needed at Level 2 and higher.

How do we get from here to the brane new world?

The privacy requirements are a work in progress. They can be modified if there is a viable alternative.

Human nature paradox □ too much choice causes shutdown.

Can we change defaults for different demographics?

Is it possible to design a user interface so that the actions of the user can drive questions asked?

We have to watch how we scale this so there is no need to establish pair-wise relationships between relying parties and data stores.

Impact of Devices as an Entry Point into Online Ecosystems/Data Platforms

Wednesday 2C

Convener: Vicki Milton

Notes-taker(s): Dave Hebert

Introduction

- Devices are increasingly building in the ability to incorporate digital identity into a device so that access to various services and the associated data can move across devices.
- Online identity is being brought into the devices as an entry point into online services and potentially the data platforms associated with them.
- Data platforms can tie devices together in the cloud.
- Most discussions at this forum have focused on the protocols and services, but little attention has been given to the devices themselves used to access these services and platforms.
- The device is actually a participant in this process.

How will this work? What role will the device have in this? How does the devices itself add value to this process now that identity is being tied to the device?

Responses:

1. There is a human factor once you get to the device itself.

2. Devices could provide a better level of trust in the data à "the device is something I have and that can be more closely identified with me."

3. A device adds an array of sensors that could be used to compliment à NFC, gps, camera, etc

4. It is a huge jump to say the device "knows" about the identity. Just because I authenticate to a cloud platform from a device doesn't necessarily provide identity to the device. I must have unique identifiers that are stored on or are part of the device (serial #, phone #, etc).

5. Is this different if a device has multiple IDs? Depends on how the device is being used.

a. Example of my address book àI could put all my personal addresses in an address book on a device that is unique to me making the device and the data stored more closely associated with me.

b. A device can aggregate information in a way that cannot be done just in the cloud.

6. What role does device play in protecting your privacy?

a. Device could have a personal data store.

b. A device may already store credentials that are not protected. I may store my credit card number on a device, but it 1) may only be marginally protected or 2) may not be connected to me in a claim-based way.

c. Tokenization is one way to solve this on the device.

d. The device could provide greater control over privacy concerns or issues. "I am better protected because the device is with me all the time. Other sensors on the device can indicate when I am away from the device and can protect me by securing the device, etc"

e. Device security characteristics can provide compliant security systems

f. Devices could provide cryptographic functions

7. Challenges:

a. Existing industry structures that require collaboration across many entities and the government àISPs will need to collaborate with mobile carriers, etc.

b. Regulatory requirements in certain industries will place demands on the overall solutions (examples: Financial Services, Healthcare)

c. Consumers are fundamentally naïve about both identification and privacy. Devices will need to perform identity and privacy events on behalf of users à make sure device is secure, let end user know what is going on and what risks they are taking. "Protect the naïve."

d. Data aggregation in the cloud: helpful tool, but very powerful. Without a secure device, I could 1) be compromised or 2) allow ISPs to use my data in a way I don't want. How do you drag all this data into the light-of-day?

e. Existing data platforms (examples: NOAA, Facebook, Google, PayPal, eBay, Twitter, Mint, etc) are fundamentally at odds with best interest of consumers/end users?

8. How does the role of the Data Platform change when in a Wall Garden? As an Ecosystem?

a. Doesn't matter if the data can protect itself. Cryptographically protected blobs of data. Can the data protect itself

b. There will be issues around management of keys

c. Still would need a resource that vouches for user's identity and/or related keys

9. Things MSFT is thinking about (announced already for Windows 8):

a. Support for using Windows Live ID in Windows 8 for device logon

b. Use of additional components on the device like TPM to provide secure boot

c. Ability to set up isolated accounts on the device (already present in Windows, but enhanced)

d. Management of multiple online account credentials to provide single sign-on.

e. Virtual Smartcard infrastructure

f. Still early. More to be announced TBD

CSDIP Cross Sector Digital Identity Program

Wednesday 2F

Convener: John Biccum

Notes-taker(s): Amanda Anganes

CSDIP session - John B. from Microsoft
Cross Sector Digital Identity Program

Goal: interoperability of state-issued identity credentials
started in VA - workers in northern VA (DC area) may not live in VA - maybe maryland, west vA, etc
started looking at private-sector issued credentials
States have said that even if there were no other RPs, it would still make budgetary sense to issue a good state ID that was interoperable between other state departments

CSDIP is wanting to do an initial build and test out issues, get social-political group feedback

idea: state wants to be able to transfer car title online. Currently, states loose lots of money on this transaction b/c fee is not high enough to cover costs of paper trail. CSDIP predicts that if they started trying to build this capability, they may run into state laws that need to change - law might say "must sign form X to transfer ownership". No form X if it's online.

CSDIP is group of companies, state workers, defense contractors
Microsoft, CA tech, Northrup Grumman, state of VA, a few others

Current goal is to build a small-scale model of a complete ID ecosystem (IDPs, RPs, attribute provider framework, trust framework, etc). Predict that it will fail and fail early - want to "assess the area of suckage" - if we build this, what breaks? legal issues, social policy issues, technology issues?

First use case - public sector ID provider provisioning a credential that is used for an edge service that would have RPs in other states. Need a schema for representing attributes on the user, at known levels of trust, that are of interest to RPs.

Federally funded but state-administered benefit programs: For example, a benefit program may require that the beneficiary prove lawful presence in a particular state. States may attempt to satisfy this req in different ways. State A may ask for self-assertion of “lawful presence”. State B may request a passport for proof. State C scans passport, makes a web query to state department to verify accuracy of the passport. All of these checks are setting the same boolean to 1 - but each check means a totally different thing. Need an ontology, way of understanding the questions that RPs may ask about attributes.

CSDIP is asking state programs what attributes they’re looking for to make authZ decisions. Hypothesize that different states will have similar but slightly different answers - state implementation of a federal program.

Meeting in Reston VA next week; hoping to produce an architecture that will be built for first version & chunk up work assignments.

Some open-source code exists for a similar problem at streetidentity.com. Uses OID connect, etc.

Hypothesize that they could probably pull off authN at a standard level; but that authZ development/standardization is in process, may not be ready yet?

Question - If using VA DMV to proof VA vita credential for public IDP - who is proofing DMV?

Don’t want to force something weird by settling on only 1 trust framework/proofer - solution may require several or it may not, but don’t want to decide on that prematurely.
But, challenge is figuring out liability. Liability is a big issue for private IDPs.

Work’s goal is not to come up with answers, but the right questions.

CSDIP is working with “a certain national bank” that is very close to provisioning IDs to citizens at large, but is being held back by liability issues (vs low monetization opportunities).

Hypothesize that a way to move forward is to define what the IDP is doing, in plain English. Serve notice that the IDP is ONLY doing what it says - RPs need to look at that declaration and decide whether it’s good enough for them or not.

International finance lease corporation idea:
Identity insurance body, with relationship to private sector entities - attach a financial risk model to individual entities, provide a scoring index.
Governance issue

Look at what we currently have:

FSSCC - bunch of bank under NIP - guidance given to banks regarding proofing ids of customers

AAMVA - guidance to states
NASCIO - RP, possibly trust framework?
NAPHSIS - public health (birth certificates, marriage, death, etc); also a trust framework
There are a lot of these organization already existing, but not working together and not being applied to the digital ID fronteir.

Liability:
One way to deal with liability is insurance.
Another way is to somewhat ignore it - say that someone can sue us, but so what? We have a legal department and enough money.
Third way is to pass it on to someone else w/o a financial transfer (such as providing notice of what your product does; do not try to use it for seomthing else or it will break and you can't call us asking for recourse).

Converging Cyber and Physical Identities for access to Facilities, Critical Infrastructure, etc

Wednesday 2H

Convener: Vik Ghai

Notes-taker(s): Bret Tobey

Tags for the session - technology discussed/ideas considered:

Physical Identities

Identity Convergence

Critical Infrastructure

Merging Online and Physical Identities

Screen shot of process overlaps between Physical & Online/Digital/Cyber Identities. Several overlaps were identified: 3 depicted here are – i) Levels of Assurance (LOA), ii) Trust (oAuth), iii) Correlation (of activities in physical and logical domains)

Other Key discussion points:

Nouns & verbs between the two frameworks are discordant though managing the same person (identity)

Lower LOA systems can be combined to create stronger, lower friction identity proofing

Adding Mobile phone to ID Attributes for cyber & physical access could present opportunities and challenges

Several opportunities exist for example access to cloud-based application with multi-factor authentication that may include Physical Location Verification, Physical Access activity verification, Google Authenticator, etc

Can there be or are there frameworks for aligning two domains? Probably we need some recommendations or working group..

Functional Areas:

ID Proofing

Authentication

Risk Management Assignment

Real life use cases were discussed that validated the need for joint approach that can be very useful to fight fraud, provide better customer service, etc

Other organizations that can be invited to address a joint LOA approach

Physical Security Interoperability Alliance PSIA

(http://www.psialliance.org/)

Security Industry Association (SIA)

(www.siaonline.org)

NSTIC Interoperability

Wednesday 3B

Convener: Jeremy Grant

Notes-taker(s): Hank Mauldin, Iana Bohmer

Notes from Hank:
Interoperability is one of the 4 principles that NSTIC has

Definitions review - wanted to know if NSTIC has the right definitions
 want to accept a variety of credentials
 want portability

2 types of interoperability
 technical
 policy-level - most complex

Questions posed:

What does interoperability mean?
How can multiple solutions?
Is there a single architecture?
Can trust frameworks achieve the goal?
What else should the steering group consider?

Policy: under a regulatory industry there are laws and regulations and self-regulatory organizations
 self-regulatory organizations work well
 However, if you get complacence officers in a room, they will interrupt the regulations differently

Also, the regulations need to be open-ended so as technology or processes improve it is possible to move easier to the better processes.

Trust Framework is a system problem, but we are still tackling the problem with silos
 What is needed is the system requirements, not an architecture.

Attribute Providers - some data has more than 1 owner
 complex relationships - want to separate roles clearly and yet operate together

Policy - legal actions liability
 every group has new contracts and need a way to understand level of liability
 government can not define or get it the way

user experience - why should a user adopt a particular technology
 other side of argument is users adopt around value propositions

some opportunities could save $billions with regard to meeting compliance

Question around which use cases is NSTIC being scoped for?
 Only consumer to government?
 Who are the users?

One thought we needed to escalate above everyone's use case

What is Cyberspace? is it just the web? Consensus is no. Cyberspace is more than the web.

User Experience does not need to interoperate with IdP

Want an interoperable identity to cyberspace

Three layers are all needed
 Regulations - Laws
 Legal Agreements
 Technology

Question around if interoperability is too large a goal for now. Should Consistency be used as the standard?
 Consistent user experience
 Are there ways to be consistent with all players?

What happens to portability if there is not interoperability from all actors viewpoints (RP, IdP, AP)

Set the bar high and do it right from the beginning. It is hard to fix later.

Discussion around the PKI forum and the 4 bridges forum. described how 4 independent groups have come together to create cross bridge environment.

How to get the private sector involved and what they need

liability
scalability
bi-lateral agreements

Get the proper rules around roles (both technical and legal)
need to think about these as active roles not entities

Many people have more than 1 credential
Need a way to connect credentials together and/or keep them separate

It is really hard to pull back any information

Is NSTIC focusing on identity or credentials? Credit cards are not about identity, but credit.
Answer: what is appropriate to the transactions. it is a fuzzy line.

Notes from Iana:

NSTIC Interoperability

Jeremy Grant

Wednesday, 10/19/11, 11:30 a.m. – 12:30 p.m.

Jeremy Grant showed slides related to interoperability from the NSTIC Strategy document. He discussed the concept of technical interoperability vs policy-level interoperability. He then put up on the screen the following five questions as a basis of discussion:

What does interoperability really mean (and what should it mean) in the context of NSTIC? Are there aspects of the NSTIC definition that deserve more thought or attention?

How can multiple solutions, i.e., different technology and policy "stacks" coexist in Identity Ecosystem? Different business models?

Is there a single architecture that can support multiple solutions?

Can trust frameworks be the way to achieve and enforce interoperability?

What else should the Steering Group consider?

The group did not really stick to a discussion of answers to the questions. Following is a summary of the comments made during the session:

The current rules and regulations that exist for cyberspace are based on old technology. Furthermore, government is years behind in even the existing technology.

Implementation of a broad trust framework is a system-wide problem, but it is being tackled as a silo problem. Stakeholders are locked into monopolies and self-perpetuating siloes rather than looking at the issue as a system-wide problem.

While it is the private sector that needs to develop and implement an identity ecosystem, giving it totally over to industry may be shirking the responsibility on the Government's part. While no one would want the Government to dictate how the Identity Ecosystem should be implemented, they should have a facilitation role. A good example of this is the Federal Government's dissemination of TFPAP.

However, attribute providers need to be treated differently than IDPs and RPs. Attribute providers could manage attributes for specific industries rather than on a system-wide level. Required attributes can be defined within industries/communities – but the question will be how can they be extended across communities, i.e., interoperability? Is it possible to have a certain number of templates that work across communities?

What is needed is some standardization within communities and enough standardization to transverse across communities.

There is also the issue of legal interoperability because of the related liabilities, particularly the U.S. requirement for liability insurance.

An example discussed was that of the credit card/debit card systems because of the effectiveness of their related legal agreements. But identity is different than credit cards.

It is important to leverage the architectures that already exist (e.g., http) and determining whether the protocols can be enhanced to solve technical issues associated with identity interoperability. One question that needs to be answered: is cyberspace limited to the Web? Is it the entire Internet?

There are many related areas that will require standardization in order for the Identity Ecosystem to work, e.g., data modeling. Many connectors will be needed, but standardization will be the key to success. The Identity Ecosystem needs to establish federated standards, but we have to recognize and accept that we need to allow more than one way dictated on how interoperability will be accomplished.

The value proposition to underlying entities also must be addressed. For example, the financial services industries could save a lot of money with the standardization of secure authentication. Ideally, a user could use a single token to access any of its banks. Stakeholders may need to come together to agree on how to achieve widespread use and cost savings.

Importance of taking the user's experience into consideration. A user needs to authenticate to their particular identity provider, but what has to be determined is how to convey assertions to/from relying parties. User experience has to do with relationship of the user with his identity provider. It is important to remember that once a user lets his/her identity to go, it's impossible to pull it back.

Need to address that the Identity Ecosystem needs to be addressed broadly and quickly; otherwise there will be weak intermediate solutions that may be as bad as what we already have.

Another successful example discussed was the Federal PKI Bridge. Communities leveraged the functionality of the Federal Bridge, e.g., Biopharma and Aerospace &Defense, by creating bridges to the Federal Bridge. These are successful examples of federation and interoperability using a single technology. Question: How can these bridges be scaled and extended?

A good starting point would be to extend PKI to accommodate privacy enhancing technologies. PKI, for example, drove the x509 standard to be what it is today.

Must differentiate between roles and entities IDP is a role, not necessarily an entity. Need to define the right roles around technical interoperability.

Open ID Connect Flows and Levels of Assurance

Wednesday 3H

Convener: John Biccum

Notes-taker(s): Dave Sanford

Rick started indicating that as the world is digital, we replicated too much of the physical model - it doesn't fit. The model he articulated includes:

1) External Entities - which includes:

Relying parties

Identity Providers

Medical

Business

Work/Employer

Collaboration

Entertainment/Games

... Government

2) Rules of Engagement interface layer which involves:

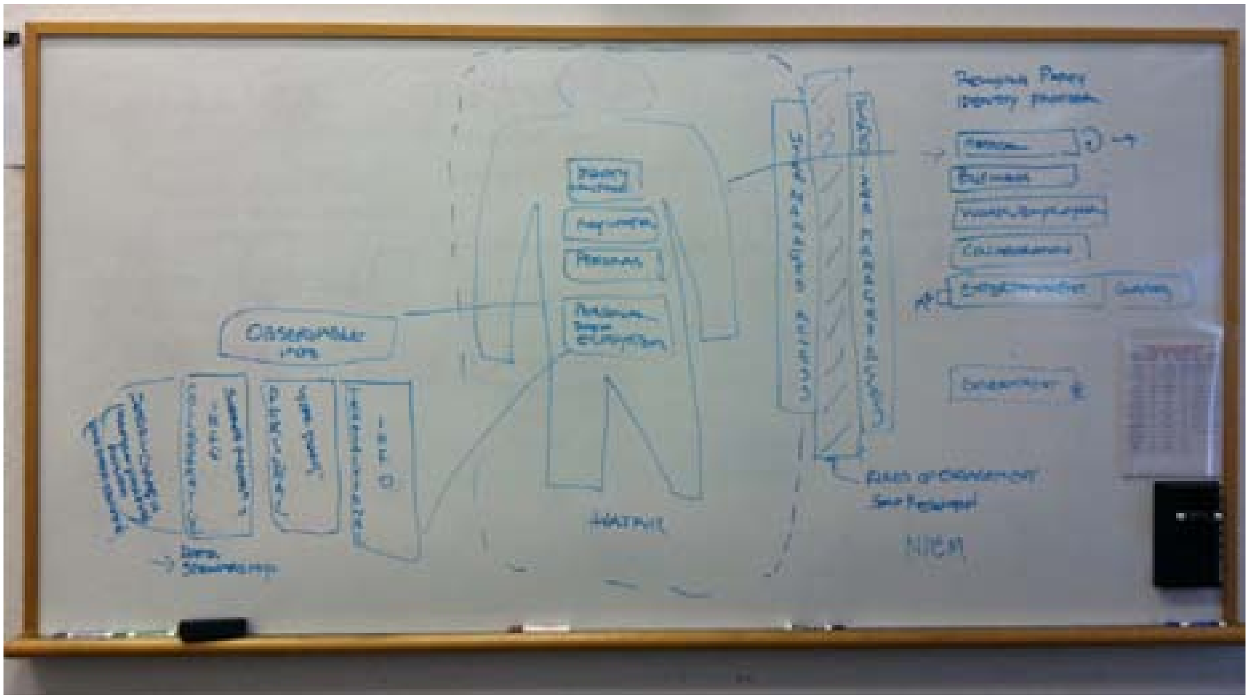
- user managed access
- provider managed access
- industry self-regulation

3) About me is the avatar with includes:

- identity and authorization
- reputation
- personas
- personal data ecosystem, creates collaborative info, some of this is observable data (mostly not controlled by me)
- personal (dear diary)
- transactional

The data stewardship of this avatar managed data should be shared responsibility with me. The avatar is a platform that uses the services of the external entities, they should in general not retain information unecessary for registration of the transaction.

The model relies largely on industry self-regulation (exchange rules might be from the National Information Exchange Model (NIEM).



A National ID for the US?

Wednesday 3I

Convener: Amanda Anganes

Notes-taker(s): Rick Campbell

url to notes also located: https://docs.google.com/document/d/1xTC28EYXOE1Cs2sYtaXq7TmWlsxNXzgDDZey3kHkcUo/edit?hl=en_US

The following is an attempt to capture the flow of the conversation around "National ID for the U.S.?" in Day 2, Session 3 of IIW XIII.

Is the Social Security Number a national id? A bit of debate, then tabled.

When one changes their name, there are many places that you have to go to to make that change. Sometimes, things come up later that cause one who changed their names, where they have to keep revisiting the change.

Discussion of British National ID. Started as being beneficial to individual, then through "feature creep" it came to inspire controversy, e. g. no ID means no medical care

John Biccum suggested that state level vs. Federal level, means greater decentralization and more difficulty/friction for either by Federal or other information seekers. States, for example, can push back on, e. g. FBI requests using various means (54 different state and territorial constitutions).

The president of the national Governor's association (Nepolitano) led an effort against Real Id, saying: we will not do this. Arizona prohibited any state employee from implementing any federal Real Id legislation.

Real Id has been optional. Cost estimates by the states for Real Id adoption was much higher than federal estimates.

Reasons not to adopt a National ID include:

- Single point of failure
- Single "choke point". Once you move to ubiquitous, everyone can demand it.
- (anecdote) Germany and Austria consider personal information to be government property. If you want someone's birthday, you can petition the government for permission to read birthday from the id.
- Germany has some data protection laws that are meant to prevent even the government from coordinate data.
- Distinct ids separate out the aspects/facets in a way that's harder to coordinate.
- Google Belay (??) issues distinct ids for distinct contexts, similar to e. g. a Health Club id that simply says that you have Health Club membership

Reasons to adopt a National ID include:

- Convenience - multiple ids are cumbersome
- Accuracy - multiple IDs means multiple places that can be wrong, which must be addressed individually when there are errors or updates.

Is the current status quo sufficient? Generally, no.

First name, zip code, and date of birth, uniquely identifies 95% of the people in the United States.

Some of the claimed benefits of National ID can be accomplished through other means. Right now John's Washington State Driver's license is usable as an International Id in a number of contexts, e. g. traveling into Canada. Nexus card will work to get into France from US or back, without Passport and it's not a National Id.

You can choose to prove age with Passport rather than Driver's license.

Estonia National Id:

- if you believe it's a success, it's great that you don't need to buy a train ticket -- your national id gets you on. (and then billed??)
- you don't believe it's a success, you might be creeped out by the government knowing your tram activity.
- can tap on a parking meter and notify the government of your location, etc.

Individual companies get together and collude with multiple distinct IDs today, but National Id makes it much easier.

As time goes on, correlation of data, even without National ID, is becoming easier.

One of the things that Real Id asks of people is one driving record per person. For a long time, some people kept licenses in both states.

In the Netherlands, national ids and drivers licenses are explicitly linked.

Dave Burhop, Deputy Commisioner / CIO of the Virginia Department of Motor Vehicles notes that DMVs have historically pushed back on being an identity verifier, preferring to focus on certifying people as eligible to drive.

In Britain the public has been turned off, because of large scale identity theft that was explicitly facilitated by the use of the national id.

One argument for a national id might be if there were a private sector globally unique id that people used, and were comfortable with. Then people might be more accepting, however, currently polls suggest that most people are opposed.

A quick Google search found a 2003 survey that said that 65% were okay with a national id. Search: Public Perception of Nationa Id.

Of the first CIO of DHS, Dave asked: What do you think of a national id? Answer: We don't need one. Through the networks that we have and systems that are hooked together, we effectively have one today.

Decentralization might hurt in cases like the No Fly List. Teddy Kennedy had to use the power of his position as a Senator to get him off of the No Fly List. His staff argued that you should not need to be a Senator. Now there is a redress number and you add it when booking a flight.

If we attach redress number to a unique national id, it's easier for someone to get that number as well.

John Biccum described the story of Michael O. Hamiltons. One, a convicted cop killer (served and released), and one who never had a parking ticket, both of whom rode Harley's in WA, and the troubles that ensued.

NSTIC Privacy

Wednesday 4C

Convener: Jeremy Grant

Notes-taker(s): Iana Bohmer

This was an open discussion on privacy. Below are the comments that were made during the session from participants:

- There is the appearance that the Federal Government may be pushing privacy policies on IDPs that go beyond the law. However, the issue is that there are no laws yet in this area so there is the chicken-egg problem. The expectation is that privacy policies would emerge, and possibly be enacted into law, as a result of the orderly development of the Identity Ecosystem.
- It would be very important that IDPs would have appropriate incentives to implement privacy safeguards.
- On the user side, success will depend on mitigating users' suspicions of conducting transactions in cyberspace and how their identities will be used.
- Jeremy introduced the concept of having an established set of privacy defaults and how are these defaults explained to the users, as an example of increased transparency within the identity ecosystem.
- The Federal Government has not made any decisions on the privacy model. A key concept of NSTIC is transparency with respect to privacy practices.
- Individuals may have the right to exchange information with a default to ensure that requirements will be the minimum necessary to conduct any given transaction.
- Depending on how the model is built, it may limit the IDPs ability to participate, because they may not have all the information/attributes on an individual to conduct the transaction.
- Recommendations that are in the NSTIC strategy weren't developed in a vacuum. And currently there is a lot of discussion on the Hill regarding privacy.
- NSTIC is a policy experiment. While it is a document with the president's signature, it isn't a law.
- NSTIC lays out a vision that would build on FICAM, but it would still be based on private sector.
- Participation in the Identity Ecosystem is a choice that every company will make regarding participation because participation is voluntary.
- The Government's goal and reason for its involvement is to allow cooperation in solving these problems rather than have laws/regulations come down with a hammer.
- Common thread in NOI responses is that government should serve as the privacy advocate for individuals.
- Potential tradeoff between user privacy and business utility needs to be researched. Need to put forth the business case for private sector stakeholders.
- There are many organizations, not just individuals, who care about privacy protections because they serve these individuals as their customers.

- The user needs to be able to trust in the identity ecosystem. One idea is to have the IDP act as the main party that the individual trusts. The IDP could take the role of sanitizing the data to suit the customer desires based on the transaction type. Individuals will weigh the value of the service based on what privacy safeguards are provided.
- It will be important to clearly define levels of privacy and be able to implement then with privacy-enhancing technologies. But several commented that the Government can't make the bar too high right at the beginning.
- Several participants made the comment of how traditionally NIST has not be open to discussing privacy enhancing technologies, that it seems as though there has been more interest in privacy from the private sector than from the Government.

Data Portability - Wading through the BullShit

Wednesday 4H

Convener: Steve Repetti

Notes-taker(s): Steve Repetti

Data Portability is one of the 3 cornerstones of user-centric computing

Privacy, Security, Portability

It is the ability for people to reuse their data across interoperable application

Encapsulates the ability AND the right to exchange information

Whose data is it? Who "controls" your data?

Control vs. ownership

Implicit transference: starts with you -- you have the power...until you transfer it

Propagation by proxy

authorized, accidental, unintentional, unauthorized

You grant access, share control, and then progressively lose control

The reality is, portability today is controlled by the owners of the data store

It can be influenced (in varying degrees) by the user

Currently policed by no one

Public opinion matters, but rarely has the necessary voice to change behavior

The concept of data stores inadvertently introduced the concept of walled garden

All data stores are walled gardens

The difference between private, public, and open source can simply be measured by the height of the wall

(If you doubt open source falls in to this category, just check with the Internet Timezone database guys)

Still, there is certainly a difference between with moats and turrets versus lawn edging

Governed by disclosure, commitment, and accountability

Disclosure is the actual or implied “contract” in which you share your information

Commitment is the willingness to abide by the original “contract”

Accountability is

Data Portability War: Who’s more open: Google or Facebook?

Depends on which snapshot in time you are looking at

Both companies have historically exerted their control over your data

In February, took a shot at Facebook, preventing Android (2.3.3 on the Nexus S) from integrating with Facebook, claiming Facebook’s policies “created a false sense of data portability”

Shortly thereafter (in July), Facebook retaliated by blocking a chrome extension from exporting Facebook Friends

Still, both companies are moving towards more openness

Both companies have hired high-profile advocates

Google’s Data Liberation Front

“Users should be able to control the data they store in any of Google’s products”

Facebook’s profile export functionality

High stakes game

Big players want to control the data store

Control and influence equals power

Ownership and control is a significant asset

Contrarian view: value can be achieved through openness

The quest for openness and decentralized control spawns opportunity and new players

Personal Data Vault guys

Personal.com

Data Death

Accountability

Economic value

Ownership/control of user data is an asset

Developer benefit

NSTIC and Privacy

Wednesday 5C

Convener: Jeff, John Biccum, Dave Sanford

Notes-taker(s): Rick Campbell

Some privacy compromise is an expected part of doing business, e. g. fraud analysis by credit card companies. In Identity parlance, the IDP (or Attribute Provider - AP) needs to know the RP, not just the user.

NSTIC - motivation is fundamentally that there is a public good.

FIPPS could be that public good.

Things that government can do:

- put money into it (analagous to building roads)
- begin to define regulartions in ways that help people understand
- Incentivize the desired behavior, e. g. define procurement regulations for suppliers

Proposal: Some modification to the trust framework could enable private sector IDPs to make money. (See credit card thing above)

PETS - Privacy Enhancing Technologies - to model a coin (???).

Levels of Protection

Wednesday 5E

Convener: Mary Rundle

Notes-taker(s): Iain Henderson

Challenge: How do we foster a standard around degrees of rigour required around identity and data sharing.

We would like to enable data to flow internationally, and reduce friction in volunteered information sharing.

Previous paper published on legal aspects of levels of protection:

- Architected around 4 levels.

- Works for discloser and recipient.

- Draws on OECD, EU, other prior work and principles.

- 1 = lightweight protection (language like ‘should), 4 = heavy duty (language = must).

- Onward data transfer is pulled out as an area of specific focus.

- Technology not specified at that stage

Todays discussion is aimed at the technical side, building on Mary's prior work and paper on the legal aspects of this issue:

Problem - technology changes really quickly

Potential help:

3 separate security accreditation (bring them together)

Fundamentals:

- Flexibility, not prescriptive

- Auditability and oversight, varies by level

Issue: What about the PDEC scenario, how do levels of protection apply if/ when the individual uses a personal data service (i.e. not going to set about using ISO standards or accreditation)

Could a rating system or reputation management system help?

Should decisions be made based on type of data (categories)?

Is 4 levels granular enough?

Is contract law usable/ necessary? Wrapped in a trust framework?

What's the role of federations?

Work being done by Kantara Information Sharing Workgroup on standard agreements is relevant (equivalent of Creative Commons for sharing information, standard agreements in human, lawyer and machine readable forms)

Will there be a proliferation of trust frameworks?

Is this really a user experience issue.

It really requires a user-centred design process

Is There a Business Case for Click Stream

Thursday 1G

Convener: Sid Sidner

Notes-taker(s): Rick Campbell

Notes located:

https://docs.google.com/document/d/1bLbMqkvsoYqswD6ROncHbz5k_Oy_XNLeXann3HbzLTY/edit?hl=en_US

Overview: Is there a business case for something similar to the Credit Bureau, where multiple retailers send in their click-streams and then pay to get back an aggregated version of the click-stream, but with the individual controlling access to the aggregated data.

How do you get started?

Amazon, e. g., has a lot of click-stream data, but not necessarily a lot of incentive to "give away" their data.

Little guys (Think Geek, etc) have more incentive, and if things were started up, it could reach a critical mass that might make the big players

"Nobody is going to get sued for collecting their own data" (?)

(aside) Someone has a system for adding annotations to arbitrary places on the web. There is some legal argument that if you have an overlay, that might be a derivative of a copyrighted work, but if you did "side wiki", you might avoid that. Some else noted that there is case law to suggest that it depends on where it is done. If the "mash up" is done on your server, you have legal exposure. However, if you have it mashed up on the client, at the request and with the consent of the end user, you have no exposure. Ad Block has established (?) that the user may add things to their client that are at odds with the owners of the sites that the user is viewing.

Another note: These ideas are great, but there may be a need for some form of legal defense fund, but the existing case law may mitigate the danger.

In addition to considering the motivation/incentive of the retailers, there must also be incentive for the end-user to use the system. Opportunities exist:

- You could enable cross-site features that are currently limited ot single sites, e. g. when Amazon says, "You purchased this item on XXX" or Google saying "You visited this site on XXX"
- How about a message like this: You're looking at a desired product on Walmart and get a message saying that the item that you want is available for less at Target. (this can incentivize merchants as well.)
- Entering into the market might not be an explicit event -- over time, you might build interest in something. By the time the user realizes that they're actively looking for a product, they may already

It might not be too difficult to collect click-stream data.

VRM - You might create a search engine for retailers to search for customers that are interested in what they want to sell.

One problem is reverse mapping -- making it hard to scrape sites, etc. -- to get from retailer-specific identifiers to products. What if you could figure out a "crowd sourcing" way to build up the reverse mapping across a large set of retailers. With some distributed approaches, you could have competition among "evaluators" that map urls/ids to products. (aside) just modeling a "product" and what makes it unique and/or related to some other product is also a hard problem. Large online retailers devote a *lot* of human and other resources to each aspect of these problems -- product modeling, price comparisons.

User adoption is hard because of chicken-and-egg problems. You need a lot of data to attract users, which enables you to get a lot of data.

There are existing businesses that are operating in the interest of sellers to reverse engineer urls, etc in order to target customers - Behavioral Targeted Advertising. Sid suggests that perhaps these could be "rehabilitated" -- perhaps doing the same or similar things, but for the benefit of the customers who choose to participate.

Axiom aggregates data from public records, build a profile on you, and sell that data to others. If Axiom makes a claim about your data, e. g. salary, that might be a stronger claim that the individual making a claim about their salary. This might also be "rehabilitated" to be valuable to the consumer who *wants* to be able to have someone.

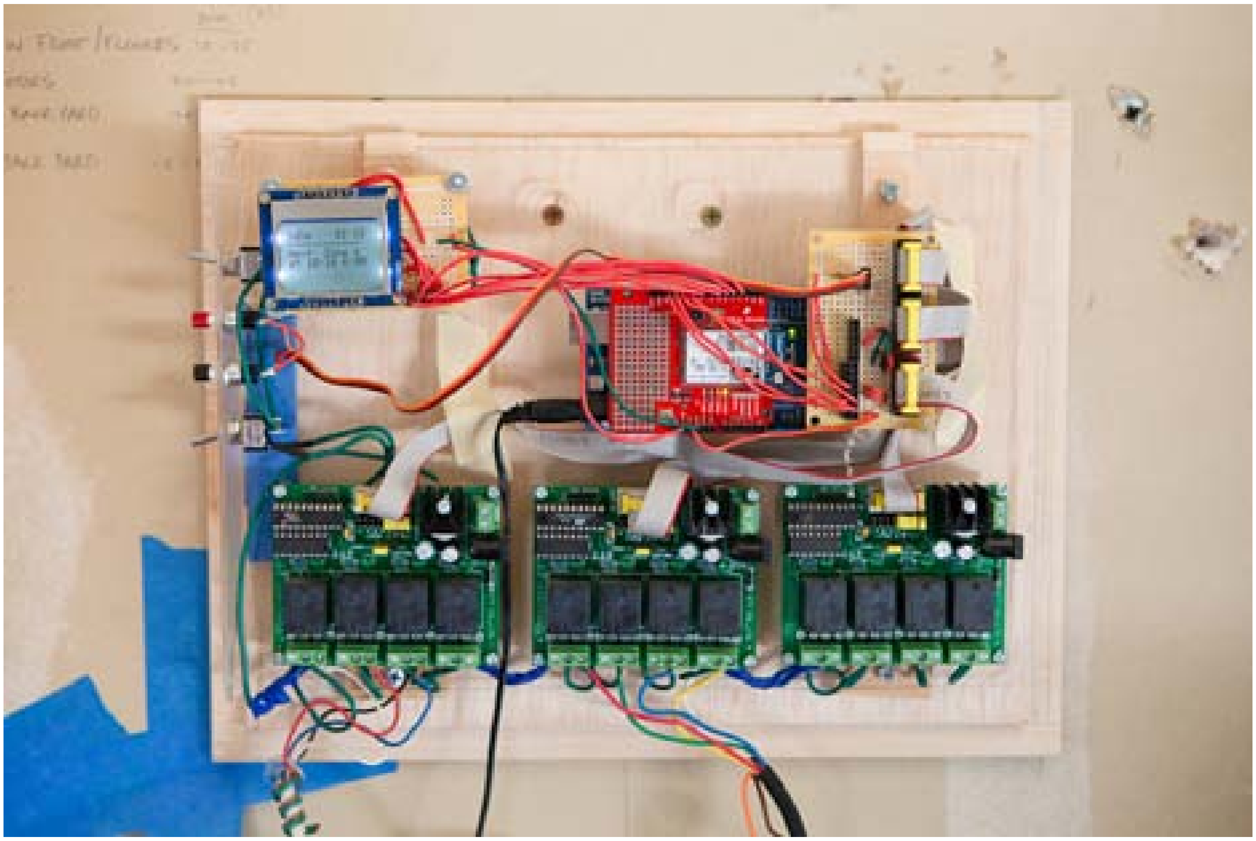
My Personal Event Network Waters My Lawn

Thursday 4F

Convener: Sam Curren

Notes-taker(s): Sam Curren

We talked about my prototype Arduino based sprinkler controller. We discussed lessons learned (keep the controller simple) and discussed possibilities for other types of micro-controller based cloud connected devices.



Europe vs. Facebook

Thursday 4J

Convener: Markus Sabadello

Notes-taker(s): Markus Sabadello

Tags for the session - technology discussed/ideas considered:

Facebook, Privacy, EU

According to the “Europe vs. Facebook” initiative, which was started by a group of young law students from Vienna, the Facebook legal structure subjects Facebook users outside of the US and Canada to EU privacy law, especially the well-known “Data Protection Directive”. The group has successfully requested and received a set of personal data stored by Facebook, filed a complaint with the responsible regulator (the Irish Data Protection Commission), and generated a large amount of attention in European media. By now, Facebook offers an automatic web form where users can request a copy of their data, however, the group pushes for further action, claiming that Facebook's reaction is insufficient. The group, which is intimately familiar with both US and EU privacy law, demands more transparency and the use of open standards, and explains that a world-wide solution to online privacy must consist of both legal and technological measures. As of now, the investigation against Facebook is still ongoing. On the website http://europe-v-facebook.org/, a detailed list of complaints and the history of the effort are documented.

Strangers on the Net

Thursday 5H

Convener: David Patterson

Notes-taker(s): Kevin Marks

Kevin Marks, salesforce.com
David Patterson, duceme.com

No-one knows you're a dog. - how do you bootstrap to reality?

verification problem for individuals - there are badge companies eg trufina.com myid.is

data.com is a business version of this.

If you were going to do a home exchange or sublet, what would you like to know about them?
Role should be a common acquaintance.

NSTIC should provide some basic identity.

If you have one authed account, you can bind related profiles with bidirectional rel="me"

could then add verifiable information about income, age, profession.

Employment and Usability of Cryptographic Credentials

Thursday 5K

Convener: Francisco Corrella, Karen Lewison

Notes-taker(s): Karen Lewison

Tags for the session - technology discussed/ideas considered:

Privacy-enhancing technologies (PETs), PKI certificates, TLS, HTTP, cryptographic credentials, privacy, NSTIC, deployment, usability,

Idemix, U-Prove

Link to the Power Point presentation which was the basis of the discussion:

http://pomcor.com/documents/Deployment.ppt

Another relevant Power Point presentation for background about privacy-enhanced credentials:

http://pomcor.com/documents/ProsAndCons.ppt

Presented a scheme for levels of privacy (levels 0, 1, 2, 3), and the current deployment problem for cryptographic credentials which are needed for privacy above level 0. (Slides 3 and 4)

Three proposed missing technologies needed to implement cryptographic credentials are listed in slide 5--an audience member suggested that a fourth technology, revocation technology for PKI certificates, was also an issue.

For both deployment and usability reasons, it was then proposed that cryptographic credentials should be managed in the browser (slide 6). There was some discussion about the ability to synchronize credentials between browsers on different devices, but most people agreed that it could be done without a lot of difficulty.

Privacy-enhancing cryptographic credentials should be “built into the fabric of the Web” by support by HTTP and TLS; TLS to reduce “overhead” and for credential presentation by the browser (slides 7 and 8). The point was raised that this might be too much for browsers to expect to do; Francisco commented that this scheme was only a suggested architecture. The issuance and presentation protocols for PETs are very similar, so these crypto protocols could both be run within TLS, and PRF can be used to generate a common reference string.

The user experience could be managed by the browser, and include different personas associated with different credentials (slide 9), which would in turn require user education re: persona management.

One open question is: Is the user entitled to know the privacy provided by a given credential, and how to explain that to the average user? (slide 10) Alan Karp has been recently involved in usability testing and provided several insights including: the concept that privacy expectations depend on the user’s trust relationship with the provider, and that the use of a “private browser mode” might serve as an indication to the user that the privacy level is elevated. Tony Nadalin added that Microsoft had the same substantial problem with user education with InfoCard.