Internet Identity Workshop 14

Book of Proceedings

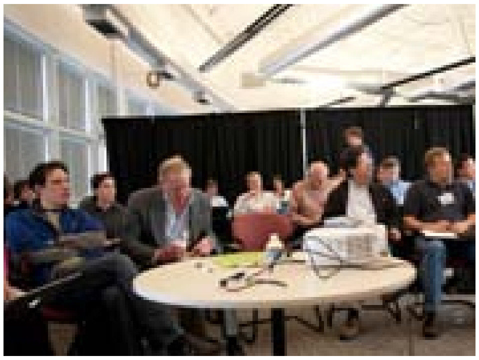
www.internetidentityworkshop.com

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_14_Notes

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

May 1-3, 2012
Computer History Museum
Mountain View, CA



Contents

NSTIC Update, Pilot and Governance Recommendations

Tuesday 1E

Convener: David Temoshok

Notes-taker(s): D. Temoshok

Tags for the session - technology discussed/ideas considered:

Ideas: Governance Recommendations, Steering Group By-laws, pilot process

Discussion on NSTIC NPO activities over the past year, principally Governance NOI, NIST Recommendations Report and Recommended Charter, and pilot activities.

Following pilot down-select, there is current period to submit complete proposals due by May 10. Pilot evaluation is on schedule to expect awards in July. Comment that NIST should publicize selected pilot awards as soon as possible following award – that is the intent.

Discussion of distinction between NIST recommendations for Governance Structure/Charter and discussion draft of Steering Group By-laws issued yesterday. NIST Recommendations were based on public comments to NOI and reflect NIST analyses and synthesis of the 57 NOI responses. The Recommendations stand as issued – NIST recommendations for Steering Group Governance Structure. The draft By-laws were formulated by NSTIC NPO. The draft By-laws should be considered "Straw man" to accelerate and advance further discussions for the development of the SG By-laws.

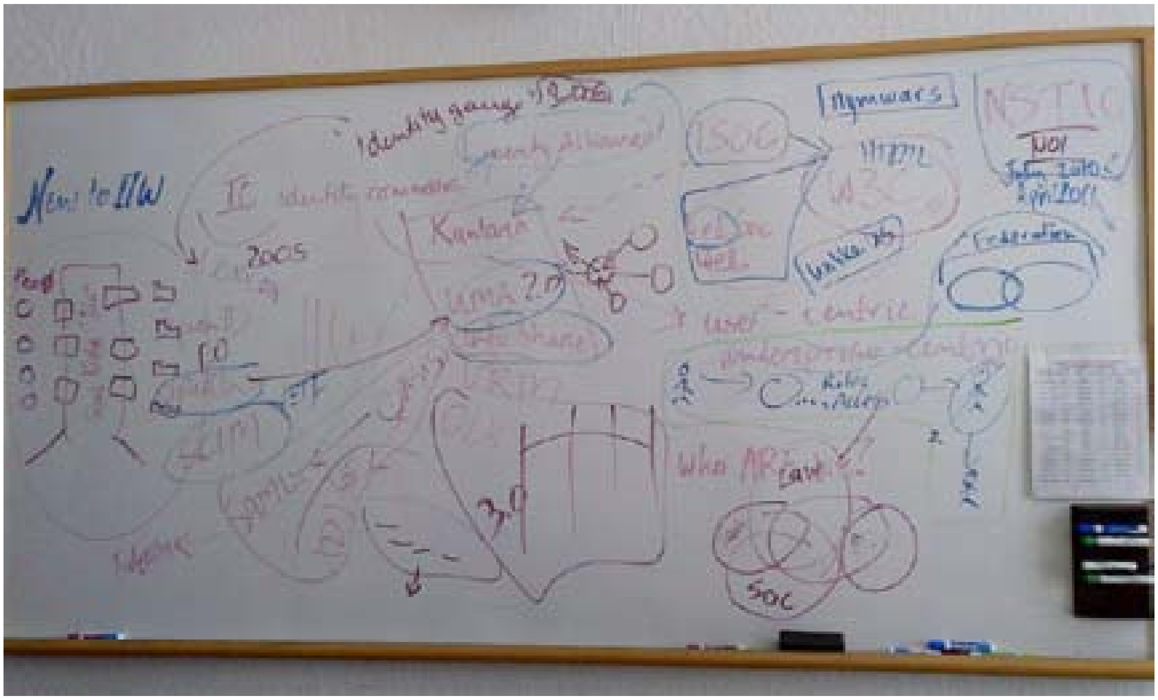
Discussion on Governance Recommendations focused on explanation of terms, 2-tier body of the Steering Group – Plenary and Management Council, and the recommendation for representational composition of Management Council based on self-declared stakeholder categories.

New To IIW

Tuesday 1G

Convener: Kaliya

Notes-taker(s): Bruce Ratoff



OIX Attribute Exchange

Tuesday 2A

(presentation located on wiki)

OpenID Connect

Tuesday 2B

Convener: Pam Dingle & Justin Richer

Notes-taker(s): Paul Madsen

Elevator pitch - protocol framework based on OAuth - adds an identity layer to bare bones OAuth 2.0

The features of OpenID Connect can be divided into

a) those features required for a full platform (e.g. discovery & client registration)

b) standardization of identity pieces (e.g. UserInfo endpoint, id_token)

Note: some of the features defined in OpenID Connect are being fed back into the OAuth WG working on evolution of OAuth 2.0

Difference between a client & relying party? A relying party makes a *decision* based on a token/ assertion it receives from elsewhere (an Idp). A client simply *uses* the token on an API call.

Justin went through the 3-party flow

User

RP

(consumes tokens & attributes)

OP

(issued tokens)

OpenID 2.0 – focused on front-channel

OAuth 2.0 – focused on back-channel

OpenID Connect – closer to OAuth 2.0

OP returns

- id_token
  - o JWT carries issuer, userid etc
  - o Logically similar to SAML assertion
- access token
  - o Used on API call to UserInfo to retrieve attributes
  - o Theoretically also used on calls to arbitrary APIs

Pam makes the point that OAuth & OpenID Connect makes different assumptions about how to apportion complexity between the OP/IdP & RP/SP than does SAML.

Question – what is the diff between the info in the id_token and that returned by the UserInfo? The former is bound to a session, with a small set of claims, the latter more long-lived.

OpenID Request Object allows relying party to describe its conditions

Phil Hunt asks about live deployments. Mike replied with description of ongoing interop tests at http://osis.idcommons.net

OAUTH+SASL Open Issues

Tuesday 2K

Convener: Bill Mills

Notes-taker(s): Bill Mills

Reviewing outstanding issues in the current draft, notable the current HTTP style format and auth endpoint discovery.

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

Simon asked about GSS-API bindings, can we make this stronger and use this for bootstrapping GSS-API mechanisms.

Discussion about “To HTTP or not to HTTP” which ivolved into the next item. In general:

HTTP is seen as a bad option here, which we knew.

If we’re going for a new format the feeling was that we should not try to build in anything extra in the short term and that new tokne profiles should define their own extensions to the base framework.

Detailed dscssion of the flow. A *great* question was asked about discovery, that in the case where we have multiple potential IDPs, we have a big problem because all IDPs have to provide compatible access tokens to the protected resource. This needs to be looked at seriously.

* Need to add text here that federated login and the password grant are almost incompatible. The solution is probably to make the IDP for the PR be populated with a password to be used for things like IMAP when in fact there is a federated auth situation with multiple IDPs. This is still outside the true scope of the spec but is well in scope for security discussions.

Discovery is still very hard, and it is becoming clearer that supporting the password grant is probably the legacy support case and that federated login and the OAuth 2 password grant are probably really incompatible, because a protected resource sever can cause a client to give up the password to the wrong place.

Discovery in federated situations almost certainly has to point to the domain discovery endpoint, and the client has to discover further, potentially an OpenID connect flow or other flow rather than the password grant.

FreedomBox Demo

Tuesday 3C

Convener: Markus Sabadello

Notes-taker(s): Markus Sabadello

In this demo, 5 plug computers (Guruplugs by GlobalScale Technologies) were handed out to volunteer participants and connected to power outlets.
Upon being plugged in, these small personal servers booted their Debian operating system and custom demo software.
Each volunteer of the demo was able to control one of the boxes via a web interface.
The first step was to connect one’s box to the other boxes.
The second step was to sign in to the network with an identifier, in order for boxes to be able to find each other.

After being connected and identified, the demo allowed participants to do the following:

1. Enter personal data which is stored in an XDI-based Personal Data Store on the box (first name, last name, email, etc.)
2. Establish a relationship with other participants, which allowed access to the personal data on their boxes via XDI Messaging.
3. Sending text messages from one box to another.
4. Sending an "intent" to all boxes on the network, indicating what one would be willing to buy at a given price.
5. Viewing "intents" received from the network.

There was a lot of good discussion about the potential of such a personal server for the Personal Data Ecosystem and Vendor Relationship Management.

The general idea behind the FreedomBox is to enable data sharing, communication and social networking that can not be monitored or censored.
This demo was neither created nor endorsed by the FreedomBox Foundation, but was simply meant to demonstrate what its idea is about.
The actual software used during the demo was developed by Project Danube.

Standard Information Sharing Label

Tuesday 3G

Convener: Joe A.

Notes-taker(s): Braden Maccke

Standard label.org

Creates a "Sharing Terms" sheet, similar to a Nutritional Facts label.

When a user searches Google (for example), user will be able to click on an icon to display the terms label outlining:

DTA Referencing Label:

Where: Physical location of data.
Who: Google, Inc
What: Form Data (search query)
From: HTML Form (form may be highlighted on click w/ "show me" button)
When: Interactive / On submit
Why: Recommend Websites
For How Long: Indefinitely
Output To: Resulting Web Pages
Addt'l Terms: Aggregated Products
Related Agreements: This or that, etc…. http://
3rd Party Ratings: AFF / ACLU / etc (like an ebay feedback rating) / Or your personal network…
Storage (of the record of this agreement): Place this record is being stored. (portable contex.org)
? Redistribution: who's it going to.

“Data Laundering” – With the form, the user has been notified, had an opportunity to understand it, and can’t come back and say they were misinformed.

3 Steps

Label
Trust Framework Agreement
Default Terms – ultimately users set their own terms.

Standard Terms
Semantic data
Promotion

Add location – Storage?
Button State – Reviewed?
Explain purpose binding
Redistribution terms
Multiple form?

Federated Authorization - XACML, OAuth & TVE

Tuesday 3I

Convener: Ian Glaser & Paul Madsen

Ian sets context. Problems facing higher ed, doing amazing things but SSO isnt enough.

What happens after you sign-in is the important stuff.

Federation has dealt historically with federated authentication. But knowing who the user is is less important than knowing what they can do.

Ian describes two different types of authorization policy – admin & runtime. Very different, typically different admins etc

Metadata?

Paul presented the XACML pattern for authorization

- PDP
- PEP
- PAP and policy store
- PIP

Who is asking or on whose behalf for authorization might be part of the authorization process

Where do you draw the enterprise boundary regarding the XACML decision pattern

Geroge Fletcher asserts that there is a some authorization in federated SSO – references Shib

Discussed federated runtime auth versions fedeated admin auth

- OAuth is an example of federated runtime auth with no federated policy admin (PAP and its output was mashed into code and comments)

Paul described TVEverywhere use case

- described SAML style TVE

Problem was back-channel conversation btw HBO and Comcast for example

- Eve asked why "channel subscription" wasn't an attribute
- OAuth pattern for TVE

JWT includes the permissions that were established for customer

Eve claims there is a prosoal within UMA to handle this problem

- How you describe resources
- A pattern for describing scopes – mini-WSDL
- Authorization possibilities can be as finely grained
- Standardizes application semantics

Point raised that if you have a delegate chain of authoriation decisions I could make a local decision via a delegation assertion and that would be honored at the service-side

eduPerson entitlements

- Map groups to eduPerson entitlements
- We need SPs to pubish lists of entitlements
- Map strings from our side to your side

Guy from Stanford raises the issues of standarizing scopes

Bjorn of UnboundID asserts that this is more complicated. Raises issues of obligation. Provider can perform decision making or local decision made.

- must move beyond "you give me a name of a group and I'll make a decision"

Further delegation of authorization – raised by Alan of HP

Eve drew a continuum of app versus remote service responsibilities

- Getting entitlements is the same a getting needed attribute in a sense

What happens when PDP and PEP are in truly different domains?

- What if they have conflicting or unalign goals?
- UMA has had these conversations and it sounds like this falls back to trust framework interop(?)

Description language missing. The RP is not describing what it is that they are doing. Definitely not machine readable.

Performance considerations. Hitting PDP every time is costly. Entitlements can be cached and might be more performant decision mechanism.

Does a trust framework have to establish semantic meaning?

Session Topic: What happens when federated identity fails?

Tuesday 4G

Convener: George Fletcher - AOL

Notes-taker(s): Jon Webb - Sony

A user within a service may have a username record which is referenced by a pid (provider ID) and a puid (provier user ID). This tuple allows login so long as these remain valid. But what happens if you lose federated ID?

How to lose fed id?

- IDP goes out of business

- Personally delete the account

- Disconnect from the RP (e.g. revoke OAuth token)

-- You just reconnect

- compromised accounts

- IDP blocked the acct (e.g. law enforcement action, etc)

Need to define best practices!

- Not necessarily a big deal if I can post to pinterest because my IDP went out of business

- Potentially a big deal if I can't login to eTrade or some medical/govt entity

One approach is to allow creation of another set of auth credentials and link it to the original record.

- What information does the RP know about the user to allow them to recover?

- What information is strong enough?

-- First name, last name, address, favorite animal??

- Previously seen device?

- Phone/SMS challenge

What about if your original IDP account comes back?

- Either way, need re-connection flow

Bottom line - RP's need enough data to recover accounts!

This somewhat flies in the face of some of the privacy principals of OpenID for being an RP. You might be able to have a recovery flow as a part of business you're already doing. E.g. it's one thing to request the user's phone number just so you can have a recovery flow, it's another thing if you request their number because you're legitimately providing a service based on that attribute (same would go for billing info for example).

What about the case where your IDP is simply down or non-responsive temporarily?

- One idea is that you could temporarily allow someone access through an alternative auth mechanism

- Could use the same basic recovery flow, possibly with reduced access/capabilities

-- why?

- Again, this is recreating the problem of running against the privacy principals we'd like to maintain

Examples:

Federated login through plaxo.com, trippit.com. The former will not ask you for an additional username or password, but will allow you to "locally" add new profile photos etc. The latter asks you for an additional local password as well.

One potential enhancement:

- When a user chooses to login with a button from the nascar, you could at least check to see if the IDP is up

-- Launch a hidden iframe to check to see if IDP will respond before allowing the user to login with that provider

This recovery issue exists because users see vested value in certain accounts. Some accounts have more value than others. In facilitating recovery, there are two sides to the risk:

- Consumer risk: access to private information, impersonation, reputation, purchasing, etc

- RP risk: public perception of service, regulators, lawsuits, security, fraud, etc

General discussion around whether or not a RP could push a user towards an IDP that provides "better service" from the perspective of the RP. That could either be better guaranteed availability or levels of assurance or quality of recovery flow and/or turnaround time on recovery. Is there a possibility for a business to provide this recovery service outside of an IDP?

What about heuristics based approaches? Allow account recovery based on the user's interaction with the RP itself (transactions, activity, login time/location, etc).

- Most RP's don't want to hold and secure this information

- Some discussion about these heuristics being error prone in general

Perhaps the conclusion is that this is a balance between allowing customers back in and losing those customers, and that balance will be defined by the service itself and the choices it makes with regard to the storage of this heuristic information/data attributes, and less strict recovery flows or a lack of recovery flow.

Writing APPs that are easier to defend than attack

Tuesday 5A

Convener: Alan Karp

Notes-taker(s): Alan Karp

Link to presentation:
http://www.hpl.hp.com/personal/Alan_Karp/Cornerstones2012.pptx

BioMetrics into the Net with Smart Phones / Why not use Biometrics for Internet

Tuesday 5D

Convener: Shin, Takashima, Yamada

Notes-taker(s): Christopher Arnold

Toshiba - Biometric data transfer over the internet

ACBio - International Standard

Internet enabler for Biometrics

Smartphone for authentication device

Authentication Context for Biometrics

Data format standard for evidence of successful biometric authentication in internet

Toshiba started and standardization May 2009

Fingerprint, finger vein, palm vein, facial image used as verifier of identity

Biometrics currently used for passport, driver's license, ATM (In Japan)

But not supported in internet as a wide protocol. Why?

Other approaches:

Passwords get attacked by phishing, key logging, Impersonation by stollen passwords Passwords forgotten

Device paired authentication:

For token, Tamper resilience is good. But if the IC card is stollen with pin. Often forgotten as passwords

Biometrics Good on impersonation, good on operation. Without ACBio weak on internet.

Q: There is an “equal error rate” for passwords. False negatives and false positives are equal. So that’s why we still use passwords today.

AC Bio address internet protocol recording and transmission data format for the evidence data of biometric authentication.

Biometrics typically not used on internet. Why?

Unfair use case in music over the internet. (Compromised device or inappropriate rights)

Block special devices used to impersonate others

Possible leakage of biometric data leaked from site?

Should user register biometric info, which may be dependent on service, for each service?

Send binary evidence information securely over the internet to a verification server with ACBio.

Debate: hash security and location of pairing of evidence with stored biometric challenge.

Slide Notes:

Storage template (Portable Device, IC Card) offer comparison to sample data.

Client application puts in data, evidence information validation sent to server. Then validated against ACBio validation server.

Two streams combined. Evidence data of device and sample of execution of biometric authentication are paired.

Comparison result and evidence data are validated later

Q: Passwords can have an untrusted device and use the hash algorithm?

BPU information

X.509 certificate of the BPU

Report on BPU

Control value block

Challenge (Challenge from validator in order to prevent replay attacks)

Biometric process block

Data type and hash value of input

Data type and hash value of output

BRT certificate information block (

Certificate for the registered template)

Challenge from validator in order to prevent replay attacks.

Definitions:

BPU=Biometric processing Unit

BRT=Biometric Reference Template

Means to prevent compromised devices to all systems that use the central revocation list

Current operating standard: ISO/IEC 24761

There is a standard now, but not operationalization

Plan to partner to realize the scheme.

Two OEMs in Japan considering. One carrier.

Debate: Software vendors who want to use ACBio to pass “Liveness tested palm vein”liveness detection

Other models are paired NFC chip to computer (Embed validation server in car in case loss of internet service.)

Possible tie into Car entry or location based Door unlock

Personal Data Ecosystem Consortium (PDEC)

Tuesday 5G

Convener: Kaliya

Notes-taker(s): John Biccum

Tags for the session - technology discussed/ideas considered:

Personal Data Ecosystem

Kaliya began by asking why attendees chose this session. Answers included:

Watching it evolve

Recently joined, communication, synergy, language (vernacular)

Awareness

Terms (vocabulary) are a challenge

Get latest info

Learn "How to…"

Learn about Business Models

Like to float to sessions, this one sounds interesting

Want to know what is on the forefront of identity

Want to know where to find information

Trying to start a company, want to learn about political , technical, privacy regulations that would affect my business

Like a challenge

Came because Kaliya is "fun"

Want to know history of development of PDEC

Session "Strongly recommended" by a colleague

Here to see if we should try to set up local chapters of PDEC

Kaliya "bucketized" all of these individual perspectives into three uber-buckets:

PDEC History

Economic models discussion

What should PDEC do next, what can PDEC do better

History of PDEC

Drivers

World Economic Forum is interested in this subject

European Privacy Directives are a driver for the personal data ecosystem

NSTIC interested in this area

Activities:

Publishing the Journal

Start Up Circle

NSTIC business model workshop

Economic Models

What does the Market Look Like (and how do we define it)

Individual and their data store (Personal, Blue, others)

Vendor Relationship management

Data aggregation Markets (e.g. Arbitron)

Infomediary Model (e.g targeted advertising based on data in container

What can (and should) PDEC do better?

What are we doing to educate people?

Telling stories that show value

What are the choices (e.g if I don't want FB to have all my data…"

What are the bridge strategies from the business model we have now to this brave new world of the PDEC?

Define what would Level 5 on the Capability Maturity Model look like for PDEC

Define the steps that would have to be taken to get to Level 5

Highlight specific examples of features that accrue to the PDEC

Work on a publications page

Create a "You know you are a PDEC candidate if…" page

VRM + CRM: Timing? Outreach? Coordination? Purpose?

Wednesday 1B

Convener: Judi Clark

Notes-taker(s): Judi Clark

Four constituent groups:

- CRM software sellers: oracle, IBM, salesforce, sugarCRM, MS Dynamics,
- B2B:
- VRM developers
- media people who have been covering this: Mitch Leibeman & Josh Weinberger at CRM Magazine - also possible sponsors, is it still too early? Dennis Pombery?

Also Value-added resellers: Planetwork is working with Fujitsu, etc.

Hosting an effective open space: invitation (Kaliya) - knock here if you're interested approach would be effective. Check with key folks and their schedules.

Not like a Customer Commons event. New and mature developers getting together, finding common ground to move forward.

How ready-to-go are big developers? Drummond: code samples, here's how you would connect to personal cloud, demo apps included, pre-Cybos.

Doc: changing mission and constrain costs: hand-pick companies (Mydex, Personal, Singly, Qii, PDEC start-up circle)--do a speed-dating event.

Planetwork is focused on bringing technology to the table. Next 2-3 years to make it happen. (Judi will talk with Kelly about PDEC doing this event.)

Collaborative, innovative effort to get parties together, see what we can build.

Venue: Doc says he'd be surprised if Stanford didn't have a space. Also Newstar might have a room (east coast, DC area) auditorium. Also Harvard or MIT. Brad Feld and others gave money to Singly, so Denver/Boulder may be a possibility. Barbara Bowden has connections in this area.

Things in VRM dev community are moving along, but unevenly.

Kaliya offered her event infrastructure to mash-up or organize this event.

VRM is perceived by CRM as challenging their business. They may not want to lend credibility to an effort that challenges what they're doing. They want to keep moving their own work forward.

Retailers: Doc has spoken to Best Buy, some people are open & listening. Robert Stevens left a month ago, is relocating his family to west coast.

Barbara working with Interest networks, also a possibility to do event in Minneapolis.

Focus on end-game, trying to advance where this is going from user and vendor perspective. Future Business Relationships as focus, or Customer Relationships. Everyone with loyalty scheme would show up.

Following release of Doc's book, event in Sept. This meeting is to discuss what this means to the future of customer relationships. Thought of sending out a copy of the book to Fortune 100 picks: Nordstrom, Walmart, etc.

What do we want to accomplish? Critical mass of VRM companies that have solutions, ready and willing to demo to CRM and customers, to establish that is a signal. Barbara could be ready, Drummond could (likely) be ready. William and Mydex might be ready. Showcase certain products and companies--why not feature at SweetWorld or other CRM events? or speaking sessions, collaboration speaking, breakout events? Might get drowned out. CRM companies have their own events.

Connections between VRM and CRM doesn't need to be proven but it's inevitable. SugarCRM is open development. Doc might call Nick Halsey --could we do a VRM implementation by Sugar's spring conference? Develop for prototype implementations. (Specific tactical follow-through)

Any industries leading? (Ford was at Berkman last event) Talking with banking, credit reporting agencies, real estate, medical.

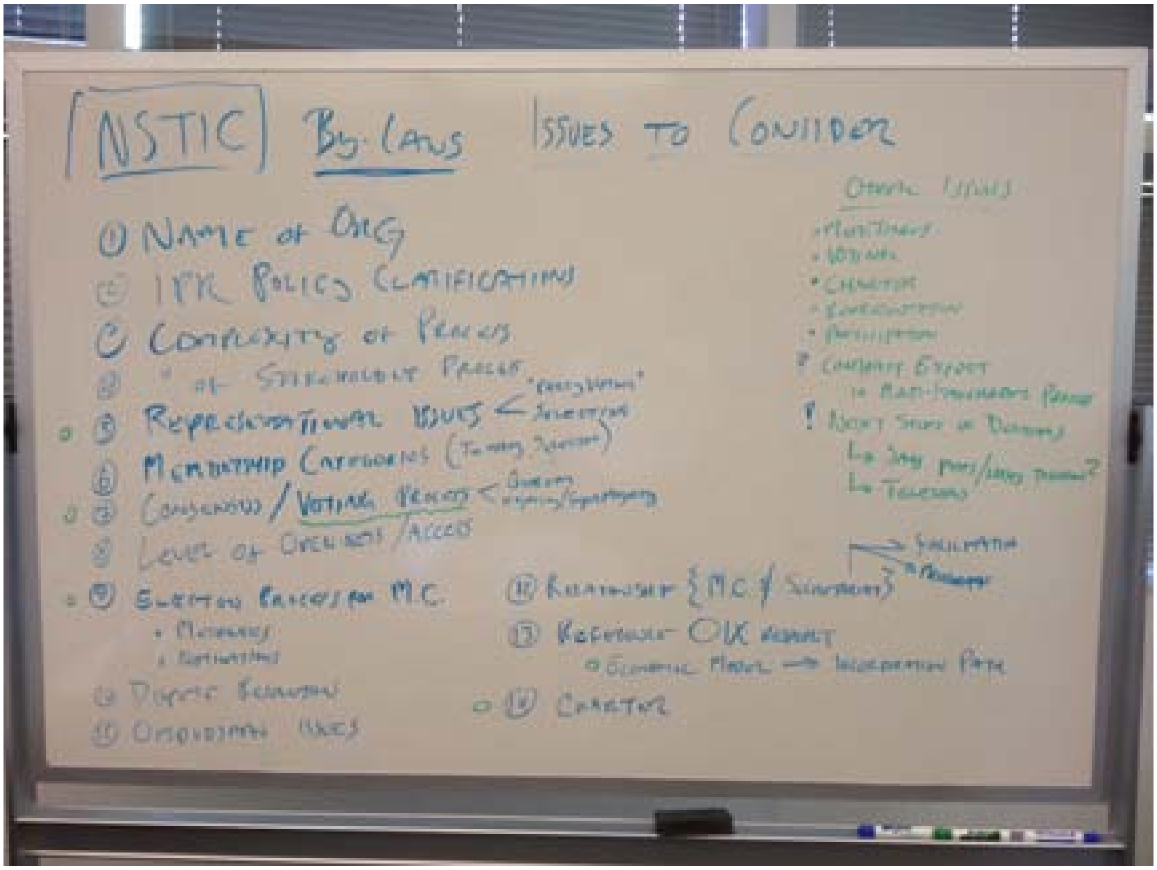
Bottom line: September may not be the most optimal time to hold this event to connect CRM and VRM communities generally, but makes sense for PDEC and Start-up Circle to convene a conversation.

NSTIC Bylaws

Wedsnesday 1D

Convener: David Temoshok

Notes-taker(s): Trent Adams, Mary Ruddy


NSTIC By-Laws Issues to Consider
① Name of Org
② IPR Policy Clarifications
③ Complexity of Process
④ " of Stakeholder Process
⑤ Representational Issues < "party voting"
⑥ Membership Categories
⑦ Consensus / Voting Process < Quorum
⑧ Level of Openness / Access
⑨ Election Process for M.C.
⑩ Dispute Resolution
⑪ Ombudsman Issues
⑫ Relationship {M.C. / Secretariat}
⑬ Roadmap
⑭ Charter
Other Issues
• Charter
• Participation

(Notes from Mary Ruddy) NSTIC ByLaws – Session at IIW on May 2, 2012

Issues comments

How NSTIC works with Standards orgs – for IPR

Scope of plenary, there will be 100’s of members, too big to steer.

The mgt group is doing the steering

Some of the bylaws track to the recommendation

Can we change the name to the NSTIC community – probably not a bridge too far

The idea is adoption – this is marketing

NSTIC bylaws issues to consider

1. Naming of the “steering committee”
2. IPR policy needed exercise left for the reader
3. Complexity of process, entire process is overloaded
4. Complexity of stakeholder process (self selection of stakeholder categories and election process
5. Representational issues (multiple layers, “party voting”)
6. Membership categories (not stakeholders) Qualifications are ambiguous, too many sectors
7. Consensus plus voting process (base consensus and appeal, majority, super majority and quorum)

8. Recommendations for openness and transparency in proceedings were ok (level of openness/ access)

9. Election process for the mgt council

    Mechanics

    Nominations – vetting of self selection

1. No dispute resolution process

2. Ombudsman issues (secretary needs to nominate, needs to be approved by governed)

3. Relationship between the secretariat and the steering committee

4. OIX advisory board issues

    What is the legal form of the steering group

    What is the economic model?

Charter (principles document)

Meetings (notice and attendance and frequency)

Next steps

Complex stakeholder consultant is coming to dinner – Scott V. – multi-stakeholder interview and systems engagement process. (Utilities to radical NGOs.) He took group through a process that cut emissions by 80%. How does this compare/contrast with the ombudsman?

The steering committee can request funding from NIST for programs. Funding will be limited

We are in a pre-secretariat period. Need a pre convening set of discussions and meeting – David T. concurs. Want to be moving by the time the secretariat is in place. How do we fund this?

- Have a meeting on Thursday to talk about other issues
- Have a series of short telco's.
- Other issues
- Meetings
- Voting
- Charter
- Representation
- Contract expert – multi-stakeholder process.
- Next steps

Account Linking Service & CAS- Galois

Wednesday 1F

Convener: Isaac Potoczny-Jones

Notes-taker(s): Isaac Potoczny-Jones

Tags for the session - technology discussed/ideas considered:

Account Linking, federation, Open Science Grid

The Account Linking Service (ALS) enables grid scientists to collaborate across organizational boundaries by linking multiple user identities together. It lets users access restricted data with any of the linked identities. This makes it easier to develop web-based collaboration tools since web applications can accept user credentials without being tightly coupled to any particular identity system. ALS is built on top of the open source CAS project.

In this session, we discussed the ALS system, its pros & cons, and how it could apply to the Sony Playstation Network and other use-cases.

More information:

http://grid2.galois.com/whitepaper-grid2-galois-2012.pdf

Patents and Open Standards

Wednesday 1G

Convener: Kevin Marks

Notes-taker(s): Kevin Marks

Overview

Recently the UK government has been dealing with conflicts between corporate entity's patent interests and the desire to keep government identity initiatives largely in the Open Source community.

History

Patents started as a grant of a monopoly by Queen Elizabeth I to the single chosen maker of a product or provider of a service. During the reign of James VI the laws were repealed and patents were only granted for new inventions or services. In the US, patents were originally granted for the promotion of science or art. However, recently there has been an explosion of case law so now just about anything can be patented. In the UK mathematical concepts or scientific methods or presentation of information can't be patented unless it's "part of something else".

Proposed Goals

- Don't allow a concept that was open source to be patented after a period of time like a year.
- Prevent patent trolls from taking over open source concepts just because they have the money to litigate and open source community does not.
- Place burden of proof on those who file patents instead of on those accused of infringement.

Options to Achieve Goals

- Open Source groups funding litigation to prevent patenting of open source concepts
- Twitter's IPA approach
- Extending Open Web Foundation Agreement to a defensive patent group
- New hashtag #fixpatents, need to establish a wiki page, mailing list or forum (KM now has fixpatents.org)
- Educate (or require by regulation) the patent offices about searching through open source or open

standards to document prior art, even though it wasn't part of an existing patent.

- Promote the rebalancing of patent law to reflect the real world that includes open systems and standards
- Promote organizational cultural behavior changes
- Commit to defend against patent trolls if the concept is part of OWFA or IPA (???)
- Find ways to streamline doing things the right way, like Twitter's IPA
- Cultural education like the recent piece about the patent town in Texas featured on "This American Life"
- Change the perception of the investment/VC community about the value of patents versus ubiquitous open standards
- Instead of deriving power from "the crown", derive it from consensus

Notes by Scott Rice

Whiteboard photo:

http://flic.kr/p/bDXGt7

OAuth in the Enterprise

Wednesday 1H

Convener: RL "Bob" Morgan, Dave Sanford

Notes-taker(s): Dave Sanford

This session was to explore some of the problems that Enterprises, including mid or small sized are having in being able to apply Oauth (and other mass market identity solutions) to solve real problems in their space.

Oauth typically is not used in the internal Enterprise context. There is the need to use 'consent close' in the Enterprise context. Currently Bob has lots of Rest based applications using X.509 certs and internal developers hate them. The developers believe that Oauth would be easier, controlling access within the Enterprise.

Alan (HP) asked about whether there is a need to extend internal Oauth to Federations and external users? Bob would like to be able to support them. There was agreement that currently for most organizations, how to do this is very ad-hoc.

There are differences in the perceived managers of permissions - currently with Federation and with X.509 certs – administrators can revoke, with Oauth the intent is to allow permissions to be managed and chosen by users, some of the time.

There was information from Ping Identity discussing the systems they provide that allow administrators and/or user to revoke tokens.

Much discussion about the fact that the relying party in Oauth has the advantage of not having to revoke them, tokens. Bob indicated that various legacy applications should not be in the business of validating tokens. The need for front-ends in this case was discussed.

Justin discussed the work that has been going on within Mitre for years applying enterprise Oauth – most of this has been using two-legged Oauth, but they also have use cases where Oauth is used in the context of the user, but is auto-approving authorization on their behalf. By policy Mitre knows that it is appropriate in these cases to take action on behalf of the user, however the token is appropriately scoped to the user in these cases. Mitre is using hexblobs for most tokens today. Mitre has some consent cases between DMZ to internal case (social app in DMZ, talking to internal system). This uses lots of code Mitre has created, but has made it easy for developers.

Ping Identity discussed that they are primarily seeing SAML for the Federated piece, with Oauth for native apps. Mike Schultz indicated that since providing an OpenID Connect IDP – they are starting to use it for their internal use.

Bob re-iterated as part of discussion that client certs are a pain in the ass, and difficult to use. Justin indicated that Oauth, SAML, OpenID connect can all be pulling from the same user store, they just use different end-points. OpenID connect on top of Oauth allows you to build out standardized identity APIs, consistent with Oauth, and also provides discovery.

Salesforce discussed the fact that they have stood up Oauth and have built OpenID connect – in a way that provides single sign-on and have the ability to provide cryptographic bearer tokens (essentially these are signed SAML assertions).

Salesforce is providing this for customers and still sending people through authorization. Administrators can take control of an application and administrators have the ability to authorize on behalf of all of their users, or have the ability to allow the users do it directly. From the application level it is the same.

Lots of discussion of how Salesforce provides Oauth service to customers – mostly around the fact that they are providing bearer tokens and are not re-validating the user upon use.

Justin indicated that in the Enterprise you are likely to end up with lots of authorization servers, and while you may want to consolidate, you probably cannot every do it fully. Rogue authorization servers are inevitable. Mitre is building mainly on the Spring Security Oauth project, and will continue to provide some open source code to the community, that may be useful to enterprises in building and using Oauth internally.

Ping Identity indicated that if the Enterprise customer has a lot of mobile apps default Oauth says authenticate for each time. They are looking for more standard ways to bulk token authorization. Mitre indicated that they have a helper app to allow that to happen. Various issues were discussed involving bulk tokens crossing organizational boundaries (Federated bulk token case).

Justin indicated that members of the Oauth and OpenID working groups are committing code out to Open Source – Apache Amber project, Spring Security. Those interested should start at protocol pages and will find links from there to various open source efforts.

Backplane 2.0 Widget Collaboration Protocol

Wednesday 2B

Convener: Johnny Bufu

Notes-taker(s): Tom Raney

Tags for the session - technology discussed/ideas considered:

Backplane 2 messaging protocol layered over the top of OAuth2, http://backplanex.com

Johnny Bufu presented an overview of the Backplane 2 communication protocol and the status of the specification, currently an implementer's draft.

Johnny announced that Janrain released their implementation of the specification as open source software earlier in the week. See https://github.com/janrain/janrain-backplane-2.

All specifications and further details about Backplane are maintained at http://backplanex.com.

SCIM 101 and 201

Wednesday 2C & 3C

Convener: Travis Spencer

Notes-taker(s): Travis Spencer, Kelly Grizzle

Tags for the session - technology discussed/ideas considered:

SCIM, OAuth, provisioning, cloud

SCIM 101

http://www.ietf.org/proceedings/83/slides/slides-83-scim-2.pdf

Where things are at

3 interops (including the one at this IIW)

2 shipping products today w/ others in beta

IETF

WG being formed

Prelim schedule puts spec pub date @ 2014

Charter finalized

Work on going on 1.0 "branch" for bugs and small fixes needed for current implementations

All other work happening at IETF

SCIM 201

Authorization – how and to what extent?

Multitenancy

Proxying/targeting/etc.

Etc.

Trust Framework

Tuesday 2D

(presentation located on wiki)

NSTIC How do we bring relying parties to the table?

Wednesday 2F

Convener: Jim Sheire

Notes-taker(s): Willian Lowe

How to bring a wider variety of stakeholders to the table. Get more relying parties.

NSTIC ball is rolling. Bringing government to the table as relying party. Online communities, people, governments: We need more Entities at the table.

NSTIC pilot funding: short term addressing chicken/egg problem of universalized identity. How do we market the business model and value proposition?

Who is not at table yet and how do we approach them?

Where are venues that NSTIC can engage in community building? Retailer shows, banking shows, nonprofits, etc.?

NSTIC wants to Generate excitement, increase engagement. Possibly social media.

Target rp's? Developing top 100 target list. What would constitute critical mass in addition to government that would be sufficient adoption to have snowball effect?

List of target 100 RP's will be publicized. Please send your own top 10 RP's to James Sheire. Individual contacts appreciated.

The problem of successfully attracting rp's: at the moment, a good bit of business value is tied up in the internal relationship between rp identity and idp. Everyone wants to be an IdP.

We're going to have trouble getting major RP's on board until solutions are clarified and are ready for implementation.

What are the generic drivers (influencing factors) for big RP's to get involved? It would be helpful to catalog influencing factors.

The current value proposition problem from enterprise standpoint: you're asking me to change and from my perspective this is a solved problem.

Are there communities of interest that already have shared values (like InCommon)? The way any federation has grown well = shared mission in value.

Lack of awareness for NSTIC. Companies are going to come to table when their customers see value in it as well. Just because they have a cumbersome process for identity doesn't mean they're ready to change. Often it is simply chalked up as a "Cost of doing business."

Possibly a theoretical strategy to get RP"s to the table: Start putting out stuff they hate.

Marketing to big companies: 3 things they care about: revenue generation, cost savings, risk mitigation.

We want to target senior technical advisors (i.e. "principal architect", "technical fellow"): these are the people we want to influence so they can take our pitches back to executives.

Rough List of Communities of Interest:

HIM's

RPG's (games)

SXSW

Consumer Electronics

Boyscouts/Girlscouts

MochaMoms

Maybe better off bootstrapping the solution because big companies aren't nimble enough to quickly adopt and implement new frameworks.

The leading edge of the problems we face are exemplified in a small sector: Porn. Very nimble, creative, and always changing. One step below is the gaming community.

Most of general public doesn't know there's a solution to the identity problem. The more aware they are the the more demand there will be on RP's to adopt.

Nobody is communicating the problem to a broad base, possibly because we don't have a set solution yet.

Nobody who does x number of banking transaction / mo. perceives there's any problem with what they're doing. Everybody hates 100's of usernames and passwords. But they hate it because convenience, not security.

If we can address some of the risk issues, etc. COPA compliance, safeharbor, that would equal another audience of people getting engaged.

Focus on Reputational Risk. Identify the harms.

Ongoing Efforts:

Better communication from NSTIC. What is it about. Why is it important.

Communicate to the general public.

OnguardOnline.gov is currently best government internet security website. NSTIC should be more visible.

Simplified approach

NSTIC How do we bring relying parties to the table?

Wednesday 2F

Convener: Jim Sheire

Notes-taker(s): Willian Lowe

How to bring a wider variety of stakeholders to the table. Get more relying parties.

NSTIC ball is rolling. Bringing government to the table as relying party. Online communities, people, governments: We need more Entities at the table.

NSTIC pilot funding: short term addressing chicken/egg problem of universalized identity. How do we market the business model and value proposition?

Who is not at table yet and how do we approach them?

Where are venues that NSTIC can engage in community building? Retailer shows, banking shows, nonprofits, etc.?

NSTIC wants to Generate excitement, increase engagement. Possibly social media.

Target rp's? Developing top 100 target list. What would constitute critical mass in addition to government that would be sufficient adoption to have snowball effect?

List of target 100 RP's will be publicized. Please send your own top 10 RP's to James Sheire. Individual contacts appreciated.

The problem of successfully attracting rp's: at the moment, a good bit of business value is tied up in the internal relationship between rp identity and idp. Everyone wants to be an IdP.

We're going to have trouble getting major RP's on board until solutions are clarified and are ready for implementation.

What are the generic drivers (influencing factors) for big RP's to get involved? It would be helpful to catalog influencing factors.

The current value proposition problem from enterprise standpoint: you're asking me to change and from my perspective this is a solved problem.

Are there communities of interest that already have shared values (like InCommon)? The way any federation has grown well = shared mission in value.

Lack of awareness for NSTIC. Companies are going to come to table when their customers see value in it as well. Just because they have a cumbersome process for identity doesn't mean they're ready to change. Often it is simply chalked up as a "Cost of doing business."

Possibly a theoretical strategy to get RP"s to the table: Start putting out stuff they hate.

Marketing to big companies: 3 things they care about: revenue generation, cost savings, risk mitigation.

We want to target senior technical advisors (i.e. "principal architect", "technical fellow"): these are the people we want to influence so they can take our pitches back to executives.

Rough List of Communities of Interest:

HIM's

RPG's (games)

SXSW

Consumer Electronics

Boyscouts/Girlscouts

MochaMoms

Maybe better off bootstrapping the solution because big companies aren't nimble enough to quickly adopt and implement new frameworks.

The leading edge of the problems we face are exemplified in a small sector: Porn. Very nimble, creative, and always changing. One step below is the gaming community.

Most of general public doesn't know there's a solution to the identity problem. The more aware they are the the more demand there will be on RP's to adopt.

Nobody is communicating the problem to a broad base, possibly because we don't have a set solution yet.

Nobody who does x number of banking transaction / mo. perceives there's any problem with what they're doing. Everybody hates 100's of usernames and passwords. But they hate it because convenience, not security.

If we can address some of the risk issues, etc. COPA compliance, safeharbor, that would equal another audience of people getting engaged.

Focus on Reputational Risk. Identify the harms.

Ongoing Efforts:

Better communication from NSTIC. What is it about. Why is it important.

Communicate to the general public.

OnguardOnline.gov is currently best government internet security website. NSTIC should be more visible.

Simplified approach

Dynamic Multi-Attribute Authentication

Wednesday 3F

Convener: Mary Ruddy, Don Thibeau, Joop K.

Notes-taker(s): Mary Ruddy

This session included an overview of the OASIS Electronic Identity Credential Trust Elevation Methods Technical Committee (TC), its phase 1 deliverables and a request for input to structuring phase 2.

What is trust elevation?

Trust elevation - Increasing the strength of trust by adding factors from the same or different categories of trust elevation methods that don't have the same vulnerabilities. There are five categories of trust elevation methods: who you are, what you know, what you have, what you typically do and the context. What you typically do consists of behavioral habits that are independent of physical biometric attributes. Context includes, but is not limited to, location, time, party, prior relationship, social relationship and source. Elevation can be within the classic four NIST and ISO/ ITU-T levels of assurance or across levels of assurance.

This includes concepts of step up authentication, continuous authentication, risk based authentication and dynamic multi-attribute authentication.

This is different from the traditional 3 factor model. The ITU-T¤s x1254 added the behavioral factor and we elevate context to a fifth factor.

We reviewed some representative method examples captured in our survey. See below for link to TC¤s website.

Why is it becoming more important

More and more, when dealing with consumers and citizens, there is a need for dynamic authentication. A customer should only be asked to do multi-factor auth when they want to do high value transaction, not as a prerequisite to visiting a website. Few consumers have high LOA-credentials.

Technical Committee’s three phase approach

¤ Phase 1 - a survey of methods of trust elevation and a taxonomy of
five method factors (done)

¤ Phase 2 - an analysis of the methods, which methods counter which threats and are complimentary, etc. (starting to structure the analysis)

¤ Phase 3 - a proposed protocol

We had a good session. People were comfortable with our five factor taxonomy.

We discussed different ways to talk about the inflexion point in the adoption of more dynamic authentication (rather than authorize once and you are done, authentication.)

The chief feedback was that the analysis should include the dimensions of a privacy and making processes acceptable to users (usability and adoption can be as important as risk management in some sectors.

For more information, see: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el

Cipher

Wednesday 3H

Convener: Chris K.

Notes-taker(s): Chris K.

Cipher programming language
session led by Christopher Kula (cjkula@gmail.com)

Cipher: lightweight programming language for cross-platform crypto
http://cipher-lang.wikispaces.com/

Being developed to provide a layer of dependability and abstraction to consistently implement cryptographic algorithms and other data transformations between diverse platforms. Currently in parallel development in both JavaScript and Ruby, development being driven from the same suite of RSpec test. It is one approach to crytpo-in-the-browser.

Existing language in same space is "Cryptol", which is proprietary code owned by Isaac's employer, Galois: http://corp.galois.com/cryptol/
HOWEVER, the spec is open source, so worth considering an open implementation. Could be a possible alternative to further Cipher development?

- Review some possible language structures
- Discussion of security issues with running crypto in the browser
- Discussion of decentralized identity using browser-created keys
- Discussion of issues being encountered by W3 surrounding crypto in the browser, including sandboxing
  (There are few people that understand all the relevant issues, and they are very busy!)

Related W3 working group: http://www.w3.org/2012/webcrypto/

What might a common crypto language need?

consider common needs of crypto algorithms. What are the typical shared abstractions?

mutli-threading for use in a server or cloud context

modular back end: hub and spoke design

task time estimation

secure execution space assurances

algorithm validation / verification

Personal Cloud Special Interest Group

Wednesday 3J

Convener: Johannes Ernst

Notes-taker(s): Joaquin Miller

Tags for the session - technology discussed/ideas considered:

'Personal Cloud'

<the quote marks are to tell IIW volunteers handling these notes that the intent is that this is a single tag; kindly forgive your notetaker's ignorance of tag syntax>

The goal of the session was to nucleate a group of folk who want to spend some time this year (and perhaps beyond) puzzle out what we actually mean by 'personal cloud' and how we can contribute to bringing that about.

One participant drew a picture of what they are building. Others contributed refinements to the picture.

Readers of these notes should expect to hear more about the setting up of some way for such folk to work together.

For a short time, one place to watch for news-until there is a better place-will be:

joaquin.net/PersonalCloud

When there is a better place, a link will also be added at the IWW session page:

IIW XIV W3J Personal Cloud work

Open Source Communities and Authentication with Tiqr & Animate

Wednesday 4F

Convener: Roland Van Rijswijk, Isaac Potoczny-Jones

Notes-taker(s): Isaac

Tags for the session - technology discussed/ideas considered:

AnimateLogin, Tiqr, 2-factor authentication

Notes from the session attached. Links:
https://tiqr.org/
http://corp.galois.com/blog/2011/1/5/quick-authentication-using-mobile-devices-and-qr-codes.html

Move the project from SVN to GitHub to increase involvement of developers

Include a roadmap / backlog to help people understand how to be involved

Create a mailing list to gather user input

Promotion via Youtube videos

For the standard, consider using RFP-type formats – a tool to consider is XML2RFC API binding / standard for OATH

Look at other verticals – NGO, healthcare

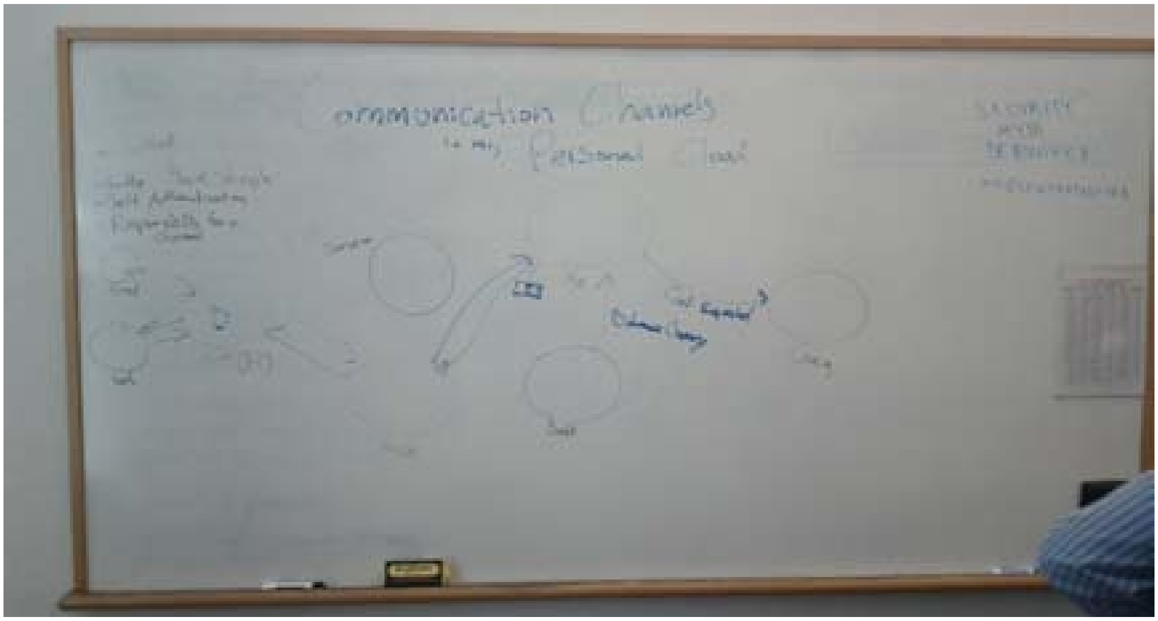
Bob talked about broader uptake of open source community in education / R&E

Communication Channels in our Personal Cloud

Wednesday 4H

Convener: Sam Curren

Notes-taker(s): Augustin Bralley



Sam Curren:

Primary communication channels today are inadequate: e-mail, sms, etc.

Let’s build an new protocol for communication between personal clouds, devices, services

How would it work?

Channels - multi-purpose, thin, communication protocol.

Based on Evented APIs

Setup once, used repeatedly

Channels can be service & party specific, i.e. Between Bob and Joe there can be multiple channels

Channels could ignore all traffic not of a particular type

Channels could be between active and semi-active things

Alan Karp:

How does delegation of authority work? New channel created when authority delegated?

Marc Stiegler:

Watch my YouTube video on Security Myth Debunkers.

“Can human beings manage large numbers of fine-grained permissions?”

Anwser: yes, with an effective UI

Alan Karp:

To do things you have to designate, then bundle designation with authority

Channel properties: revokable, self-authenticating

Phil is writing a white paper covering this topic

Where does OAuth come in? -> Before the event channel is setup

Mozilla offline notifications - browser functions as receiving agent

Virtual compute space needed in cloud (ala Kynetx)

URI endpoints

Sam:

The fundamentals of the connections/channels should be standardized.

There will be need of translations services between standard and proprietary systems

Dave Sifry:

What about retrys? Should this be built into the protocol?

Sam:

Depends on the service, we don't know enough about use cases to build that into the protocol now.

Alan:

Itempotency? Resiliency at scale?

Not all services are fully deterministic.

Dave:

Hold up. What's the point of a new communication protocol? Can't we just use SMTP, IMAP?

It's already ubiquitous. They've solved many of these fundamental protocol questions.

Alan:

It's possible, but it's ugly. Private channels?

Dave:

There are hacks for that, encodings in subject, etc.

Alan:

But it's a little used hack. May as well start anew.

Marc:

Two types of engineers:

99% say there's a patch to make existing system do whatever we need.

1% say we should rebuild the entire thing to be better.

1% group usually loses, but when they win, change is dramatic…

Client Certificate Authentication & Browser Pitfalls

Wednesday 4I

Convener: Vivek Gupta

Notes-taker(s): Vivek Gupta

We are providing an Authentication service for our customer's all internal applications (about 500). The service provide various type authentications e.g. Username/Password, Kerberos, RSA, Certificate.

Certificate Authentication is quite different than other type of authentications because, the authentication process starts during the SSL/TLS connection establishment.

We found that when a user wants to switch to Certificate authentication after the SSL/TLS connection establishment, the browsers behave differently.

SSL/TLS renegotiation can be used for getting the client certificate if you want to perform the Certificate authentication after the SSL/TLS connection establishment.

All the browsers cache the SSL/TLS connection for some time. During that time, if you perform the SSL/TLS Renegotiation and ask for client certificate, the browsers do not provide the client certificate.

We need to close the SSL connection at the browser end and then re-establish the new SSL connection to the same server and ask for then client certificate.

The API to close the connections varies from Browser to browser. In Firefox, you use window.crypto.close() to close the connection. In IE, you have to use documen.execCommand("ClearAuthenticationCache") to close SSL connection. IE however deletes all the session cookies also with this command. So this command in IE does more harm than just closing the connection.

Browser like Chrome, Opera, and Safari do not have any APIs to close SSL connection. Safari infact doesn't support SSL/TLS renegotiation.

One way to resolve this situation is to off-load the Client certificate authentication to another Server instance (or URL) that is protected by Client Certificate authentication. This way the browser will create whole new SSL connection to a new URL and provide client certificate. The problem with this approach is maintenance cost and a whole new proprietary API/System to handle this certificate authentication.

It will be nice to have standard and same Crypto functions available in browser. I guess W3c crypto is trying to resolve this issue.

Demo – Social Verification Google Street Identity

Wednesday 4J

Convener: Stephen Ufford

Notes-taker(s): Tanis Jorge

Tags for the session - technology discussed/ideas considered:

Google Street Identity, ID Proofing, social, Trulioo, global user identity management

Slide Show:

Link: https://docs.google.com/open?id=0B5xBL7auvlKlWEFHemJCT2hlZ0U

Stephen presented a short slide show covering Trust Elevation and how a social verification process can help to build trust on an Internet scale.

Slide 2: The current trust model on the Internet is fragmented. Authoritative and verified attribute data available from governments, credit bureaus and data aggregators is heavily regulated and geographically limited. Self asserted attributes are widely available through the social networks, but can not provide relying parties with required trust levels.

Slide 3: Currently only social networks and IDPs have a direct link to the end user, due to the nature of how the identity is built (user involved). Bureaus and Aggregators must rely on high friction KBA processes to verify users.

Slide 4: The challenge is to find a way to allow users to move-up (never down) the trust elevation latter while maintaining a low level of user friction, and providing the greatest geographic coverage possible.

Slide 5: Outlines how a social ID proofing process can help achieve targeted trust elevation, friction, economic and coverage levels.

Slide 8 -14: An explanation on how social verification works, Predictive analytics determine if a social networking account can be used for verification. Crowd souring provides verified user attribute data. The value proposition of social verify is to deter fraud by displacing the monetary value of the fraud with the associated cost base of perpetrating the fraud.

Slide 16: An invitation to apply to join the Trulioo/Google Street Identity pilots, and to submit use cases to for social verification to the OIX Attribute Exchange, Business Sub-workgroup.

Demo:

Link: http://dev.trulioo.com/uni

Stephen presented a live demo integrating Trulioo's global identity proofing API with Google Street Identity. The demo focused on the distance education use case, whereby universities have the need to verifying overseas students applying for courses to be taken exclusively online.

Backplane 2.0 -- Implementation

Wednesday 5F

Convener: Tom Raney

Notes-taker(s): Tom Raney

Tags for the session - technology discussed/ideas considered:

Client side integration with Backplane 2, OAuth2, http://backplanex.com

Tom Raney discussed the nuts-and-bolts sequence of steps to integrate with the Backplane 2 protocol. Vlad Skvortsov from Echo talked about the history of Backplane and its creation from the need to alert JavaScript applications in a browser context of identity login events. Echo and Janrain chose to create and maintain the Backplane specification as an open standard to promote growth of the Backplane eco-system.

Janrain released their implementation of the specification as open source software earlier in the week. See https://github.com/janrain/janrain-backplane-2 and http://developers.janrain.com/documentation/backplane-protocol/.

All specifications and further details about the Backplane community are maintained at http://backplanex.com.

Asset Discovery for simple web payment (opentransact)

Wednesday 5I

Convener: Tom Brown

Notes-taker(s): Tom Brown

Considered three scenarios

1. Given an email, discovery of relevant assets in basic e-commerce checkout
2. Given a phone number, discovery of relevant assets in point of sale checkout
3. Allow a user to easily add a new asset provider to a mobile payment app

1. discovery with email

we considered webfinger.

given email-like address, merchant
a. merchant fetches /.well-known/host-meta
b. merchant passes payer's email-like address to lrdd template url
c. merchant finds wallet links inside xrd document: http://webfingerclient-dclinton.appspot.com/

lookup?identifier=tbrown@afternoon-waterfall-33.heroku.com&format=web
d. merchant fetches a wallet to find payer's asset types: https://picomoney.com/wallets/herestomwiththeweather
e. merchant chooses compatible asset url to accept payment in: https://picomoney.com/currencies/picopoints
f. merchant presents payment method selection. for instance, merchant may accept up to 20% of payment in picopoints and the rest dollars
g. merchant can redirect payer to asset provider to simply submit payment html form (or ask for authorization of oauth token)

2. discovery with phone number

while an email-like address allows xrd document to be fetched from domain of address, this is not a possibility with a phone number.

instead, it was suggested that, similar to how xri resolves inames, a central site resolves phone numbers into urls.

3. add new asset provider to mobile payment app

the differences between UMA's implementation and OpenID Connect's implementation of dynamic client registration are currently being worked out into a combined future IETF draft.

given an email-like address, the mobile app can also use webfinger to populate list of asset providers from wallets.

4. other issues

it seems helpful to at least start off with an unofficial list of asset provider urls. one of the problems with openid attribute exchange was that there was no consistent repository of agreed on urls to start with although axschema.org was an attempt.

VRM – Where will it start?

Thursday 1F

Convener: Kaliya, William, Jenny and Drummond

Notes-taker(s): Augustin Bralley

Presenters:

Jennifer Cobb - Smart disclosure

Drummond Reed - Retail organizations

William -

Benefits - VRM + CRM = knockout proposition

Question - where does it start?

Doc Searls -

We start with individuals. We can’t just say we’re going to improve advertising.

William -

Utility: Individuals aren’t going to go through a whole new set of steps. There has to be utility, convenience.

Geography: Will this take off in some particular region?

Vertical sector: public, private, not for profits?

Facilitators: technical and legal

Incentive: Aspirin or Candy?

Jennifer - smart disclosure

Cass son stein (sp?) at the white house - office of regulatory affairs

Smart Disclosure: “The timely release of complex info and data in machine readable format that enables users to make smart decisions”

Instead of making companies release data, use behavioral economics

Nudge - build “choice architectures” for people to make better decisions

Invitation to release data instead of a requirement

Examples:

Blue button initiative - a VA hospital patient can click a button and get a digital copy of health records

Vendors (e.g. Walgreens) have signed up to take the data and offer services (e.g. price comparison)

Green button - energy industry - companies have agreed to release their energy data

Idea: data should spur innovations, new businesses

Start with the data, match up with some of the VRMish approaches

This may be a wedge into the VRM problem

What are the major incentives for the community at large?

VRM = new tools and services that make customers independent of sellers

More people have more ways to spend money than before

Intent casting puts money on the table

There’s a lot of problems in customer databases, giving customers access/control will clean up this data

Citizens are in a better position to do things with their data than government is

Drummond -

VRM ultimately has to be a win for vendors and customers

Grid: 4 party system

1st party - customer

2nd party - vendor

3rd party - vendor cloud

4th party - personal cloud

Similar to the four party system with credit cards

What's the incentive in the credit card system?

Credit cards reduce friction of transactions

VRM reduces the friction of sharing data

How do we get this started?

Going to the vendors, getting traction in higher value retail sector (e.g. Car buying, Nordstrom)

Say to businesses, "We believe the value to you of opening a personal channel between your CRM and the personal cloud is high enough for you to want to pay for it, just like credit cards"

Personal channels are:

trusted communication channel with vendors (individuals can dial it down, or turn it off)

Similar to the target irrevocable address concept patented by IBM for email

Bi-directional data sharing

Vendors can send offers to users, users can send intent to vendors

Intent casting

Customers can broadcast their intent to multiple vendors

Continuous customer channel

Can't be unintentionally broken

Doc -

E.g. Car rental business

1st party - customer

2nd party - Avis, Hertz

3rd party - Orbits, Kayak, Travelocity - agent for the vendor

4th party - Autoslash (games the reservation systems), Rental Magic (gets lowest rate, $20/month) - agent for the customer

William -

Where do we think this VRM thing is going to start?

Group -
Life context, with individuals
High value transactions
23 and me - health medical records
Organizations who have a high commitment to customer service (e.g. Nordstrom)
People who work in office buildings
Freelancers
High net worth people may be more concerned with privacy?
Reduce the cost of being Nordstrom (customer service cost)
Family CIO, Family HelpDesk
Improve non-profits' already good relationships with their members
Coop concept - a credit union for data
Life-time value of a customer
Young people care a lot less about privacy than older people?
There's an awful lot of ad-hoc VRM happening now

William -
The BBC created a cultural asset that puts digital culture in one place (thespace.org)
PII will be kept in a personal data store, ask users to share that data someday
There's no business model, they just think it's the right thing to do
Ethical leadership
The principles of VRM are so right, that there's an ethical leadership opportunity
Maybe this will happen on the non-commercial side first

Group -
Is the channel the relationship itself?
It's mechanizing the relationship - The channel is the dance
Creating an asset structure around my channel

Some sort of trust is necessary
More likely to create those game rules as a non-profit than a startup
People simply want to be able to say that someone us looking out for me in this context

Experian research showed that people trusted experion more than a startup (Personal)

The public good can be defined broadly and individually

I'd like an organization built around the interests of the customer (individually)

Different people have different levels of mistrust of various sectors (e.g. banks, data aggregators)

We need to set baseline rules for trust

PDS is an example of the kind of viral adoption dynamic needed for this to take off

Intrinsically harmonious relationships

How do we get consumers to be concerned and get them to act?

What are the trigger points?

Behavioral economics: how do we make people change their behavior?

Making choice architectures

Really complicated solution, but a powerful idea

We need the invention that is the mother of necessity

Customers need to get PDS without even knowing they got it

Problem: trusting vendor to vendor

Matrix

X: -Right : +Pragmatic

Y: -Individual : +Organization

It's far easier to go to a company that competes on its ethical proposition: Quadrant 2 (-x, +y)

The amazing hyper connected API + XDI based world / Beyond calf-cow escape from client server

Convener: Judi Clark, Doc Searls

Notes-taker(s): Mark Sabadello

The goals of the session were to:
- Imagine the VRM-enabled network we want to build and its properties
- Think "outside the cow", i.e. build a system that does not rely on a central authority

Ideas raised during the session:
- Today's online world is a set of domains, and the web is just one app on the Internet, which was originally meant for endpoint-to-endpoint communication
- On the web, there are always dependencies which we cannot escape
- But the offline world is different, e.g. you get into your car and you can do with it what you want
- The web allows us to publish, but not to selectively share and protect personal data
- The web does not provide good mechanisms for referencing, sharing and linking the data we are dealing with
- Must get the right data to the right people to empower us and even save lives

- To achieve this, stable identifiers are needed (DNS and IP addresses are not stable)
- XRI could provide such identifiers, and XDI could provide the technology for referencing and linking data
- Content-centric identifiers such as magnet: URIs also exist

Data is like seashells.. I have the largest collection of seashells, I keep them on the beeches around the world!

To get rid of cow/calf model, we need different architectural models, e.g. Federations, Personal Data Stores, FreedomBoxes, etc. instead of centralized silos.

We need to be more inclusive of things other than hosts and other than individuals.
For example, include groups, organizations and the Internet of things in our vision.
Also abstract concepts, not just concrete things from the real world.
Need to be able to discover and describe all those entities.

Necessary technologies that were mentioned during the session:
XDI, RDF, Semantic Web, Persistent Identifiers, Torrents, Global Registry, Distributed Hash Tables, Distributed Edit Histories

Other important ingredients for the ecosystem:
Contracts, Agreements, Disclosure, Informed Consent, Provenance, Infrastructure

Are custom URI handlers EEEEEEvil?

Thursday 2G

Convener: Bill Mills

Notes-taker(s): Bill Mills

Posed the initial question.

Discussing one of the possible ways to protect the URI handler, Saleforce addt'l noce explained (we hope).

Alternatives:

Push notifications mentioned as an alternative.

Localhost: $port mentioned as an alternative.

How do you get the app back in focus on mobile apps.

"Colluding 3rd party server": probably a "long poll". Workable but you still need a way to have the web flow put the focus back on the phone.

Nonce checking: the app provides a nonce that must be checked before doing anything. *** This is probably the winner

Nonce checking would be where the app registers a URI for callback and prepends a per event or per app non-guessable (probably a random number, but could be a deviceID). The URI handler can then check that prefix before doing any more processing. For example:

Myapp:nonce_UFTh2j4yg4dh5gr?token=&session=

Another good recommendation! Limit your token callback to just that purpose. If you need other custom URI handlers register a second one.

How to add an account chooser to your website

Thursday 3A

Convener: Eric Sachs

Notes-taker(s): Eric Sachs

Presentation link:

https://docs.google.com/a/google.com/document/d/1gZ-J-m_TfvvaxFcLuE8vNJjt00EXgRBOXsc0WYGbyiU/edit

Trust Framework System Rules

Thursday 3F

Convener: Dazza Greenwood (@dazzagreenwood)

Notes-taker(s): Note-takers: Eve Maler (@xmlgrrl) and Jamie Clark (@JamieXML)

Resources under discussion are generally available at: http://civics.com/

What's the definition of a trust framework? Does it have boundary conditions? Is it a "club with rules"? The rules seem to have business, legal, and technical aspects. Could the boundaries be set dynamically? Perhaps, but it seems odd to include someone in the club without their knowing it.

Accounting for the regulatory aspects of trust frameworks is challenging. Better to just consider all "contractual" elements? Trust framework system rules are multilateral agreements. That set of contractual elements are not literally regulatory. Private parties get together and define a boundary for their "bubble".

Does such an agreement have to be legally enforceable? Are a bunch of tennis partners that expect each other to take turns buying the beer afterwards could be described as being (lightly) bound by a trust framework. But generally, what's at stake has high value in the aggregate, so enforcement -- whether legal or getting kicked out of the club -- is a part of the expectations.

For today's discussion, we're talking about explicit, written, agreements that involve business, legal (ideally enforceable), and technical elements. There are elements of verification, duties, and so on. Precedents: payment systems (e.g. ACH), supply chains (e.g. EDI), credit cards (e.g. VISA), and identity federations (e.g. InCommon)

People tend get lightly bounded when they visit a site through at least click-through ToS agreements or similar. Other ways of entering a trust framework are typically more tightly bounded. An important component of rules is exception rules, or "error trapping".

The Technical super-section of the sample Table of Contents starts with use cases, to capture the scope. The Legal super-section might include legal criteria for participation, so that (e.g.) for a insurance industry framework, shoe sellers wouldn't be eligible. Standardized liability statements aren't really available; they tend to be quite specific to the circumstances.

Dazza will soon publish his recent work on the insurance industry trust framework that he showed today. See other samples at: http://civics.com/idfederation-framework/

Trust frameworks have to emit pheromones that say "come play", so that they'll survive.

How do parties know what trust frameworks they should be joining? Right now, there are a bunch of efforts that aren't really ready to be joined yet. How to translate the credit card model to identity? OIX et al. are creating tools around this, but for right now, you'd probably know about them because they're idiosyncratic to your community. The trust mark aspect of the TOC shows a way that trust frameworks could be branded. This typically involves certification so that you can use the mark. Think of UL listing: http://www.ul.com/global/eng/pages/ In the future, maybe we'll see "OIX Listed" sites.

Cisco connects to 400 providers. It's painful to set each of these up. The use cases include both B2B and SaaS connections.

A lot of the TOC comes from or is inspired by the "PKI days". The supposed openness of those early projects actually added friction because people weren't sure if they were or should be considered within the boundaries. So the more bounded frameworks have worked better since. This is why business use cases are the starting point for filling out the TOC. There's an ROI for each potential member; some may choose not to join, or not to join now. The whole point of the multilateral agreement is scalability; this is a big part of the value.

Dazza is working with Jamie and OASIS to standardize this TOC approach. Operating rules/system rules are a persistent phenomenon. If you don't have rules like this, you basically can't "federate" (= operate under some set of rules).

Historically, forming the framework has been a matter for deep experts only, and it's had trouble scaling because the work product looks like it. :-) The current rules would "gag a yak" :-), and thus don't scale to the consumer market.

Typically it's "RPs" (parties who need to be assured that others' interests will sufficiently align with theirs) who get together and become the policymakers that create the rules. See: http://openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf

Perhaps what we'll see is some successive approximation over time, a la open source licenses. Interoperability starts to become a well-known best practice.

What about the VRM fourth-party type of discussion? And what about other use cases that don't strictly use the IdP/RP/user triangle? Does the system rules model sale to n parties? Yes; you can define as many roles as you want. A party might be in more than one role, so you may have to consider interlocking duties.

"User-centric" frameworks are new, but Dazza had an opportunity to work on a research project that was related to veterans returning from war and using an Android app that behaviorally predicts PTSD etc. What do you with highly sensitive mobile, personal, and military data? The advice he got was to take the veteran's point of view in doing the system rules. This has a strong personal datastore aspect. Here's an example: http://civics.com/pd-tf-sysrules/

Some other trust frameworks Dazza has known and loved before: http://civics.com/trust-frameworks/

Dazza is starting to share some standard clauses between these projects and XACML and SOA system rules. These are shaping up to look a bit like the UMA Trust Model rules: http://kantarainitiative.org/confluence/display/uma/UMA+Trust+Model

Starting with the assumption that the individual owns their personal data and in full control of whom they share it with is often the best way to proceed. This is the operating assumption in healthcare records too.

Nailing down copyright licensing is a good backstop if other things go wrong, but the tactics need more work.

Join the OASIS TC discussion list and visit civics.com to continue the discussion! They're working on the TC charter proposal now, and is looking for proposers. They plan to launch in June.

Entropy via DNS

Thursday 4G

Convener: Bill Mills

Notes-taker(s): Bill Mills

Turns out DNS has fundamental properties that make it unsuitable for delivering reliably entropic entropy beyond that inherent in DNS itself.

Cool discussion with good folks! My thanks!

-bill

UMA Open Meeting

Thursday 4J (Part 1) and 5J (part 2)

Convener: Eve Maler

Notes-taker(s): Eve Maler

UMA site (we courage people to become participants): http://tinyurl.com/umawg
UMA FAQ: http://tinyurl.com/umafaq
UMA protocol spec: http://tinyurl.com/umav1
UMA trust model spec: http://tinyurl.com/umatrust