Moonshot Developers Meeting

14th & 15th October 2013

Attendees

Henry Hughes, Janet

Rhys Smith, Janet

John Chapman, Janet

Rina Samani, Janet

Adam Bishop, Janet

Josh Howlett, Janet (video)

Sam Hartman, Painless Security

Margaret Wasserman, Painless Security

Mark Donnelly, Painless Security

Alan Buxey, Loughborough University

Scott Armitage, Loughborough University

David Chadwick, University of Kent

Suleman Tariq, STFC

Stefan Paetow, Diamond

Mario Szpuszta, Microsoft

4xstudents, Southampton University (Day 1) (video)

Jim Schaad, Independent (Day 1) (video)

Kristof Bajnok, NIIFI (video)

Alejandro Perez Mendez, University of Murcia (video)

Code update

- Last updates mainly security related e.g. Moonshot Id Selector now stores passwords encrypted. If you don't select save password next time you run it remembers the id and the service and prompts for password. This will be coming to Windows soon.
- Next version will force TTLS and will require channel binding for mutual authentication. So if you are doing SSH you will need to know how to use certificates on clients.
- FreeRADIUS examples /etc/freeradius/sites-available

janet

- /usr/share/doc/moonshot-ui/examples has an example provisioning file. * means it applies to everything, otherwise you list the services it applies to.
- moonshot-webp -f default-identity.msht (-f stores in flat file store not the id selector)
- Will remove .gss_eap_id from future versions as it doesn't include a certificate hash.
- We would appreciate any bug reports and patches. – Discussion: moonshot-community@jiscmail.ac.uk reports: http://launchpad.net/moonshot
- One outstanding bug - multiple versions of crash on exit / segfault on exit on Ubuntu

Web Issues & Shibboleth Approach

- Painless Security will create an API that Javascript developers can use to access Moonshot. Will use existing frameworks where possible. This will allow anyone to use Moonshot more easily in a web environment. Compared to current technologies, this get rid of the discovery issue and have greater security against phishing, A web plug-in will also be good for rich web apps. It will allow a User to control privacy – it will use the ID selector, but it won't disclose to the SP what identity you are using. The plan is to integrate with the Shib SP in Apache as one of the ways to take advantage of this technology, but it can be used in other ways. It will be RESTful from Javascript.
- Do we want it directly integrated into Shibboleth or have a separate module to provide the Moonshot glue? If so, the design work will be initiated.
- Could be fun integrating with webRTC for audio video collaboration. Also provides adequate security.
- We want to provide building blocks for people providing web apps – we need to know how this will interact with OAuth and Openid Connect etc. We're open to input, but this is an engineering project not a research project. This will be open source, but if we use SSP on Windows that won't be open source. Raw GSS build on Windows might be open source, but that might have issues.

OpenStack

- All federated stuff is independent of protocol - SAML, Openid Connect, Moonshot.
- It was implemented by an MSc student and a GÉANT researcher will be picking this up when she starts on 23rd October. The OpenStack specs have timed out, but will be picked up again by the new researcher.
- RedHat is interested in ABFAB - Adam Young - Senior Software Engineer - a member of Red Hat's OpenStack team and a core developer on Keystone, the identity management server for OpenStack.

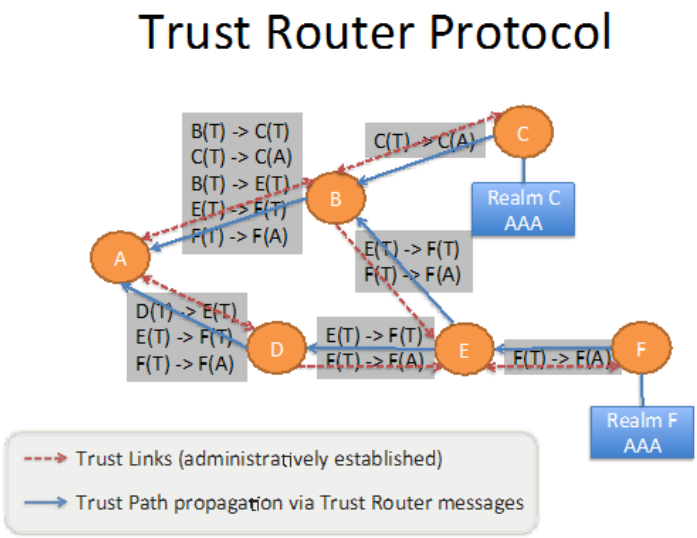
Delegation

- We don't yet have a solution for the delegation use case, where you SSH into a server and then need to get to another server. There is no user control over authorisation (hence no delegation).
- Hal Lockhart, co-chair of XACML gave a talk at last year's MIT consortium on delegation - http://www.kerberos.org/events/2012conf/2012slides/lockhart-2012-kerberos.pdf.
- Nothing fundamental in Moonshot that prevents delegation, this can happen out of band or future eap methods may allow this.
- What about having an attribute level above what we are doing? Trust Router and Communities does this by delegating a policy to an IdP. Would this approach work with unmodified applications? That's the interesting question.
- Or just have multiple profiles and if you need more permissions then use su -.

- Great to know which policy applies, but there are no implemented solutions to the technical side. Alejandro uses Moonshot to jump to Kerberos.
- Where does attribute handling take place? IdP or SP or 3rd party?
- Fast re-authentication is a constrained delegation.

Trust Router Discussion

The next version - 2.0 – will allow more than one Trust Router in a federation, peering and will run the trust router protocol to exchange trust links.



- Margaret described the Trust Router Protocol.

The Trust Router Protocol is used to exchange information about available Trust Links within an ABFAB Federation. This information is used by Trust Routers to determine the best Trust Path to use for transitive trust establishment across the federation.

The Trust Router Protocol runs between pairs of Trust Routers. Each Trust Router will have one or more peers with whom it exchanges information about its own Trust Link Database, including its locally-configured Trust Links, and Trust Link information that the local Trust Router has received from other peers.

Each Trust Router uses the information that it has received from peers to create trees of all of the available transitive Trust Paths, rooted at the local Trust Router. A Trust Router will, at least conceptually, maintain one tree of Trust Paths per COI.

The diagram above shows a portion of the Trust Link information that might be propagated between 6 Trust Routers for 2 AAA Servers, all within a single COI. The dashed red arrows represented administratively configured, unidirectional or bidirectional Trust Links between realms. The Blue arrows represent the flow of Trust Link Database information for the two AAA Servers shown in the diagram – the Realm C AAA Server, and the Realm F AAA Server. The Trust Router in realm A receives two Trust Link Databases, one from Trust Router B, and one from Trust Router D. Trust Router A can build a tree from this information that shows two possible paths from Trust Router A to a AAA Server in Realm F:

- A(T) -> B(T) -> E(T) -> F(T) -> F(A)
- A(T) -> D(T) -> E(T) -> F(T) -> F(A)

Formatted: German (Germany)

The Trust Link between Realm B and Realm E is unidirectional, so there is only one Trust Path between Realm A and the AAA Server in Realm C:

- A(T) -> B(T) -> C(T) -> C(A)

- (T) denotes a Trust Router link , (A) = AAA server , (R) could represent a Radius server infrastructure
- These are GSS and TCP connections so we're using Moonshot to make Trust Router work.
- Assumption that a CoI is inside an APC. Conceptually you could have a CoI that spans APCs. Sam would not expect A links to appear in a CoI graph.
- AAA links will only have an APC associated with them.
- Say Janet ran a UK universities' APC and Renater ran a French Universities' APC. If a member of the UK APC runs a service they want to offer to French universities then how to do so? Peering? Or should a service join both APCs?
- A COI may be willing to trust more than one APC. The APC states the rules that are trust worthy or not. As an individual Trust Router I can't say anything other than I trust something or not. e.g. If we trust Trust Router E to give us information about Realm F AAA and it gives us rubbish then we have to trust the rubbish.
- Don't peer with someone you don't trust.
- The APC policy must include rules for what trusting a Trust Router means.
- An RP can trust somebody, an IdP can trust somebody, a member of a CoI can trust somebody. Anyone creating a COI has to trust the APC.
- JSON is used for sending trust links (source, target, type)
- What areas need to be fleshed out for review - document needs a little bit more work. Jim agrees with most of it, but needs to see the details. MRW will send out for review 'very soon'.
- Sam thinks of each community as separate graphs. otherwise people may assume more connectivity than there is. e.g. a node might appear in more than one graph but that doesn't mean those graphs are connected.

janet

Error messages

- Would like a different message from "I've never heard of that COI" and "I know the COI, but my routing system doesn't talk to your AAA server".
- Answers get so far then fall in to the problem that RADIUS doesn't have a useful error message. Might be solvable as we can inject whatever we want in to an accept/reject message
- There's a rule that says you can't have another message if you have an EAP message.
- Need a way of fixing what error messages are returned.

Security-certs

- Sam is concerned about the reliance on MSCHAPv2. If you don't check certs an attacker can collect enough information that in 11 hours and with $200 someone can recover your password. This is the state of the art if you are using wireless access to AD.
- Makes it as secure as TTLS PAP.
- There's no PAP-EAP method but Stefan has found a work around.
- What could we do? Write to Microsoft security team who is familiar with their security implementation and SSP and say "Is there anything you would consider implementing?"
- EAP MSCHAPv3 or EAP-Kerberos.
- Managed Service could help with this
- Need a deployment tool that pushes out the correct security certs.
- EAP-PWD inside TEAP might work.
- Enterprise deployment is probably going to be the main way of rolling this out so deploying a certificate at the same time may be achievable.

Microsoft

- Mario described Windows Azure and Windows Azure Active Directory - a multi tenant directory service. It supports WS-fed and SAML allows you to manage users on the cloud and authenticate and access content on the directory via the directory graph api. This service can be used by on premise and public cloud applications to include federated identity. Microsoft is using the infrastructure for authentication for Office365.
- Kim Cameron's team wants to Moonshoot the CIPM infrastructure to have Moonshot as an authN option for Azure.
- Kim's team will do the integration into CIPM, but before then there are things we need to do.
- Other opportunities - leverage Windows Azure as a cloud burst solution for HPC to run Scientific Linux VM and use Moonshot and RADIUS for cross premise AuthN and AuthZ.
- For both direct integration and bursting we need the basic infrastructure running and to have a trust relationship. So the first step is to set up a RADIUS server in Azure and see if it works with Microsoft's infrastructure. Theory is it should just work, but in practice may be more difficult.
- Also would like to get eduroam into Microsoft internal IT, but this will be a bureaucratic process.
- Mario will liaise with Sam and Margaret once their Radius server is up and running.

Managed Service

- Plan is to design services to be offered in a cloud - private mainly, but possibly public too.

janet

- The RP side will be multi-tenant to get a Radsec certificate or PSK on your service and you'd be told which RADIUS server to go to and would look up in a database what the appropriate constraints are.
- The IdP side will have dedicated VMs for a customer, configured from a cloud service. Would want tenant isolation on the machines. Customer would be running own AD or LDAP or connecting to Azure AD for directories and the service will glue that into Moonshot world and allow policies to be applied (realm, OU, Groups) all this will be managed by the Moonshot management portal which would automatically select AAA server based on groups.
- Purely a cloud solution that needs a route back to a home directory. VPN? If so, what? If an appliance (on a VM or hardware) you just open a reverse connection.
- Why not use OAuth 2.0? Moonshot allows you to federate services and get security advantages that OAuth 2.0 doesn't. But if Moonshot doesn't give you an advantage then use something else.
- OAuth 2.0 can handle delegation and it is theoretically possible that you could link to them.
- Painless Security would like to understand the features that would be required and details on the potential problems that would be faced by the users.

Mobile

- Jisc has some core funding for mobile AuthN and AuthZ to better understand options available and what we should be looking at. This isn't Moonshot specific, but should consider Moonshot.
- We should consider how the web plug in can develop into a mobile solution (not part of the current scope).
- There's not been a user requirement yet, but something that may come up so we should be prepared.
- CESG now allowing BYOD in PSN as long as certain things have been covered.
- Information security - governance, management - all coming to the fore and being pushed as part of government cybersecurity efforts.

Security-packages

- Who is responsible for making security decisions (as some things are in EPEL packages)?
- Diamond admins just want to get updates from their distro repository - they don't want to have to maintain multiple repositories. Diamond would like a statement from Janet on who is responsible for the security aspects.
- Would Janet be monitoring all related tool packages - xmltool, Shibboleth - how safe are these bits of software?
- Shibboleth is fairly safe. Janet is a core funder of Shibboleth Consortium with Internet2 and Switch (and open to other members) so funding is stable and the team is responsive to security issues.
- Who pushes updated packages to distributors? Does the Shibboleth Consortium deal with RedHat or CentOS etc.? Everything the Shibboleth Consortium has direct control over is updated by them. Other things aren't.
- We are pushing out Moonshot-specific builds.
- From Open Source side, security bugs need reporting through http://launchpad.net/moonshot. Painless Security has some responsibility for dealing with open source issues and has a broader remit for supporting Moonshot under the Janet contract. For anything else, customers should come direct to Janet.
- Distros that use Moonshot will have some responsibility too.

janet

- Who is responsible for all the bits that Moonshot cobbles together?
- Janet and Painless will publish a list outlining where responsibility lies for packages that are outside the normal distribution channel.

Questions

- Have SSH patches gone upstream yet to RedHat or OpenSSH consortium? OpenSSH folks have not been willing to take GSS patches so Simon Wilkinson maintains Debian, Ubuntu and RedHat patches. Simon may try and submit some to OpenSSH. We haven't submitted patches to Simon yet - got stuck with Sam - someone else needs to take on this task. Sam confident that they will be taken up and put into distros. No patches are required on the client for SSH.
- pam_gss - if pam doesn't get a response it leads to time outs. This is Luke's code that he has contributed to the community, but has not been really taken up yet. If people want to use it then we'll make it a more priority (Diamond using it for console logins).
- Stefan can't get SSH and pam_gss to work. Can they skip GSS-API and use pam_gss instead? pam_gss has a different threat model than GSS-API and exposes a long term credential (the server gets a copy of your federated password). pam_gss doesn't have a way of getting the trust anchor if the home IdP so always vulnerable to man in the middle attacks (no channel binding). It isn't clear whether this is okay in a Trust Router world or not. Maybe need to add additional checks, but you may be able to depend on RADIUS authentication for pam_gss as the client and server will be on the same computer.
- Diamond admins were interested in Moonshot – which is a good sign.
- Managed SAML service could be the SAML COI attribute authority

Geant Moonshot Trial

- Over the next three months the trial will focus effort towards the deployment of Trust Router. Trust Router peering would be ideal to test end of 2013, however Painless Security feel it may not be ready by this time. Sam suggested that interested sites deploy and familiarise themselves with Trust Router, by which time the Janet Trust Router will be operational for the pilot.