Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

* The IETF plenary session
* The IESG, or any member thereof on behalf of the IESG
* Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
* Any IETF working group or portion thereof
* The IAB or any member thereof on behalf of the IAB
* The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Logistics

- Audio stream:
  - http://videolab.uoregon.edu/events/ietf/ietf782.m3u
- Jabber:
  - fedauth@jabber.ietf.org
- Scribe

Agenda

- Agenda Bashing
- A description of the use cases - Klaas Wierenga (15min) and Josh Howlett (15min)
- Discussion on use cases (15min)
- Related work - Shawn Emery (5min)
- Moonshot problem statement - Hannes Tschofenig (10min)
- The Moonshot proposal - Josh Howlett (25min)
- Technical discussion (30min)
- Charter overview (5min) - Sam Hartman
- Charter discussion (30min)

A description of the use cases

Hum#1

Do you understand the problem?

Hum#2

Is it useful to work on this in the IETF?

Related work

Moonshot problem statement

The Moonshot proposal

Technical Discussion

Hum#3

Can we proceed with charter discussion?

Many technologies provide the ability for users from one organization to access web services and sites offered by other organizations. The web content provider does not have access to the credentials that the user uses to authenticate to their organization and may not even be aware of the authentication technology in use between the user and their organization. This decoupling of roles is called federated authentication These web federation technologies include OpenID, Security Assertion Markup Language (SAML), OAuth, Information Cards and others. Web federation technologies typically provide some combination of authentication, authorization and personalization services.

Based on experience with these technologies, users and organizations would like to gain federated access to other applications such as IMAP, XMPP, SSH, NFS and a variety of non-IETF protocols. This working group is chartered to develop a solution to these problems .

In particular, one user community has come forward with requirements to support SAML as a mechanism for managing authentication and authorization to service providers for non-web applications for both user and service principals, such that a common mechanism can be used for both user-to-service and service-to-service use cases. In order to be successful, a solution needs to address how federated authentication is integrated into application protocols and how relying parties communicate with identity providers. Web federation technologies explicitly do not address how users communicate with their organization's identity provider. However it is undesirable to depend on a web browser for authentication in the non-web case. Therefore, a standardized solution for communication between the user and identity provider is required. In developing such a standard it is desirable to work on scalability to a large number of identity providers and to avoid introducing exposure to phishing attacks. Re-use of existing technologies is strongly desired.

This working group will develop a solution to the non-web federated authentication use-case. The Generic Security Services Application Programming Interface (GSS-API) (RFC 2743) will be used to integrate federated authentication into application protocols. AAA protocols such as RADIUS and Diameter have significant success in federation for network access. Based on this success, they will be used to provide communication between the relying party and the identity provider. The Extensible Authentication Protocol (EAP) (RFC 3748) will be used to communicate between the user and the identity provider. The solution will support SAML for authorization and personalization. It is desirable for the components of this system to be reusable in other environments. For example it would be desirable to be able to extend the solution to support another authorization mechanisms besides SAML.

This work will require close coordination with work going on in the OASIS Security Services Technical Committee (SSTC). There should be sufficient overlapping participation between the SSTC and this working group for informal coordination. The chairs of this working group may work with the SSTC chairs in case formal coordination is required.

Concerns have been raised that additional work is required in keying AAA associations in a federated environment; draft-howlett-radsec-kmp-00 describes one set of concerns and proposes a potential solution. The working group is chartered to explore these concerns and if needed, specify protocols that use existing AAA key management mechanisms to address these concerns. The working group may not change RADIUS or Diameter; in the unlikely event that these key management concerns require changes to RADIUS or Diameter, those changes must happen elsewhere.

The solution will use draft-howlett-eap-gss-00, draft-howlett-radius-saml-attr-00, and draft-hartman-gss-eap-naming-00 as a starting point. Through the normal consensus process the working group can make changes from this starting point.

In addition, the working group will explore the usability and user interface issues associated with federated authentication. The work is not chartered to standardize protocols or recommend best current practice in the area of usability. The working group should explore the area and write informational documents describing the issues and recommending appropriate work for the IETF in this area. As future work in dealing with user interface in this area progresses, the architecture of the system may need to expand to include additional components or make significant changes to adapt to improvements in understanding of user interface. In describing architecture work, the working group will emphasize this possibility of change.

The deliverables of the working group are:

• An update to the EAP applicability statement in RFC 3748 describing the applicability of EAP to application authentication and placing appropriate requirements on this new EAP use case
• An update to the EMSK root key applicability statement in RFC 5295
• An architecture document describing how the components of the solution fit together to address the use cases and open issues that will require future changes to the architecture
• A standards track solution for using EAP methods to provide authentication within the GSS-API
• A standards-track protocol for carrying SAML messages in RADIUS
• A standards-track description of GSS names and name attributesrequired by the solution
• Informational descriptions of usability and user-interface concerns related to this work

Hum#4

Are you ok with this charter modulo agreed changes?