SAML
Security Assertion Markup Language
February 10, 2005
Discussant: Dennis Kafura

Relationship to other languages/models

1. (Haiyan Cheng) What’s the difference between role-based access control and attribute-based access control?

2. (Craig Bergstrom) The purpose of SAML is "...to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information." The goal of XACML is to "...standardize access control language in XML syntax." Are these goals not similar enough to merit a single solution? In general, how can we develop an infrastructure to allow for better collaboration and identification of possible partnerships between entities attempting to achieve the same or similar goals?

3. (Glenn Fink) How is SAML related to WS-Federation? Is SAML an enabling protocol there like it is for Shibboleth, or do SAML's functions overlap WS-Fed more?

4. (Glenn Fink) Are SAML artifacts the equivalent of WS federation security tokens?

5. (Ranjit Randhawa) What is the difference between SAML authentication assertion and other authentication protocols in a federated environment?

6. (Darrell Hyatt) Referring to figure 6 (in Secure Web Services) showing the relationship among the web services standards, who, if anyone, is using this?

7. (Muhammad Abu-Saqer) It seems that SAML need SOAP in carry its assertions, could SAML provide a mechanism to do this by itself.

8. (Muhammad Abu-Saqer) To what level does SAML belong, transport level or message level scheme.

9. (Muhammad Abu-Saqer) It is obvious that SAML doesn't provide standalone solution and it just one building piece of the overall security. The question is how we can build security using just one solution, what are the obstacles prevent such solution.

10. (Muhammad Abu-Saqer) What are the advantages of the proposed solution over the federated system.

11. (Muhammad Abu-Saqer) What are advantages of the message-level scheme opposed the transport-level in the security transactions?

12. (Glenn Fink) What is the equivalent of the WAYF in SAML?
Role/Properties/Assumptions of SAML

13. (Haiyan Cheng) Is there a time constraint for the validity of the assertion? How long is the assertion remain valid in the asserting party to guarantee effective user tracking?

14. (Darrell Hyatt) Aren't we effectively working to turn a browser into a state-aware machine? Could this very state-awareness be used against the user?

15. (Muhammad Abu-Saqer) In section 5 User Tracking (GroB paper), the author has mention that source site S sends a pieces of verification information vi back to browser B. My question is where the user’s browser keeps this pieces of information, is it the same thing as cookie?

16. (Muhammad Abu-Saqer) Does SAML support nonrepudiation? (Nonrepudiation means that a communicating partner can prove that the other party has performed a particular transaction).

17. (Muhammad Abu-Saqer) Does SAML trace the user transaction?

18. (Aparna Sharma) The secret to Centralized Identity paper states that ”To mitigate risk, SAML systems use timed sessions, …”. How are sessions timed by SAML to reduce risks and can the user decide these timings for added security?

19. (Vinod Eligeti) The paper says the timed session eliminates the risk of the three threats. But how can one be sure of it. If some hacker sends some messages within the bounding time he/she can do whatever an authorized user can do.

20. (Vinod Eligeti) The author says that each artifact should be used only once. It assumes that if at all any one taps the messages and replays it the checker made the request invalid and wont give permissions for that request. But what if the hacker sends the first message by altering some parts of the artifact request?

21. How fine must the timing granularity be in a SAML deployment to mitigate the three well-known attacks?

22. (Muhammad Abu-Saqer) One of the shortcomings I see in SAML that when the issuing party send the assertion statements, it has no control over it. The relying party can extend the working time for this assertion forever. Is this right and how is could be fixed?

23. (Glenn Fink) How does a SAML service know where to find the proper authentication chain? How does insurance.com know to ask cars.com for the user's credentials?

24. (Glenn Fink) SAML is built of building block specifications that can be put together into a profile to solve a particular problem. How interoperable are different profiles built on the same specification?

25. (Glenn Fink) How can Single Logout Protocol achieve nearly simultaneous log out in a widely distributed system?

26. (Glenn Fink) It is the user's responsibility in SP-initiated Post-Post web profile, and the service provider's in redirect-Post, but how much does the user or SP have to know to set up and use the IdP's service?

27. (Glenn Fink) How is this Intersite Transfer Service established so that it knows how to find identity providers?

28. (Glenn Fink) The specification recommends use of an underlying PKI. Why does it select this technology as opposed to another identity framework?
Agreements/Trust Among SAML Sites

29. (Haiyan Cheng) Is there an interpretation mechanism for attribute statements among all participate parties.

30. (Varun Pandey) The specification of the SAML framework says that its up to the Service Provider to trust the assertions provided by the identity provider. Lets suppose a case where the service provider doesn't support the identity provider. What in that case? It would be interesting to ponder, can the current specification be extended to provide a hierarchy of identity providers, wherein the lower level identity provider becomes the relying party and the upper level identity provider becomes the asserting party. Or can we use the current protocol to extend the system horizontally if not vertically? The point here is that we cannot expect one identity provider to be trusted by all service providers.

31. (Ranjit Randhawa) Are there any rules/regulations for organizations becoming SAML authorities to new organizations or is it based on pre-existing trust?

32. (Lee Smith) How do two sites establish the relationship that allows them to transfer authentication tokens between each other, and have those tokens have meaning. There has to be something to prevent me from creating my own web service to give me authentication tokens, which can then be transferred to another site, giving me access to it. So how do two sites trust each other’s tokens?

Authentication/Authorization Issues

33. (Haiyan Cheng) How does the authorization decision from the asserting party affect the authorization for the relying party?

34. (Aparna Sharma) What happens in the scenario where the user Attribute Statement does not contain all the information required by the requesting party? Can the requesting party in such request for specific attributes in the SAML assertion request?

35. (Darrell Hyatt) Referring to the Open Federated Model (in Secure Web Services), if multiple entities can vouch for me, what is the order of preference? As a resource manager, when do I consider someone to be sufficiently vouched for?

36. (Ranjit Randhawa) Are all SAML sessions timed and if not how does SAML deal with expired/invalid authorizations/authentications?

37. (Vinod Eligeti) I feel there is some confusion for the user as where he has logged in. Particularly if there is Identity provider along with Service provider in one domain and the user requires Identity provider which is located in a different domain? Now there are two options, either the user can get the identity from the service provider or from the other identity provider. SAML does not distinguish these two cases clearly?

Security Issues

38. (Darrell Hyatt) If user tracking is not reliable, why do they appear to attempt to mandate it? (you don't necessarily know that session X is still a customer of yours)
39. (Aparna Sharma) SAML requests and responses are carried in SOAP body over HTTP binding. So, does SAML suffer from the security flaws that might be present when SOAP and HTTP are used or does SAML overcome any of SOAP and HTTP related security shortcomings?

40. (Glenn Fink) Seems like SAML is secure like a pipe: strong walls and open ends. Is the best approach to subverting it to attack the end-points rather than SAML itself? If so, it has done its job.

41. (Glenn Fink) If you can replay a SAML assertion permitting a certain kind of access, but somehow can prevent the timely validation of the accompanying digital signature, can you foil the protocol?

42. (Craig Bergstrom) SAML "...will be widely used in business-to-business scenarios to reduce user-management costs", but was designed with several known vulnerabilities that have been addressed independently. Is it not better to trust a system that was designed from the ground up to be safe rather than to trust a system with known but fixable flaws?

43. (Muhammad Abu-Saqer) In this centralized model, how can we overcome the disadvantages of the centralized system like one point of security failure?

44. (Varun Pandey) It would be interesting to know the details of the "artifacts" because it seems to me that after the authentication stage, there is no reference to the user in the artifact that is used later. There is reference to the user's host computer's IP, or to the session number but apparently not to the user. Probably if there is a reference to the user using certificates in every communication as suggested in the Grob's paper, it would provide more security.

45. (Varun Pandey) The protocol doesn't define anything about what if the response in any stage gets lost or doesn't come. The fact is there can be cases of dangling artifacts as noted in the Grob's paper.

46. (Ranjit Randhawa) Can the solutions to the three types of attacks be integrated into the architecture or do they have to be handled on a case by case basis?

47. (Glenn Fink) Assuming single-sign-on is achievable in the general case, have we opened Pandora's box by allowing cascading failures? Can I now hack one authentication service and have effectively hacked them all?

48. (Glenn Fink) The Secure Web Services paper states that the underlying security technology must be able to address concerns that would normally be handled by a priori business or personal relationships. Isn't this a bit of a reach?

**Privacy Issues**

49. (Darrell Hyatt) Referring to the Open Federated Model (in Secure Web Services), how do I know, as a user, who has access to what information of mine? What if I like a compartmentalized life?

50. (Muhammad Abu-Saqer) When the SOAP client passes the user information returned form the LDAP in the SAML token, does the user have the control on which of his attributes is packet in the token. Does SAML give the user this option? How the user privacy is preserved in this model?
51. (Darrell Hyatt) Referring to figures 9 and 10 (in Secure Web Services), by introducing a one-card-for-all (figure 10) to indicate seamless access across networks, the author introduces a single point of failure. Can the same thing be said for the seamless login in figure 9? It seems that we are simply shifting the burden of self-protection onto an unaware and uninformed public.

52. With anonymous SSO, can a collection of attributes be used over time to erode the anonymity of the subject?

53. (Darrell Hyatt) Do we, as humans, really want all service networks to be able to talk to one another? Why does American Airlines need to know what brand of ramen I prefer?

54. (Aparna Sharma) Does the user know the information that is being passed on to the relying party in the form of SAML assertions?

55. (Aparna Sharma) Can the user configure the SAML assertions so that the user is in complete control of the information passed?

56. (Glenn Fink) Assuming we achieve "seamless access across networks," has the consumer then put all his identities in one basket?

57. (Glenn Fink) Does identity theft on one platform now equal global identity theft?

58. (Glenn Fink) What kind of remediation is possible for such complete identity theft?

Utility/Deployment

59. (Ranjit Randhawa) Is the SAML architecture implemented in a real-world system and if so who uses it?

60. (Muhammad Abu-Saqer) Since SAML has potentially large message payload, Does this slow down the system that uses SAML?

61. (Muhammad Abu-Saqer) Does centralizing and linking provisioning, password management, and access control makes life simpler?

62. (Aparna Sharma) The web browser SSO example described in the paper shows numerous process steps for different binding problems. Though transparent to the user, these steps are quiet an overhead in the system, would it not be more secure and simple if the user logged in again at the Service Provider site?

63. (Corban Rivera) While it's true "One benefit of centralized identity management is simplicity and unified access-control management." is it also true that scalability becomes problematic?

64. (Glenn Fink) Is the SAML approach actually less costly than the non-interoperable one where the services are separate? What factors determine the costs of using SAML? Setup? Upgrading legacy systems? Complexity?

65. (Vinod Eligeti) Is centralization a good idea? Because whenever there is a centralized system the issue of performance, scalability of the systems are affected.

66. (Glenn Fink) The Secure Web Services paper states the XML D-Sig is the farthest along. This is obviously dated. What is the current state of the SAML specification?