January 14, 2015
Dear Cathy Tilton
Chair, IDESG Standards Coordination Committee (SCC)
Cathy.Tilton@daon.com

Update and Response

Update

Since our acceptance of the solicitation from IDESG SCC to develop KBA Performance Metrics Standards we have made much progress.
At the time of our acceptance of the solicitation we were in the process of seeking OWASP approval for the Knowledge Based Authentication Performance Metrics Project. We have since been approved and are now underway at **Knowledge Based Authentication Performance Metrics Project** **(KBAPMP)**. We have been encouraged by the OWASP Board in our work and the possibility of OWASP's expansion into this area. Board member Jim Manico has attended or listened-in on some of our meetings. We have been meeting weekly or bi-weekly.

The OWASP KBAPMP team is pleased to respond to your questions and provide additional information about our project. The KBAPMP team agrees that OWASP as an organization provides a number of opportunities for standards development that will be very useful going forward as the world undertakes the development of standards for the emergent facets of cyberspace including identity ecosystem interaction, privacy, identity management and human trust. OWASP offers opportunities in global, grassroot, affordable and open standards development. OWASP provides the possibility of finding common ground through agreed upon standards across cultures, languages and nations. The KBAPMP believes in the potential for good expressed by the NSTIC Strategy and Guiding Principles and welcomes the opportunity to participate in developing standards aligned to NSTIC.

Ann Racuya-Robbins, Luis Enriquez, Co-Project Leaders and Bev Corwin, IDESG Member Representative from OWASP are available to participate in a telecon with you. The details of this meeting will be set out at another time.

Responses

1. Please provide a list and description of completed projects (or their URL) that are in the domain of identity management. (Incomplete projects can be provided as well but the SCC is most interested in those that have been completed.)

We think it is fair to say that there can be no identity management or trustworthiness without security. For this reason we are forwarding information about OWASP's work on its Application Security Verification Standard. See the answer to 2. below.

But identity in cyberspace, as IDESG knows well, involves new dimensions and challenges that were not addressed until recently, such as identity privacy, civil liberties, fraud, and theft among others. OWASP does have an extensive open body of knowledge on key aspects of identity management such as authentication, authorization, accounting, auditing and access. A simple search for “authentication”, “authorization” etc. on the OWASP site retrieves more information than can be organized here.

2. What normative standards has OWASP completed that have been adopted in industry? Have these standards been ratified by organizations accredited by ANSI or ISO, or any other standards organizations?

OWASP is a leader in cyberspace security with its fully documented, tested and widely adopted and used **Application Security Verification Standard** still evolving and serving the needs of developers around the world.

> “A broad range of companies and agencies around the globe have added ASVS to their software assurance tool boxes, including Aspect Security, Astyran, Booz Allen Hamilton, Casaba Security, CGI Federal, Denim Group, Etebaran Informatics, Minded Security, Nixu, ps_testware, Proactive Risk, Quince Associates Limited (SeeMyData), Serviço Federal de Processamento de Dados (SERPRO), Universidad Distrital Francisco José de Caldas. Organizations listed are not accredited by OWASP. Neither their products or services have been endorsed by OWASP. Use of ASVS may include for example providing verification services using the standard. Use of ASVS may also include for example performing internal evaluation of products with the OWASP ASVS in mind, and NOT making any claims of meeting any given level in the standard.”

See also OWASP Industry : Citations:
https://www.owasp.org/index.php/Industry:Citations#National_.26_International_Legislation.2C_Standards.2C_Guidelines.2C_Committees_and_Industry_Codes_of_Practice

OWASP is known for its concern for good documentation and further guidance including “The Software Assurance Maturity Model (SAMM) an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

- Evaluating an organization’s existing software security practices
- Building a balanced software security assurance program in well-defined iterations
- Demonstrating concrete improvements to a security assurance program
- Defining and measuring security-related activities throughout an organization

ESAPI (The OWASP Enterprise Security API), OWASP’s API web application security control library .ES ”The following organizations are a few of the many organizations that are starting to adopt ESAPI to secure their web applications: American Express, Apache Foundation, Booz Allen Hamilton, Aspect Security, Coraid, The Hartford, Infinite Campus, Lockheed Martin, MITRE, U.S. Navy - SPAWAR, The World Bank, SANS Institute .API”

3. Can OWASP provide a list of new team members, if any, since submitting the Expression of Interest to the SCC?

New Team Members
Laureano Batista, JD New York University, Business Intelligence
Donald Gooden, OWASP New York Chapter Leader and OWASP Brooklyn Chapter Leader, Former member of Infragard

Founding Team Members
Noreen Whysel KBAPM Team Member and OWASP Community Manager
Bev Corwin OWASP NIST NSTIC Initiative (NNI), OWASP Brooklyn Chapter Leader
Luis Enriquez, KBAPM Co-Project Leader
Ann Racuya-Robbins KBAPM Co-Project Leader, KBAPM Project Manager

4. Can OWASP provide a project plan/roadmap and approach to complete this work within a reasonable timeframe (< 2 years)?

Updated KBAPMP Project Roadmap

Generally speaking OWASP divides Project development into Incubator Projects, Lab Projects and Flagship Projects described further below. Incubator projects typically should be completed in one year. After that projects can apply to progress to Lab Projects, and Flagship Projects.
The KBAPM Project believes it can complete its development of the Knowledge Based Authentication Performance Metrics Standard in less than 2 years.

“OWASP Project Inventory
All OWASP tools, document, and code library projects are organized into the following categories:

> **Flagship Projects:** The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.
>
> **Lab Projects:** OWASP Labs projects represent projects that have produced an OWASP reviewed deliverable of value.
>
> **Incubator Projects:** OWASP Incubator projects represent the experimental playground where projects are still being fleshed out, ideas are still being proven, and development is still underway.”

5. What efforts have been made to attract project contributors with technical expertise in ICAM and KBA, and others with legal background?

We are just beginning our outreach campaign. Our operational tools are being setup. We have applied to give a paper at the 2015 AppSec Conference in Amsterdam in May 2015. We have also put out a call on OWASP listservs for participation. We anticipate being in full swing by February 2015.

6. Since only a limited number of projects are active, and the participation rate seems focused on coding issues, how do proposers intend to activate/energize participation in their project once approved?

We believe the assumptions of the first part of your question are incorrect. Please provide support and sources?
Our project has been approved by OWASP and research, development and outreach are underway.

7. Is OWASP's project goal to have a completed standard for KBA performance metrics, or input to a potential standard (e.g. studies, best practices)? If input into, have you identified and coordinated with an SDO?

We responded to the solicitation from IDESG SCC to develop KBA Performance Metrics Standards. We are already underway on this project.

8. Please describe the public review process, including how reviews are performed and how comments are adjudicated.

OWASP is a fully open and transparent organization. We will be following an informed use of the review processes and comment adjudication OWASP followed in its successful development of the Application Security and Verification Standard among others. The team has already been discussing the ethical framework for our work and we are currently developing a set of policies in support of our approach. OWASP has a Governance listserv and a Code of Conduct.

Regards,

Ann Racuya-Robbins
Co-Project Leader and Project Manager for the OWASP KBAPMP Team