Open Web Application Security Project (OWASP)

Global Industry Committee

Notes for a presentation given by Colin Watson colin.watson(at)owasp.org at OWASP London chapter meeting on 12th March 2009.

Title page

Intention is to explain briefly briefly what the Global Industry Committee is, and what it's been doing for the last 2-3 months.

The World of OWASP

Structure

But first, what are the global committees are and how do they fit into OWASP? This wasn't clear to me initially, so I've tried to explain my view of it using a diagram.

OWASP has many participants around the world – including people who use an OWASP tool or simply attend chapter meetings. Some of these are members – individually or associated with a organisation supporter or accredited university supporter.

There are a small number (six) of vital busy employees.

Some of the participants are chapter leaders, project leaders and project reviewers. The five board members are some of these people.

There are many projects, of different sizes, involving many people. Many more than the number of circles shown here. Some people take on more than one project role at a time.

Global Committees

The six committees were formed at the OWASP Summit last November in Portugal to focus on key functions. Committee members are endorsed by their peers and most were appointed during the summit. I joined the Global Industry Committee in what is called the "2009 second wave applicants". Although I was at the summit, I somehow missed the whole session on global committees – I think I was helping someone with their presentation or copying handout materials at the time.

Each committee has a representative from the board allocated.

Global Industry Committee

OWASP's mission is to make application security visible, by making good tools and documents, and then making these visible. The Industry Committee is contributing to the visibility work.

The Industry Committee was formed to expand awareness of and promote the inclusion of software security best practices in Industry, Government, Academia and regulatory agencies. We will accomplish this through outreach; including presentations, development of position papers and collaborative efforts with other entities.

Our draft plan is to:

- Step 1: Identify specific organizations worth working with to spread the OWASP gospel
- Step 2: Prioritise the proposed liaisons based on potential impact, and also realistic likelihood of the organization actively working with us
- Step 3: Execute, leveraging global OWASP resources as much as possible to maximize impact
- Step 4: Evaluate progress & repeat Step 1-3

The members are (Location/Chapter[held in]):

- Rex Booth (US/Washington)
- David Campbell (US/Denver)
- Georg Hess (Germany/Germany[various])
- Eoin Keary (Ireland/Ireland[Dublin])
- Colin Watson (UK/London)

and the Board representative is Tom Brennan.

What are we doing?

Currently:

- **Outreach (O)** *= broadcast*
  - Speak and present to spread the word about application security and OWASP
- **Position paper / response (P)** *= submit*

  The preferred approach for response to draft legislation, standards, etc is:

  - Read from original document document and supporting information
  - Consolidating that information into a 'what is relevant to OWASP' briefing document,
  - Harvesting OWASP's community knowledge about it,
  - Figuring out what is OWASP's position,
  - Documenting OWASP position,
  - Getting the committee + board agreement on your interpretation of that

OWASP position,

    - Sending it to the relevant parties,
    - Handling any questions from the other side (and media (or community) coverage / response / comments)

- **Collaborate with other organisations (C)** = *engage*
    - Identify target organisations and rank them by how likely we are able to work with and influence them

O, P and C activity types are used to label the following slides.

(O) InfraGard (Dec 2008)

David Campbell gave a presentation on application security titled “The Web is a Dangerous Place” to InfraGard's Denver chapter.

InfraGard is a collaboration between the US FBI and other organisation who have an interest in promoting the protection and advancement of the US critical infrastructure. They try to cooperate with others in the interchange of knowledge and ideas for mutual protection.

(P) DPC BS 8878:2009 (Jan 2009)

Provide response to "BS 8878:2009 Web accessibility. Building accessible experiences for disabled people" Draft for Public Comment (DPC)

BSI British Standards is an organisation we would like to work with, and we are investigating how this might be undertaken more formally, but in the meantime we are providing official OWASP responses to drafts for public comment.

Whilst web accessibility may not be central to application security it was seen as an opportunity to try to get OWASP mentioned in the bibliography, and possibly some mention of security in the text.

Issues of validation, conformance, expert review and contracting web design and audit services were commented on.

http://www.owasp.org/index.php/Industry:DPC_BS_8878:2009

(P) Digital Britain Interim Report (Mar 2009)

UK Government's "Digital Britain Interim Report Jan 2009" is an action plan to secure the UK's place at the forefront of innovation, investment and quality in the digital and communications industries.

What's it about? An action plan to secure the UK's place at thefore front of innovation, investment and quality in the digital and communications industries. Why is this relevant to OWASP? The terms of reference for the report include:

"Empowered and informed consumers and citizens fully equipped to take advantage of the opportunities convergence brings."

"Internet: looking at a range of issues affecting internet users, such as user security and safety and a workable approach to promoting content standards."

and from the interim report:

"We need to ensure that UK internet users can operate with security and confidence."

but the principles list only relate to privacy, personally identifiable information and illegal material.

The interim report was issued last month and contained a lot about, access, speeds, digital rights management and protection of vulnerable groups. Very little else on information security. The Online Safeguard section was very brief, compared with other sections.

Provide response to – this was announced through the UK chapter lists and following discussions, drafts were created an improved upon. Has now been submitted to the Digital Britain Team.

http://www.owasp.org/index.php/Industry:Digital_Britain_Interim_Report

(P) Draft NIST SP 800-122 (Feb-Mar 2009)

Provide response to "Draft NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

National Institute of Standards and Technology (NIST) is part of the US Department of Commerce). Aim is to assist Federal agencies in protecting the confidentiality of personally identifiable information (PII). Contains practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII.

Document included some examples that were online web systems, but some aspects of security in the discussion could have been expanded upon.

http://www.owasp.org/index.php/Industry:Draft_NIST_SP_800-122

(P) Draft NIST SP 800-53 Revision 3 (Mar 2009)

Provide response to "Draft NIST Special Publication 800-53 (Revision 3) Recommended Security Controls for Federal Information Systems and Organizations"

NIST has released for public comment a revised draft of Special Publication 800-53 (SP 800-53), Recommended Security Controls for Federal Information Systems and Organizations, the document's "first major update ... since its initial publication in December 2005." As most of you know, the document aims to help federal agencies implement changes to comply with the Federal Information Security Management Act (FISMA) and other federal information assurance regulations. It is the key infosec control framework in the US federal sector.

A group of about a dozen OWASP participants are working on this.

> Stage 1
>
> Activities: All participants perform a high-level, document-wide review to develop a familiarity with the document. Reviewers should note where rev 3 has introduced changes and where OWASP has the greatest potential for impact. Comment development is not required for this stage, but are a welcome side-effect.
>
> Results: By the first status meeting, each participant should have three lists: 1) noted updates within the document 2) areas of the document most closely related to OWASP interests 3) initial draft comments (if appropriate).

Stage 2

Activities: Participants will be asked to perform a focused review on the sections of the document identified in Stage 1 as most relevant to OWASP. These "target sections" may be divided among project participants depending on project population and the number of target sections.

Results: By the second status meeting, each participant should develop a refined and detailed list of comments for their assigned sections.

Stage 3:

Activities: Participants will revise comments as needed and project management will consolidate and format comments for submission to NIST.

Results: A final list of comments for submission to NIST (26th March 2009).

(P,C) Consensus Audit Guide (Ongoing)

The Consensus Audit Guide (CAG) is meant to be the Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous Federal Information Security Management Act (FISMA) Compliance. 20 categories in fact, one of which is Application Software Security. Critical controls (draft 1.0) are:

- Inventory of authorized and unauthorized hardware.
- Inventory of authorized and unauthorized software; enforcement of white lists of authorized software.
- Secure configurations for hardware and software on laptops, workstations, and servers.
- Secure configurations of network devices such as firewalls, routers, and switches.
- Boundary Defense
- Maintenance, Monitoring and Analysis of Complete Audit Logs
- Application Software Security
- Controlled Use of Administrative Privileges
- Controlled Access Based On Need to Know
- Continuous Vulnerability Testing and Remediation
- Dormant Account Monitoring and Control
- Anti-Malware Defenses
- Limitation and Control of Ports, Protocols and Services
- Wireless Device Control
- Data Leakage Protection
- Secure Network Engineering
- Red Team Exercises
- Incident Response Capability
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training To Fill Gaps

They are a subset of the NIST SP 800-53 Rev 3 Controls (see later slide). For application security, the NIST SP 800-53 Rev 3 controls are AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11 and SI-3. Categorised as:

- Quick Wins (fundamental aspects that do not normally require large organisation changes)
- Improved Visibility and Attribution (improving the process, architecture, and technical capabilities)
- Hardened Configuration and Improved Information Security Hygiene (reducing the number and magnitude of potential security vulnerabilities as well as improving the operations of networked computer systems)
- Advanced (everything else)

David and Rex are translating the OWASP Top 10 into a format requested by SANS for inclusion in the CAG.

(P) DPC BS 10012 (Mar 2009)

Provide response to "BS 10012 Specification for the management of personal information in compliance with the Data Protection Act 1998" Draft for Public Comment (DPC).

This draft standard purpose is to enable organizations to put in place a personal information management system (PIMS), to which provides an infrastructure for maintaining and improving compliance with amongst other things the requirements of the Data Protection Act 1998 (DPA).

Implementation sections include:

- 4.13 Security issues
- 4.13.1 Security controls
- 4.13.2 Storage and handling
- 4.13.3 Transmission
- 4.13.4 Access controls
- 4.13.5 Security assessments
- 4.13.6 Notification of security incidents
- 4.13.7 Contingency plan

http://www.owasp.org/index.php/Industry:DPC_BS_10012

Intrinsic Security Working Group

ISWG is an OWASP initiative set up with a charter:

1. Contribute our security knowledge towards standards organizations

2. Act as a consumer awareness group for web application frameworks security mechanisms and browser security features

3. Serve as a platform for OWASP members who want to affect change at any of the building blocks in today's or tomorrow's web applications

In November a discussion on the board between members led to the creation of a Google group aiming to create an HTTPOnly standard for browser makers to follow. ISGQ is making a first cut at a standard after some deliberation, and have been in discussion with some browser vendors for feedback. This has an extremely positive and global effect. The Global Industry Committee has been asked to support this initiative by submitting a letter to browser vendors and work with the ISWG further.

Contribute

Most important is participating in projects – since these generate so much of OWASP's output. The Industry Committee can help spread the word about the projects.

Identify organisations to engage with and legislation/documents/standards/drafts to comment on or a topic that requires an official OWASP statement.

Provide input to the response creation and review process (web page, mailing lists).

http://www.owasp.org/index.php/Global_Industry_Committee