Open Web Application Security Project (OWASP)

Technology Strategy Board

Notes for a meeting with Paul Lewis on 18th February 2010.

Colin Watson, Chair Global Industry Committee

OWASP

Legal structure:

- OWASP is registered in the US as a 501c3 not-for-profit charitable organization focused on improving the security of application software.
- Over 130 local chapters around the world, including 3 in the UK.

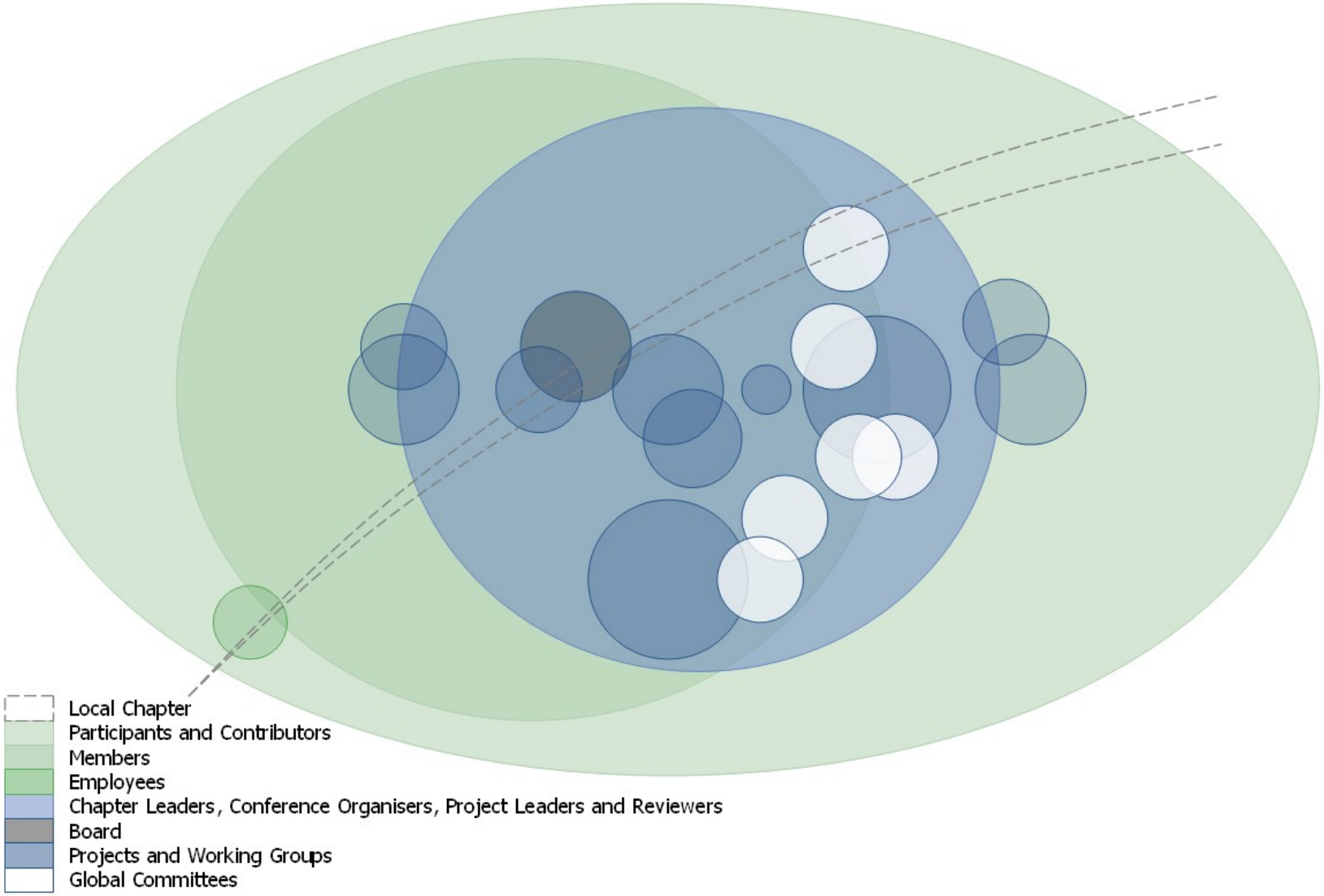
Mission:

- To make application security visible, so that people and organizations can make informed decisions about true application security risks.

Free and open:

- Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

People


Local Chapter
Participants and Contributors
Members
Employees
Chapter Leaders, Conference Organisers, Project Leaders and Reviewers
Board
Projects and Working Groups
Global Committees

Mapping of Secure Software Development white paper with OWASP Projects and Initiatives

Sources http://www.ktn.qinetiq-tim.net/content/files/groups/securesoft/SSDSIG_softwareSecurityFailures.pdf and http://www.owasp.org

Mind map as an image file: http://www.owasp.org/images/a/a4/Ssd-ktn-20100215.jpg

Accredited University Supporters

Source: http://www.owasp.org/index.php/Membership

Benefits

- Raise awareness of the University worldwide
- Be recognized as a supporter by posting your university logo on the OWASP website (Image size for logos: gif, jpg or png with a size of 150px X 45px at 72dpi)
- OWASP and the University can jointly publicize season of code events which provide funding for students or faculty to perform security based research
- OWASP and the University can work together to host security seminars or provide introductory training sessions for students on OWASP tools, documentation and security skills.
- NO COST
- Note: This is intended for the University as a whole to become involved with OWASP. This does not imply individual or organizational membership for the University, students or faculty. However, all students and faculty are encouraged to explore the benefits of becoming an individual member.

Cost

- No Charge - Contact Your Local Chapter Leader to get involved.
- Bartered Requirements
  - provide meeting space 2x per year and include OWASP in the education awareness & curriculum to students.
  - encourage students to apply for OWASP Grants and work on projects for OWASP Foundation that will help them build real world industry experience.

Organsational Supporters

Citations

National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice

Full details http://www.owasp.org/index.php/Industry:Citations

Canadian Cyber Incident Response Centre Canada

- TR08-001 Alleviating the Threat of Mass SQL Injection Attacks (also in French), 18 June 2008 v1.0.0

Center for Internet Security (CIS) USA

- Apache Benchmark for Unix, October 2006 v1.4 & 1.5
- Apache Benchmark for Unix, November 2006 v1.6
- Apache Benchmark for Unix, July 2007 v1.7
- Benchmark for Apache Web Server, December 2007 v2.0
- Benchmark for Apache Web Server January 2008 v2.1
- Benchmark for Apache Web Server November 2008 v2.2
- The CIS Security Metrics - Consensus Metric Definitions 11 May 2009 v1.0

Cloud Security Alliance (CSA) USA

- Security Guidance for Critical Areas of Focus in Cloud Computing April 2009 v1.0
- Security Guidance for Critical Areas of Focus in Cloud Computing December 2009 v2.1

Club de la Sécurité de l'Information Français (CLUSIF) France

- Sécurité des applications Web - Comment maîtriser les risques liés à la sécurité des applications Web ? September 2009

Defense Information Systems Agency (DISA) USA

- Recommended Standard Application Security Requirements (Draft) 11 March 2003 2v.0 (draft)
- Web Server Technical Implementation Guide 11 December 2006 v6 Rel 1
- Application Security and Development - Security Technical Implementation Guide 24 July 2008 2 Rel 1
- Application Security and Development Checklist 24 July 2008 v2 Rel 1.1
- Application Security and Development Checklist 26 June 2009 v2 Rel 1.5

Defence Signals Directorate Australia

- Australian Government Information and Communications Technology Security Manual (ACSI 33) September 2008

European Network and Information Security Agency (ENISA) Europe

- Web 2.0 Security and Privacy Position Paper 10 December 2008
- Cloud Computing Risk Assessment 20 November 2009

Federal Chief Information Officers (CIO) Council USA

- Guidelines for Secure Use of Social Media by Federal Departments and Agencies September 2009 v1.0

GovCertUK UK

- SQL Injection 16 January 2009 1.0

Information-Technology Promotion Agency (IPA) Japan

- Secure Programming Course from the IPA Information-technology SEcurity Center (ISEC) 2002
- Study of Web Server Mandatory Access Control March 2005
- Symfoware ST (Symfo-06-DS3001) in the JISEC Certified/Validated Products List. 9 May 2007
- Open Source Software Evaluation Lab Environment November 2007

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Worldwide

- ISO/IEC TR24729-4, Information technology — Radio frequency identification for item management — Implementation guidelines — Part 4: Tag data security March 2009

ISM3 Corporation Worldwide

- Information Security Management Maturity Model April 2009 v2.10
- Information Security Management Maturity Model November 2007 v2.3

Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire France

- Guide de réalisation Java *Translation: Java Development Guide* July 2009 v2.1
- Guide de réalisation PHP *Translation: PHP Development Guide* July 2009 v2.1

National Infrastructure Security Co-ordination Centre (NISCC) UK

- Secure web applications - Development, installation and security testing (NISCC Briefing 10/2006) 27 April 2006
- Commercially Available Penetration Testing - Best Practice Guide 8 May 2006

National Institute of Standards and Technology (NIST) USA

- Framework and Roadmap for Smart Grid Interoperability Standards September 2009 v1.0 (draft)
- Interagency Report 7628 (draft) - Smart Grid Cyber Security Strategy and Requirements September 2009 Draft
- Interagency Report 7581 - System and Network Security Acronyms and Abbreviations September 2009

National Security Agency/Central Security Service USA

- Oracle Application Server on Windows 2003 Security Guide (I733-032R-2006) December 2006
- Web Application Security Overview and Web Application Security Vulnerabilities (I733-034R-2007) 2007
- Minimize the Effectiveness of SQL Injection Attacks (I733-021R-2008) May 2008
- Service Oriented Architecture Security Vulnerabilities Web Services November 2008
- Manageable Network Plan 8 July 2009 v1.1

Payment Card Industry Security Standards Council (PCI SSC) Worldwide

- Data Security Standard September 2006 v1.1
- Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified 15 April 2008 v1.1
- Data Security Standard October 2008 v1.2
- Information Supplement: Application Reviews and Web Application Firewalls Clarified October 2008 v1.2

SAFECode Worldwide

- Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today. 8 October 2008

SANS Institute USA

- Top 20
- November 2005 v6
- November 2006 v7
- November 2007 v8

Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) Australia

- Information Security Principles for Enterprise Architecture June 2007
- Defence in Depth June 2008
- User-access management June 2008