Open Web Application Security Project (OWASP)

Request for comments on licence conditions relating to security risk assessments

Introduction

This official response has been developed by an open consultation process across the eight UK chapters of the Open Web Application Security Project (OWASP), and is submitted to DECC by the OWASP Global Industry Committee.

Detailed Response

All three consultation questions have been responded to.

1. Do you consider that the draft licence conditions deliver the policy intention outlined in this document? Please provide comments on where the drafting could be amended or clarified.

No, we believe additional licence conditions are necessary to deliver the policy intention.

The risk assessment and audit will be based upon the definitions in the licence conditions. Appendix A paragraph Z.5 defines equipment to include associated software and ancillary devices, and provides a definition of "secure" in paragraph Z.6 - the definition of "secure" is not sufficient. In addition to the existing three items, the Supplier End-to-End System is Secure if both the System and each individual element of it is designed and operated to ensure that it is not subject to interference or misuse that:

- allows any connected communications network to be used for unauthorised purposes
- allows the collection or processing of unauthorised data by the software
- results in applications undertaking unauthorised activity
- allows the designed software features to be misused
- gives rise to the presence of unapproved or malicious code within the authorised software
- allows installation of unapproved software
- permits use of any part of the system to attack other elements of the System or any other external information system.

These are all common security vulnerability classes which are not currently mentioned in the conditions.

There is also the potential for supplier awareness of risks to vary considerably. OWASP recommends the risk assessment by each supplier should always address a common, centrally maintained, register of known smart meter risks, instead of each supplier developing their own. Each supplier would therefore have to address these in addition to any other organisational, technical, processes or physical risks they deem in scope.

Guidance on assessment of impact in each risk assessment should be provided to ensure that impacts are not solely based upon risks to the suppliers themselves (e.g. loss of license, inability to issue bills, etc). Impacts on individuals (whether customers or not), wider society (e.g. national infrastructure, availability of assets/power, economy, trust) and other partner organisations should also be addressed.

The current proposed conditions do not take into account the need to address any major change to the risk profile; for example should a major new threat be identified in smart metering then a risk review should take place promptly (i.e. within weeks not months).

2. Do you have any comments on the proposed approach that suppliers should carry out a number of good practice security disciplines and procedures as is set out in this document?

Yes we have additional comments.

Security requirements should include a baseline minimum set of mandatory requirements, not simply those based on a risk assessment. These should be drawn from existing work elsewhere. In terms of application security we recommend:

- Application Security Verification Standard (ASVS), OWASP
  https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- Fundamental Practices for Secure Software Development 2nd Edition, SAFECode
  http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf
- Overview of Software Integrity Controls, SAFECode
  http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf
- Security requirements, OWASP
  https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
- Software Assurance Resources, DoHS
  https://buildsecurityin.us-cert.gov/swa/resources.html

and other national application security guidance listed on OWASP Citations http://www.owasp.org/index.php/Industry:Citations

All software within the Supplier End-to-End System should be developed with security built in at all stages of the development life cycle. There is no guarantee that systems can be made secure very late in the life cycle when problems are found. Fixes to fundamental design flaws may require months of redesign, retesting, and redeployment. Security controls available at the tail end of the process may not be sufficient or appropriate to mitigate the risks that are found. Finding problems at the very end of the lifecycle is the most expensive (in terms of time and money) to mitigate. If issues are found, suppliers will have to wait for the findings to be mitigated, perform another series of end-to-end tests and security risk assessments, and then hope that the identified issues were fixed.

The following documents provide software-specific process recommendations:

- BITS Software Assurance Framework, Financial Services Roundtable
  http://www.bits.org/publications/security/BITSSoftwareAssurance0112.pdf
- Building Security In Maturity Model (BSIMM)
  http://bsimm.com/
- Open Software Assurance Maturity Model (SAMM)
  http://www.opensamm.org/
- Security Considerations in the Information System Development Life Cycle, SP 800-64 Rev2, NIST
  http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
- Team Software Process for Secure Systems Development (TSP Secure), CMU
  http://www.cert.org/secure-coding/secure.html

Other smart grid and national infrastructure specific guidance should also be used from CPNI in the UK and ENISA, ISA, NIST, and WIB.

The draft conditions should require those who supply equipment, software, or services in the smart meter ecosystem demonstrate they have staff who are qualified to build it securely in the first place. It should also address what security processes they might apply during the development of hardware, software, and services. We recommend these requirements are added.

Testing will be required as part of security life cycle, and mandating that testing is performed by qualified testers is reasonable. The DECC should ensure that security-qualified staff are involved in the deployment, operation, and monitoring of smart meter systems. The DECC should mandate that suppliers demonstrate that they retain security-qualified staff with recognised appropriate certifications. Likewise, the suppliers should mandate that providers of smart meter hardware, software, and services should have staff on-hand who are qualified in software security, so that there is a greater chance that the product include appropriate security controls and mechanisms.

3. Do you have any further comments with regard to the issues raised in this document? We also welcome general comments around the approach to small suppliers, the processes expected of suppliers in general, and any related costs.

Yes we have further comments.

All security risk assessment, information security policy and information security management system should be available for public inspection. If these are based around closed standards such as ISO27001, these should be made available to the public as well.

The conditions should be comply with the recommendations 5, 6 and 7 in Smart Grid Security Recommendations, ENISA, 11 July 2012 available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

About OWASP

This official response has been submitted on behalf of the Open Web Application Security Project (OWASP) by the OWASP Global Industry Committee, following our own consultation process with the UK chapters in Bristol, Birmingham, Leeds, London, Manchester, Newcastle, Royal Holloway University and Scotland.

OWASP is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organisations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. It is a voluntary organisation and is vendor neutral. Further information:

- OWASP Foundation
  http://www.owasp.org/index.php/OWASP_Foundation
- About The Open Web Application Security Project
  http://www.owasp.org/index.php/About_OWASP
- OWASP Global Industry Committee
  http://www.owasp.org/index.php/Global_Industry_Committee

OWASP and OWASP in the UK are listed in ENISA's Who-Is-Who Directory.