Open Web Application Security Project (OWASP)

Response to Protecting Consumer Privacy in an Era of Rapid Change - A Framework for Businesses and Policymakers

Introduction

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.

Response

The OWASP response is to eight of the FTC's questions for comment, which we have labelled a) to h) for our own purposes. The questions responded to relate to aspects within OWASP's mission to "to make application security visible, so that people and organizations can make informed decisions about true application security risks.". In some cases where OWASP does not have an agreed opinion, questions are not answered explicitly and instead we have raised application related matters which may affect consideration of other responses to the question.

a) Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services > Incorporate substantive privacy protections > When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?

i) When technology solutions cannot be applied (because of legacy systems or because of other reasons), other procedural and organizational countermeasures must be put in place that, together with the technology, provide an increased level of security. Bit although it may be economically infeasible to change legacy systems, it is often the case that these systems are modified, or access provided to them through new mechanisms (e.g. by a web service, or using a mobile application). The changes and additions should have privacy built in.

ii) For legacy data systems which cannot be altered, the techniques of data minimization, data integrity checking and data tokenization should be considered first. Thereafter conventional administrative and technical controls (e.g. segregation of

duties, principle of least privilege, etc) should be applied based on a risk assessment, but we would like to highlight the following application-specific controls:

- documentation of security defaults and options that affect security
- secure configuration of the application and application environment
- application event log analysis
- application layer firewalls
- application surface exposure minimization
- application layer intrusion detection and prevention
- content (data) egress monitoring

iii) If multiple channels (e.g. desktop application, web site, web service, mobile application, accessible web site) are used to deliver a business process, all of these should have similar levels of privacy protection built in, so that one channel can not be used to circumvent another, and similarly for non-online alternatives (e.g. customer call center, walk-in shop, telephone self-service, etc).

b) Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services > Maintain comprehensive data management procedures > How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?

i) Privacy requirements should be built into development & procurement practices. Verification processes must be undertaken to ensure these have been delivered - a risk based approach should be used to ensure effort is applied proportionately through the portfolio of processes. To encourage this, greater transparency is required through the supply chain, and all parties involved in delivery.

ii) It is not sufficient just to use privacy enhancing technologies (PETs) - they must be installed, configured and operated correctly. And, they must be verifiable. For example, selection of weak algorithms, exposure of keys or provision of access to decrypted data through an application can all circumvent "encryption as a solution". The use of TLS (SSL) can be undermined by exposing session variables over plain HTTP, SSL can be set up incorrectly (it is not "secure by default") and many applications (e.g. websites, mobile apps, email clients) make it very hard for users to tell whether SSL is being used correctly, and there is little consistency in visual signals for users. We would recommend that guidance is created defining the minimum technical standards for each PET, and also related procurement specifications, audit checklists and self-assessment questionnaires.

iii) New developments and deployments of PETs can be assessed and compared by research and consumer-education organizations like OWASP. These organizations serve an important purpose: providing organizations, developers and consumers with information about privacy and security on the Web. Such organizations are transcendent of any individual company or individual's gain, and serve as an objective voice on leading practices. As a result, OWASP and other similar groups have an opportunity to recommend or promote practices with respect to development and deployment of PETs, and this objective promotion can be a free publicity incentive for organizations who develop constructive and helpful technologies.

iv) OWASP has the leading repository of application security knowledge (see these standards, guidelines, etc which reference OWASP

http://www.owasp.org/index.php/Industry:Citations); for example has a begun a "Cheat Sheet" series, one of which relates to HTTP over SSL (TLS): http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet Separate guidance with different emphasis and detail would be required for various audiences. OWASP has continuing voluntary efforts to translate its materials into many world languages.

c) Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services > Maintain comprehensive data management procedures > What roles should different industry participants – e.g., browser vendors, website operators, advertising companies – play in addressing privacy concerns with more effective technologies for consumer control?

i) Every part of the supply chain throughout the software development life cycle (including operation and disposal), needs to be able to understand the privacy-affecting aspects and effects. For services delivered over web technologies, besides the operators of the services, the software programming languages, code libraries, frameworks, host environment, network and browser can all affect the efficacy of privacy protection. Consumers should be able to have knowledge into all these layers of the supply chain, to be able to understand, and check the whole service. There is also a need for increased visibility between suppliers and customers in the supply chain.

ii) Consumers, though often assumed to take responsibility for their own privacy, are not in a good position to do so. But consumers are neither best placed, nor have sufficient resources, to undertake checks on the controls in place. Some measures might be enforced more economically at one point in the process and its delivery, than another. For example, removing cross-site scripting (XSS) vulnerabilities on a single high-traffic website, protects many consumers from some attacks that are used to steal their data.

iii) Owners of websites and other online applications should take responsibility for protection of consumer data. This includes all the actions taken by their application, and any third party content included.

iv) However, not all collection/tracking of consumer data may be undertaken by legitimate (non-malicious/privacy compliant) websites and other legitimate applications. Legitimate sites may become compromised due to the presence of security flaws and lack of mitigating measures so that content from malicious hosts is included (e.g. drive-by downloads), or users are redirected to those. But consumers may also be tricked into visiting malicious sites (by phishing, or because the sites are genuine in some way), or they may choose to download files to view or execute which unknowingly contain malicious code. In these cases, protective measures in the browser and operating system, and operators of legitimate sites have no control over these aspects. They can of course use development and deployment practices which build security into their own services; but these do not help if consumers visit other locations.

d) Companies should simplify consumer choice > Commonly accepted practices > Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

i) In the report under "fraud detection", the use of "web server logs" are explicitly mentioned. These are not the only source of event data, and in any case, are not considered sufficient for most data protection purposes. Practices should include the collection, aggregation and analysis of all types of event information (which could contain data about consumers). We would suggest changing the phrase "ordinary web server logs" to "network security and traffic management devices, web server, database transaction, security event, audit, local client, local operating system and other logs".

ii) The list of commonly accepted practices should add "misuse tracking, detection and prevention", including aggregation of such data and this should be across multiple sites, domains, servers and other systems. This is quite similar to the existing "fraud prevention" practice already included, but not all suspicious activity and attacks involve "deception or personal gain" as the intent. Not all unwanted activity is necessarily a "crime". The intent may be to alter, delete or steal data, or to view unauthorized information, or to prevent access to the service by others. Included in this should be process verification (e.g. testing and audit) which are not malicious, but do form part of detection & prevention. Misuse tracking, detection and prevention is used to protect consumers and their data. It must not of course be used for other purposes.

iii) The list of commonly accepted practices should include data required for "state management" purposes (e.g. using cookies as user identifiers, use of basic/digest authentication, identifiers in URL paths and parameter names & values, identifiers in form fields, temporary storage of user state properties at the server, authentication headers). Many applications will not work at all unless session management data are allowed. This data may need to be replicated across locations for load balancing and redundancy. A consumer would expect a particular web service to be available when they want it, and to have all their relevant information available and accurate. This requires data storage and replication. This data of course is still subject to privacy controls, limitations to use, etc.

e) Practices that require meaningful choice > Special choice for online behavioral advertising: Do Not Track > How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?

i) Not all tracking is necessarily undertaken on a server elsewhere. Some applications may utilize local storage (on the consumer's device). Intermediate network devices may also store data, even if transiently. These should also be considered.

ii) The selected mechanism ALSO needs to be clear, easy-to-find, usable, and understandable by ORGANIZATIONS involved in developing, operating, hosting and delivering online services, otherwise the consumer's choice may be meaningless. Guidance on who is responsible for what, and how each party needs to support the mechanism would be required. For example, if an HTTP header is to be used, the issue of intermediate devices such as proxy servers, traffic management and firewalls would presumably also have to act upon the instruction? It would need to be clear what is, and is not, tracking in these locations. Data may be gathered by the application, by intrusion detection systems, in audit trails - as well as in web server logs. Online websites may also contain code hosted by third parties e.g. widgets, buttons, syndicated content, code libraries, and these potentially would also have to act upon

the instruction.

iii) Some options for implementing a Do Not Track mechanism may leave no trace of the consumer's requests. For example, HTTP headers are typically not logged by network devices, web servers, web applications or back-end databases. This means it may be impossible to prove whether a consumer did opt out of tracking or not. The ability to verify this, or investigate a consumer complaint against an organization, needs to be considered and clear guidance given to system designers and developers about what is expected and required. The use of an HTTP header may be simpler to add (than some other options), but it easy to ignore, and currently very difficult to prove whether it existed or not. It would therefore be useless if it needs to be verified.

f) Practices that require meaningful choice > Special choice for online behavioral advertising: Do Not Track > Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?

i) It would perhaps be short-sighted to restrict the consumer client software to only be websites delivered over HTTP. Existing Rich Internet Applications (RIAs) may communicate using other protocols. A consumer might expect that opting out of behavioral advertising in one software application, applied to all software applications on the device.

ii) It could be difficult for consumers to differentiate between "online" and "mobile" - for example mobile applications can sometimes incorporate web pages. It may also be useful to think of email clients as another example. The consumer doesn't actually care about the underlying technology - it's all "online data".

iii) Behavioral advertising is not the only use of consumers' data that they may find undesirable. We believe that the consumer should authorize any use of his or her web use habits since the behavior is potentially private or identifying. We recommend that any tracking restriction mechanism apply to all tracking that consumers would not reasonably accept, and not for any specific purpose. Tracking for the sole purpose of increased consumers' safety, security or privacy online should be considered generally acceptable. Tracking for any other purpose, or any use secondary to what a consumer explicitly authorized, should not be considered reasonable.

iv) Tracking transcends technologies; it should not be limited to one platform or Internet standard. Whatever device is connected to the Internet can potentially be used for tracking. Additionally, any technology of the web (electronic mail, HTML, interactive content, streaming video services, etc) that collects consumer information can potentially be used for tracking. Any recommendations or regulations should not be specific to a technology, but should instead be specific to behaviors within or uses of any type of technology.

g) Companies should increase the transparency of their data practices > Reasonable access to consumer data > Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

i) With applications, the data sharing can be occurring at the same time as it is being provided, and not necessarily subsequently. For example, including code from a third party within a web page where the user is identifiable. In these cases, it may make sense to inform the consumer in advance.

ii) Ultimately, consumers should know how their data is being collected and used and by whom. Any functional entity (such as a business or any contractors authorized to do their business solely on behalf of the initial company) who shares a consumer's information with another independently-operating functional entity, should disclose this relationship and where possible, provide consumers a way to limit this sharing.

h) Companies should increase the transparency of their data practices > Reasonable access to consumer data > Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

i) Users should receive a clearly understandable message THAT a specific benefit was denied and WHY. For example, the user should be informed about the "used" data which caused the deny. Sometimes a combination of several collected individual data on different systems may have to be used to determine the denial of benefit. We realize such an information may break smooth usage (e.g. alert windows) and this may annoy users; it is an aspect that requires further work to find a USABLE and CONSISTENT solution (across many devices and protocols).

ii) Note that denial of certain benefits may be against local moral, cultural or legal expectations (e.g. national laws, contractual obligations), and could also impact on human safety.

About OWASP

This response is submitted on behalf of the Open Web Application Security Project (OWASP) by the OWASP Global Industry Committee. 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 organizations 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. The OWASP Foundation is a U.S. recognized 501(c)(3) not-for-profit charitable organization, that ensures the ongoing availability and support for our work at OWASP. 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
- The Open Web Application Security Project
  http://www.owasp.org/
- OWASP Global Industry Committee
  http://www.owasp.org/index.php/Global_Industry_Committee