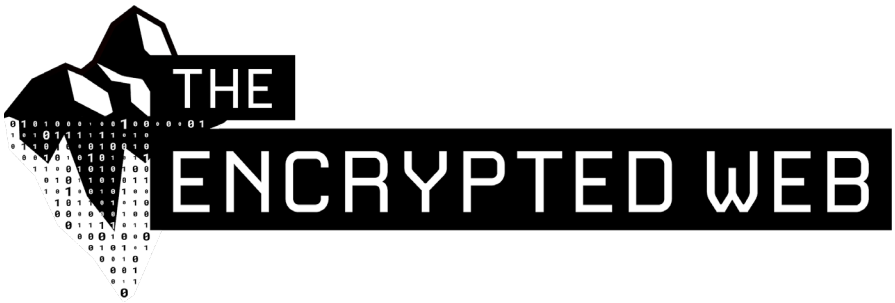

Content Implementation Plan

Overview

This purpose of this implementation plan is to provide guidelines for developing future content for the Encrypted Web. This plan is based on feedback received during a group user feedback session.

Implementation Phases

Phase	Tasks	Status
0	Initial review and brand development	COMPLETE
1	Brand implementation and UX research	COMPLETE
2.1	**UX Feedback Changes:** Layout, responsiveness and other display changes	COMPLETE
2.2	**Content Update:** Linking jargon and terminology to internal or external sources. (see: section A #4)	TO DO
2.3	**Content Update:** “Why EW Cryptography Matters” (see: section B #1).	TO DO
2.4	**Content Update:** “Get Started Guide” (see: section B #3)	TO DO
2.5	**Content Update:** Use cases for 4 pillars and other updates to 4 pillars (see: section B #2)	TO DO
2.6	**Review:** Content tone, quality and comprehensiveness of content (see: section A)	TO DO

A. Setting the Tone

The main goal of the Encrypted Web (EW) is to teach developers how to implement data security and user authentication into their applications themselves, but before we can do that we need to convince them why doing so matters.

One consistent point of the feedback we received was that the website was too informal and flippant in tone, which made users take the content less seriously. At the same time, we don't want to present as overly formal to the point where the content becomes too dull and difficult to understand. Below are some guidelines and examples on setting the tone for content on the site:

1. **Focus on why EW Methodology is Necessary**
   When comparing EW methodology with other cryptographic methods, the focus should be on how and why EW methods are best for security rather than just saying other methods are bad. When explaining the pitfalls with other methods, use a more objective tone.

   For example:

   "Multi-tenancy key management in the cloud is foolish"

   →

   "Keys must be controlled by a single owner/organization because . . ."

2. **Address the Difficult of EW Methodology**
   EW proposes that developers address data security within their applications, which is generally more challenging than leaving it to an external source such as the cloud. The content should address the challenges and position EW as a guide that makes the complex process more simple.

   For example:

   "Learn simple crypto in less time than it takes to shower"

   →

   "While implementing data security in your application is challenging, the Encrypted Web offers some simple guides to get started!"

3. **Advocate for the End-User first, then the Organization**
   While the target audience of the EW is developers, we are encouraging them to develop applications that are more secure for their users. As the first step is to convince developers why this matters, we should argue that it is most beneficial for their users. Once the developers are convinced that this matters, they'll need to be equipped with the convincing arguments to take to their organization.

   For example:

   "Passwords suck and leave your organization vulnerable to breaches and lawsuits"

   →

   "Your users are often frustrated with having to change passwords frequently to keep their data protected, which passwords hardly guarantee."

4. **Make Jargon Accessible for the Average Developer**
   Cybersecurity has plenty of jargon that even most developers may not be familiar with. While we can't avoid using jargon altogether, we can offer short definitions for cybersecurity terminology as well as internal links or external ones to trustworthy sources to help users learn more. It is important to keep in mind that while our audience may not understand cybersecurity, they are still developers, so don't get carried away trying to define developer common-knowledge such as "API" or "Javascript".

   For example:
   "There are two types of basic cryptoprocessors: TPM and HSM"

   →

   "There are two types of basic cryptoprocessors: Trusted Platform Module (TPM) and Hardware Security Module (HSM). A TPM is a . . . An HSM is a . . . ."

B. Content to Develop

Below are the suggested content pieces and where they should appear on the site.

1. **Why EW Cryptographic Methods Matter**
   As previously mentioned, EW needs to argue why developers should care enough to implement data security and user authentication in their applications. While these arguments should be done throughout the site as needed, we need standalone content that makes this case too.

   The ideal place for this content is in a short-form on the homepage under the header. This can then have a link to a more detailed page for more information.

2. **Use Cases**
   While our site currently explains the main pillars of cryptography, it doesn't detail the process and how they each can be used. Each of the existing pages for the pillars of cryptography ("FIDO2 Authentication", "Encryption and Tokenization", "Digital Signatures" and "Key Management") should have at least one example use case to illustrate how they can be effectively implemented.

3. **"Get Started" Guide**
   While each page on cryptography pillars links out to our API documentation, we should have a single page to guide users through each of the steps to experiment with implementing the methods.