Statement of Interest on behalf of the W3C TAG

While exploring new ideas for adding security to Internet protocols and Web formats and languages, we should also be encouraging the use of the current existent mechanisms which can add security to existing Web transactions.

The TAG is working on a best practices document which will highlight these currently available techniques and technologies, with a view to influencing greater adoption by Web sites. In particular, we plan to focus on the use of Perfect Forward Secrecy over HTTPS, key strength, certificate pinning, use of up-to-date versions of security algorithms, HTTP Strict Transport Security and the general use of TLS in more circumstances.

These practices are currently being used on some high-volume production Web sites, but the whole Web would benefit from their adoption in more places and in more scenarios, especially when confidentiality is desirable. Currently some of these techniques may not have come into wide use due to cost of implementation or a perception that the majority of users are using browsers that do not support them. However, with the increased industry attention on security and anti-snooping, and considerting that most modern browsers have implemented these techniques, adoption should be widely encouraged.

Furthermore, we believe that additional work needs to be done in order to further secure the Web platform, particularly in light of emerging Web APIs into privacy-encoraching device information such as the user[1]s address book, calendar, camera, microphone and geo-information.

We look forward to working with the wider community of practice on all these topics as we work together towards a more secure Web that is less susceptible to pervasive monitoring.

Daniel Appelquist
Co-Chair of W3C TAG