Kobe, Japan & online
10–14 November 2025

Threat Model for the Web

What are we working on?

@w3c@w3c.social

@simoneonofri

simone@w3.org

Simone Onofri (W3C)

Why a Threat Model for the Web Platform?

According to ethical web principles, the **web platform must be secure, and respect the privacy of users**.

To bring this to the ground, **before entering CR**, a **horizontal review** is made that includes **privacy and security**.

And is asked to write the **security and privacy consideration sections**, which should contain **threats related to the specification and mitigations**.

Such sections, should be **the result of a threat model**, as specified by the questionnaire, but on the one hand **we don't have a shared threat mode**l and on the other hand there is **no shared approach on how to do threat modeling** (and how to integrate it into the standardization work).

What is Threat Modeling? And when?

Threat Modeling is the process of **defining a system model (the scope)**, identifying **threats and resulting attacks**, addressing them through **responses**, and **continuous revalidation**.

It is **normally used during the design phase of software development** (Howard & LeBlanc, 2001), and it **fits standards as they defines a technology for the implementation phase**.

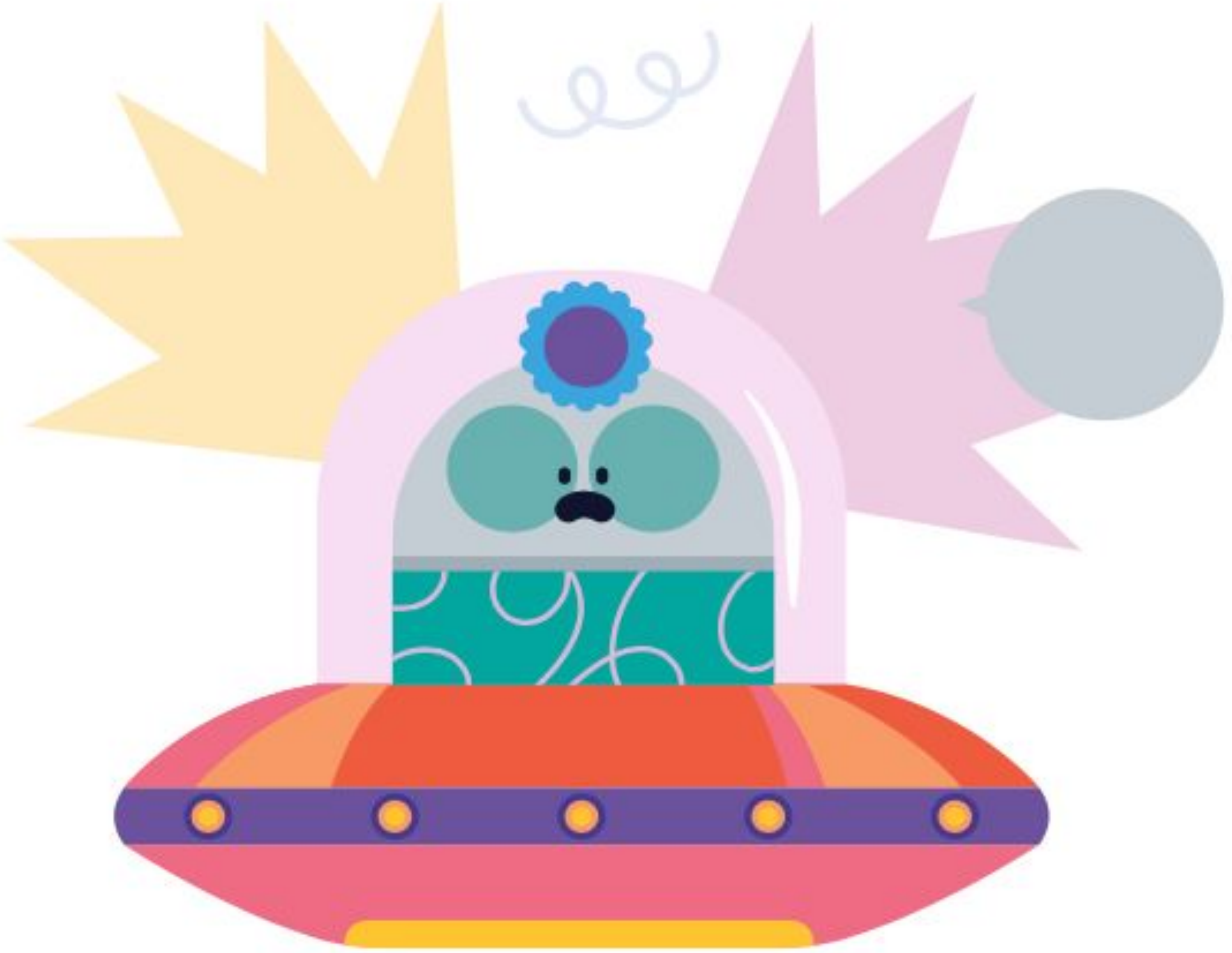
We should start **doing it right after the features are defined** (according to the W3C process, starting **with the explainer** and **not just before the review**).

What kind of model?

Based on the assumption that “**all models are wrong, but some are useful**” (Box, 1979), between the **Security Interest Group** and the **Threat Modeling Community Group** we are working on two models at two different levels.

A **high-level minimalist one**, where the **networking layer and protocols used** (e.g., HTTP, TLS, and DNS, etc...), and a **mid-level one where the web features are in the browser**, which **defines a common architecture and terminology for all of the major components involved in realizing the Web**.

Having **a shared Threat Model for the Web can help spec developers** be faster in **identifying the threats of a Web APIs**, and a good in understanding in **which Web APIs or Web Features are useful** to develop.

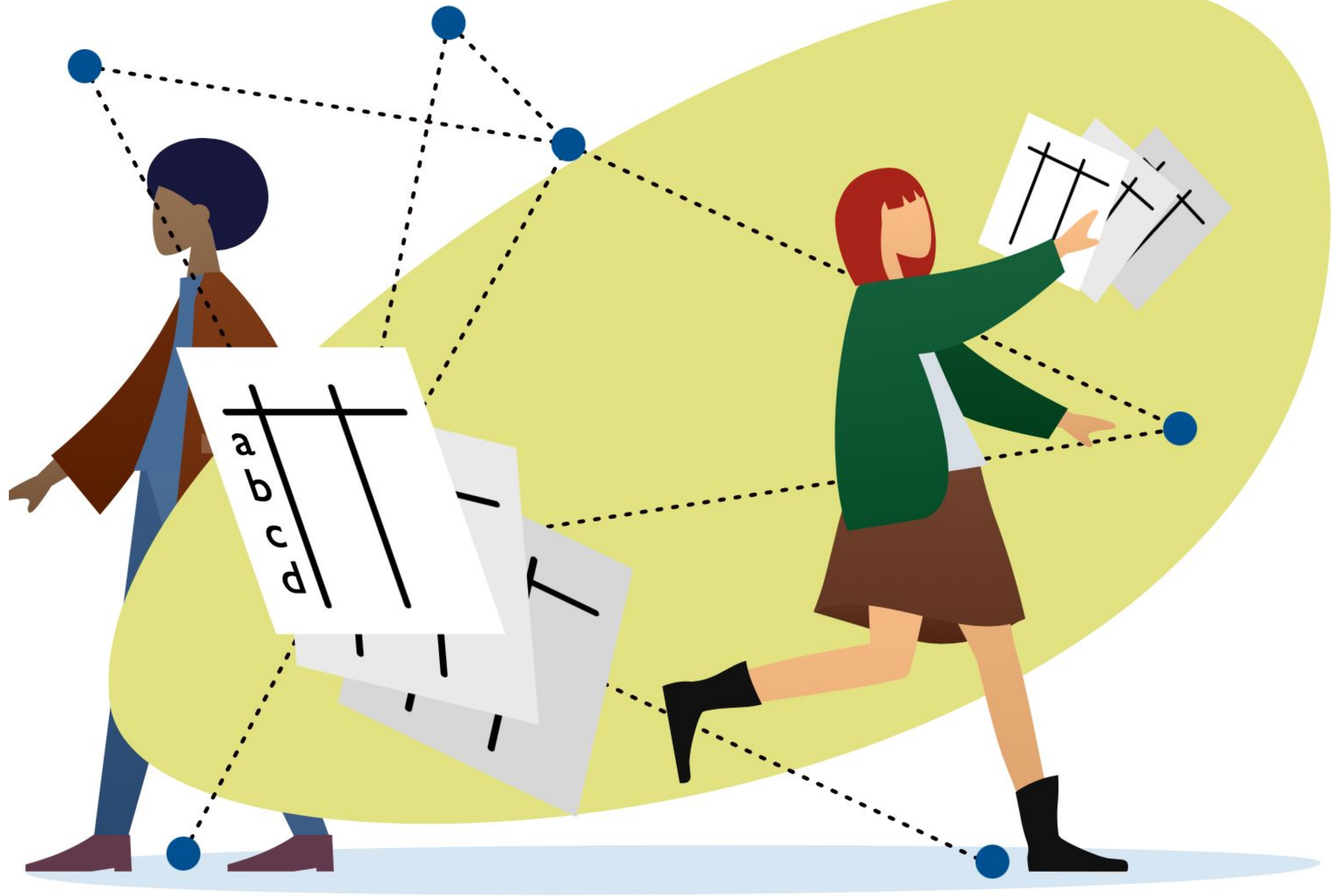


What are we doing?

We started with some **bibliographic research**, although **public information is not always up to date**, as the web platform moves quickly.

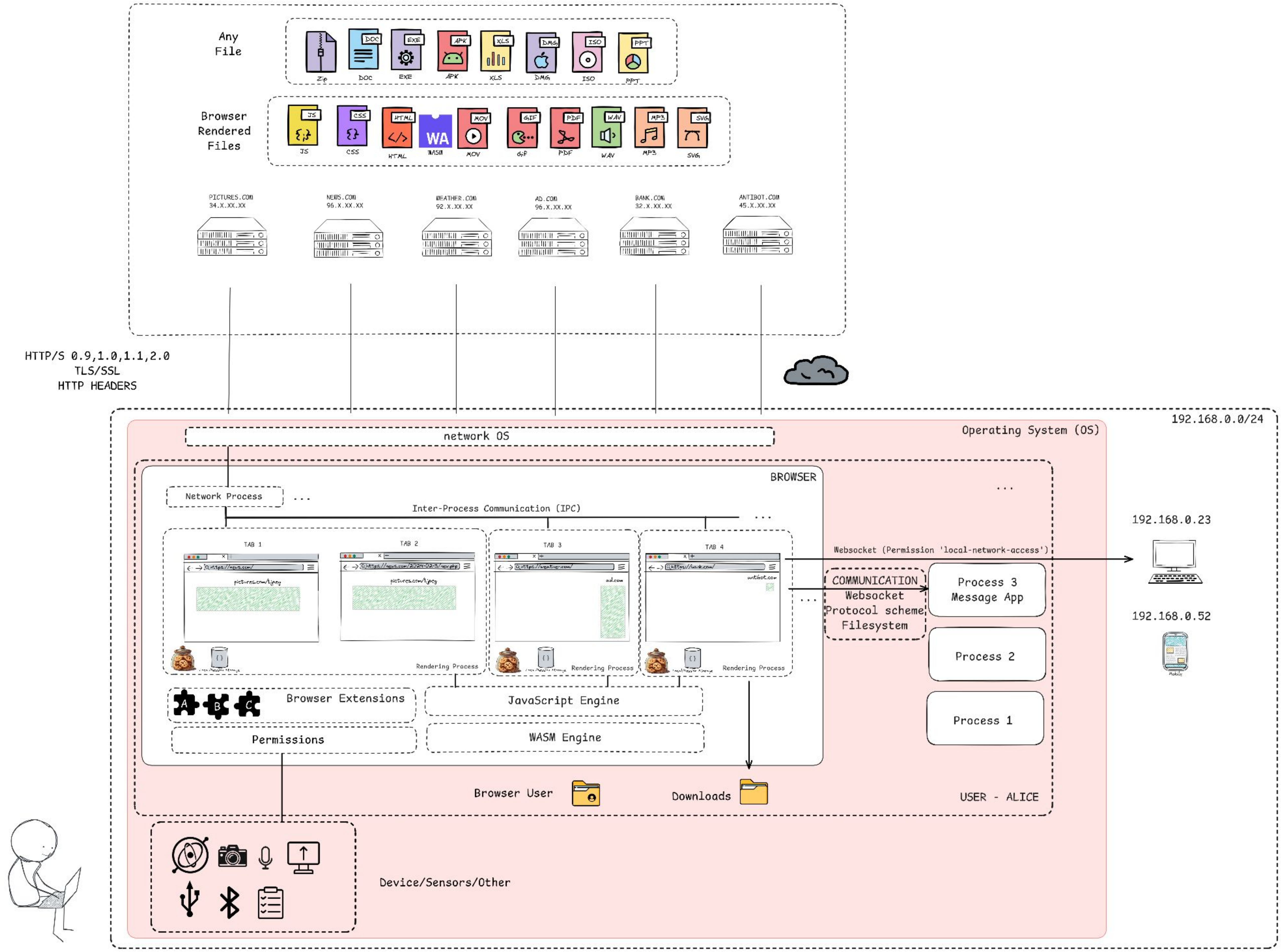
For example, a recent discussion in WebAppSec WG made the point that **current protection for powerful features like the Permission API can be done in a different way** with **user-initiated actions**, **avoiding tedious pop-ups** and making it the user's own action to initiate the ceremony, and thus to know the specific context in which the feature is activated.

We **discussed this at Web Engines Hackfest 2025**, to collect initial feedback to understand “**what are we working on?**” and then move onto the other typical threat modeling questions.



What are we building?

We began by mapping the **components**, according to an **abstract structure of a web browser** (e.g., its kernel, rendering engine, extensions, storage, javascript engine...), then the **elements on which it depends** (e.g., OS, Network, Native Applications...), the **Entry Points** (e.g., UI, Network, Web Content in different forms, user input, extensions...), what **assets to protect** (e.g., User Data, User Privacy, the History...), the **Security Features** (e.g., Sandboxing, SOP, CSP, Security Headers...) and a **Data Flow Diagram**.



Do you want to help us do a good job?

More than welcome issues, pull requests, editors, authors…

https://github.com/w3c/threat-model-web/

@w3c@w3c.social

@simoneonofri

simone@w3.org

Thank you.

Questions?

Support us

Your support makes a huge difference to our operations as a public-interest non-profit and to make the web work – for everyone.

Learn more at: http://www.w3.org/support-us/