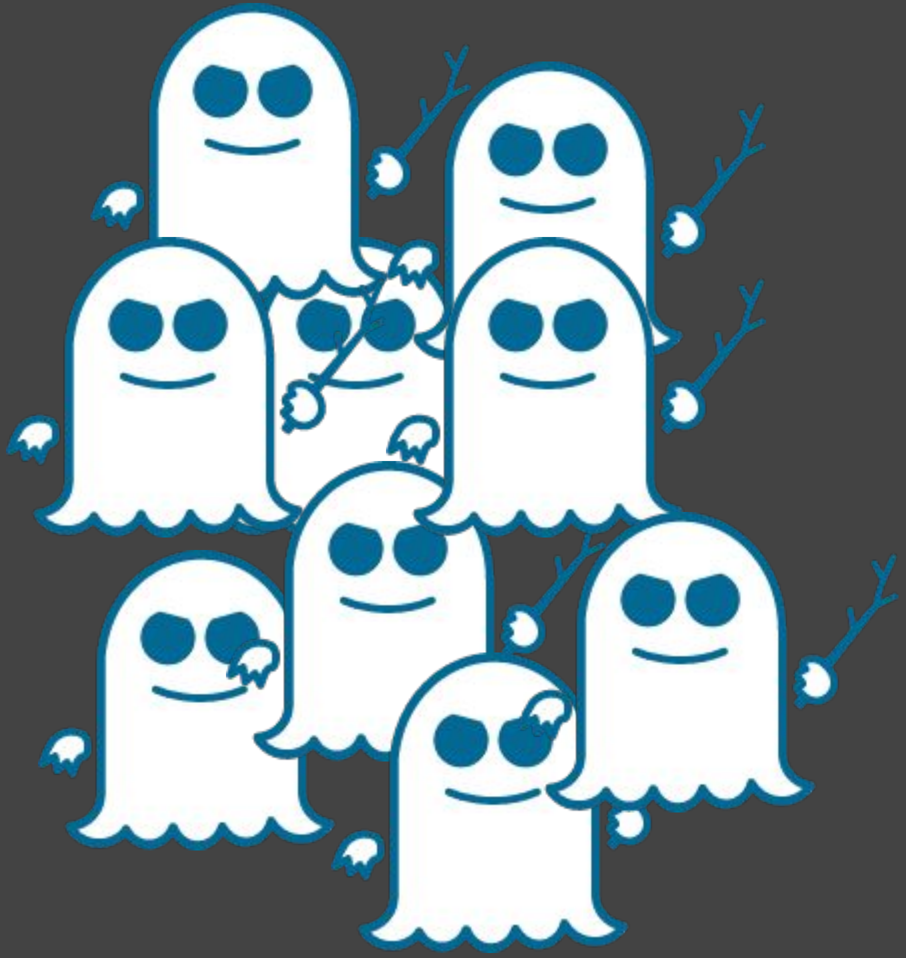
Isolation by Default

XSLeaks Summit 2020-12-01 — Camille Lamy & Mike West

Status quo ante:



Status quo: Well-informed developers will adopt CORP, XFO, COOP, and COEP. Less-informed developers remain vulnerable.

The Future?

Browsers will isolate documents *by default*. Developers who require cross-origin collaboration can opt-out of isolation.

A Few Modest Proposals

User agents should:

1. Apply `COOP: same-origin-allow-popups` by default: https://github.com/mikewest/coop-by-default/

2. Require embedees to opt-into framing rather than out of it: https://github.com/mikewest/embedding-requires-opt-in/

3. Deprecate and remove impediments to origin isolation by default (most notably `document.domain`: https://github.com/mikewest/deprecating-document-domain)

A Few More Modest Proposals

User agents should:

4. Require opt-in for communication across network boundaries: https://wicg.github.io/cors-rfc1918/

5. Shift towards credentiallness requests by default (`SameSite=Lax` on the one hand, `COEP: x-bikeshed-credentialless-unless-cors` on the other): https://github.com/mikewest/credentiallessness/

6. Strict MIME type checking, in conjunction with CORB/ORB.

What else should we try to ~~break~~ fix?