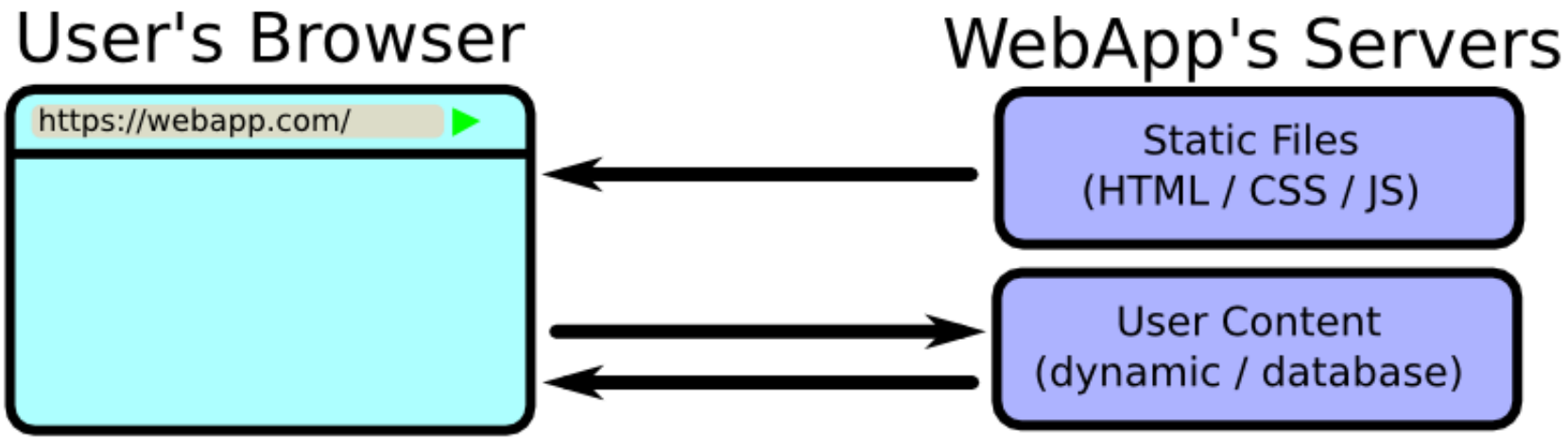
Bring Your Own Chat

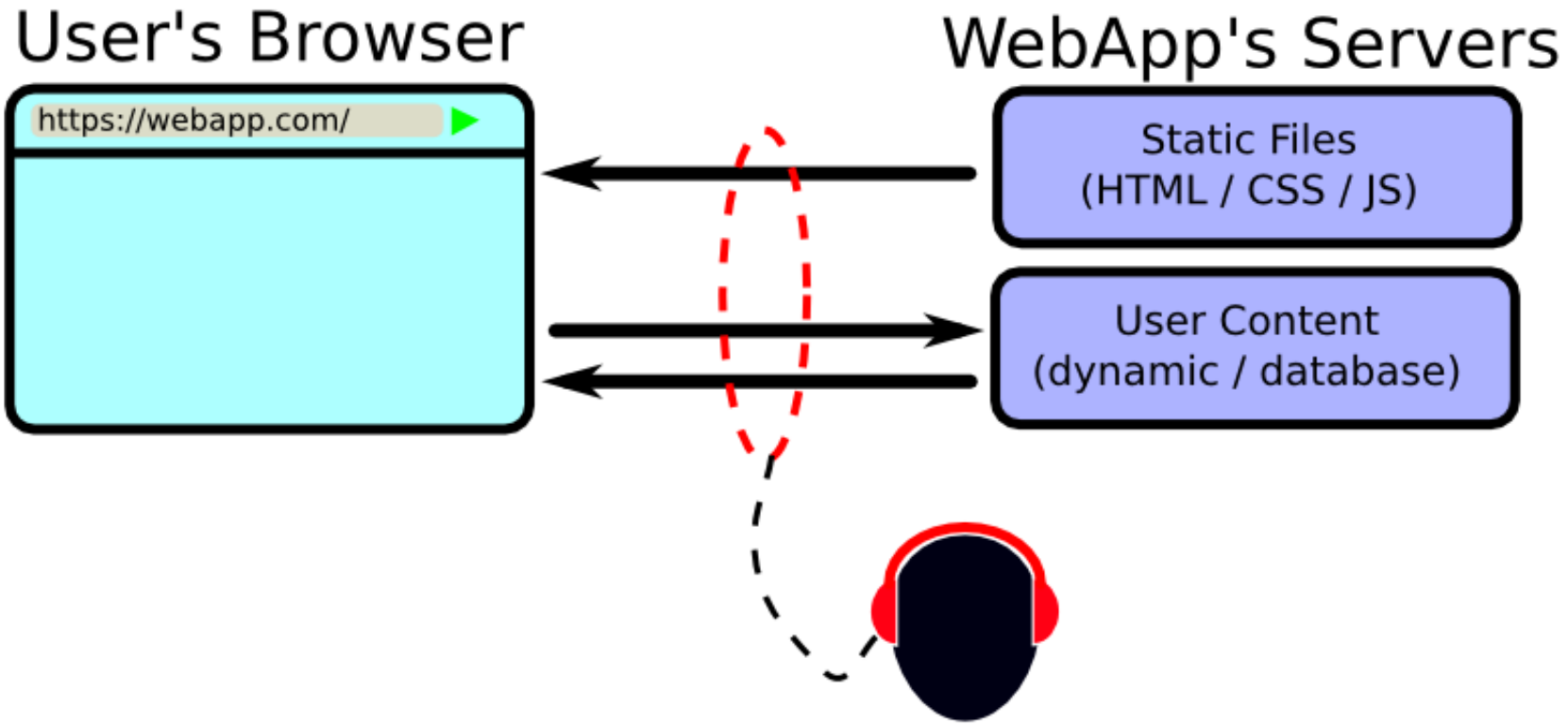
A secure, zero-knowledge chat webapp

using only a Drobox account and a browser

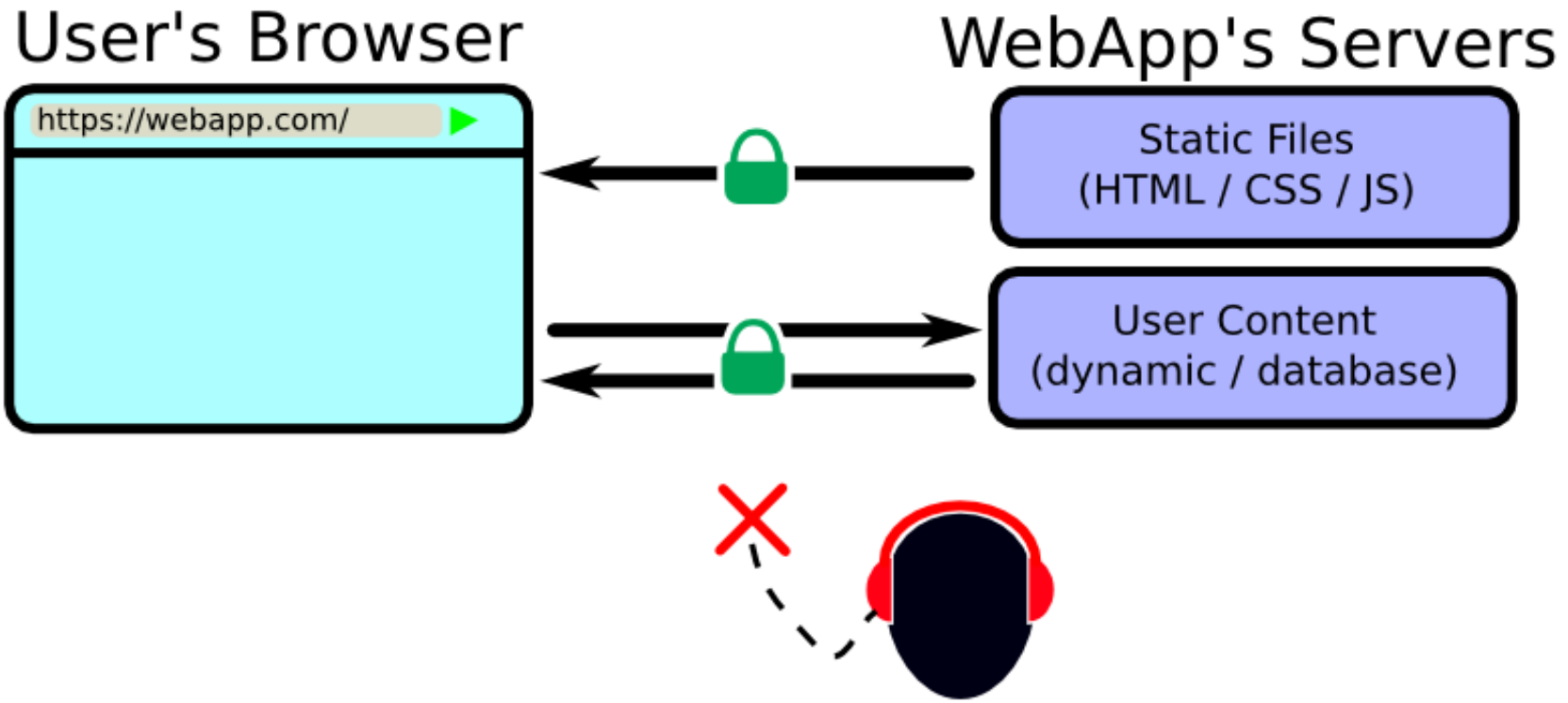
typical webapp flow



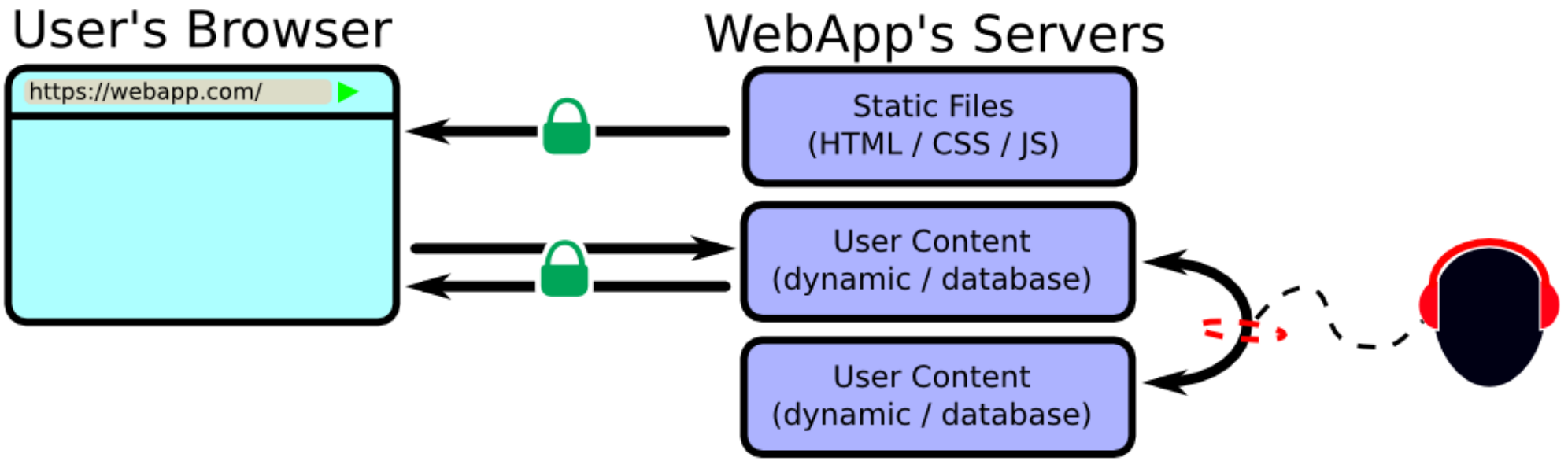
easy to tap


User's Browser
https://webapp.com/
WebApp's Servers
Static Files
(HTML / CSS / JS)
User Content
(dynamic / database)

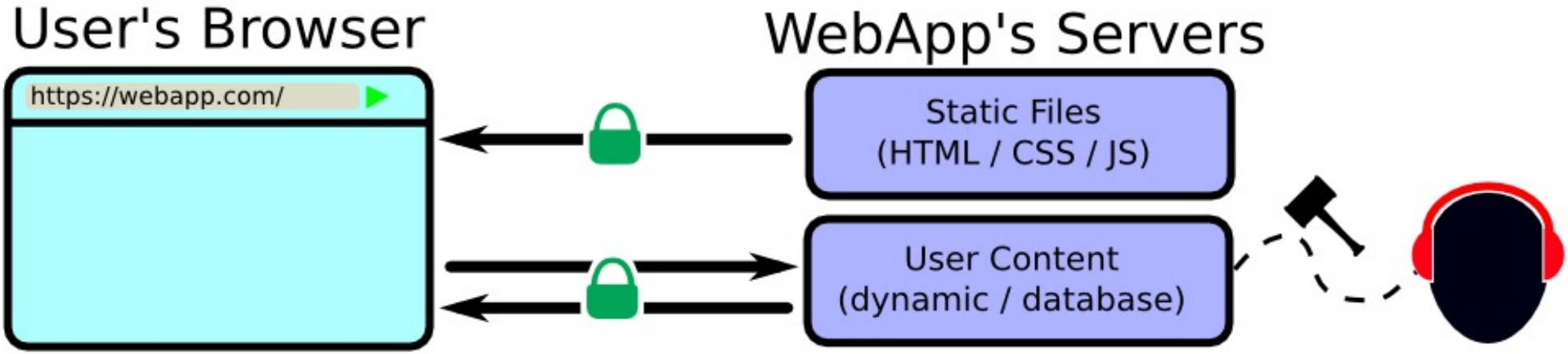
https to the rescue



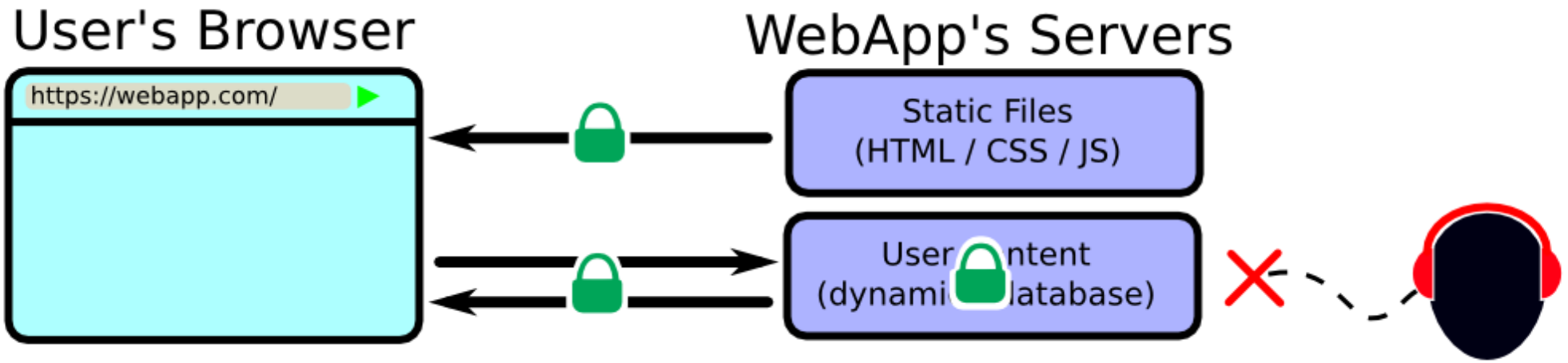
intra-company taps



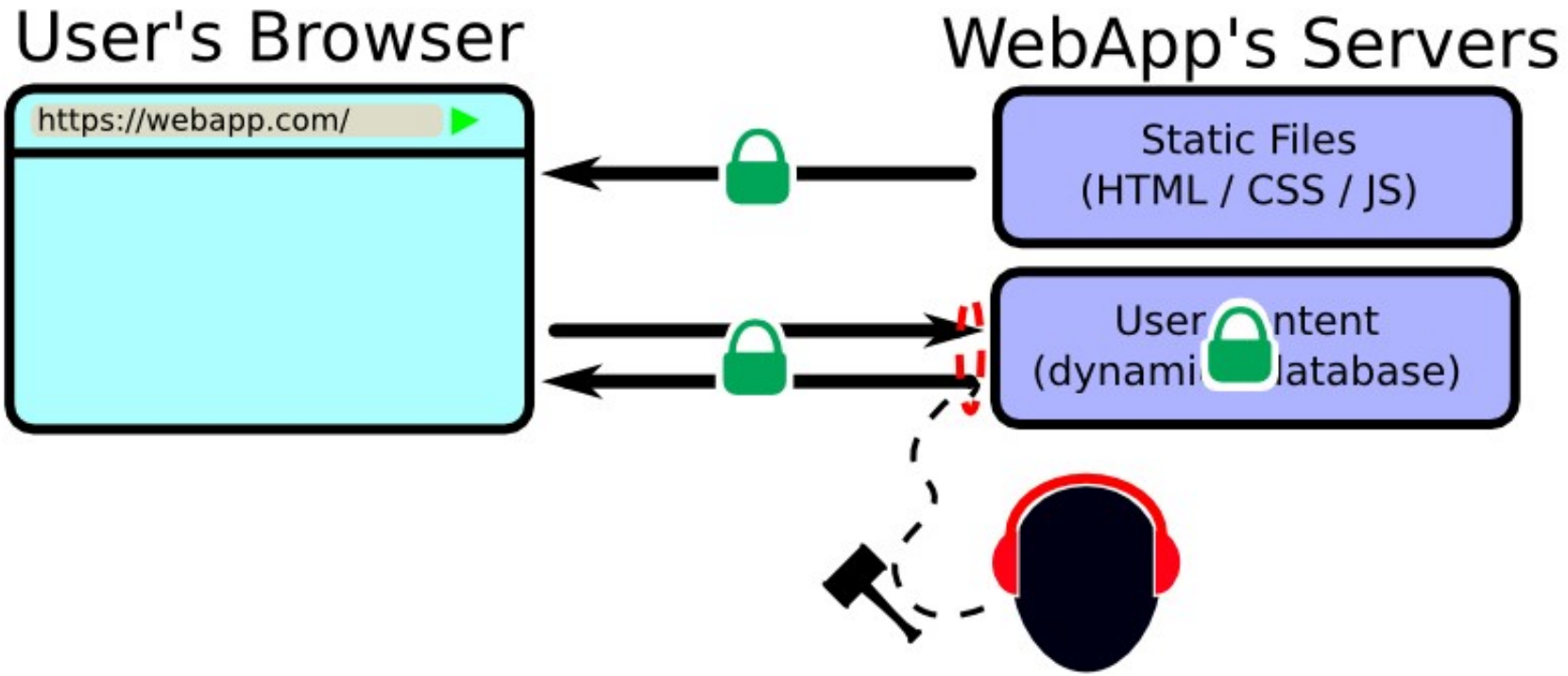
secret blanket court orders



internal encryption to the rescue

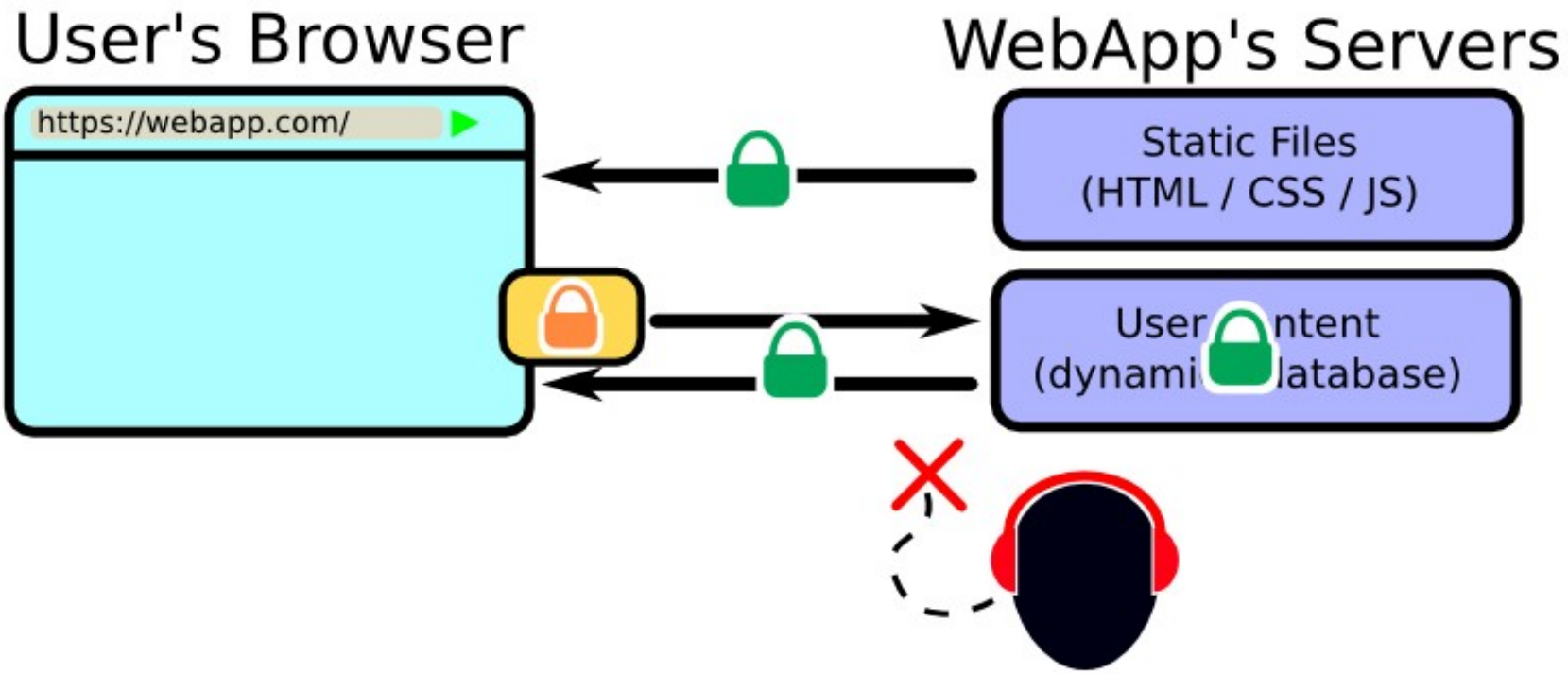


get ssl key via court order

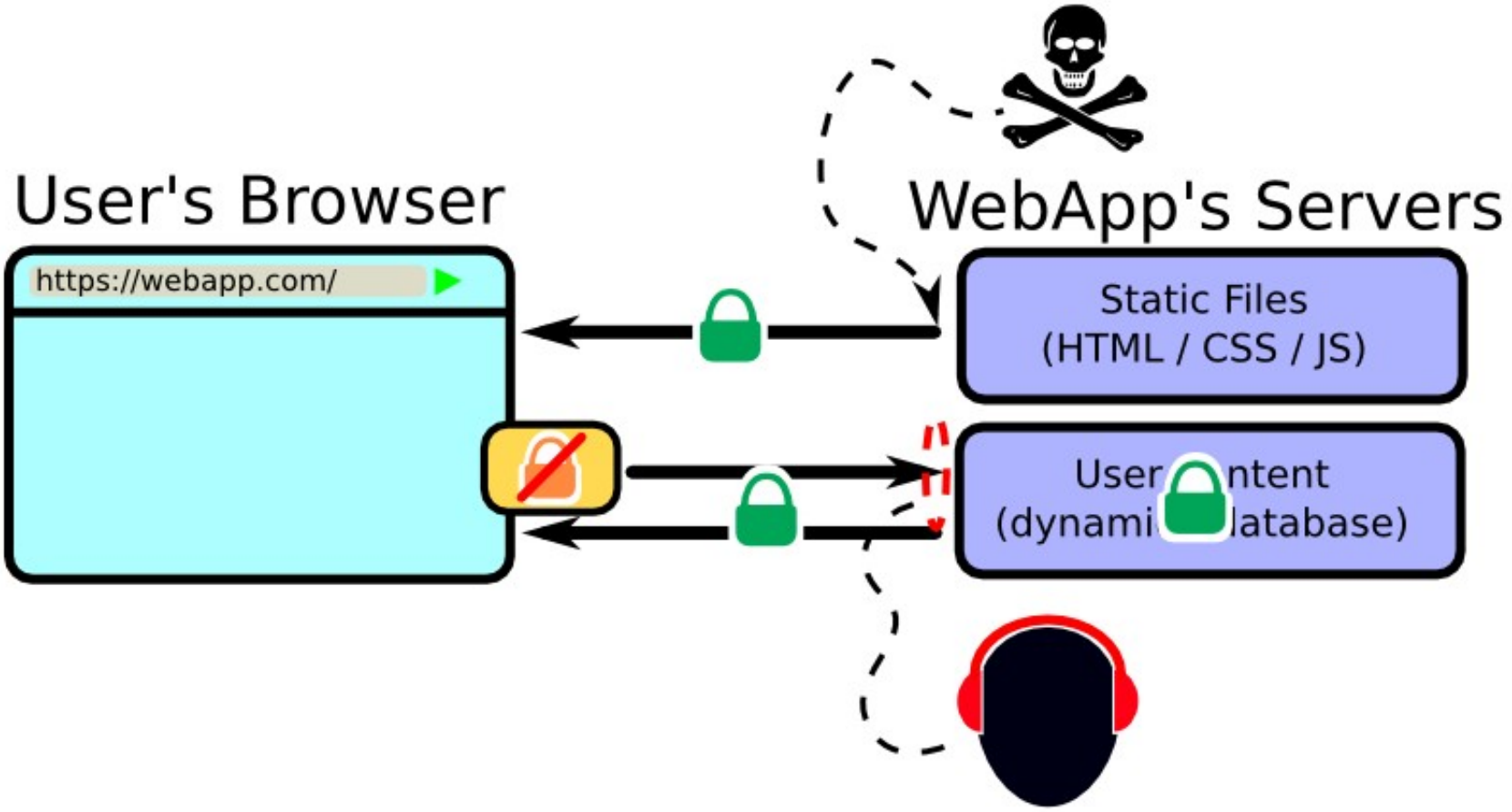


present day

client-side encryption to the rescue

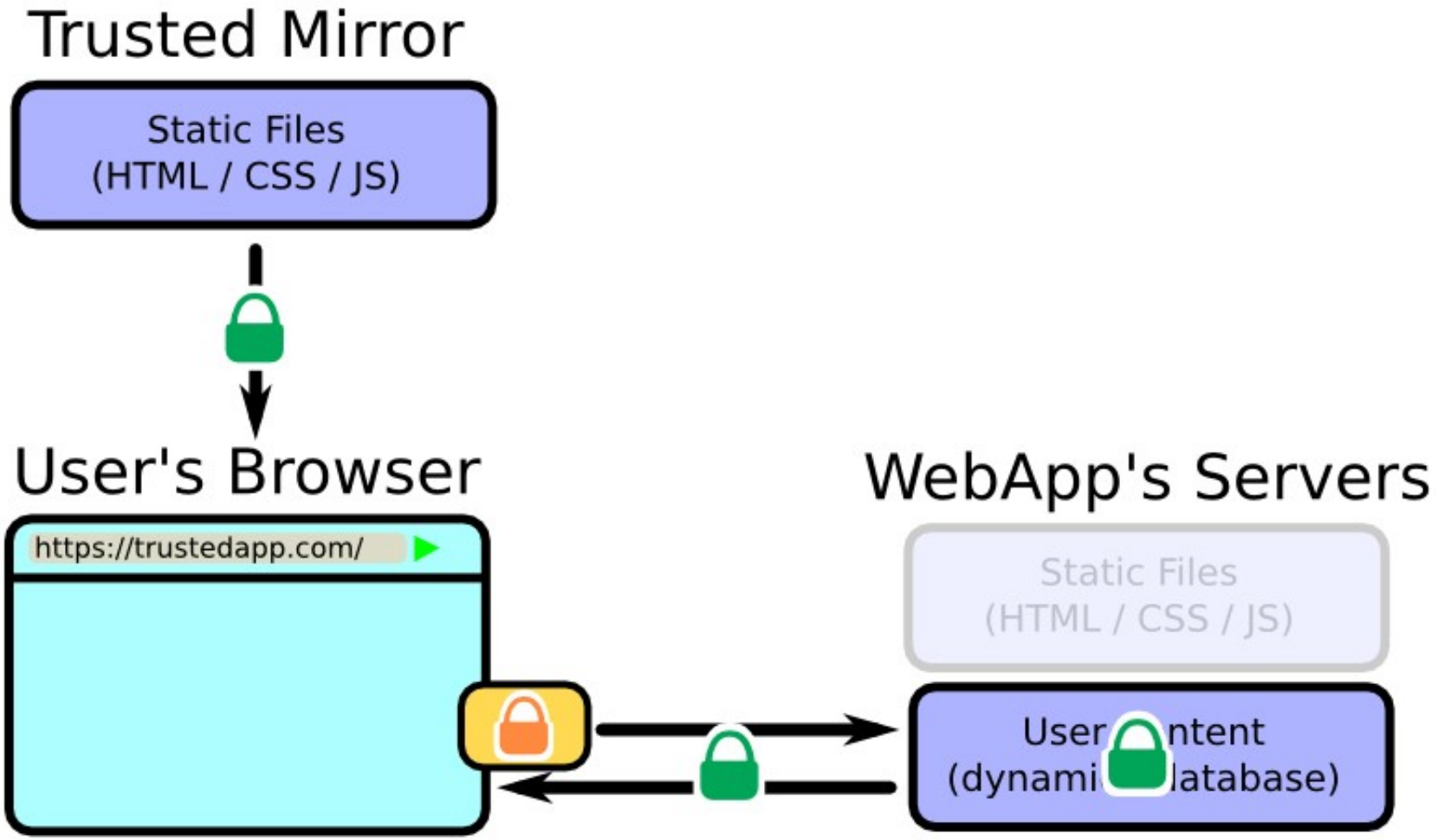


malicious javascript injection

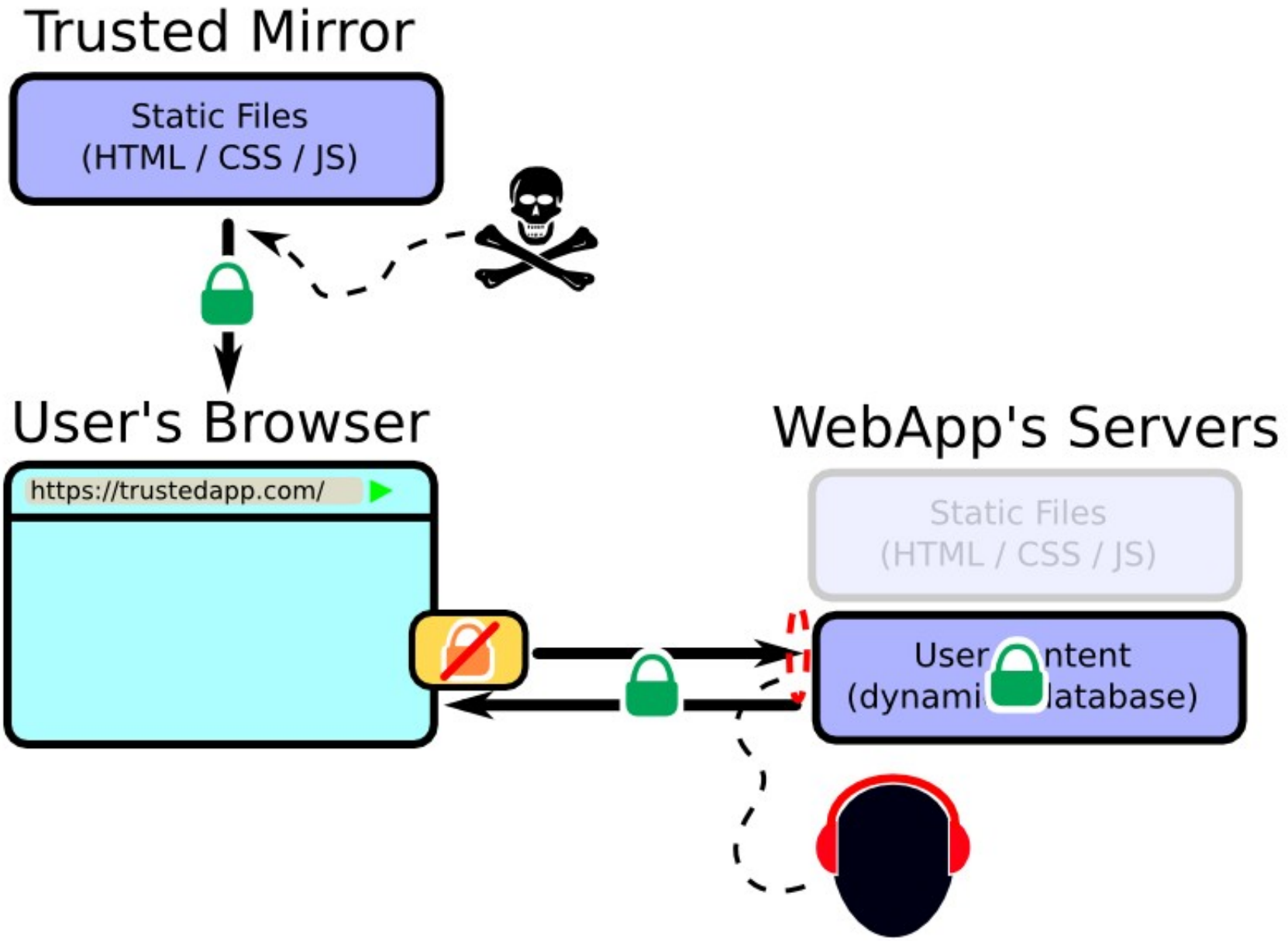


fundamental flaw of client-side crypto

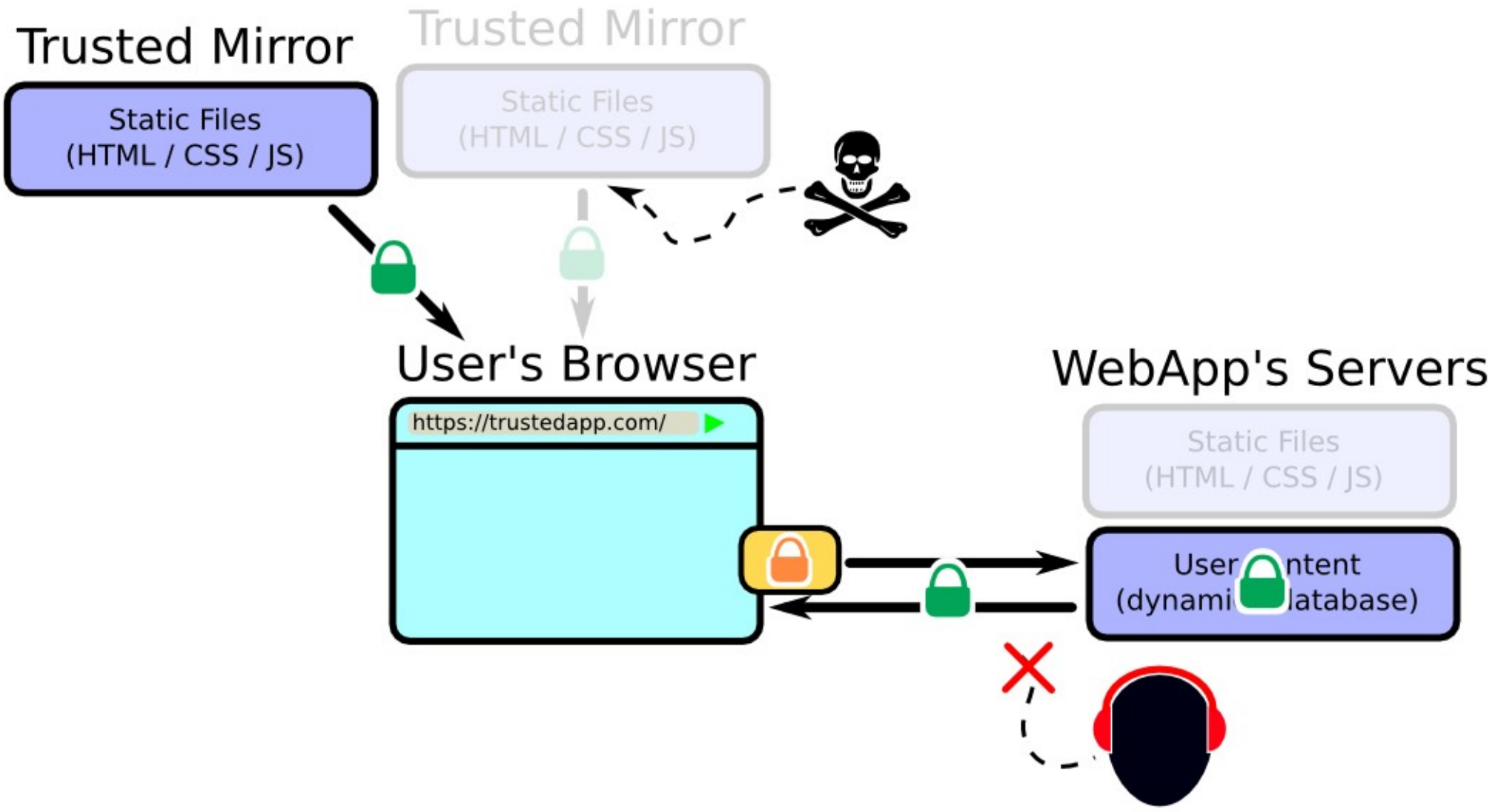
byoFS to the rescue



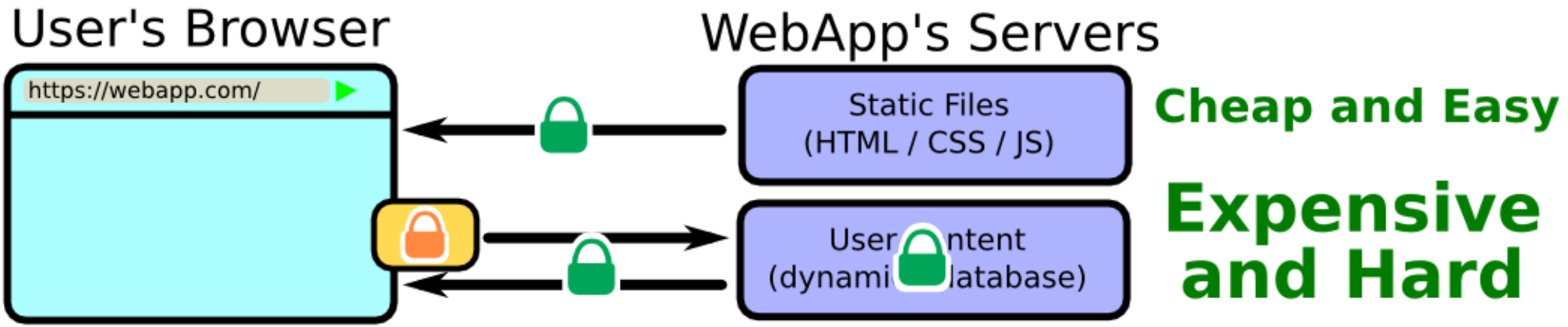
same fundamental flaw



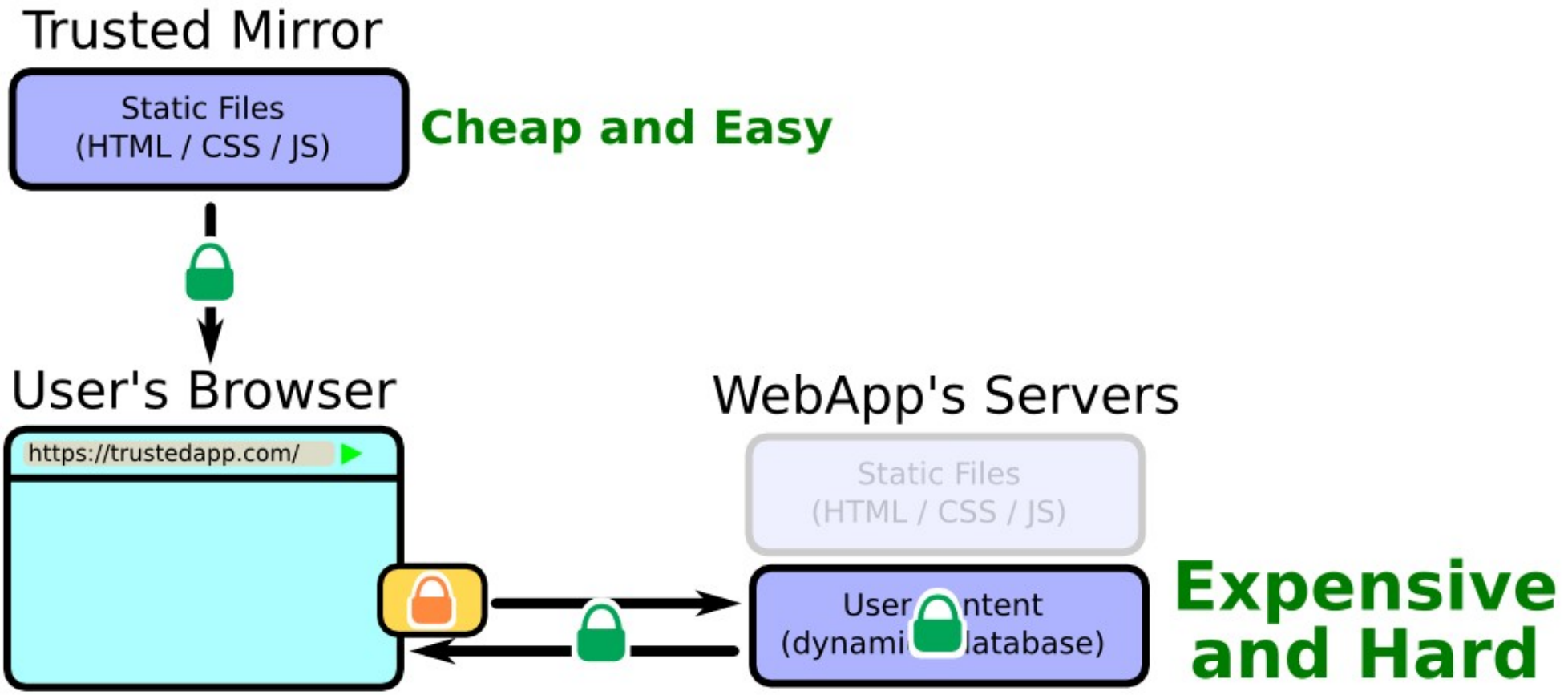
game of cat and mouse



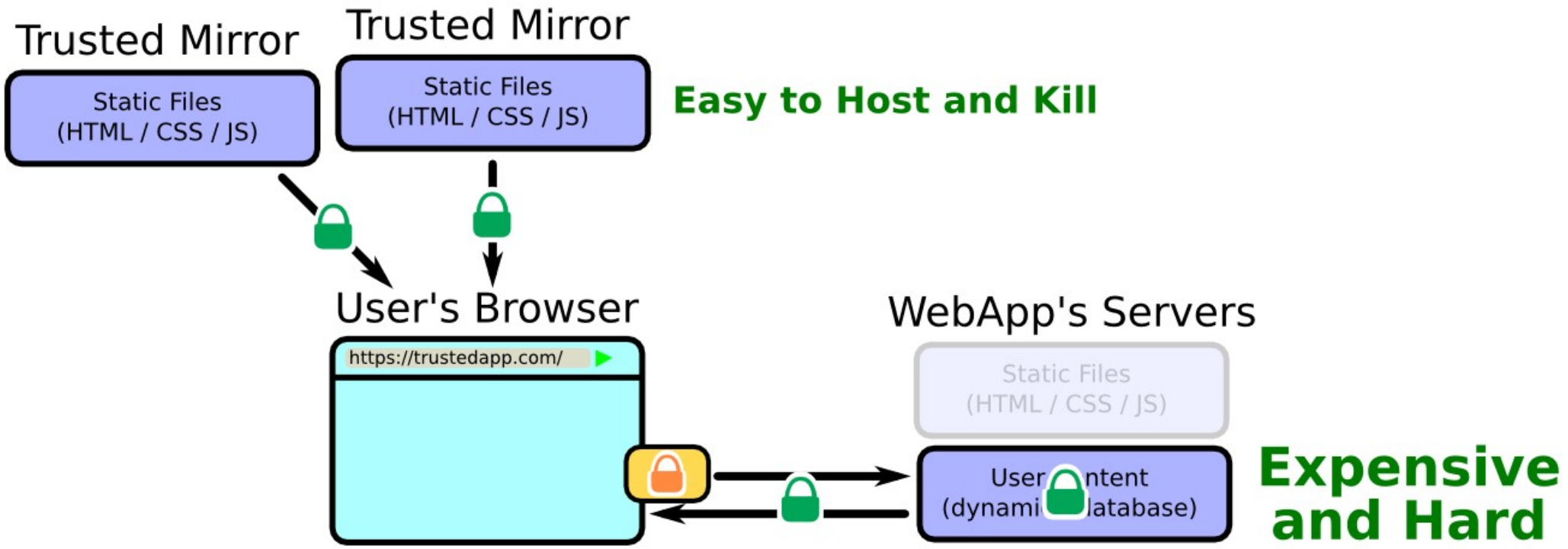
let's talk about money



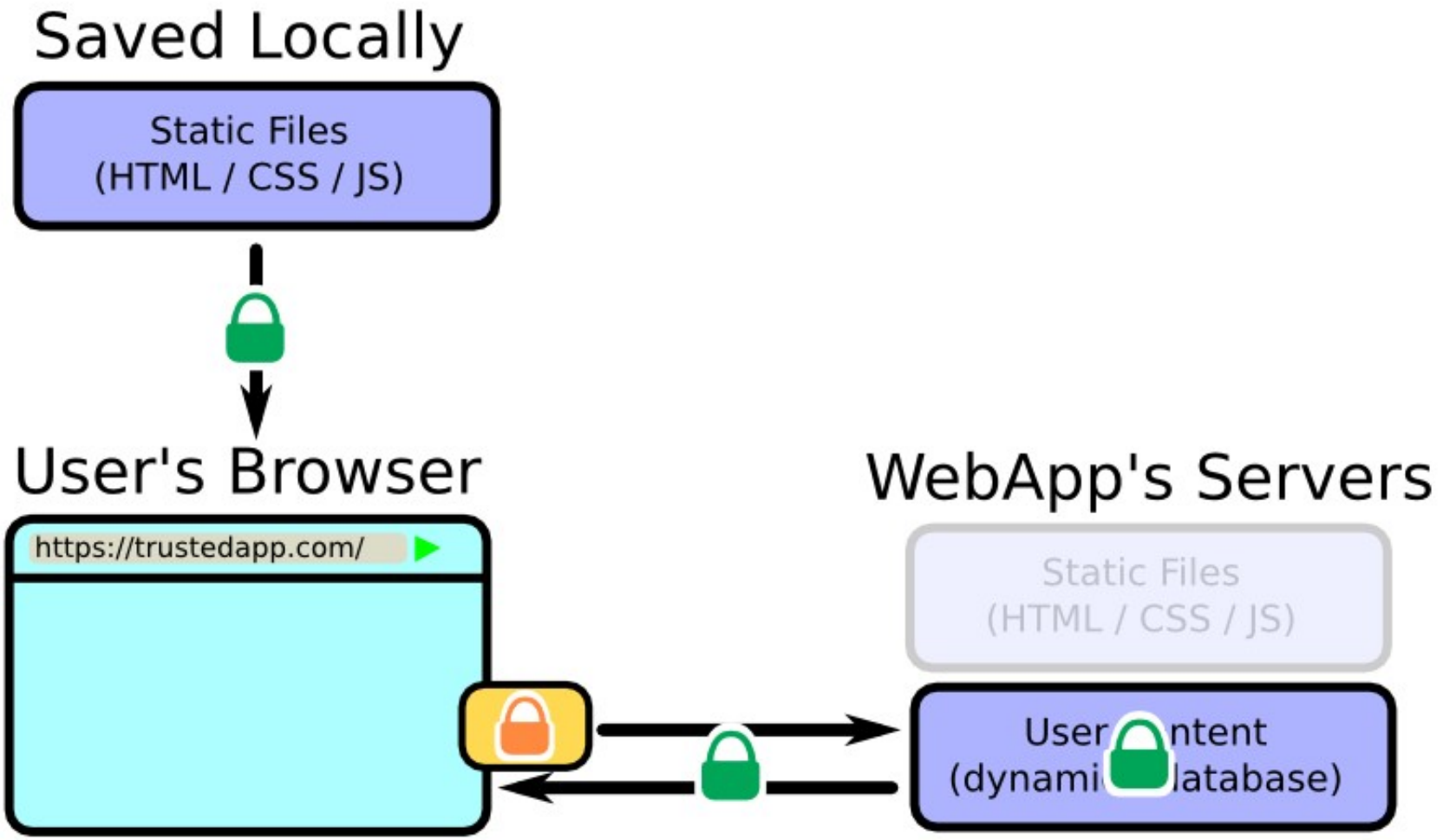
let's talk about money



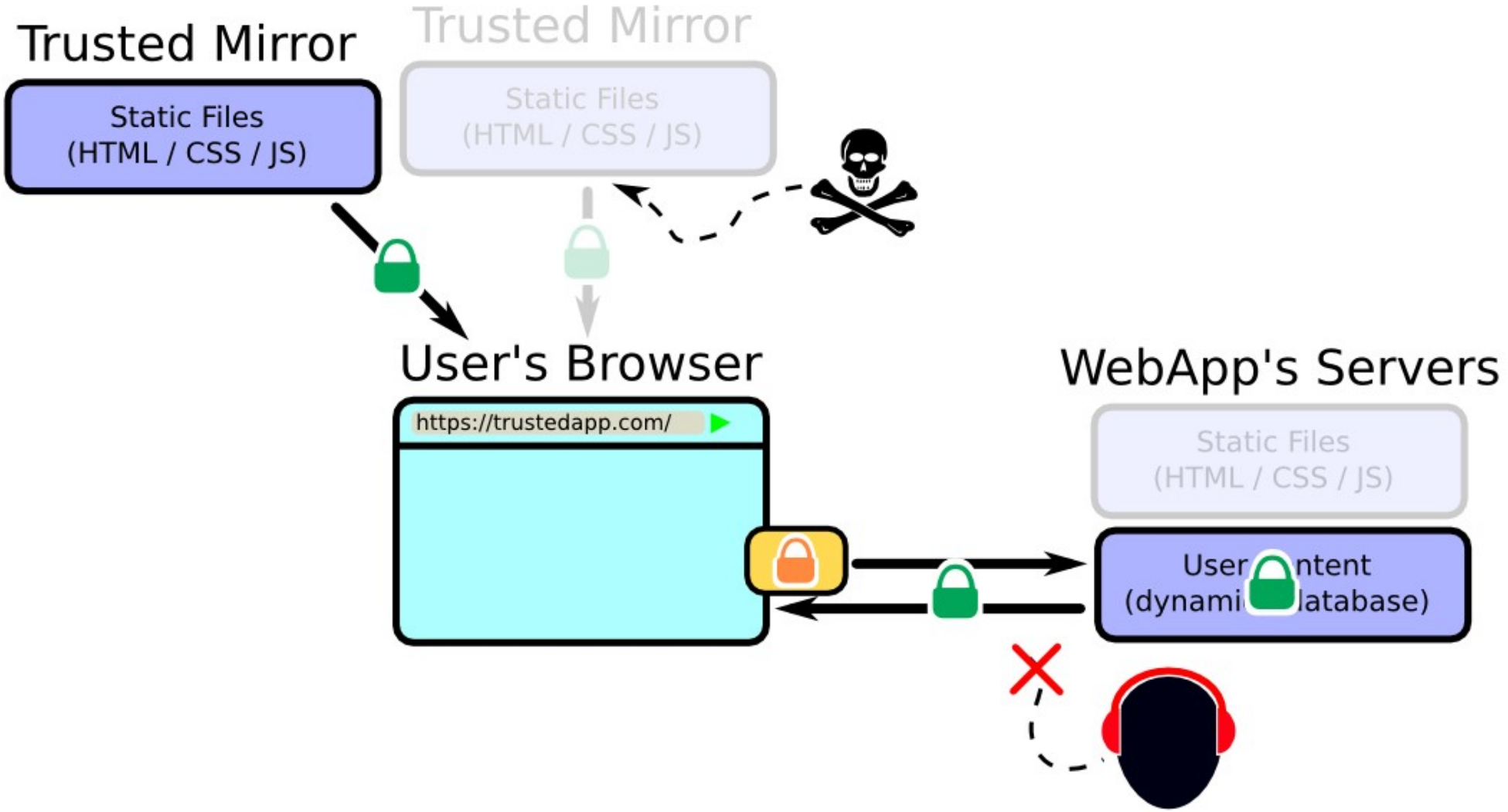
easy to host and kill



you can even save it locally



byoFS lessens the fundamental flaw



demos
https://github.com/diafygi/byoFS/