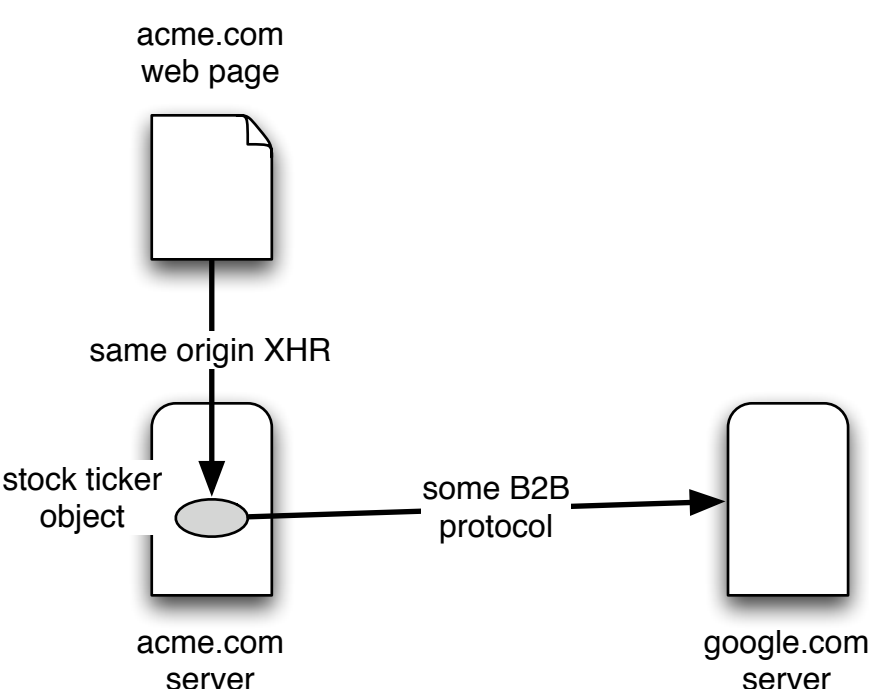
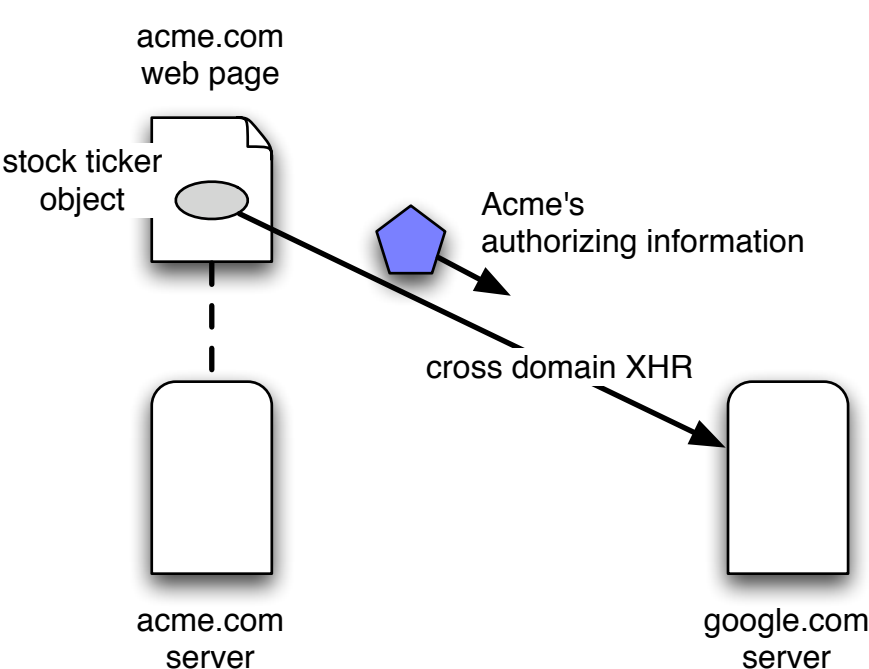


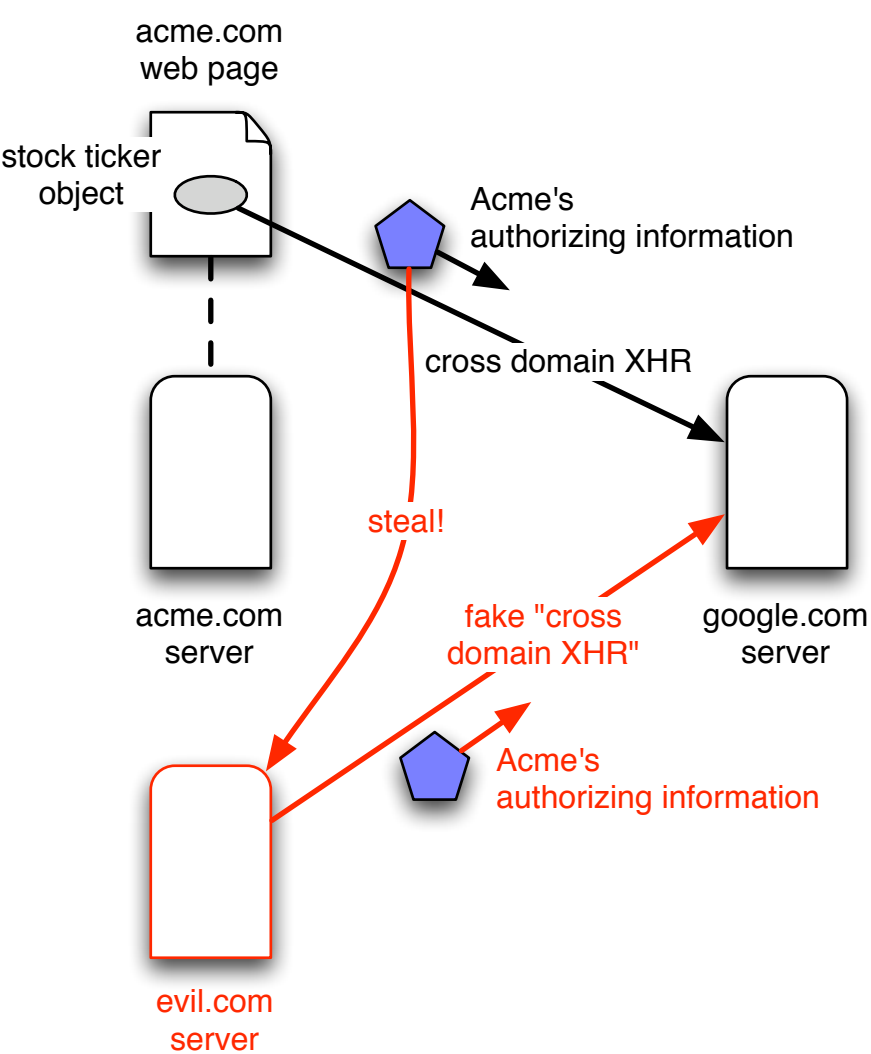
1. Acme Finance provides a cool stock ticker. Google Finance provides raw financial information. Acme has an account at Google, which it legitimately uses to get stock data. All traffic from Acme's Web pages goes through the Acme server, where the "stock ticker objects" are hosted. This ensures that nobody can steal Acme's authority to use Google.



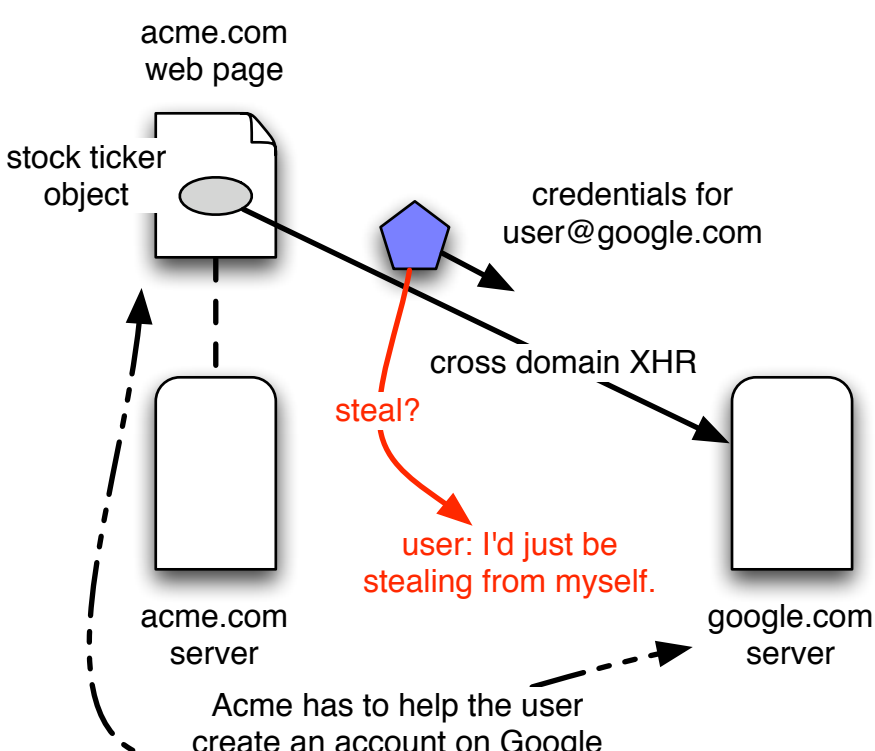
2. Acme wishes to make its application more efficient. It wants the stock ticker object to reside in its users' browser, and make direct calls to Google. It does this by providing enough authorizing information to its web page such that the page may make cross-origin requests to Google.



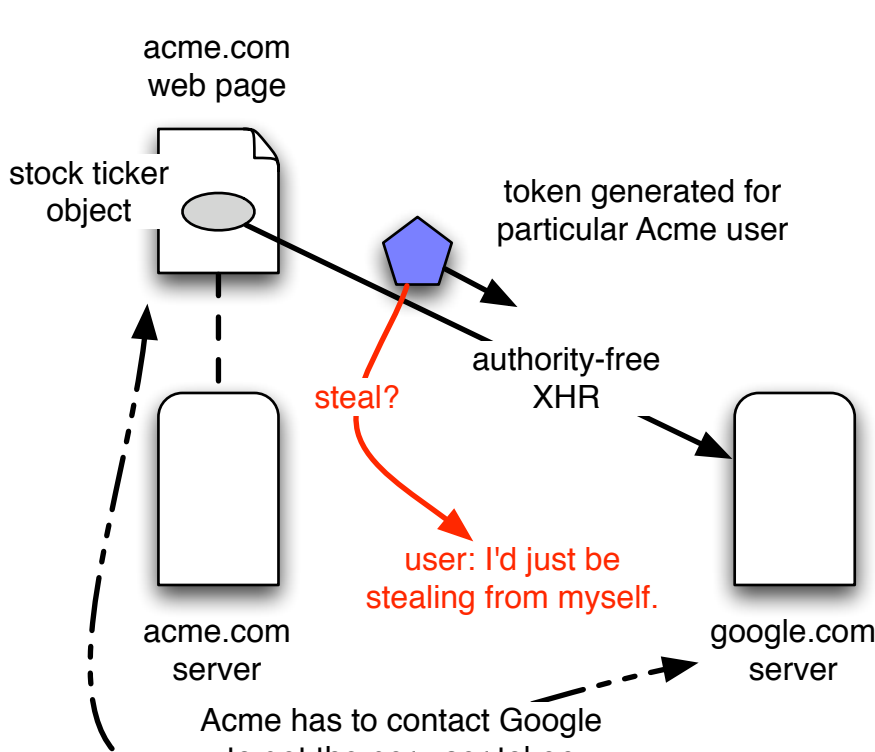
3. This situation is dangerous because a malicious user of Acme, who works for Evil.com, can steal Acme's authorizing information (e.g. by running their browser in a debugger) and use them to run their own site. The Google usage gets charged back to Acme.



4. With cross domain XHRs, we can avoid this problem by having each Acme user get their own account on Google. This requires either the user logging into Google, or Acme helping them get Google accounts. The credentials being transferred are now the user's, not Acme's, and so the user gains no marginal benefit by stealing these credentials.



5. With a capability protocol, we can do the same thing if Acme gets a new capability to Google for each of its users. This requires per-user B2B communication between Acme and Google at least once per Acme user. This has the same security properties as #4.



6. The cross domain scenario, #4, has one advantage vs. capabilities: *If the user already has an account on Google and is logged in*, then no B2B communication between Acme and Google needs to happen. This works for a centralized world where there is one Google and a few satellite Acmes, but not for a distributed world with many collaborating entities. It also does not work if the user has two accounts -- bill@google.com and bob@google.com -- and wishes to decide which one to use for the Acme application.

