Secondary Certificates

Solving the Easier-to-Attack problem

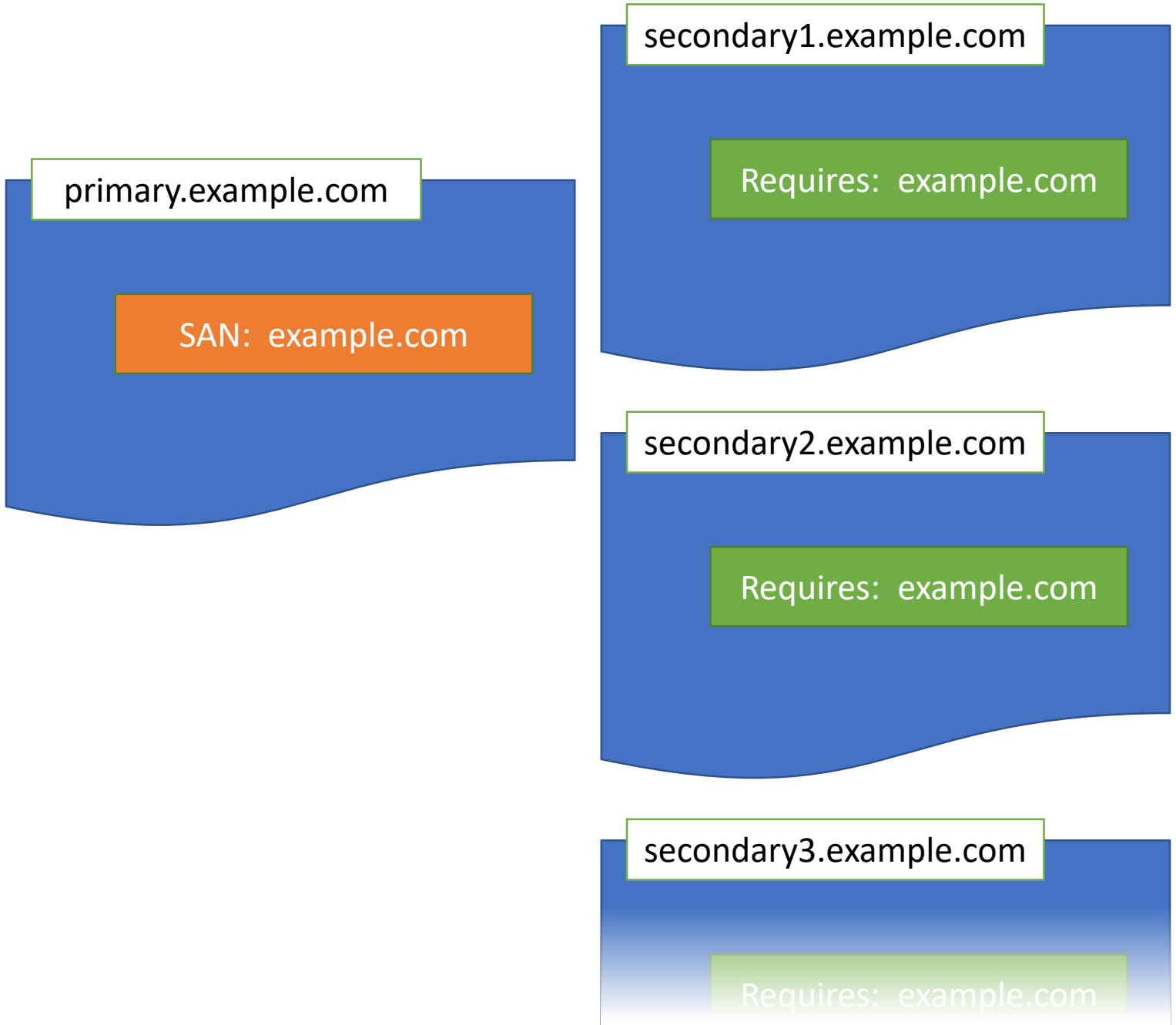
Reminder: Easier To Attack In Two Ways

Misissued certs are less traceable

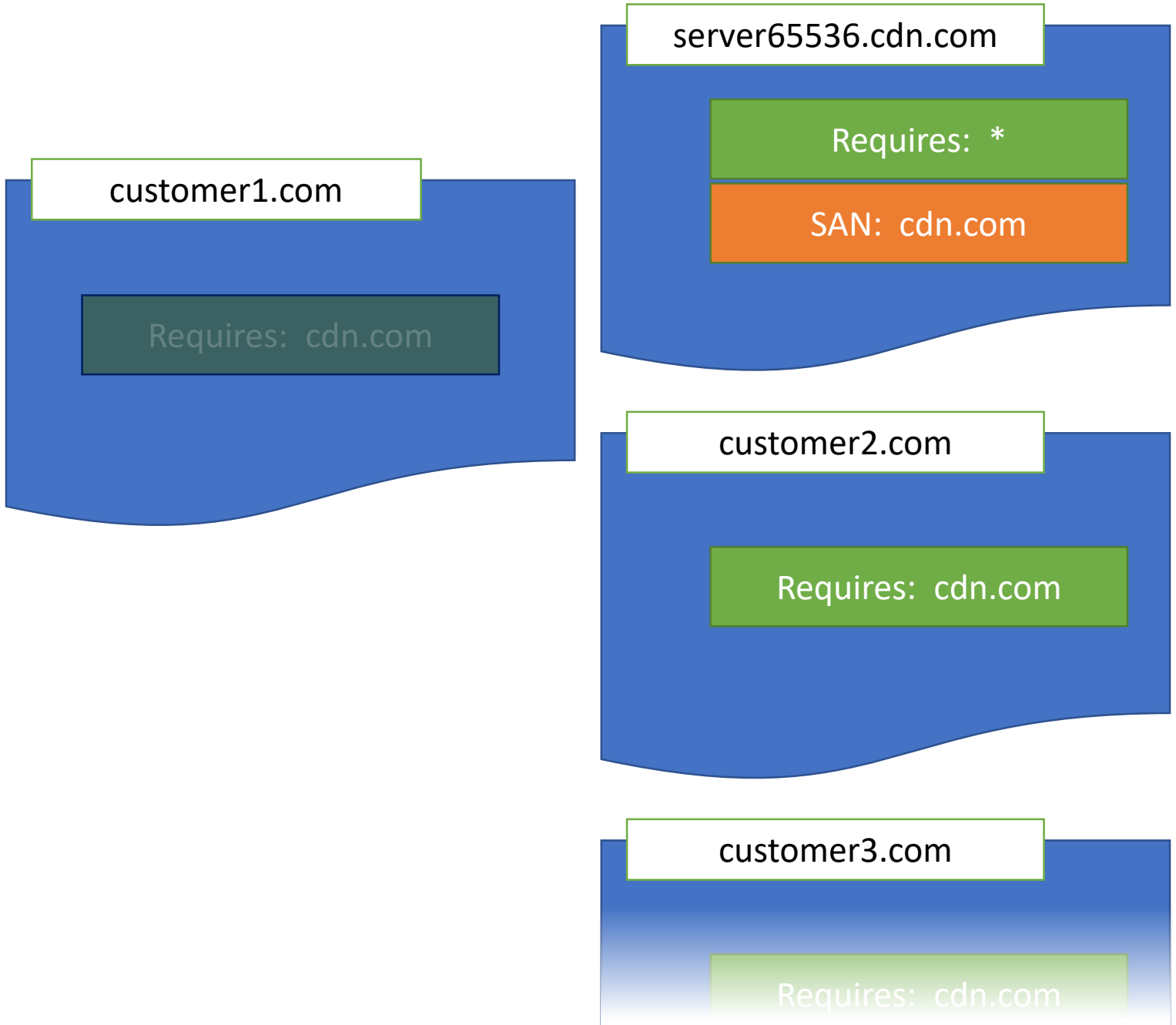
- **Without:** Attacker needs cert containing both attacker's domain and victim domain; this cert will appear in CT logs
- **With:** Attacker can use separate certs for the two domains / take the misissued cert to a CDN, with no recorded link to them in CT logs.

Compromised certs are easier to use

- **Without:** Attacker needs to hijack a TCP connection
  - Subvert IP routing or DNS resolution
- **With:** Attacker needs to induce navigation to an attacker-controlled origin



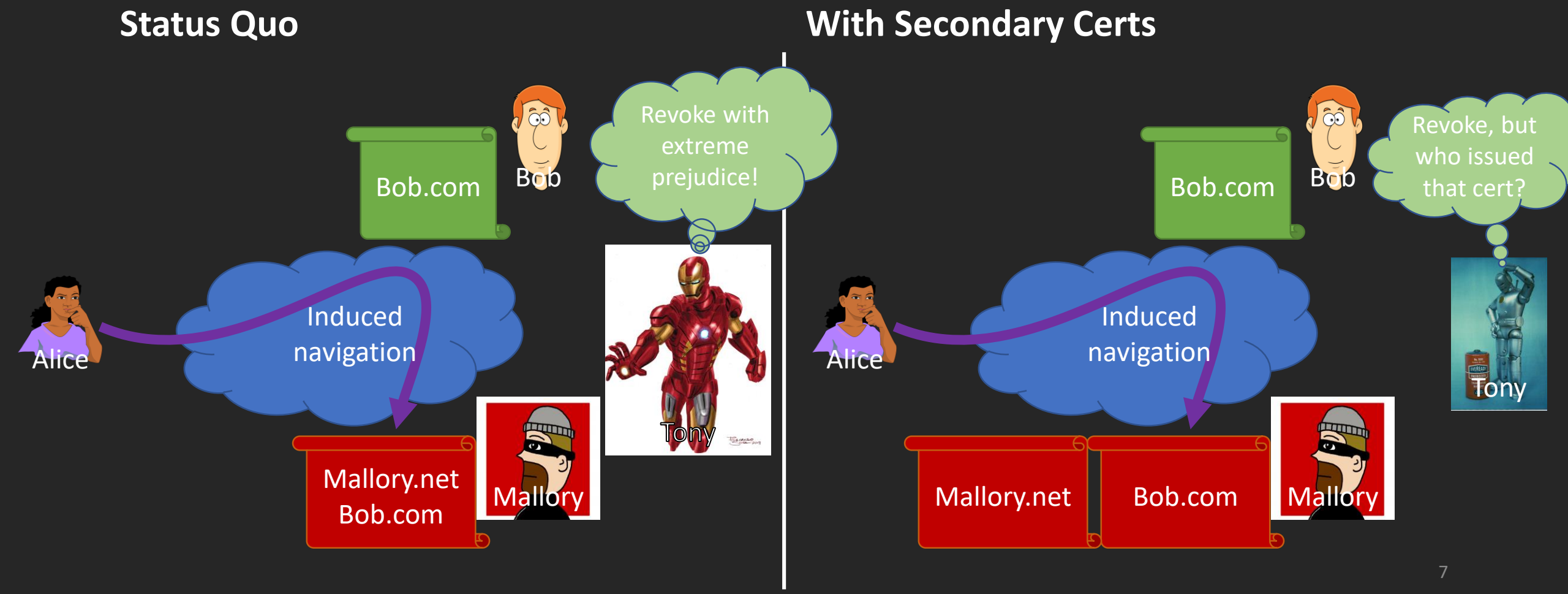
- Certificates indicate a required domain which must already be proven
- Can put required hostname in all certificates
- Can have explicit primary certificate



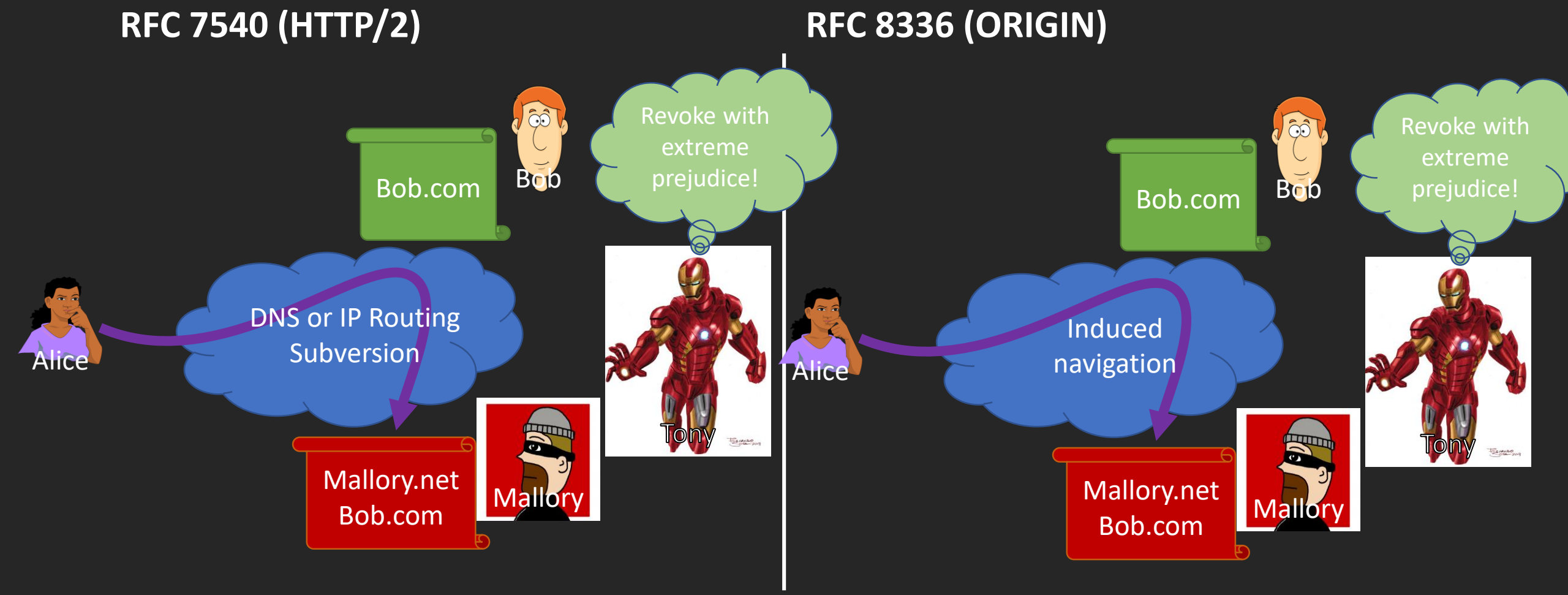
- CDN customers put only one extension in their certificates
- CDNs need to prove the CDN identity before using another customer's certs
  - One additional ExpAuth

That only fixes one problem!

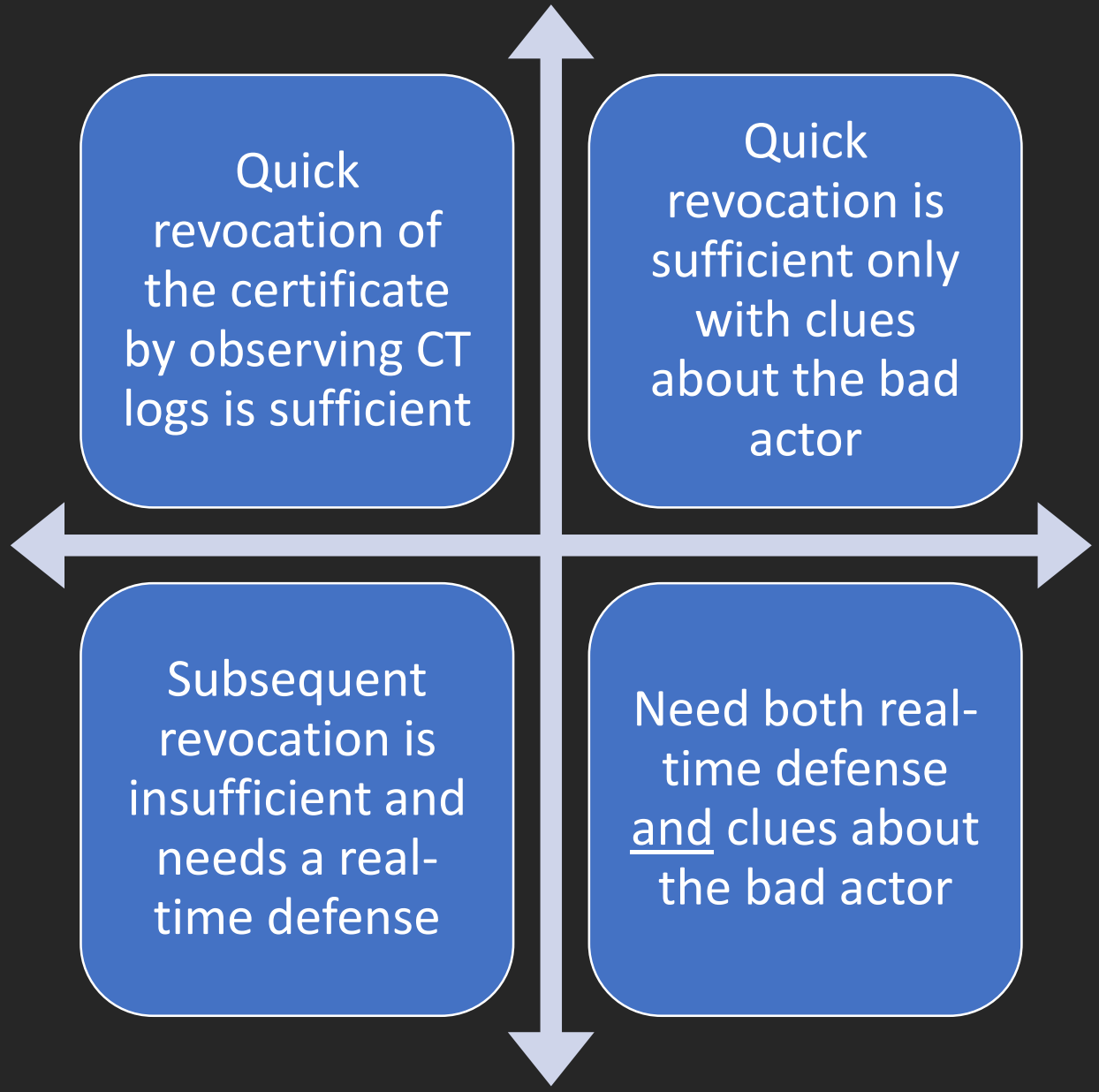
Remember: Misissued Certificates



Half the Problem Was Already There



Which Quadrant Are We In?



Limit use of wildcards in Required Domain

DNS check (or alternative) needed in both ORIGIN* and Secondary Certs

*Draft exists

Parallel Discussions

Does a Required Domain make Secondary Certs sufficiently comparable to Primary Certs?

Does the mis-issued cert case indicate broader discomfort with changing concepts of authority?