Adam Barth, Collin Jackson, and John C. Mitchell.

Robust Defenses for Cross-Site Request Forgery.

In 15th ACM Conference on Computer and Communications Security (CCS).
October 2008.

By Llyle van Schalkwyk. (October 2009)

Paper Summary

- Contributions made by the paper include:
  - Explanation of the CSRF threat model.
  - Explanation of existing CSRF defenses.
  - An experiment on Referrer suppression.
  - A proposal for the addition of an Origin header.
  - Advice for protecting against CSRF on October 2008.

Paper Summary cont.

- What is a CSRF attack?
  - In a CSRF attack “the attacker disrupts the integrity of the user’s session with a web site by injecting network requests via the user’s browser.”

- Paper is successful in terms of citations
  - After one year it has 13 or more citations.
  - Citations are from papers that explored CSRF.

Appreciative Comments

- The paper provides a comprehensive introduction to CSRF.
  - Ambitious in providing the **5** aforementioned contributions.
  - Paper can be used as a foundation for further research into CSRF.
  - The experiment targeted Referer Header suppression between requests, leaving other CSRF defenses open to investigation.

Critical Comments

- The Secret Validation Tokens technique was dismissed without sufficient technical reasoning.

- In Section 4.1 Secret Validation Token, the following statement is made:
  - "**Secret validation tokens can defend against login CSRF, but developers often forget to implement the defense** because, before login, there is no session to which to bind the CSRF token."

Critical Comments cont.

- In the same section the author states:
  - "Given sufficient engineering resources, **a web site can use the HMAC technique to defend itself against CSRF attacks.**"
  - HMAC of Session Identifier is a secret validation token defense against CSRF.

- The Origin header was proposed in section 5.
  - "To prevent CSRF attacks, we propose modifying browsers to send a Origin header [...]"

Critical Comments cont.

- The paper does not compare the valid Secret Validation Token defense to the proposed Origin header defense.

- Given the aforementioned, the paper still concludes with proposing the addition of an Origin header.

Question

- What technical security implications do you think the addition of an Origin header would have?
  - Assume that Secret Token Validation is a capable CSRF defense.

- Thoughts:
  - What guarantees web site developers don't also make a mistake implementing the Origin header defense? (It was stated that mistakes are made in current implementations using the Secret Token Validation defense)
  - Adding another feature could increase the attack surface available to CSRF attackers.
  - Increased choice of defense is not necessarily beneficial because focus on one valid defense could be lessened, albeit slowing standardisation of valid CSRF security techniques. (Perhaps focussing efforts on improving one valid defense is better.)