Formal Verification of OAuth

1. Definitions
IdP (identity provider) = an identity provider, e.g. Facebook, Google, Paypal. See ‘Log in with Facebook’ feature’
Relying party = someone who uses Facebook as an identity provider

2. Discussion of OAuth process.

3. Properties to be proven:

Session Integrity:
Authentication: An attacker can not login at an RP under the user’s identity unless the IdP is corrupt, or the user’s browser is corrupt
Authorization: An an attack should not be able to obtain or use a protected resource.

4. FKS model. (Discussion of Model)
In previous work, these three authors developed and demonstrated a scheme for modeling web systems.

6. Attacks.
While attempting to verify the three safety properties described, the team discovers four attacks by which these properties can be violated. They fix these attacks in their analysis, but describe them in the paper.

307 Redirect
IdP Mix-Up Attack
State Leak Attack
Naive RP Session Integrity Attack

7. OAuth Model
Oauth Mode, Corruptible at any time, Client Secrets,  Http or Https, Multiple windows, forward/backward neavigation, cookie based session mechanism.

Does not worry about authentication at IdP. That is, if the IdP authenticates a set of credentials, this is assumed to be valid.

8. Results
They prove the properties by hand.