OAuth Security

Torsten Lodderstedt
Mark McGloin
Phil Hunt
Antony Nadalin

draft-lodderstedt-oauth-securityconsiderations-02
draft-ietf-oauth-v2-threatmodel-00
OAuth WG session at IETF-81, July 27th 2011,

draft-lodderstedt-oauth-securityconsiderations-02

- Based on draft-lodderstedt-oauth-security-01
- Focus on
  - protocol implementation by service providers and application developers
  - "what" and not the "why" - for "why" include informative reference to security document
- Text has been incoporated into core draft -16 (section 10) and now evolves with the core draft
- Core draft (informally) references draft-ietf-oauth-v2-threatmodel (was draft-lodderstedt-oauth-security) for comprehensive threat model

draft-ietf-oauth-v2-threatmodel

- Gives comprehensive threats model for OAuth (threats & associated impact)
  - Scope: core, bearer, mac (partially)
  - Assumption: Static binding between client and service provider
- Describes respective countermeasures
- Considers design options and different client types
- Cross-references between associated threats and countermeasures

draft-ietf-oauth-v2-threatmodel: Status

- New revision (WG item now)
  - Incorporates feedback gathered from the list and at IETF-80
  - Added four new threat description
  - renamed "session fixation" to "authorization code disclosure through counterfeit client“
- Next steps
  - Discuss and decide further procedure
  - Incorporate implementation recommendations proposed by Brain Eaton
  - Add injection and redirect page stuff (include java script, validation and reliance on validation, …)