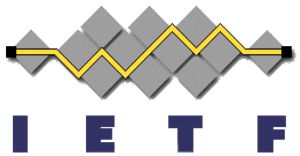
*

JSON Web Token Best Current Practices



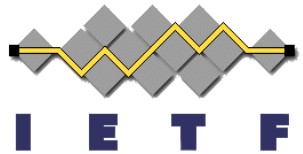
draft-sheffer-oauth-jwt-bcp

Michael B. Jones

IETF 99, Prague

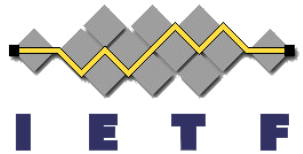
July 2017

Background from IETF 98



- We discussed reports of JWTs being implemented and deployed insecurely
- We discussed preventing confusion between different kinds of JWTs
- Kathleen Moriarty stated that JWTs are now being used in many IETF protocols
- She asked us to work on a JWT BCP

Individual Draft

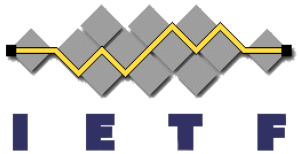


- Yaron Sheffer, Dick Hardt, and I wrote a -00 individual draft
- -01 defines how to provide explicit typing of JWTs using the "`typ`" header parameter

Structure of the Document

- Meat of the document is in two parts:
  - Descriptions of threats and vulnerabilities
  - Descriptions of best practices
- Each threat/vulnerability references best practices providing mitigations

Balancing Goals



- Document provides actionable information promoting secure implementation and deployment of JWTs
- Guidance applicable to diverse use cases
- Recognizes that many profiles and deployments will not need to change
  - Describes ways to keep them secure, particularly as their scopes may expand
  - Does not take a one-size-fits-all approach
- Recognizes the costs of changing/hardening existing deployments
- These practical tradeoffs should be discussed

Example Tradeoff

- Explicit Typing using the "`typ`" header parameter is described
- The circumstances in which explicit typing would be beneficial are described
- But does not mandate that existing already secure deployments be updated to use it
- Note that adding information to a JWT is not free when there are size constraints
  - Size increases can exceed browser URL limits

Next Steps

- Please review the document
- Please discuss its content
  - Particularly as it applies to your use cases

- Consider adoption by the working group