JOSE/JWT Security Update

Michael B. Jones
IETF 98, Chicago
March 2017

Background

- JOSE and JWT RFCs finished in May 2015
  - JSON Web Signature (JWS) – RFC 7515
  - JSON Web Encryption (JWE) – RFC 7516
  - JSON Web Key (JWK) – RFC 7517
  - JSON Web Algorithms (JWA) – RFC 7518
  - JSON Web Token (JWT) – RFC 7519
- In widespread use before and since then
- Articles have recently been published about implementation and deployment flaws

Antonio Sanso Article

- "Critical vulnerability in JSON Web Encryption (JWE) - RFC 7516"
  - http://blog.intothesymmetry.com/2017/03/critical-vulnerability-in-json-web.html
- Describes invalid curve attack against Key Agreement with Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES). Essence:
  - Attacker constructs JWE containing invalid curve point
  - Submit for decryption
  - Learn things about private key from decryption attempt
  - Repeat
- Thwarted by validating curve point before decryption
  - Some Java libraries and some JWE libraries now do validation

Scott Arciszewski Article

- “JOSE (Javascript Object Signing and Encryption) is a Bad Standard That Everyone Should Avoid”
  - https://paragonie.com/blog/2017/03/jwt-json-web-tokens-is-bad-standard-that-everyone-should-avoid
- Describes issues if application doesn’t confirm that valid crypto algorithm used
  - Deprecated algorithms and “none” can then be used
- Yet crypto agility requires apps to validate algs
  - Appropriate algorithms can and will change over time
  - Can’t just silently sprinkle crypto pixie dust and expect apps to be safe without validating crypto they’re using

Next Steps

- Encourage people to keep alerting us about security-critical implementation flaws
- Catalog and write best practices articles describing implementation pitfalls to avoid
- Publish articles at oauth.net?