OpenID Security Issues

Ashish Jain & Andrew Nash & Jeff Hodges, *PayPal* Information Risk Management

OpenID Summit
2-Nov-2009

Overview

- Known security issues with OpenID exist
  - Inherent in protocol spec
  - Due to Browser/HTTP/Web characteristics
  - Implementation & deployment practices
  - ...and combinations thereof...
- This is an attempt to help consolidate the list and agree on approaches as we move forward
  - Though, this preso is not comprehensive
- Note: *ICAMOpenID 2.0 Profile* and *Security Best Practices* are good start
  - address some of following issues

Protocol Spec Security Issues

- Browser is de-facto man-in-the-middle
  - messages/assertions are vulnerable when transiting browser
- Vulnerability to active attackers
  - Session Swapping
  - Open Redirector issue with checkid_immediate
- Association (shared secret) establishment
  - man-in-the-middle vulnerabilities
  - (RFC 2631 not properly followed)

- HTML discovery / Phishing
- End-entity Man-in-the-middle (RP/OP spoof'g)
- Protocol mods required to truly address these

Browser as Man-in-the-middle

- Messages and assertions flow unencrypted between OP and RP via browser
- Thus the browser is interesting entity to attack
    - e.g. message and/or assertion alter/copy due to..
        - no message/assertion encryption
        - most messages are unsigned
- Protocol messages lack robust linkages
    - to each other and to protocol runs
    - thus larger attack surface than if they incorporated such measures

Session Swapping (1)

- An attacker can cause victim browsers to log into RP accounts the attacker controls
    - "Positive Assertion" is not bound to the browser
    - OP authenticates Mallory (M), but M can cause Alice (A)'s browser to send the assertion to RP
    - result: A logged-in as M at RP

Session Swapping (2)

- Various Possible Consequences...
    - "silently" log A into M's account on A's favorite search engine -- M can spy on A's searches
    - M trick A into entering her credit card into M's online retail account
    - likely other possibilities...

Browser/HTTP/Web Issues

- E.g...
  - Cross-Site Request Forgery (CSRF)
  - Cross-Site Scripting (XSS)
  - Framing

- Session Swapping one example of former
- XSS/Framing could be used to siphon off assertions
  - by exploiting the browser as MITM
- There may be protocol spec and/or profile spec mitigations
  - requires investigation

HTML discovery / Phishing

- Much already written about this
- Protocol spec is monolithic
  - OP discovery is not obviously a separate component spec-wise, plus..
  - "HTML-Based discovery MUST be supported by Relying Parties."
- Profiles (e.g. ICAM) can mitigate
  - E.g. "use only 'directed identity'..."

End-entity Man-in-the-middle (RP/OP spoof'g)

- Where RP and/or OP are "rogue"
  - e.g. RP redirects browser to bogus OP and obtains credentials
  - Realm spoofing
- Difficult to address without more formal "trust" mechanisms supported in the protocol
- All Web SSO protocols struggle with this

Implementation & deployment practices

- Overall fairly well addressed in *ICAMOpenID 2.0 Profile* and *Security Best Practices*
  - though, profiles & practices such as these don't address various of the prior issues
- But more could be done
  - Different use cases may call for different profiles
  - *Security Best Practices* is a 'good start'
- Protocol evolution will affect these

Various items not mentioned above

- RP collusion mitigation
- Identifier recycling issues
- User privacy w.r.t. OP

End