HTTP Strict Transport Security

Jeff Hodges

IETF-78 Maastricht
27-Jul-2010

Problem Space

- Using HTTP over unsecured transport..
  - Vulnerable to active and passive network attackers

- HTTP over secure transport (today)..
  - Not a panacea

Problem Space cont'd

- Various vulnerabilities with HTTP over TLS/SSL (today)
  - Passive attackers + incorrectly deployed “secure” sites
    - Sniffing even secured (WEP, WPA) wireless access points is feasible (aircrack)
    - Eavesdrop and steal “non-Secure” session cookies
  - Active attackers
    - pwned wireless access points and/or DNS servers, plus..
    - Browsers facilitate TLS/SSL certificate error bypass, yields..
    - “click-through insecurity”
  - Web site bugs
    - Single unsecured load of CSS or SWF on otherwise “secure” TLS/SSL site can compromise entire site

Overall Requirement

- Minimize risks to users and sites that are due to..
  - Passive and active attackers
  - Site development and deployment bugs
  - Insecure user actions

Core Requirements (simplified)

- Sites able to declare to browsers..
  - “interact with me ***only*** in secure fashion!”

- To satisfy this, browsers must..
  - Remember such sites (“HSTS servers”)
  - Only do “secure URI loads” from HSTS servers
  - Terminate secure connections without user recourse in the face of errors

HSTS Policy Advertisement

- Via “Strict-Transport-Security” HTTP response header
- Example..
  - Strict-Transport-Security: max-age=31536000

Adoption

- Chrome, Firefox, NoScript
- www.PayPal.com Declares HSTS policy