Origin-Bound Cookies

draft-amarjotgill-origin-bound-cookies-protocol-00

Overview of Origin-Bound Cookies (OBC)

- Mechanism that updates the existing Cookies specification https://datatracker.ietf.org/doc/draft-ietf-httpbis-layered-cookies/,
- Aims to enhance cookie security by default through binding cookies by port and scheme which they are set on.
- Addresses the current weakness in cookie confidentiality where cookies are not scoped to the origin by default.

Current Security Vulnerability

- **Weak Confidentiality:** An attacker can read sensitive user data set by a secure site if it is unintentionally sent to an insecure site. For instance, if `https://somesite.com` sets a secret cookie, an attacker could trick a user into visiting `http://somesite.com` (note the insecure scheme). The browser would then send the secret cookie, allowing the attacker to intercept it.
- **Weak Integrity:** An insecure site, controlled by a network attacker, could set a malicious cookie that is then sent to the secure version of that site. Similarly, if an attacker compromises a service on a different port (e.g., `https://somesite.com:345`), they could trick the user into visiting this compromised port, and the secret cookie would be sent, allowing the attacker to read or even modify it.

Port Bound

Port Bound Behavior: The Cookie Struct will be altered to include a "port" attribute to bind the cookie by it when it is set, ensuring that a cookie set by `https://example.com` will only be sent to `https://example.com(:443)` and not to a different port like `https://example.com:8443`. Pre-existing cookies with an unspecified "port" will have a null value and be treated with current Cookie behavior.

Scheme Bound

Scheme Bound Behavior: Similarly, a "scheme" attribute will be added to the Cookie Struct and bind the cookie by it when it is set. This ensures that a cookie set by `https://example.com` will only be sent to `https://example.com` and not to `http://example.com`. Pre-existing cookies with an unspecified "scheme" will have a null value and be treated with current Cookie behavior.

Security Considerations

- Overall considered a net positive for security.
- For Clients who require the use of cookies across origins….
    - When a Cookie has a Domain Attribute set (A domain cookie), then the port binding behavior will be ignored.
    - Importantly a domain cookie is still bound to the scheme of its setting origin.
    - This behavior allows developers to opt-out of the stronger protections of an origin cookie which can help with compatibility for usages that need a particular cookie available across hosts and/or ports.
- While OBC will obsolete the purpose of the Secure attribute, this proposal does not remove support for Secure, which could be a future consideration for the HTTPWG.

Questions ?