OCF 1.0 Security CR – Bug 1470

Legal Disclaimer

This applies to Core Specification sections that define /p and /d resources and Security Specification Section 13.8 Security Virtual Resources (SVR)
Line 2403 appending the following text:

13.8 Privacy Consideration for Core and Secure Virtual Resources

Unique identifiers are a privacy consideration due to their potential for being used as a tracking mechanism. These include the following resources and properties:

- /d resource containing the ‘di’ and ‘piid’ properties.
- /p resource containing the ‘pi’ property.
- /doxm resource containing the ‘deviceuuid’ property.

All identifiers are unique values that are visible throughout the device lifecycle by anonymous requestors. This implies any Client device, including those with malicious intent, are able to reliably obtain identifiers useful for building a log of activity correlated with a specific platform and device.

There are two strategies for privacy protection of OCF devices; 1) apply an ACL policy that restricts read access to resources containing unique identifiers and 2) limit identifier persistence to make it impractical for tracking use. Both techniques can be used effectively together to limit exposure to privacy attacks.

(1) A platform / device manufacturer should specify a default ACL policy that restricts anonymous requestors from accessing unique identifiers. A network administrator should modify the ACL policy to grant access to authenticated devices who, presumably, do not present a privacy threat.
(2) Servers shall supply a temporary, non-repeating device identifier when the ‘owned’ Property in the /doxm Resource is FALSE and applies over multiple ownership transitions. The temporary identifiers shall be disjoint from and shall not be correlated to the persistent identifiers.

A new device seeking deployment needs to inform would-be onboarding tools of the identifier used to begin the onboarding process. However, attackers could obtain the value too and use it for device tracking throughout the device’s lifetime. To address this privacy threat, Servers shall supply the temporary ‘deviceuuid’ to unauthenticated /res requests when the device is unowned (i.e. ‘owned’ = FALSE). The Server shall randomly select the next temporary ‘deviceuuid’ value when ‘owned’ transitions again to FALSE. This ensures the ‘deviceuuid’ value cannot be used to track across multiple owners.

The ‘owned’ property is set to TRUE signifying the device ownership has been assigned. The server shall respond by supplying its persistent identifier (or allows the onboarding utility to provision) to the ‘deviceuuid’ property. The onboarding utility may also provision an ACL policy that restricts access to the /doxm resource such that only authenticated Clients are able to obtain the persistent ‘deviceuuid’ value. Clients avoid making unauthenticated discovery requests by having been provisioned with a /cred resource entry that contains the Server’s ‘deviceuuid’.

The ‘di’ property in the /d resource shall mirror that of the ‘deviceuuid’ property. The onboarding utility should provision an ACL policy that restricts access to the /d resource such that only authenticated Clients are able to obtain the persistent ‘di’ value.

The ‘piid’ property in the /d resource similarly should present a temporary and changing value whenever the device transitions to ‘owned’ = FALSE. The server shall provide a persistent value (or allows the onboarding utility to provision) subsequent to ‘owned’ = TRUE. An ACL policy on the /d resource protects the ‘piid’ from being disclosed to anonymous requestors.

The ‘pi’ property in the /p resource shall follow a similar behaviour as ‘deviceuuid’ and ‘piid’ properties, each shall have a temporary and changing value when ‘owned’ = FALSE and shall change to a persistent value upon ‘owned’ = TRUE. Similarly, an ACL policy protects the ‘pi’ property in the /p resource from being disclosed to anonymous requestors.