Securing WebAuthn with Attestation

- What is Attestation?
- Advantages to Attestation
- Attestation Allow List Maintenance

What is Attestation?

One of the most significant challenges any web-facing site or service has with user authentication is ensuring the user is practicing good habits with their authentication mechanisms. A great deal of effort has been invested to ensure users use strong, hard to guess passwords, but this cannot protect against users looking for shortcuts - re-using passwords across multiple sites, creating simple passwords which technically meet the recommendations and the like. With WebAuthn, this is no longer a concern, as the user’s authenticator ensures a strong authentication - if the authenticator itself meets the requirements.

To address this without compromising a user’s privacy, WebAuthn supports device Attestation. Relying Parties can request on authenticator registration that the WebAuthn Authenticator device send an Attestation certificate. This certificate contains identifying information about the Authenticator type (the GU and the credential being registered, signed with a private key unique to the manufacturer. Uniquely identifying information, such as serial number or user information is not shared. The relying party can validate the attestation certificate against the publicly registered WebAuthn attestation keys, and identify the manufacturer and model of the WebAuthn Authenticator being used.

By default, Attestation is not required. By requesting but not requiring direct or basic attestation, a web service gains a exceedingly useful benefit without adding additional friction to the user. Attestation does not require additional user input, but can offer stronger protections to their account. For a more in depth discussion on implementing attestation, Google has a set of best practices around WebAuthn Authenticators (referred to as “Security Keys” in their documentation).

Advantages to Attestation

At its heart, Attestation in WebAuthn allows a relying party to identify and verify the authenticator being used is a valid authentication product and not a malicious attack attempting to compromise a user’s account. But there are further advantages. By storing the attestation certificate for a credential, services can offer targeted warnings to users in the event vulnerabilities are discovered for WebAuthn authenticators. Services have options from simply warning users about authenticators which may place their account at risk, to limiting permissions to login events using a vulnerable authenticator to outright blocking access to accounts.

Further, services with regulatory restrictions on the types of devices which are permitted to be used as authenticators can use attestation with allow lists to limit users to only approved devices. US Federal Entities require FIPS certification on all authentication devices - attestation with an allow list enables this restriction. However, other sites or services may also take advantage of this feature, by purchasing WebAuthn Authentication devices with custom attestation for their user base, and restricting valid devices to only those which have the attestation key unique to their purchase.

In short, attestation provides a tool to sites or services to be proactive in protecting their user’s accounts, and grants a measure of control to ensure users follow best practices. Even if there is no immediate need to use attestation data, by having it on hand it opens the options to

Attestation Allow List Maintenance

If using an Attestation Allow List to direct a user’s authentication flow, it is important to keep your list up to date. This ensures new devices entering the market at accepted, while also ensure newly discovered vulnerabilities are also taken into account. There are a number of methods which can be used, including:

- The FIDO Alliance’s Metadata Service - Focus on hardware backed authenticators, with the widest range of devices
- NIST CMVP’s FIPS validated modules list - Lists only FIPS certified devices.
- CSPN Certified Products list - Similar to NIST’s validated list, CSPN lists the devices certified by the Certification Securite de Premier Niveau (CSPN).
- Common Criteria Certified Products list - List of WebAuthn Authenticators which have Common Criteria certification.

Further, information can be received directly from the manufacturer of the authenticator, as in the case of custom attestation certificates.