VIPR

draft-petithuguenin-vipr-pvp-04
draft-petithuguenin-vipr-reload-usage-04

Marc Petit-Huguenin
03/27/2012

Server-side entropy

- Only the support for server side entropy management was added.
- Now the ticket and routes are optional in the ValExchange response. If they are both missing then the validation succeeded (no need to try more methods), but there was not enough entropy accumulated.
- It is the responsibility of the server to keep the accumulated entropy in an internal storage.

Future client-side entropy

- When both the ticket and route are missing, it means server-side processing. A future extension can define client side processing, in which case the ticket returned will contain the accumulated entropy, and the route will be empty.

PVP methods registry

- IANA instructed to create a PVP method registry, with methods “a” and “b” (defined in the same document) as initial methods.

- Added instructions to register a new PVP method.

- Method name (which was one character) is now redefined as an 1*(alphanum / ”-” / ”.”) label.

Private methods

- Private methods start with the “p-” prefix.

- Private methods are used only inside the same VIPR domain, so a PVP server must always reject them if they come from a different domain.

- IANA does not accept registration of private methods.

Experimental methods

- Experimental methods start with the “x-” prefix, followed by an inverted domain name (e.g. x-org.example.fingerprint).

- An experimental method is supposed to be used between a small number of VIPR domains.

- IANA registration optional, document is RFC, either standard track or informational.

Standard methods

- Standard methods do not start with the “p-” or “x-” prefix (so “a” and “b” are automatically standard methods).

- IANA registration mandatory, document must be standard track RFC.

New method definition: login/password definition

- Selectors: A list of name-values used to find the matching call record on the terminating side.
- Selector usage: A text describing how the selectors are processed on the terminating side, especially what to do when multiple call records match the selectors.
- Parameters: A list of name-values that are used to guide the PVP processing.
- Secret: The secret data that is used to verify that the VCRs on both side match.
- Secret usage: A text describing how the secret data is generated especially when one call record can generate multiple different secrets.

New method definition: Priority

- Priorities are values between -32768 and +32767.
- A new priority is assigned between two existing priorities by using p = (p1 + p2)/2.
- Method “a” has priority 0
- Method “b” has priority (-32768+0)/2=-16384
- A future method “c” that is better than method “a” will be assigned the priority (0+32767)/2=16383.
- Multiple methods can be assigned the same priority. In this case the implementation choose the order or can run them in parallel.

New method definition: replacement

- When an experimental method is promoted to standard method, a special processing is required on the PVP client side. By indicating that a method is replacing another method, the client can ignore the replaced method if the ViprRegistration RR supports both methods. This permits a smooth transition.
- The definition must also define a date after which implementations no longer need to register the replaced method in the VIPR overlay.

New method definition: Miscellaneous

- Entropy: The entropy accumulated when this method validates.
- Potential interoperability issues.
- Security considerations.
- Privacy considerations.

ViprRegistration

- The ViprRegistration resource record now stores a list of destinations instead of just a Node-ID.

- The access control policy was modified accordingly.

- This modification is to be compatible with the support of onion routing in RELOAD.