Conditional Attributes for Constrained RESTful Environments

draft-ietf-core-conditional-attributes

(https://github.com/core-wg/conditional-attributes)

Bill Silverajan

Core Interim Meeting 2023-01-18

Current Status since IETF 115

- Version -06 submitted

- Complete remaining open issue
  - → Now completed

- Should we request a review from the IoT Directorate?
  - →Early review requested

- More reviews are welcome
  - → 2 comments on mailing list

Reference code moved

- The reference code illustrated logic and server side processing of conditional attributes in Section 3.3

- After discussions in IETF 115, we took a decision to move the reference code away from the main body of the draft

- And then add an Appendix containing explanatory pseudocode that is informative and not normative.

Early review requested from IOTDIR

Datatracker

Groups ▾ **Documents** ▾ **Meetings** ▾ **Other** ▾ **User** ▾

Review request

draft-ietf-core-conditional-attributes

Request		
	Review of	draft-ietf-core-conditional-attributes-05
	Requested revision	05 (document currently at 06)
	Type	Early Review
	Team	Internet of Things Directorate (iotdir)
	Deadline	2023-01-23
	Requested	2022-11-07
	Requested by	Marco Tiloca ✉
	Authors	Michael Koster ✉, Alan Soloway ✉, Bill Silverajan ✉
	WG chairs	Marco Tiloca ✉, Jaime Jimenez ✉, Carsten Bormann ✉
	Draft last updated	2023-01-14
	IESG document state	I-D Exists
	Completed reviews	
Assignment	**Reviewer**	**Ines Robles** ✉
	State	Accepted
	Review	Not completed yet

WG comments received (1/2)

- https://mailarchive.ietf.org/arch/msg/core/MPp2CS_W696GomNwpAsxww_SqaA/

  - "The pmax attribute risks making amplification attacks far worse but as far as I can see the draft does not say a single word about this"
  - "Before publishing I think the draft needs to describe this and normatively require sufficient mitigations from the implementation."
- Resolution steps
  - Work on Security Considerations to discuss the impact of c.pmax used for amplification attacks and mitigation steps
  - Work on Security Considerations to discuss the impact of c.epmax used for resource exhaustion and mitigation steps

WG comments received (1/2)

- https://mailarchive.ietf.org/arch/msg/core/MPp2CS_W696GomNwpAsxww_SqaA/

  - "The pmax attribute risks making amplification attacks far worse but as far as I can see the draft does not say a single word about this"
  - "Before publishing I think the draft needs to describe this and normatively require sufficient mitigations from the implementation."
- Resolution steps
  - Work on Security Considerations to discuss the impact of c.pmax used for amplification attacks and mitigation steps
  - Work on Security Considerations to discuss the impact of c.epmax used for resource exhaustion and mitigation steps

WG comments received (2/2)

- https://mailarchive.ietf.org/arch/msg/core/O8ZTPOAve3xljuZ6HwXR0yKZ8R8/
  - "The notification mechanism in RFC7641 is a protocol detail that operates under the hood to provide the functionality of keeping the retrieved resource state in sync with actual resource state. The Conditional Attributes defined by the draft interfere with the generation of notifications, so that this functionality is in its generality no longer given: The client no longer receives a representation of the actual resource state through the notifications."
- Resolution steps are still open (authors still need to discuss further)
  - Proposal from the reviewer: "Rather than interfering with under what conditions and in what way the server generates notifications, the draft should define how the server updates resource state and how the client can influence this."

Conditional Attributes for Constrained RESTful Environments

Thank you!