Requirements for Trust and Privacy in WebRTC

Peer-to-peer Authentication

draft-copeland-rtcweb-p2p-idp-auth-00

Authors: R. Copeland, K. Korre, I. Friese, S. El Jaouhari
Speaker: X. Marjou (on behalf of the authors)
IETF 97 RTCWeb Working Group, Wednesday 16th November 2016

Context: reTHINK project

- The reTHINK project proposes a disruptive **Web-centric architecture** for service delivery through specialized end-to-end network quality commitments based on **P2P and cloud technologies**, with a strong focus on **identity and security** aspects.

- draft-ietf-rtcweb-security-arch-12 describes a multi-domain WebRTC system with a multiple-IdP architecture.

- draft-copeland-rtcweb-p2p-idp-auth-00 describes additional use-cases and requirements for trust and privacy.

Call-Center

- Use Cases (u.c. 7.1 and 7.2)
  - Alice surfs on websites and calls several assurance call-centers. She wants to protect her privacy and may remain undetectable (not logged in).
  - She may also use a pseudonym if authentication is required and use an IdP of her choice.
  - At some point, Alice may decide to reveal her identity, e.g. to subscribe to an offer.
  - The worker of the call center is authenticated too, but his identity is unlinkable: Alice can't call-back the same worker. This could be revoked by the worker.

- Privacy Parameterization Requirements
  - Set privacy by standard service types, call models, and destination categories (req. 8.1.1, 8.2.1).
  - Personal information must not leak via identity assertions (req. 8.1.2).
  - Called users can reject unlinkability request to avoid nuisance calls. (req. 8.2.3).
  - Users can choose their own IdP independently from the calling services (req. 8.3.1) Services can mandate or restrict IdP choice.

Enterprise Communications

- Use Cases (u.c. 7.4 and 7.5)
  - Depending on the call context (customer or colleague), Alice may not want the same privacy properties.
  - Privacy may be handled by either the IdP, the CS, or both. Discrepancies may occur.
  - Bob may be from different companies with different, CS defined security and privacy policies.
  - Alice may want to use an untrusted service with her corporate identity (while out of the office). She want to be sure that her corporate identity is used when calling Bob.

- Requirements
  - Set privacy by standard service types, call models, and destination categories. (req. 8.1.1, 8.2.1)
  - There must be a transparent method of resolving conflicting privacy. (req. 8.5.4)
  - Users should be able to associate service-bound identities with IdP identities. (req. 8.3.4)
  - Users should be notified if a default IdP is assigned, and if other than their chosen IdP is assigned. (req. 8.6.4)

Conclusion and Next Steps

- These new use-cases and requirements for privacy must be taken into account.
- Is there some interest from the Working Group?

More information

- https://www.ietf.org/id/draft-copeland-rtcweb-p2p-idp-auth-00.txt

- R. Copeland, I. Tariq Javed, N. Crespi
  Institut Mines Telecom-Telecom Sud Paris
- K. Corre, J.-M. Crom, S. Bécot
  Orange Labs
- I. Friese
  Deutsche Telekom AG
- S. El Jaouhari, A. Bouabdallah
  Institut Mines Telecom-Telecom Bretagne

This work has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 645342, project reTHINK.

https://rethink-project.eu/
https://twitter.com/rethink_eu
https://github.com/reTHINK-project

Thank You!