

A hints based approach towards Web&Network APIs

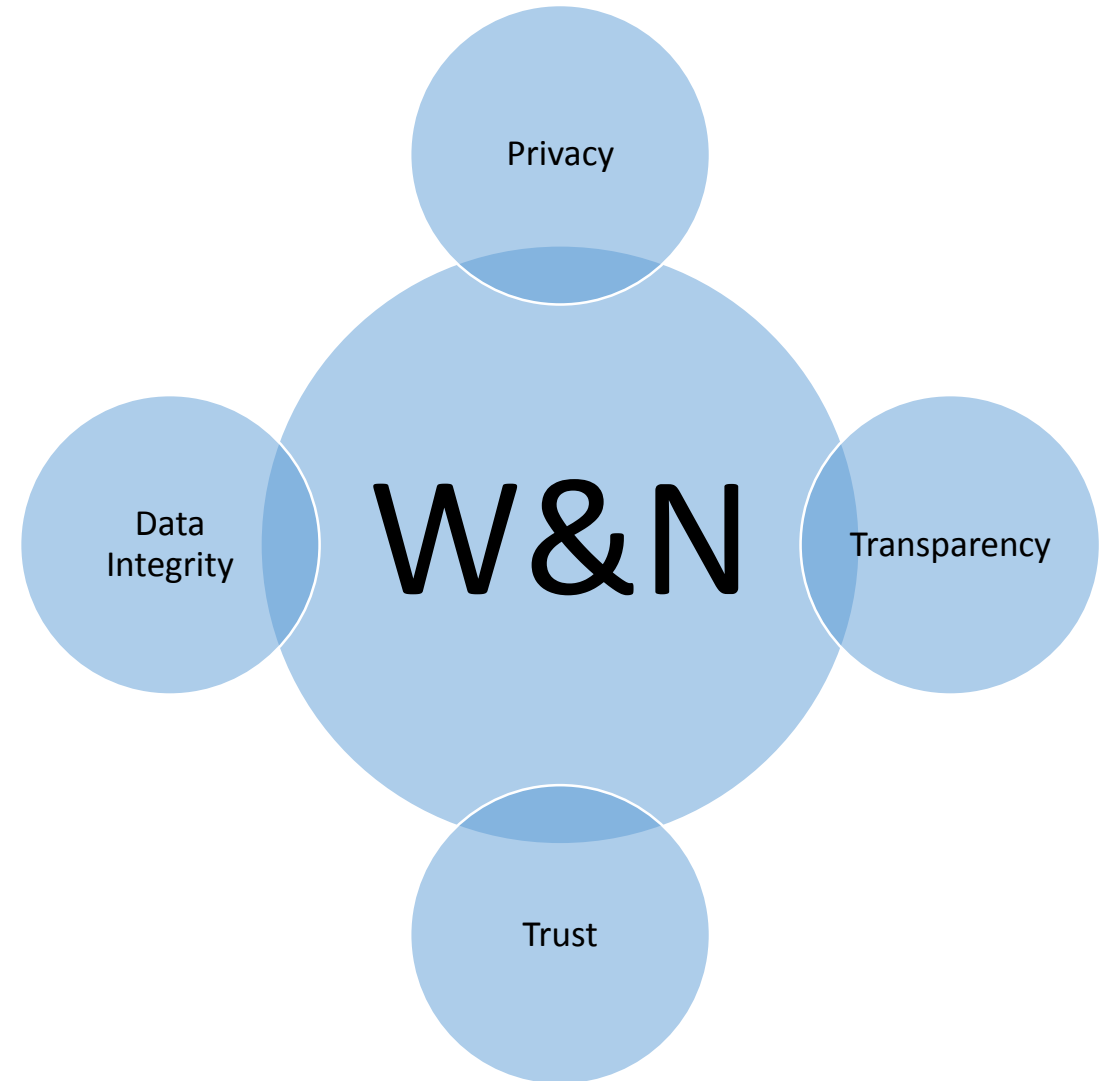
Analysis of key characteristics for viable Web <->Network info exchange APIs

Dan Druta, AT&T
Web&Networks Interest Group
W3C TPAC 2019, Fukuoka Sept/2019

High level overview

Need to consider hyper scale solutions with:

- Broad applicability and availability globally on multiple network technologies
- Guaranteed integrity of data
- Minimal exposure of personal identifiable information (PII)
- Clear user engaged consent

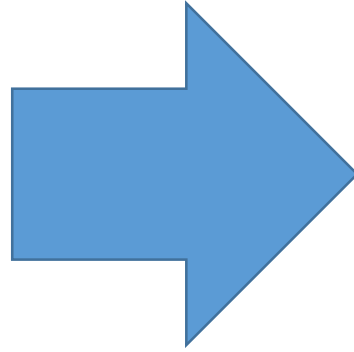


Privacy and Transparency

- Avoid passive interception and prevent man in the middle attacks
- Allow the client(user) and the server(content provider) to negotiate what and whom they want to give(or not) visibility into their flows
- User controlled privacy - this should be more than just relying on the user agent to automatically set privacy rules
- Minimize the fingerprinting entropy to avoid user tracking and long lived sticky identification of device, data flows or users

Example - GeoLocation

- Mobile network operators have accurate location data of subscribers
- Developers prefer it over the Location data obtained from the device due to minimal risk of **spoofing**
- APIs to access that info have been available to third party developers and aggregators
- Data misused for tracking and other analytics by the third parties without user's consent or knowledge



Privacy centric alternative:

1. User consents to the app access to the location info
2. App obtains GPS coord using the Location API on device
3. App uses Network API to validate that LocationData is not spoofed. Return Boolean (Y/N)

Benefits

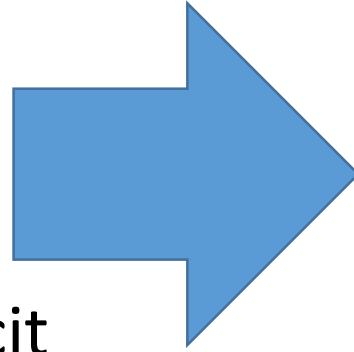
- Leverage consent mechanism in place
- No additional info disclosed

Trust

- Avoid solutions that rely on explicit trust relationships between parties as they tend to depend on sophisticated authentication infrastructures that are difficult to maintain
- Cheat-proof mechanisms based on trade-offs discourage parties to communicate misleading info are encouraged
- No guarantees expectation should be made in the process of bidirectional data exchange between network layer and web apps as there is no way to enforce these mechanisms across the Open Web Platform and all the network operators. Applications should not rely on or expect networks to always provide status info and vice versa

Example - QoS

- Quality of Service (QoS) is a network configurable characteristic for internet traffic where the app developer specifies flow priorities
- Due to the traffic prioritization requires explicit trust between the app (requesting) and the network (providing/enabling)



Sensible alternative (WebRTC)

1. Developer specifies relative priority of media tracks the app is establishing (audio/video, data)
2. Traffic is marked and the track priority is taken into account for congestion algorithms

Benefits:

- No discrimination between applications or users required
- No trust framework necessary

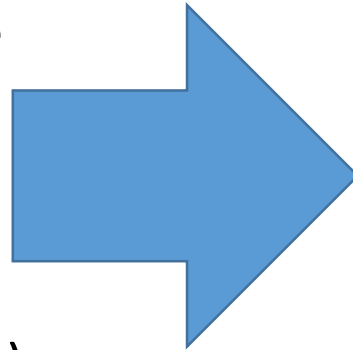
Data Integrity

- The only guarantee required for solutions should be on data integrity
- Encapsulation of data exchange should allow intermediaries in the path add info without tempering with existing flows

Conclusion: Focus on HINTS

- Solutions that provide **hints** to and from the network layer in order for the Apps to inform and be informed on:

- Network conditions
- Network access availability
- Technology support (radio, etc.)



Why:

- Hints are ... well, just HINTS
 - Not guaranteed to be available
 - Can be ignored – no contractual obligation if no mutual benefits
 - Can be used to proactively adapt the application to network conditions
 - Can reliably convey application characteristics