Security & Privacy TF Update

Junichi Hashimoto

KDDI R&D

Apr. 25 2016, Paris F2F

Background

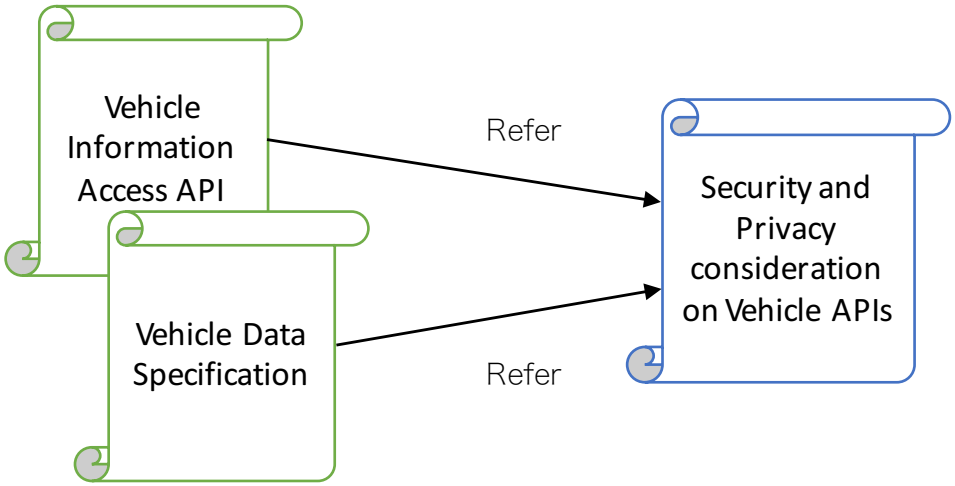
- Vehicle APIs
  - Exposing Vehicle Data to Web Apps
    - Vehicle Information Access API
    - Vehicle Data Specification
- Major concerns
  - People
    - Customer, Service Provider, OEM, …
  - Concerns
    - Invasion of Privacy
    - Data Integrity
    - Safety use of API

Need Security & Privacy Consideration

By dedicated TF

Security & Privacy TF

- Mission
  - Revising section 3
  - Investigate Security & Privacy
- Sapporo TPAC
  - Publish a separate document
  - Describe access control

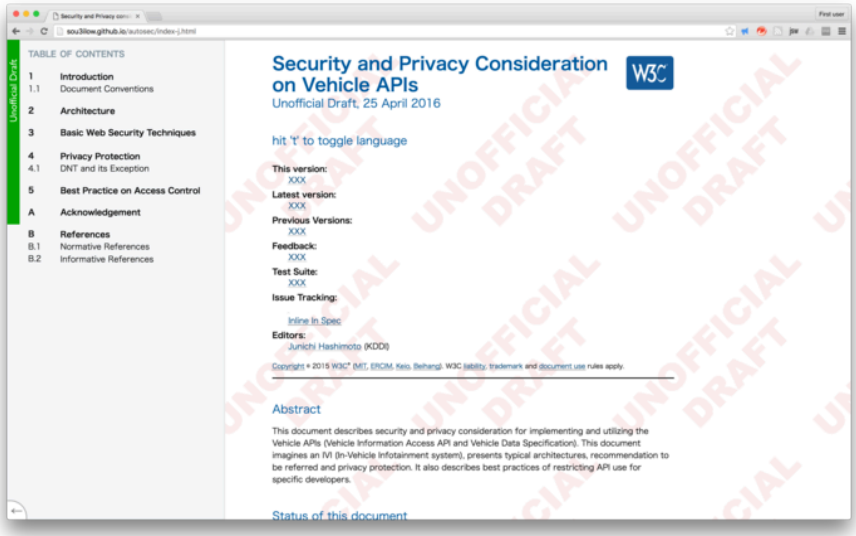


First step: Normative Reference

In the future: a formal independent recommendation

Drafting Note

- Content
  - Architecture
  - Protection against malicious code
  - Best practice on Access Control
  - Privacy Protection
    - DNT and its Exceptions
- Schedule
  - Discussing key points(today!)
  - Put on WG's GitHub(~May 11)
  - Call for comments (~May 31)



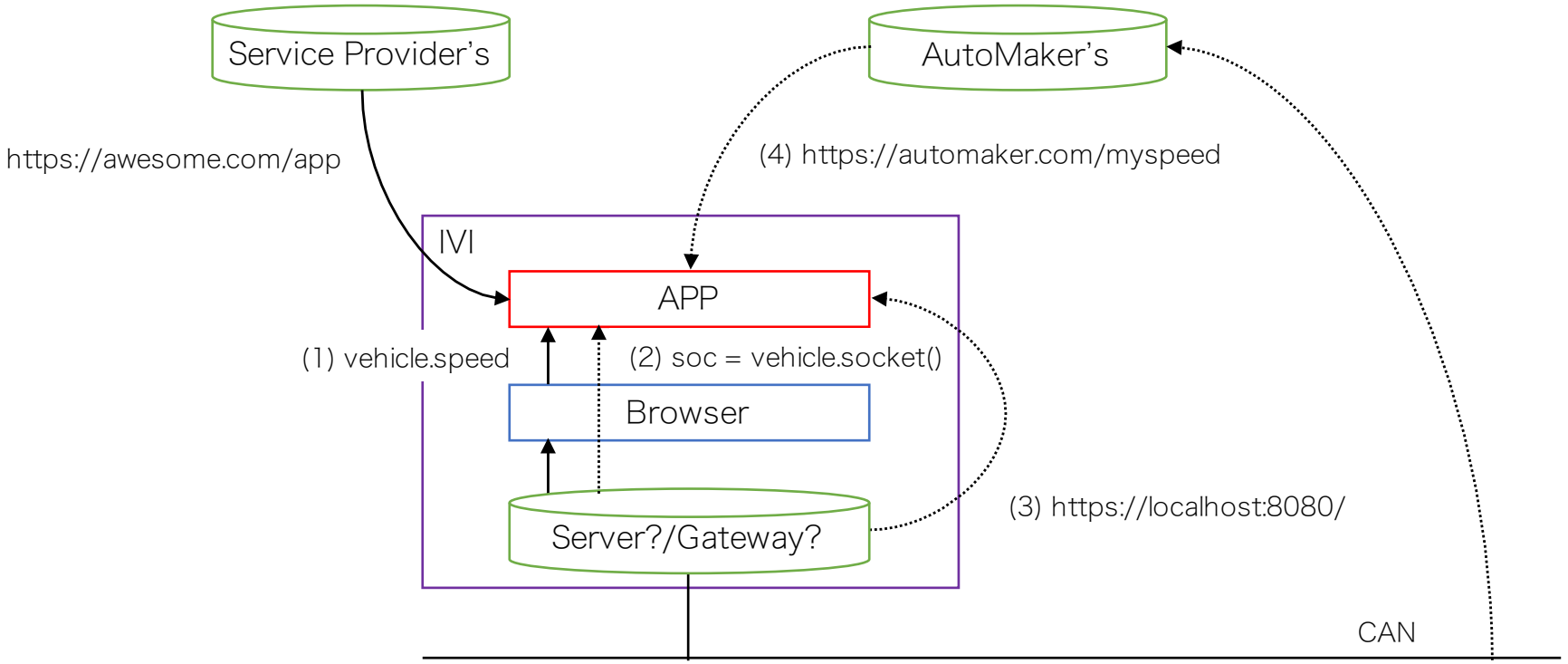
http://sou3ilow.github.io/autosec/index.html

Key points

- Scope of Note
  - Vehicle APIs for IVI
  - Web-runtime and its environment
- Protection Against Malicious Code
  - Protecting Interface of IVI/Internet, IVI/CAN
  - Basic techniques of web security
  - System Updatability
- Access Control
  - Market/whitelist/proxy/OAuth/CORS
- Privacy
  - Data from Vehicle APIs should be “personal data”
  - Service provider should take them into account.
  - Exceptions for DNT

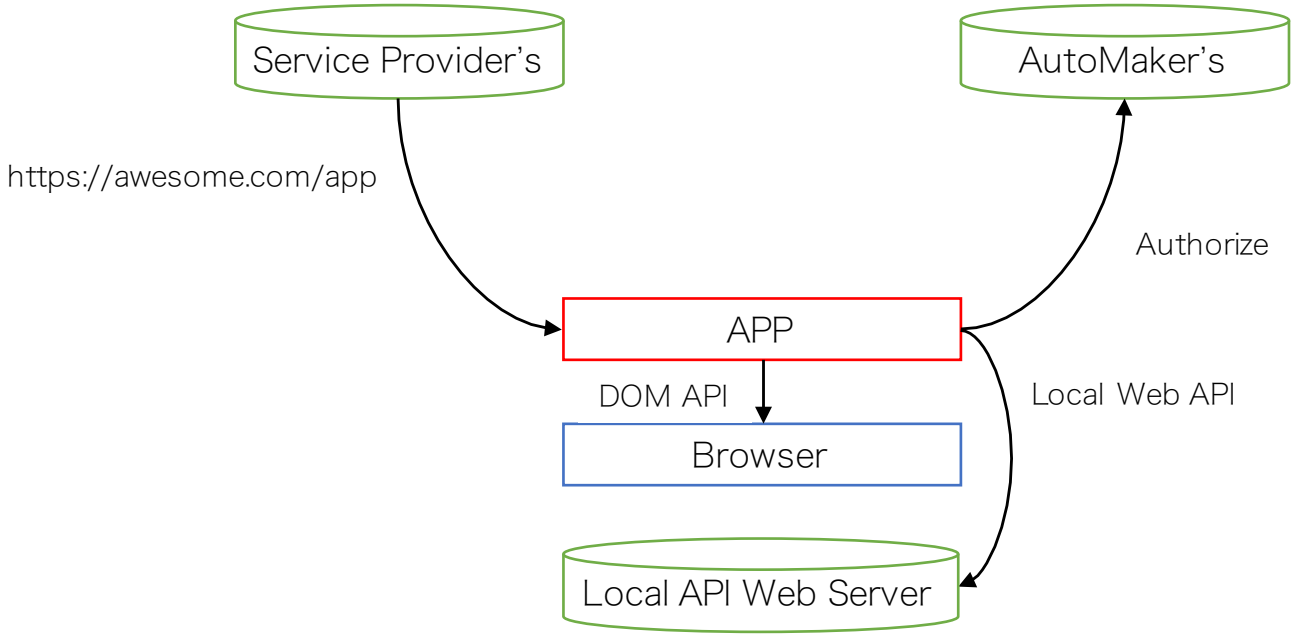
Architecture

Overall Architectures



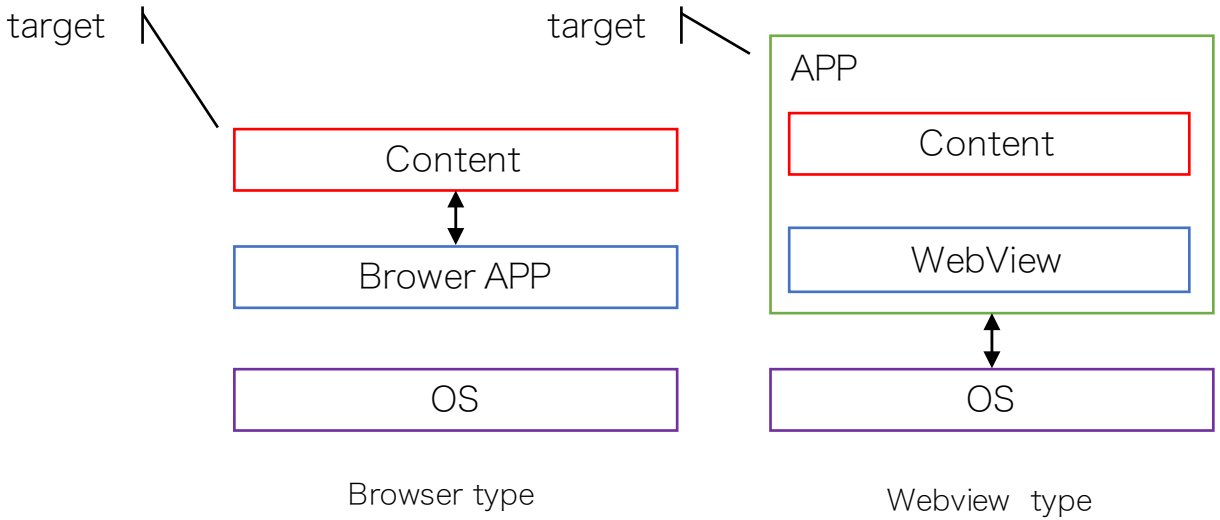
	API format	API Type	e.g.	cons
1	webIDL	DOM	Current spec	
2	Rest/Socket	DOM	#81	Drastic change
3	Rest/Socket	Web (Local)	Access(w/t polyfill)	TLS?
4	Rest/Socket	Web (Cloud)	Toyota ITC	Performance

DOM API and Local Web API



	API Type	User Permission	Access Control (Vender Permission)	Note
1	DOM	Browser shows popup	• Browser checks if SP's origin is in a predefined white list	Need to implement browser
2	Local Web	Local server shows popup (by using OS functionality)	• Local server checks if SP's origin is in a predefined white list • Local server accept an access token generated by automaker	Need to have a fixed URL such as https://localhost:8080 and its certificate.

Browser and Webview (DOM API)



	Type	User Permission	Access Control (Vender Permission)	Note
1	Browser	Browser manages	• Browser checks if SP's origin is in a predefined white list	
2	WebView	OS manages (at install time?)	• Platform would support app signing or market place	If application has a vulnerability, obtained information could leak