KDDI Research Institute

W3C Automotive BG/WG Security & Privacy Task Force

Junichi Hashimoto, KDDI Research Institute

2015 Oct. 26-30

Automotive BG/WG F2F @Sapporo

Automotive Security & Privacy TF

KDDI Research Institute

- A joint task force comprised of the W3C Automotive BG/WG
- Our mission[1]
  1. Provide envisioned incident studies.
  2. Clarify requirements of web technologies based on the above studies.
  3. Propose technical description to be added as specifications of "Vehicle Information Access API" and "Vehicle Data"
- Moderator
  - Junichi Hashimoto
- Members
  - 23 (Alibaba, ETRI, Intel, JLR, KDDI, LG, Mitsubishi, OpenCar, etc)
- Working material[2]
  - Usecases/concerns on connected car
  - Requirements and handling

(1) https://www.w3.org/auto/security/wiki/ASP_TF
(2) https://docs.google.com/spreadsheets/d/14ij-2I-H4HbilVQ_muCmUayVqmVfdbkoke690MA0kdo/edit#gid=1828778399

Procedure/Schedule

1. List up brief use cases and concerns

2. Select gathered use cases & concerns in STEP 1 for our scope and investigate them deeply adding the following contents
   - Attack Vector & Type of Threat for Security (From X to Y, or internal)
   - Actual or Envisioned Incident
   - Requirements
   - Best Practice and desirable measures in Web layer (if possible)
   - Remarks & Bibliography

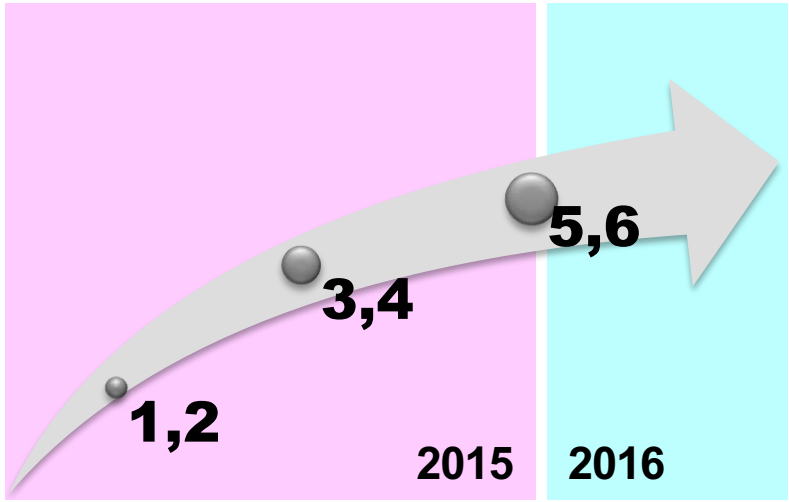
3. Derive requirements from the investigation

   <Iterate the above steps 1-3 twice or more>

4. TF members and other working groups, to exchange and discuss case studies in the sheet, focusing on the automotive web technologies.

5. Moderator and editor, to draft findings and recommendation from the work sheet, and to clarify issues to be discussed beyond LC/CR timing.

6. TF member, to generate the technical descriptions in the specs by year end of 2015. (to be in time for LC/CR)



Policy

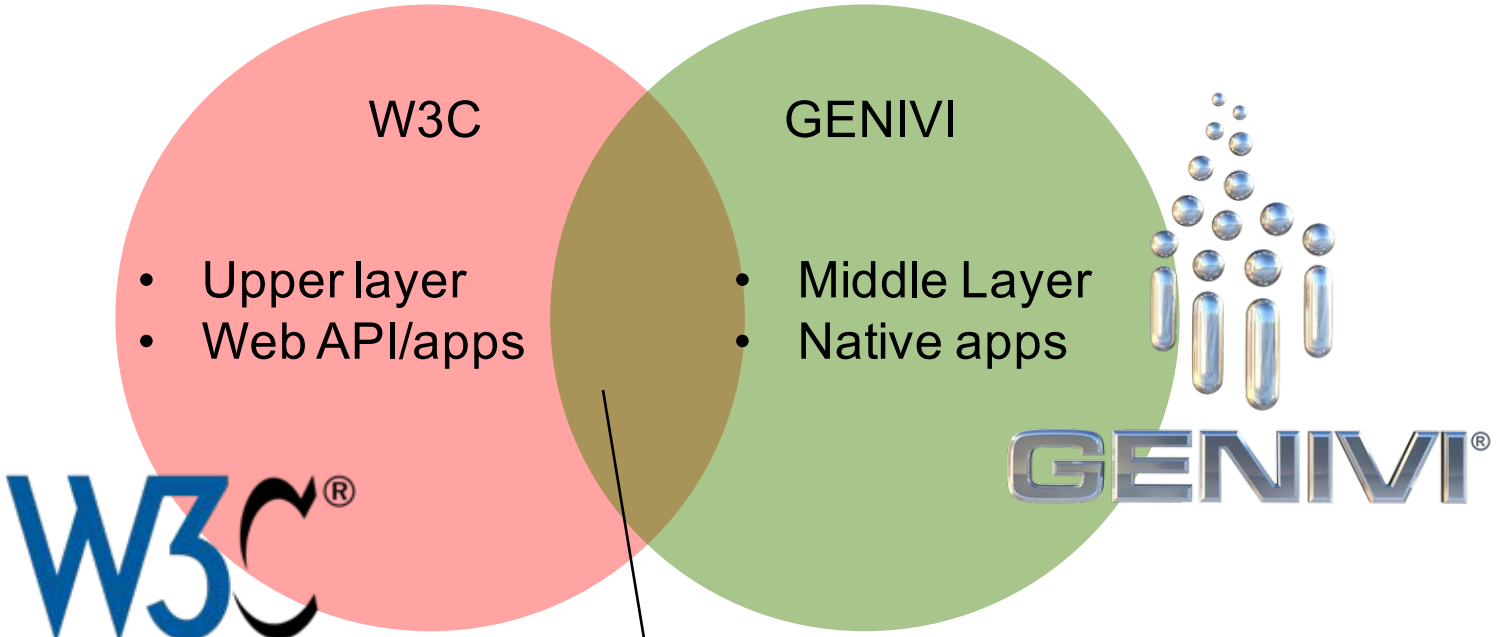
KDDI Research Institute

- We should be able to clearly explain to our customers as follows:

  - Does web make vehicle more convenient?
    - ✓ Yes, of course.
  - Does web make vehicle dangerous?
    - ✓ No. Vehicle is NOT controlled against your intention. Vehicle API demands to prohibit illegal operation by several means.
  - Does web leak privacy?
    - ✓ No. User's consensus is required before Vehicle API is activated.

- We propose addition/modification on the API Spec to achieve this,

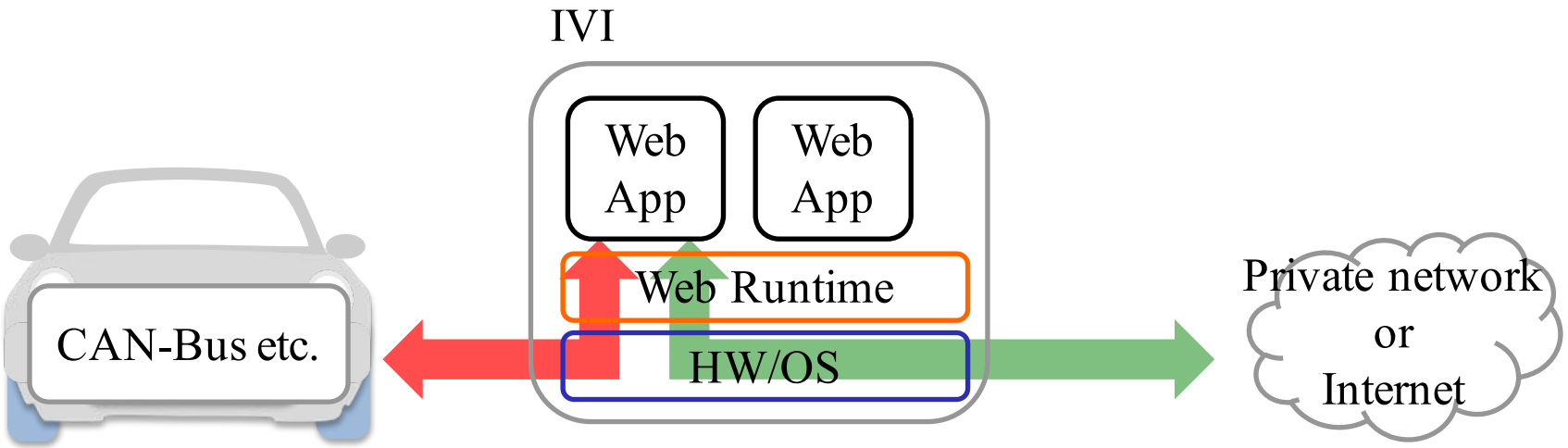
Possible collaboration with GENIVI's security group



Common interests:

- Hybrid apps security
- Web/Native app interaction
- User authentication
- Secure app distribution

Target Model

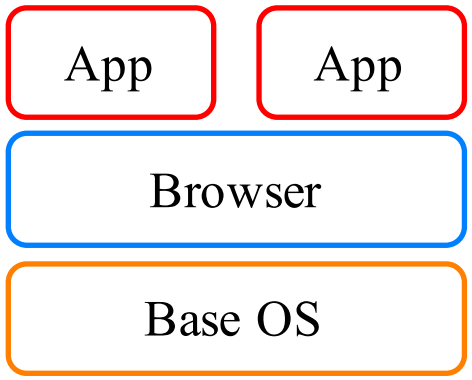


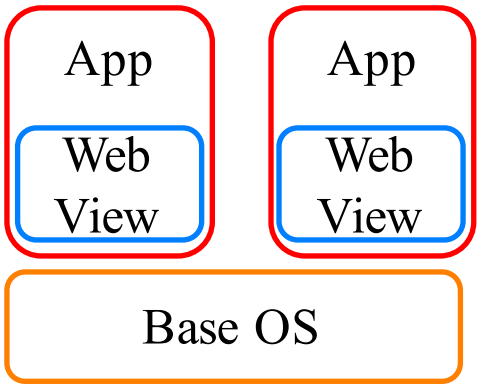
- Target: In-vehicle Infotainment system
- Apps(Web page) is securely installed.
- Apps access car via Web Runtime using Vehicle API.

Model Comparison

KDDI Research Institute

Runtime as the platform (Browser)	Model	Runtime as a component (WebView)
Usually, No.	Packaged?	Usually, Yes.
origin, domain	App ID	signature on package
runtime	Permission enforcer	runtime/OS
runtime	Inter App Communication supported by	OS
runtime	Application managed by	OS
Browser vender	Runtime updated by	OS maintainer





➔ *Component Model first*
➔ *Discussion for v2.0*

Discussion points from use case

- Protection against intrusion and attack
- 'Set' API
  - HVAC, window, drive-train
- API accessibility
  - app certification, user's permission, WebAPI (not direct), remote access
- Communication
  - With devices/home/service, To cloud data, V2X
- User's rights for their data
  - Do not track, sensitive location, Emergency
- Multi drivers/users
  - Identification, environment switch, payment

Protection against intrusion and attack

KDDI Research Institute

- Cars should have protection against intrusion or unauthorized access as its fundamental function.
  - Against intrusion 
  - Against unauthorized local/remote access 
  - Protection of source code 
    - * These functionalities may be implementation issues.

 : Feasible and scope of current spec/note
 : Beyond our scope.
 : Future scope or need further discussion

*) This marks just shows tentative remarks.

‘Set’ API

KDDI Research Institute

- Vehicle APIs are categorized in 3; ‘get’, ‘subscribe’ and ‘set’. We do not recommend ‘set’ for the initial version but we also understand there are strong demand for the ‘set’ function.
  - for HVAC 
  - for window, sunroof, door lock 
  - for ADAS 
  - for safety critical functionality 

API accessibility

KDDI Research Institute

- 3rd party wants to develop powerful apps with Vehicle API while automaker/user wants to prohibit unintentional behaviors of web apps. To achieve this, there are several approaches.
  - User's permission for Vehicle Data in each apps ○
  - Automaker provides a subset of Vehicle API ○
  - Automaker certificates each App »
  - Automaker provides API via http(s) instead of direct API »
  - Remote access to API »
    - e.g. door lock

Communication

KDDI Research Institute

- Vehicle can be seen as a big WoT/IoT device and interaction with other devices, services will be more popular in the future. Our society/infrastructure will need probe data from cars more and more.
  - Trusted communication between other devices ○
  - Secure access to external storage ○
    - but further use case investigation might be needed.
  - Data integrity for ADAS/V2X »
    - Hardware support might be needed.

User's rights for their personal data

KDDI Research Institute

- Big data analysis makes us possible to figure out a person from his activities. Because Vehicle API opens the door for probe data including sensitive ones, we should recall that user has rights to control their personal data.
  - Do Not Track ○
    - * This is just a request for servers not to track me but apps which use Vehicle API should respect the intention.
  - Generalization of data for protection of privacy »
    - * Hiding GPS data if one is in sensitive location (e.g. home)
    - * Choice of data granularity
  - Emergency: Exceptions for DoNotTrack and Generalization ○
  - Monitoring, rectification and erasure of log data ⚠

Multi Drivers/Passengers/Users

KDDI Research Institute

- Cars can have multiple drivers over its lifetime. Which data belongs to whom? A driver expects that Apps are switched by recognizing his identity. He may put his credit card number and app might store this on internal storage. Can rogue mechanics steal it at a maintenance time?
  - User identification ○
    - * Spec defines identifying methods. How to integrate with IVI system requires more discussion.
  - Protection of valuable data(Card No., Password etc) ○
    - * Up to apps basically. But a guideline will be beneficial.

Thank you

KDDI Research Institute

- Visit following page for more detail
  - https://docs.google.com/spreadsheets/d/14ij-2I-H4HbilVQ_muCmUayVqmVfdbkoke690MA0kdo/edit#gid=1828778399&fvid=190768047