Privacy and Web on TV: Policy Based Access Control
(For the W3C Web on TV Workshop, Tokyo, September 2010)

Position Paper

Shuhei Habu
Allied Resources Communications, Inc.
Tokyo, Japan

1 Background

BML (Broadcast Markup Language) has been used as a data coding and transmission specification for information browsing by television broadcasting for many years in Japan. BML is an XML-based specification developed by ARIB association as ARIB STD-B24 [1].

BML is derived from XHTML 1.0 with CSS and ECMAScript to enable interactive multimedia contents such as customized news, weather forecast, real-time emergency information, shopping, EPG (Electronic Programming Guide) and some other TV program-related information based on subscribers' personal preferences and location.

Because BML requires BML browser on TV, a large majority of TV sets in the Japanese market already implement BML Browser. As a result, it is getting ready for people to make use of BML. However, the real usage has not grown as expected.

The user's behavior of watching TV is becoming more diverse these days. For example, searching/browsing on PC or mobile phones during watching TV, so-called multi-window style and watching Internet Video sites like "Youtube" or "Nico Video" on TV are becoming popular. Therefore, the

solution for diversified usage is required to the broadcast platform technology.

W3C HTML5 (and related specifications) provides rich functions such as media playback, two-way communication, local storage and interfacing with external devices etc. in an interoperable manner.

If HTML5 is implemented in the TV sets, enjoying rich internet applications, including interactive broadcasting contents can be rendered without any plug-ins like Flash or Java. Therefore, HTML5 would be one of the promised platform for the next generation universal TV environment.

It is good for users that TV becomes more rich, powerful and easy to use with HTML5. On the other hand, powerful APIs for TV can get access to user's personal information such as user's viewing program. This means that privacy of personal information protection get more important.

2 Privacy data on TV

Some use cases on IPTV using personal information are shown as bellow

- Location (TV location, postal address etc.): used for getting local news, weather forecast, emergency information etc.

- History: used for storing watched program IDs or visited broadcasting contents URIs. Also used for getting customized contents recommendation for users

- Contents and metadata: Recording timer setting, Recorded contents, Bookmarks etc.

- Contacts: For Video phone, e-mail etc.

- Social Information: Personal information and preference for SNS (Social Networking Service)

Thus, there are a lot of possible privacy risks for users to in rich Internet contents service, especially when users needs simple and easy-to-navigate style without troublesome settings and management.

Downloading applications into TV set is one of easy to navigate styles for users.
This style seems to be gaining ground in the market. Applications can get access to stored resources containing users' personal information. If a malicious application acts like honest and convenient application, there is a risk that personal information can possibly be exposed to third-party through API.

Nowadays, some of these problems in privacy are solved by the platform layer, security-protected API, middleware or server-side service.

3 BML and HTML5 - Privacy Principle comparison

If solution platform would provide standardized privacy protection functionalities, it would be useful for most of the service provider and also good for users because it would provide consistent user interface. However, it is known that most of the fixed privacy protection policy solution never remove all privacy or security risks, because there is considerable cultural, geographic, individual, use-case or service-dependent variation.

BML has APIs for local storage, two-way communication between Client and Server, accessing Bookmarks and other broadcast specific APIs.

BML has following functionalities about privacy protection;

- BML has two types of Content Security Classes regarding to privileged levels,
    - Class-A has full access to all the extended APIs for broadcasting-purpose.
    - Class-B has limited access to the APIs.

- BML implementation requires the access control based persistent local storage system which may contain users' privacy information. When the downloaded application create the file for storage, the access condition (service provider's network ID, broadcaster's ID or service ID) is also recorded. When the other application need to access the storage, the IDs are examined. Contents provider can make their services secure from malicious third-party.

HTML5 has all APIs, required for contents storage. HTML5 has local storage API as Web Storage, general-purpose two-way communication API as Web Socket, Location as Geolocation API. DAP(Device API and Policy) WG also provides Contact API, external device control API.

HTML has general accessing API for resources related to user privacy. However, the access control policy is only discussed at DAP WG and has not yet reflected to html5 specifications.

I think that one of the most important security or privacy management scheme in HTML5 related specifications is to take advantage of policy-based security mechanism. So, Device APIs could be invoked, managed and controlled by users and Contents providers under pre-set policy customized for their services, if they need.

4 HTML5 - Privacy Protection Requirements

In this section, we would like to discuss about the policy protection

requirements.

Usecase-1: When the family members are watching TV in the living room, the parents may not want their children to watch inappropriate contents. It is easy to assume that the pre-setting policy in TV doesn't satisfy the parents requirements.. The adequate user interface for the parents to setup the family policy is preferable.

When policies are defined by user and registered in TV or Server-side system, these policies are enforced by platform. When enforced, some policies may be automatically done but some may be done in response to users' explicit decisions using graphical dialogue interfaces.

Usecase-2: When the program recording schedule is created by the user, the schedule information may be gathered by the application server to create a trend statistics. In this case, the user privacy should be protected by the gathered information is consumed only by the allowed purpose.

The followings are the requirements extracted from the use cases:

- User should be able to specify the preference in advance
- The preference template should be able to provide by the service provider
- The user interface should be easy to read and not be complicated.

There are some key components in HTML5 that may meet the privacy protection requirements, however, no well-fitted specifications or guidelines for the new concept convergence of Web and TV.

5 BML - TV-specific APIs

In this section, required TV-specific APIs extracted from BML would be discussed.

BML has the TV-specific APIs as Broadcasting Extension Functions, shown in *Table 1*.

Table 1: TV-specific APIs defined in BML

EPG (Electronic Program Guide)
TV Program Group Index
Series recording schedule
Caption Control
Local Storage
Local Storage
Local Storage with Access Control
Content Storage
Two-way Communication
Phone Audio Control
Gaiji (Extended characters) Function
Bookmark Control
Ureg/Greg
Server broadcasting Function
Scheduled Store Function
Store Function
License Function
CAS Function
Server Contents management Function
Playback Control
Contents Metadata reference Function
Communication Assist Function
and other functions

The APIs in the list are required for interactive TV set. And, some of the APIs (Local Storage, Two-way Communication, Gaiji) are supported by HTML5. However, the other APIs has not been supported yet.

6 Conclusions and Proposal

In this paper, it is discussed that HTML5 can be one of the key technologies for TV set that satisfy diversified user needs. Then, privacy data on TV set to be protected is listed.
Policy-based privacy protection is preferred by the comparison of BML and HTML5 privacy principles.
Finally, it is found that HTML5 doesn't support all of the TV-specific APIs defined in BML.

We propose that W3C should do the following actions in Web on TV:

- Consider policy-based access control scheme including in the TV web specification

- Start form the API functionalities requirement extracting from existing time –proven TV platforms like BML.

7 References

[1] Association of Radio Industries and Businesses, "DATA CODING AND TRANSMISSION SPECIFICAION FOR DIGITAL BROADCASTING", May 2006
[2] Device APIs and Policy Working Group, http://www.w3.org/2009/dap/
[3] "Internet evolution and future - Terrestrial digital media broadcasting", http://www.soi.wide.ad.jp/class/20040001/slides/09/, Jun Murai, Jun. 2004