Out-of-Band Authentication Protocol for Digital Signage and Smartphone Interaction

Hirotaka Nakajima*, Shigeya Suzuki†, Tetsuro Tokunaga‡, Kiyoshi Tanaka‡
Yasuhiko Miyazaki‡, Koichi Maruyama‡ and Osamu Nakamura§

*†Graduate School of Media and Governance,
§Faculty of Environment and Information Studies,
Keio University
5322 Endo, Fujisawa, Kanagawa 252-0882 Japan
Email: *hiro@awa.sfc.keio.ac.jp
Email: {†shigeya, §osamu}@wide.ad.jp

‡NTT Service Evolution Laboratories,
Nippon Telegraph and Telephone Corporation
1-1 Hikarino-oka, Yokosuka, Kanagawa 239-0847 Japan
Email: {tokunaga.tetsuro, tanaka.kiyoshi,
miyazaki.yasuhiko, maruyama.koichi}@lab.ntt.co.jp

***Abstract*—An interactive digital signage system which allow users to fetch detailed information using their smartphone is widely deployed. Bluetooth Low Energy(BLE) broadcast beacon is a one of possible method to broadcast a detailed information to users. However, BLE beacon doesn't provide a way to assay an authenticity of beacon since BLE broadcast is insecure untrusted communication. Out-of-band authentication is used to improve trustworthiness for such untrusted pathway. A new authentication protocol is proposed to assay the authenticity of digital signage when the information is broadcasted via BLE beacon. The authors implement the protocol and evaluate its effectiveness.**

I. Introduction

Recently, digital signage system is deployed in many places to broadcast information.

Compare to traditional signage system, digital signage system has an ability that users are able to interact with embed touch screen since digital signage allows to change the content dynamically. However, it is generally known that multiple users aren't able to use the system due to physical restriction.

To solve this issue, user's smartphone is used as a second screen of digital signage to deliver detailed or specified information on user's demand. In such case, pairing process is required to bind the digital signage and user's smartphone. Dedicated application and two-dimensional barcode are used during the pairing process in existing approaches[1].

Meanwhile, Bluetooth Low Energy(BLE) Broadcast communication is widely used to advertise information to smartphone. Since BLE broadcast communication does not define the semantics of its payload, Apple's iBeacon[2] and Eddystone[3] are protocol which commonly used to advertise information to smartphone such as iOS or Android OS devices. Both protocols are 1-way broadcasting protocol; therefore, many attractions are paid to assay the authenticity of transmitting device, called as beacon.

Additionally, it is also known that required level of trustworthiness differs according to a context of the information. As digital signage is deployed in public space such as train station, airport and commercial complex, certain level of trustworthiness is required. Communication channel is a one of key factor to determine that level. However, as mentioned above, BLE beacon does not provide a way to assay the authenticity.

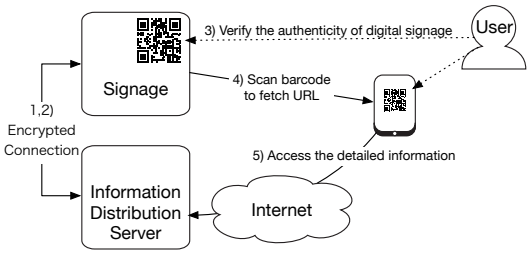

Fig. 1. A semantic structure of two-dimensional barcode integration

Out-of-Band Authentication is an authentication method to verify the peers through a separate communication channel. Since Out-of-Band Authentication is not affected trustworthiness of original communication channel, it is applicable to assay the authenticity of BLE beacon.

In this paper, Out-of-Band Authentication Protocol for Digital Signage and Smartphone interaction is proposed. Proposed protocol uses out-of-band authentication to verify BLE beacon and achieves high reliable information distribution.

II. Out-of-Band Authentication Protocol for Digital Signage and Smartphone interaction

A. Existing digital signage and smartphone integration method

Several methods are proposed to integrate digital signage and user's smartphone. Most common method is to advertise URL of information distribution server using two-dimensional barcode.

Figure 1 shows a semantic structure of existing digital signage and smartphone integration system using two-dimensional barcode. Procedure to integrate a digital signage and user's smartphone with two-dimensional barcode fellows.

1) A digital signage is securely connected to information distribution server. Transport Layer Security(TLS) is commonly used to protect the connection.
2) Content of digital signage is distributed from information distribution server upon a request of publisher or digital signage owner. Content has a two-dimensional barcode which contains URL of detailed information.

978-1-5090-2333-2/16/$31.00 ©2016 IEEE

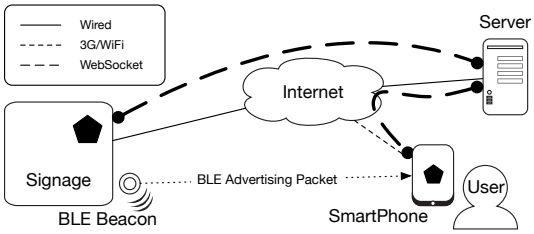

Fig. 2. A semantic structure of implemented proposed system

3) Generally digital signage is deployed on public space where facility owner administrates. Therefore, there are some expectation that facility owner removes the malicious digital signage. Due to this, user verify the authenticity of digital signage by its physical existence.
4) Once user verifies the digital signage, user scans the two-dimensional barcode with his/her smartphone using barcode scanner. At this time, user implicitly confirms that barcode shown on his/her smartphone screen is same barcode as shown on digital signage.
5) User connects scanned URL as authenticity is visually assayed.

B. Purpose of the research

As mentioned in section I, as same as other information distribution, a level of trustworthiness has an important role for information distribution using digital signage.

Section II-A shows that existing approach using two-dimensional barcode delivers information over visually recognizable pathway which user is easy to verify the authenticity of advertised information such as URL.

Meanwhile, BLE beacon is applicable to digital signage system as BLE doesn't require user to scan the barcode but just require user to approach the digital signage. Once consider BLE beacon to broadcast information from digital signage to user's smartphone, there are following possible issues.

First of all, user's smartphone does not have a way to assay the authenticity of BLE beacon since BLE broadcast communication is untrusted 1-way communication. Secondly, Out-of-band authentication which is an authentication method to authenticate the peers through a separate communication channel, is widely used when primary communication channel is insecure or untrusted. Out-of-band authentication is applicable to BLE broadcast communication to assay the authenticity of beacon. A token is a credential which used to verify the peer in out-of-band authentication. Usually token is a combination of number and alphabet. However, verifying a token in a case of digital signage and smartphone is difficult as many user's smartphone may connect the system simultaneously.

To solve those issues, a new authentication protocol is proposed. Following section explains the detail.

C. Proposed Protocol

Out-of-Band Authentication Protocol for Digital Signage and Smartphone interaction is proposed as an out-of-band authentication protocol to assay the authenticity of BLE beacon with digital signage and smartphone.

A figure 2 shows a semantic structure of proposed protocol. A proposed protocol works as follows.

1) A digital signage and information distribution server are connected via encrypted communication channel such as TLS.
2) An embed BLE beacon in digital signage broadcasts an URL of information distribution server which contains unique identifier of digital signage.
3) User's smartphone receives broadcasted BLE beacon.
4) Upon user's interaction, smartphone connects to information distribution server via encrypted communication path such as TLS.
5) Once smartphone connects to information distribution server, digital signage and smartphone shows a shared token which is used in out-of-band authentication. Since physical range of BLE beacon is approximately 70m, visually distinguishable figure is able to be used as token.
6) User authenticates the authenticity of digital signage by verifying that same shared token is shown on both digital signage screen and user's smartphone.

III. Implementation

To evaluate the effectiveness of proposed protocol, we have implemented a digital signage and smartphone information distribution system using proposed protocol.

A digital signage broadcasts a unique URL over BLE broadcast communication using embed BLE beacon. In an implementation, we have selected Eddystone as a protocol for BLE broadcast protocol.

A digital signage and user's smartphone are connected through encrypted WebSocket channel.

We have expected that Web browser has an Eddystone support which doesn't require users to install dedicated application to receive a BLE broadcasted URL. However, only a certain version of Google Chrome supports Eddystone, we have implemented the dedicated standalone application to receive a BLE beacon using Apache Cordova[4].

A graphical figure is selected as an access token for out-of-band authentication. User confirms the authenticity of BLE beacon and digital signage by verifying that same figure is shown on both digital signage and user's smartphone.

IV. Evaluation and Conclusion

We evaluated the effectiveness of proposed protocol. We prepared the proposed protocol system environment and digital signage system with standard Eddystone beacon which broadcast a URL of detailed content. On an evaluation, we have verified that proposed protocol provides a method to assay the authenticity of digital signage.

Proposed protocol achieves to assay the authenticity of digital signage. However, future work is needed as the protocol still does not provide a method to assay the authenticity before user's smartphone connects to information distribution server, which is necessary to protect user's smartphone from malicious beacons.

References

[1] J. Lee, J. Lee, H. Jung, S. Moon, and K. Yoon, "Smart digital signage using smartphone," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, Jan 2013, pp. 978–981.
[2] Apple Inc. ibeacon for developers. [Online]. Available: https://developer.apple.com/ibeacon/
[3] Google Inc. Beacons — google developers. [Online]. Available: https://developers.google.com/beacons/
[4] The Apache Software Foundation. Apache cordova. [Online]. Available: https://cordova.apache.org