Mobile Web and Payments: Challenges and Ways Forward

Giridhar D. Mandyam
Qualcomm Innovation Center
5775 Morehouse Drive
San Diego, CA 92121 USA
mandyam@quicinc.com

Mike Milikich
Qualcomm Innovation Center
9600 N. Mopac, Ste 900
Austin, TX 78759 USA
milikich@quicinc.com

***Abstract*—Mobile payments has been a challenging area that has developed in conjunction with wireless data services. Integration with operator billing mechanisms served as an early solution for handheld devices with cellular access, but payment flexibility is desired by end users and therefore mobile payment models that resemble the web are being explored. In this regards, there are areas where HTML5 extensions in the area of multifactor authentication can help in providing a multitude of options for mobile payment.**

Keywords-payments, authorization, billing, charging

I. INTRODUCTION

Monetization of services has been an issue with mobile devices for many years now. In particular, mobile application developers often require some form of payment integration depending on the type of service being offered. Payments in this case require the ability to leverage a widespread payment mechanism, a trusted form of mutual authentication between the end user and payment service, and a means of protecting the developer and end user from cases of fraud.

An approach that has achieved popularity with wireless devices in the past is the integration of the cellular operator billing service. This has taken the form of services such as Premium SMS, where text messages are sent between the end user and an SMS aggregator to automatically authorize and bill the end user. Web services that integrate directly with the operator billing and charging systems have also found widespread deployment. Note that in these cases the developer often has a direct or indirect relationship with the operator.

Nowadays, device-based multifactor authentication has enabled payments to move beyond Premium SMS yet still provide payment services a means of establishing the necessary levels of trust between the end user, online service provider (merchant) and payment service provider. In this paper, some areas where web technology on mobile devices can be leveraged to provide multifactor authentication are discussed. Based on this, browser-integrated payment services can become a possibility.

II. LEGACY MOBILE PAYMENT

Operator-integrated mobile billing services take on several different forms, but oftentimes require online merchants to integrate with 3rd-parties. Operator-integrated payment systems as a result may not offer desired flexibility in all cases for mobile payments, but they should be considered in the context of ensuring that any new browser-integrated mobile payment mechanism are either compatible or complimentary. Two operator-integrated payment methods, header enrichment and Premium SMS, will be discussed in this section.

A. Header Enrichment

Many cellular operators offer header enrichment as a service [1]. Header enrichment involves the addition of an identifying header in an HTTP transaction originating from a browser running on cellular-enabled device so that the recipient can use the information (usually an MSISDN number) for authentication and billing. The header is inserted in the operator's network, at the internet access point or mobile web prox. If the request does not leave the operator's network (i.e. the recipient server is behind the operator firewall), then the device-identifying information in the header can be assumed to be uncompromised. The web request is then routed to merchant or service provider, who can then provide the subscriber and billing information back to the operator based on integration with the operator's proprietary billing systems. There are situations where header enrichment may not be reliable or possible:

1. The recipient of the HTTP transaction is outside of the operator firewall. In this case, there is the possibility that middleboxes can compromise or simply fail to forward the identifying information in the header.
2. The HTTP transaction is over a secure socket (TLS). In this case, header enrichment would not be possible without breaking the secure connection.
3. The mobile device itself is behind a NAT. In this case, it may not be possible to receive the necessary information in the operator network that would uniquely identify the origin of the HTTP transaction.

B. *Premium SMS*

Premium SMS for mobile web payments in one of its most basic forms involves a user receiving a text message, usually as a result of visiting a website. The message is routed to the end user's mobile device either through explicit information provided by the user to the website, or through a mechanism like header enrichment. Based on receipt of the text message, the user may be advised in the message body about: (1) the nature of the purchase, (2) the cost of the purchase, and (3) a confirmation hyperlink or number to respond to via text to confirm the purchase. The merchant may then use this information to inform the operator about the purchase so that the operator may bill the end user directly.

Browser-integration of text messaging on mobile devices is feasible, but not widely deployed. There is work in the W3C in this space, but it is targeted to installable web applications.

III. AUTHENTICATION BASED ON MOBILE DEVICE CONTEXT

With the advent of HTML5, mobile browsers today are able to integrate increasing amounts of contextual information. Such information can be based on mobile hardware such as sensors, location engines, or even device-captured media. Examples of API's standardized by the W3C that could be used to provide contextual data about the user are the Geolocation [2] or Proximity Events [3] API's.

Based on contextual information, an end user can be authenticated. This should not be a primary form of authentication, but could be considered as part of a multifactor authentication mechanism under certain usage scenarios.

For instance, an end user's location in relation to a geofence may be considered as part of authenticating the user. An example would be in-store mobile-assisted shopping. The Metro Group in Germany has leveraged mobile applications for assisting shoppers in speeding up checkout [5]. Shoppers leverage NFC in their devices to scan items as they take them from shelves, and when they are ready to check out they are presented with a bar code that they have scanned on their way out of the store.

While the bar code on the device is one form of authentication, it could be considered redundant if the user's precise location is already an indication that the user is ready to check out (e.g. near the exit of the store). Leveraging a user's location as an authentication mechanism in this case would have the benefit of potentially obviating the need for a bar code scanner placed at a precise location, which requires an investment in additional in-store infrastructure [6]. This is depicted in Figure 1.

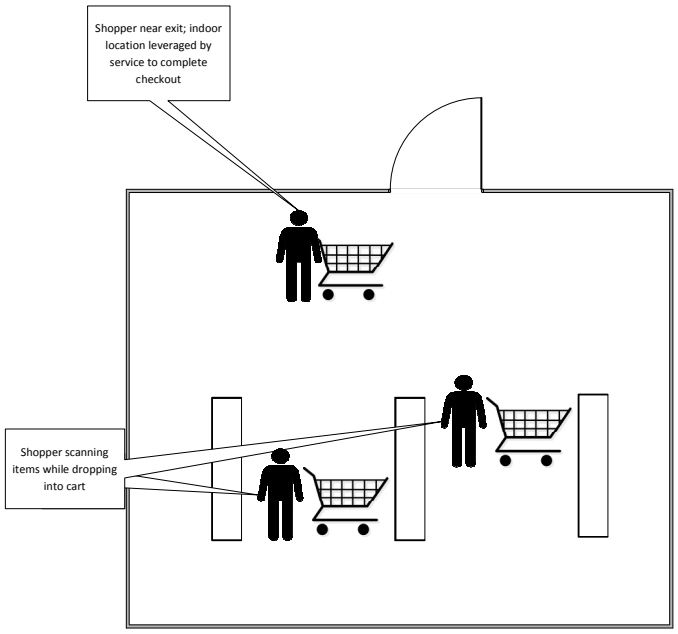

Figure 1: Shopper Checkout Using Location

Note that the browser however needs to have a means of not only retrieving contextual information on a mobile device, but also sending it securely to the merchant or payment service provider if it is to be leveraged as part of any multifactor authentication mechanism. The current W3C API's expose this information through Javascript, and this information can be manipulated by hostile parties (either the web service provider or potential intermediaries). If this information can be retrieved securely, and conveyed securely, then mobile contextual information can become part of a multifactor authentication mechanism in the context of web payments.

IV. CONCLUSIONS

Mobile devices and their associated technology can be used to enhance web payment mechanisms. Although this paper discussed the use of mobile technology for legacy (operator-integrated) payments and contextual data for multifactor authentication, there are other areas where mobile devices may be leveraged for secure transactions. For instance, specialized hardware for secure transaction processing is an active area of both research and development in the wireless technology space. However, integration with the browser is an issue. The challenges for organizations such as the W3C are: (1) whether popular existing payment mechanisms which can be ripe for abuse, such as Premium SMS, be safely integrated into the browser, (2) whether contextual information can be securely retrieved in a browser context and conveyed to a payment service provider, and (3) whether secure hardware can be leveraged by the browser.

REFERENCES

[1] Cisco. "Enhanced Charging: Provide Flexible Billing While Reducing Cost." 2010.

[2] The Worldwide Web Consortium. *Geolocation API Specification*. http://www.w3.org/TR/2010/CR-geolocation-API-20100907/. September 2010.

[3] The Worldwide Web Consortium. *Proximity Events*. http://www.w3.org/TR/2013/CR-proximity-20131001/. October 2013.

[4] M.-H. Chen and C.-H. Chen. "Secondary User Authentication based on Mobile Devices Location". *IEEE International Conference on Networking, Architecture, and Storage*. 2010.

[5] Sakr, Shafir. "Will shoppers be enticed by new ways of paying**?**". BBC Online News Service. http://www.bbc.co.uk/news/business-12310810. January 31, 2011.

[6] Zhang, Feng et al. "Location-Based Authentication and Authorization using Smart Phones". *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. June 2012. pp. 1285-1292.