Neustar® Intelligent Cloud Services

Position Paper:

W3C Workshop on Identity in the Browser

Submitted on

April 20, 2011

Primary Contact

John Hwang
Product Manager, Neustar
571-434-4693
john.hwang@neustar.biz

neustar™

How to Improve the Security around the Mobile User Authentication Process?

INTRODUCTION & INTERESTS

As a Product Manager at Neustar (Neustar, Inc.), I have recently been engaged in creating proposals and designing documents for a solution that can support the WAC (Wholesale Application Community) platform, specifically focusing on Authorization and Billing functionalities. I have been working to leverage existing Neustar services and infrastructure currently available and in use in the market today as a foundation for the WAC architecture. Major efforts are to follow the OAuth protocol and ensuring security around direct billing and User Identity Security.

I am very interested in and enthusiastic about the opportunity to participate in the W3C workshop where I hope to make contributions, as well as share and learn many other valuable ideas and information to improve User Identity Security. As a representative of Neustar, I can share information and experiences from Neustar's existing services and analyze how some of these services and technologies can support and protect the current market with respect to Internet security. Furthermore, I hope that, together with other workshop participants, we can establish a list of strategies to overcome security related weaknesses and threats, especially in Browser segments.

This position paper addresses security mechanisms and specifically User Authentication methods currently in use in the marketplace. Additionally, this paper evaluates concerns and introduces possible solution for "**How to Improve the Security around the Mobile User Authentication Process.**"

ONLINE PURCHASE FLOW

First, let's take a look at a typical flow of the mobile online purchase process. The prerequisite condition is that a developer builds a mobile widget and uploads the widget onto the online marketplace shelf via a trusted Developer Web Portal.

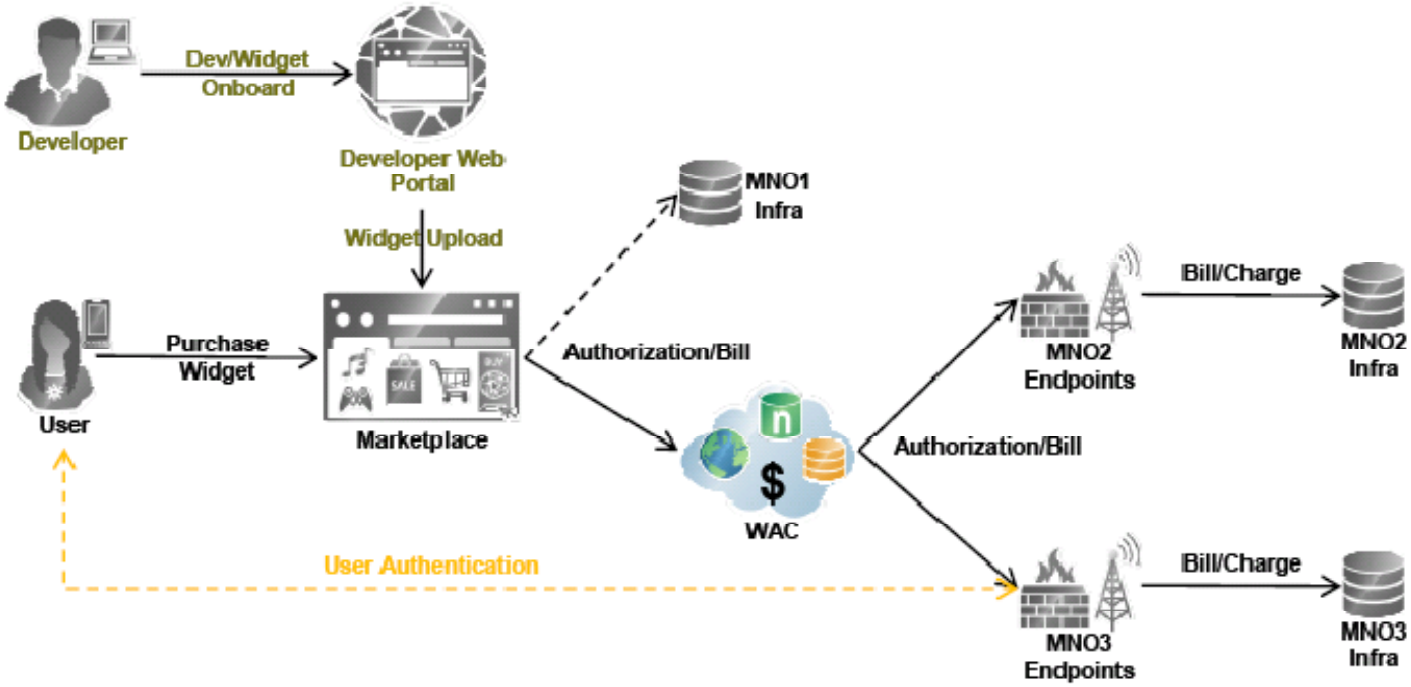

Figure 1: Purchasing a Mobile Widget

Now, let's say Jen (a Smartphone user) wants to buy and download a $5 mobile game widget onto her mobile phone. She does not want to use her credit card or other payment methods, but wants to be billed to her monthly phone bill instead. To do this, the seller (application developer party) or the marketplace must have a prior trusted connection either directly with the Mobile Network Operator (MNO) or with some billing aggregator. Or, if the widget is sold from a trusted marketplace such as the WAC, the billing process can go through the WAC and its vendors. As soon as Jen initiates a purchase transaction, the purchase request goes to the WAC system, the WAC intelligently directs the purchase request to Jen's MNO and $5 USD is billed to her monthly mobile phone bill for buying the widget from the marketplace.

The area to watch closely is the 'User Authentication' arrow. Jen directly communicates with MNO's authentication Endpoint to be validated if this user is really Jen and if so Jen will grant an authorization to the marketplace to bill on behalf of her onto Jen's monthly phone bill.

Now, let's take a look at another example in a more detailed flow diagram (Figure 2) of when Jen buys an Item in the widget. In this example, Jen is playing a mobile War widget game, and wants to buy an "Armor" item to use in the game. The Armor is priced at $1 USD and she again wants to be billed to her monthly phone bill. This time, Jen's purchase transaction is initiated from the widget application, not from the marketplace. As she initiates a purchase via her phone, the purchase request goes to the WAC system. Similarly as before, WAC discovers and directs the purchase request to Jen's MNO and $1 USD is billed to her monthly mobile phone bill for buying an Armor item for her mobile widget game.

Again, there is a direct communication between the User and the MNO with regard to User Authentication and the Access Token, which is the part of the OAuth protocol. The following diagram illustrates this example.

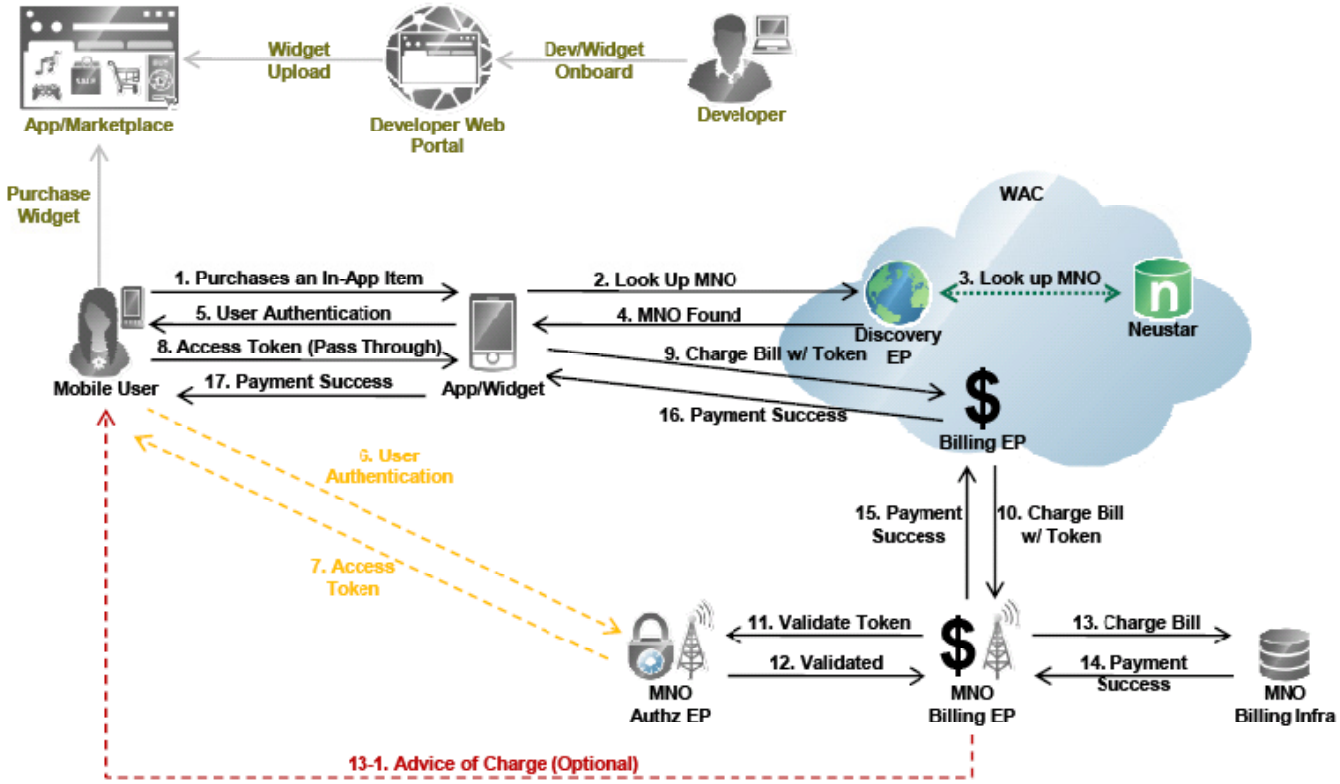

Figure 2: Purchasing an In-App Item

USER AUTHENTICATION METHOD

As shown in the previous two examples, User Authentication occurs directly between the User and the MNO, specifically for the purpose of User Identity Security. There is a number of Authentication methods currently used in the global mobile industry, and the following three cases are the most commonly used. 1) Server-to-Server; 2) Onetime PIN via SMS; and 3) User ID & Password.

1) Server-to-Server Method

In the Server-to-Server Authentication method, End User interaction is not required. The trust (or Authentication) was previously established and that trust is still valid at the time of this transaction. Basically, any transaction request will pass through to MNO Infrastructure via MNO Endpoints for that user.

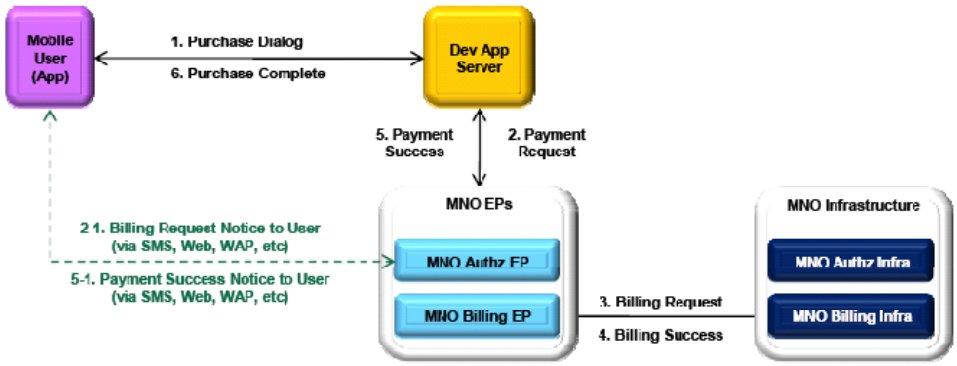

Figure 3: Server-to-Server

What if a purchase is being made on a device by someone other than the device owner? How do we know that the user is authorized to make a given purchase? The biggest pitfall with this scenario is that there is no protection against purchases made without the device owner's knowledge or permission. In this case, vulnerability lies with the user not being engaged in the Authentication Process.

For example, Jen has a younger brother and he is using Jen's phone. If the widget exercises the Server-to-Server method, he can make any purchase and bill them onto Jen's phone bill account without Jen's knowledge or authorization. This is possible since the mobile device and the widget already have an established trust Authentication and Authorization relationship from past that enabled the Server-to-Server method. Server-to-Server mechanism reuses User Credentials from past usages, and so no further Authentication is required.

2) One-time PIN via SMS Method

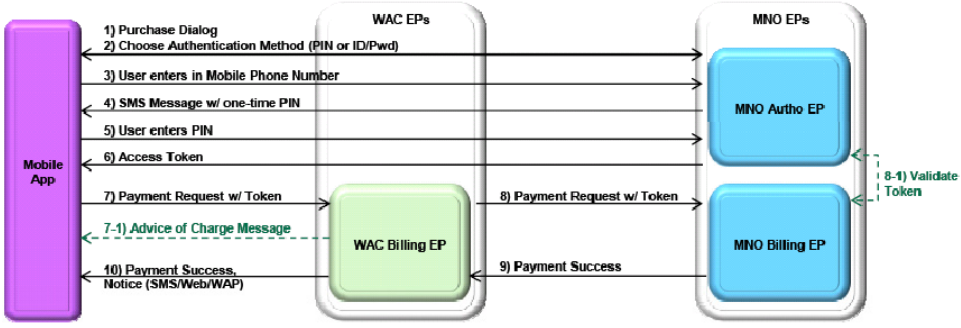

Figure 4. Onetime PIN via SMS

For One-time PIN via SMS method, the User has a choice of either receiving a One-time PIN via SMS (to the phone number that the User enters on a secure page) or typing in their User ID and Password on a secure page provided by the MNO (or trusted party such as the WAC). If a One-time PIN is selected, the MNO sends the Onetime PIN via SMS to the provided telephone number, and the User enters that PIN on a secure page provided by the MNO. Once this Authentication process is validated, the MNO issues an Access Token for the billing transaction (as part of OAuth protocol) and continues the billing process.

The vulnerable area is that, once again, if the mobile device is used by someone other than the phone owner and if that person knows the phone number, there is no protection for it. For an example, if Jen's brother knows Jen's phone number, he could initiate and request for Onetime PIN via SMS by entering in Jen's phone number. Once the Onetime PIN is received via SMS, he can simply enter in the PIN in to a secure page, and the authentication is validated even though the user is not Jen. Once again, Jen's brother can make any purchase he wants to and bill them onto Jen's phone bill.

3) User ID & Password Method

In User ID & Password method, again, User has a choice to select from, either choosing to receive an Onetime PIN via SMS or typing in User ID and Password in to a secure page provided by the MNO (or trusted party such as WAC). If User ID & Password is selected, User types in his or her User ID and Password to the MNO account to be verified. This requires the User to have already set up his or her MNO web account beforehand, and if not so, User should have a link to the MNO site to register and set up an account with MNO. This actually could become an extra works for them. Once this Authentication process is validated, MNO issues an Access Token for the billing transaction and continues the billing process.

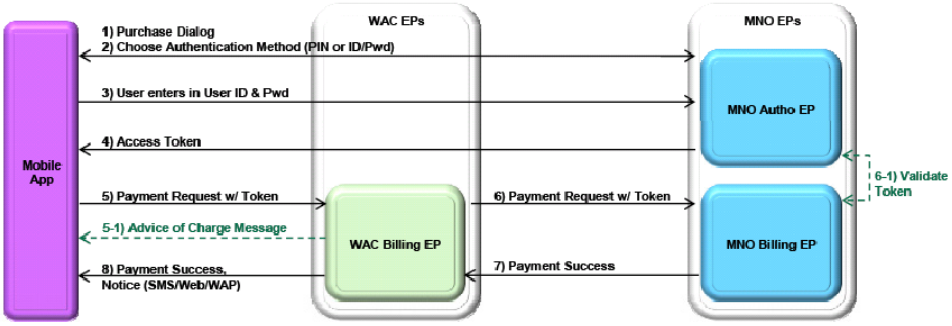

Figure 5. User ID & Password

The vulnerable area is that, if mobile app or another vendor is in between the End User and MNO for managing the Login process with MNO, this could lead into a Phishing mechanism where the User is basically entering in his or her credentials into the 'bad folks' or hackers database. That is the most vulnerable case overall.

4) Voice Message PIN Method

One possible resolution or suggestion is using User's Voice Message PIN. This is the PIN that User enters into the phone when checking voice message box. It is normally a Four digit number that user can instantaneously set up when accessing his or her voice message box for the first time. Globally, the voice message system is normally available to post-paid Users who pay their phone bills in a monthly recurring basis, and so this PIN can certainly tied into this 'Direct Billing' on to User's monthly phone bill payment model.

Similarly with the 'Onetime PIN via SMS' and the 'In User ID & Password' methods, User has a choice to select from, and chooses the 'Voice Message PIN' option and enters in his or her PIN for Voice Message Box in to a secure page provided by the MNO (or trusted party such as WAC). Again, User must previously set up a Voice Message Box Account with MNO, otherwise User should be provided with an instruction of how to set up the Voice Message Box. This could also become an extra works for users. Again, after the User Authentication is validated, MNO issues an Access Token for the billing transaction and continues and completes the billing payment process.

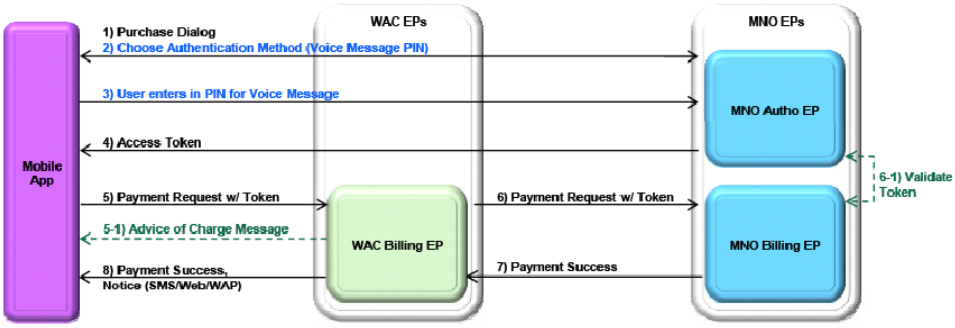

Figure 6. Voice Message PIN

The vulnerable area is that, if Jen's brother somehow finds out Jen's Voice Message PIN, he can simply abuse the purchasing activities. However, it is a very unlikely that Jen would expose her Voice Message PIN to others, and so this method is much safer option than those three previously mentioned User Authentication Methods.

In addition, OAuth protocol for 'Billing/Payment' specific transactions does not support 'Reuse of Access Token'. In standard OAuth protocol, the Access Token can be reused until it expires, however for Billing and Payment activities, it cannot be reused since all transactions have unique billing and payment information. For an example, if Jen first buys an Armor item for $1 and then a few minutes later, she buys a Helmet for $1 in the widget game, the first Access Token for Armor ($1) cannot be reused for Helmet ($1) even though those two items are priced same at $1. A separate Access Tokens is issued for Helmet item for its purchase transaction with its own product information.

CONCLUSION

As User Identity security issue becomes more important, numerous ways for User Authentication have been introduced. Those methods mainly focus on how to secure User credentials from being exposed to the others, especially to the 'bad folks' or hackers. Those concerns around the user identity security normally lead to more complex User Authentication processes and unfortunately that sometimes results in a vulnerable and easy access for hackers to use phishing mechanism. For an example, we could easily miss use too many Authentication or Verification pages requiring user information, and sometimes user does not really pay attention where the user is entering his or her credentials into. This is an easy way for hackers to use phishing pages. In addition, complicated Authentication processes will certainly degrade the End User Experience, where user has to go through 3-4 steps of Authentications. Most of the times, user will either give up and drop out during the process or will complain about the complicated processes. The Authentication Process and User Experience are certainly in an Inverse Proportional relationship. Therefore, we cannot just focus only on how to improve the 'Security', but also need to focus as much efforts on how to make user friendly as a part of the 'User Experience' enhancements. In conclusion, we must diligently innovate and improve the security mechanisms to protect ourselves from hackers who continuously look to penetrate into a tiny gap of 0.00001%.