Open *Source* | Open *Possibilities*

Identity, Security and Privacy: Mobile Web Payments

Giri Mandyam

March 25, 2014

W3C Web Payments Workshop

QUALCOMM INNOVATION CENTER, INC.

Mobile Web Payments - Legacy

- Premium SMS still popular
  - Based on operator-assigned short code
  - Customer sends text message to short code
  - Can be followed by pin exchange to verify origin of SMS
  - Customer is billed through operator
    - Identity through cellphone credentials
- PSMS market still quite strong *worldwide*
  - US operators have shut it down
  - Acc. to Transparency Research International (2013)
    - 236.9 billion in 2012 and further expected to reach to 1,134.2 billion in 2017
    - CAGR of 36.8% from 2012 to 2017
- Mobile browsers have supported PSMS from the WAP days
  - Any new web payments mechanism would have to bear this in mind
    - And all the accompanying issues, including
      - » Operator rev share,
      - » Bad debt

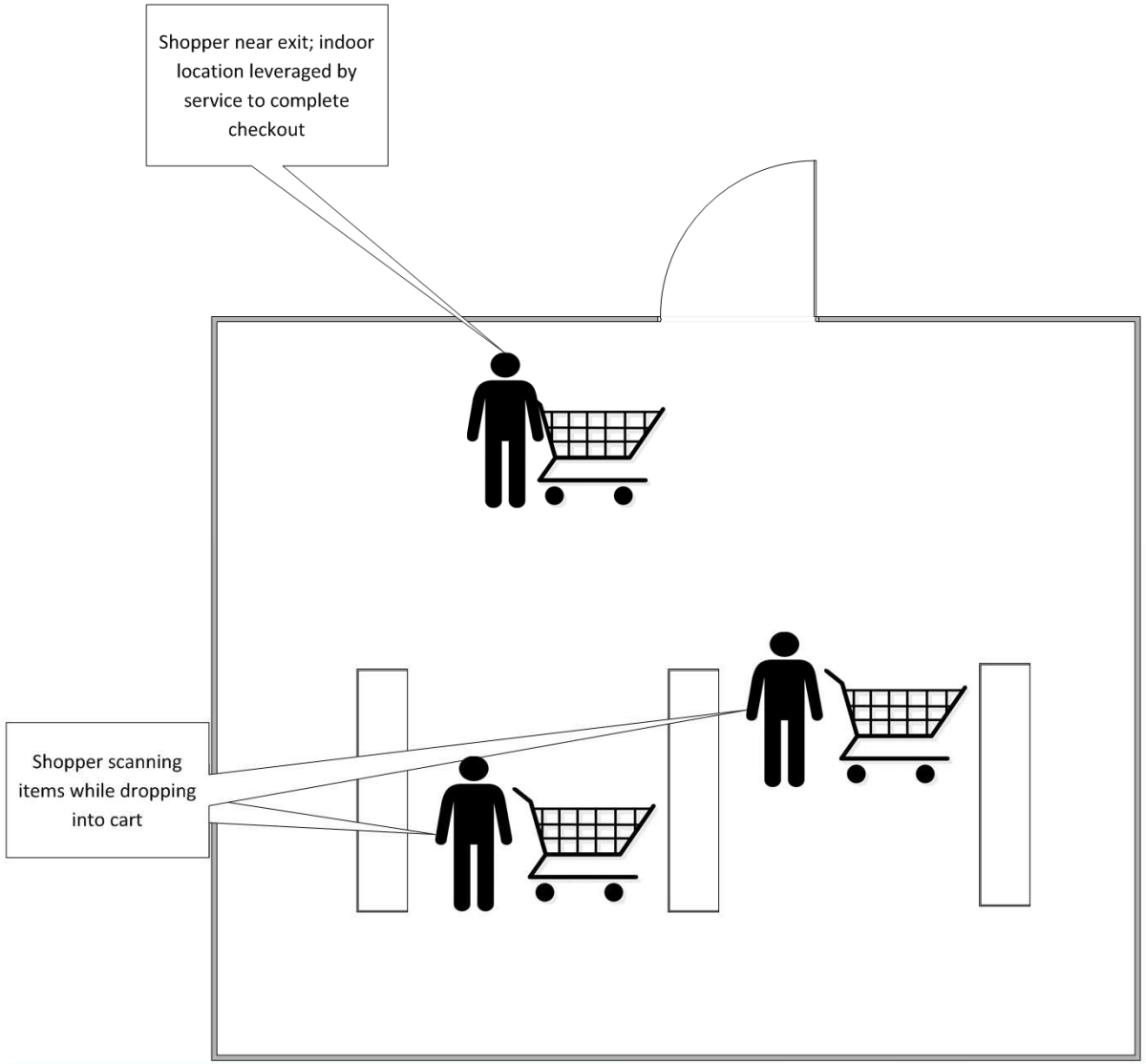
Mobile Web Payments – Legacy (cont.)

- HTTP Header Enrichment
  - Long used for mobile content management systems (CMS's)
  - Operator adds header with unique mobile subscriber ID (e.g. MSISDN)
  - Service provider works with operator to bill customer directly
- Advantages
  - Seamless billing from an end user perspective
  - No changes necessary to existing browsers
- Disadvantages
  - Not secure if path from operator network to server is not secure
    - Middleboxes can spoof headers
  - Traversing NAT's is an issue
    - Not expected to work on WiFi
  - Similar transactional issues as PSMS
    - Bad debt, operator rev share

Mobile Web Payments – Going Forward

- Multifactor authentication leveraging contextual data
  - Location, biometrics, etc.
- Retail example:
  - In-store shoppers who use bar code scanning on mobile device to scan in items as placing them into cart
  - At checkout, device produces a final bar code to be scanned is displayed on mobile device and read
    - Customer automatically billed
  - Can in-store location of shopper be leveraged instead?

Mobile Web Payments – Going Forward



Mobile Web Payments – Going Forward

- HTML5 has introduced features such as Geolocation, NFC that take leverage device API's in mobile devices and provide contextual information
  - Use of contextual information has a place in multifactor authentication
    - Previous in-store shopping example
  - Such data must be provided by a verifiable source
    - Information could be sensitive (e.g. biometric data)
    - Data sent directly by web apps using standard methods such as XHR or WebSockets may be vulnerable to attacks (even over TLS)
  - Any W3C Web Payments enabler should consider whether deeper integration into HW for multifactor auth using device API's is needed

Thank You

QuIC
QUALCOMM INNOVATION CENTER, INC.