Micropayments on the Paywalled Internet

Samvit Jain, Class of 2017
Advisor: Brian Kernighan

Project Goal

- Enable users to purchase long-form news content on a per-article basis ("micropayments")
- ...without requiring long-term commitment (subscription) or user log in

Vox

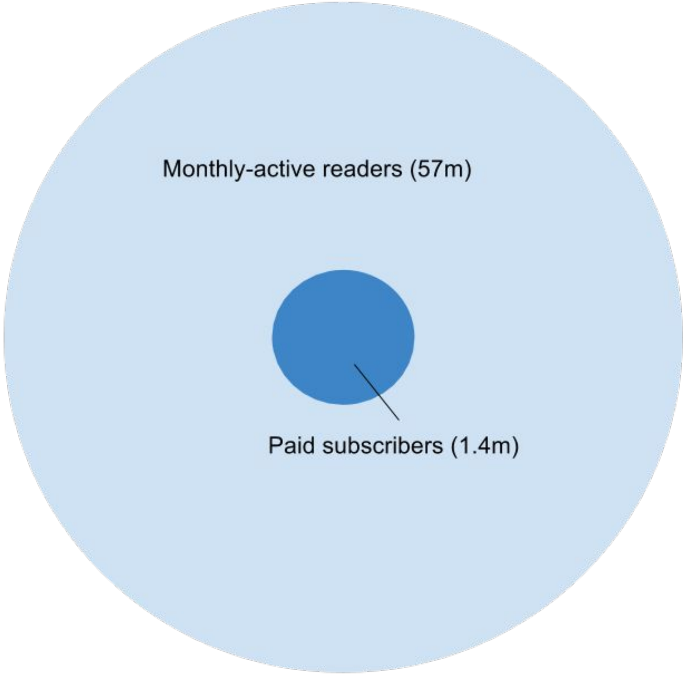
The Atlantic

THE NEW YORKER

Motivation

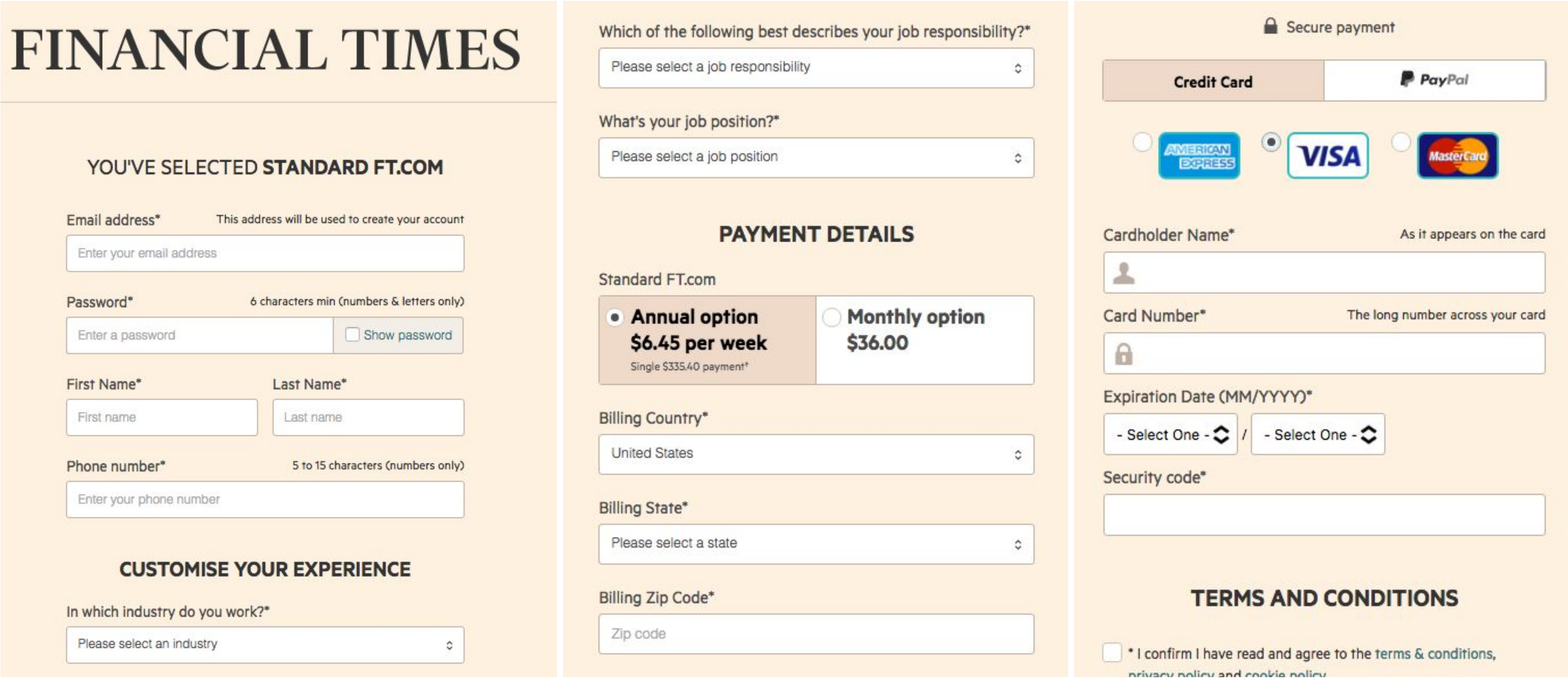
- Top news sites have many subscribers, but most others are struggling
    - New York Times - **1.4 million**
    - LA Times + Chicago Tribune + Baltimore Sun - only **70,000**

- Price discrimination failure
    - **$54m** subscription rev. on **1.4m** subscribers
    - **$42m** advertising rev. on **57m** readers
    - **2.4%** of readers contribute **56%** of revenue



New York Times 2016 Q1

Motivation



FINANCIAL TIMES

YOU'VE SELECTED **STANDARD FT.COM**

Email address* This address will be used to create your account

Enter your email address

Password* 6 characters min (numbers & letters only)

Enter a password □ Show password

First Name* Last Name*

First name Last name

Phone number* 5 to 15 characters (numbers only)

Enter your phone number

CUSTOMISE YOUR EXPERIENCE

In which industry do you work?*

Please select an industry

Which of the following best describes your job responsibility?*

Please select a job responsibility

What's your job position?*

Please select a job position

PAYMENT DETAILS

Standard FT.com

● **Annual option**
$6.45 per week
Single $335.40 payment†

○ **Monthly option**
$36.00

Billing Country*

United States

Billing State*

Please select a state

Billing Zip Code*

Zip code

Secure payment

Credit Card | PayPal

○ AMERICAN EXPRESS ● VISA ○ MasterCard

Cardholder Name* As it appears on the card

Card Number* The long number across your card

Expiration Date (MM/YYYY)*

- Select One - / - Select One -

Security code*

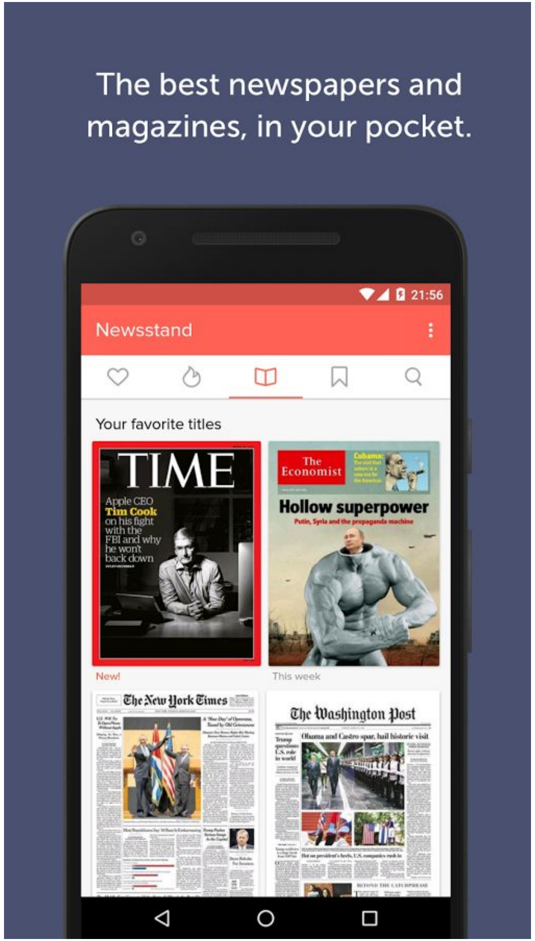
TERMS AND CONDITIONS

□ * I confirm I have read and agree to the terms & conditions, privacy policy and cookie policy

Related Work

- Blendle
  - Ad-free portal to online journalism
  - Users can buy articles individually, demand refund
  - Problems
    - Walled garden - users limited to Blendle app
    - Content licensing - publishers give up control

- Our alternative
  - Users browse the web normally
  - Articles purchased via special browser extension



Approach

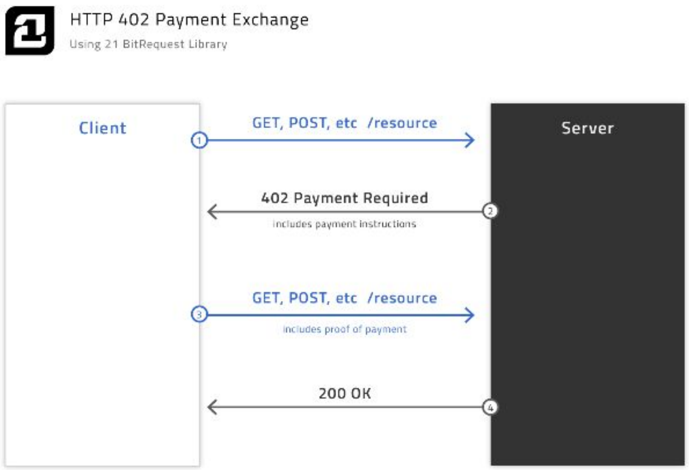
- New payment model
    - Pay-per-article pricing
        - News sites unbundle subscription content
    - Central account
        - Manage one account, instead of 3 (e.g. NYT, Economist, WSJ)
    - One-click payment flows
        - Pay for/unlock article via 1 click in browser
- New access paradigm
    - Eliminate login-based authentication
    - Use PK crypto to prove identity instead

Approach

- Software components
    - Account service
        - Holds payment credentials
    - Browser extension
        - Triggers payments
    - News site code
        - Checks if payment received

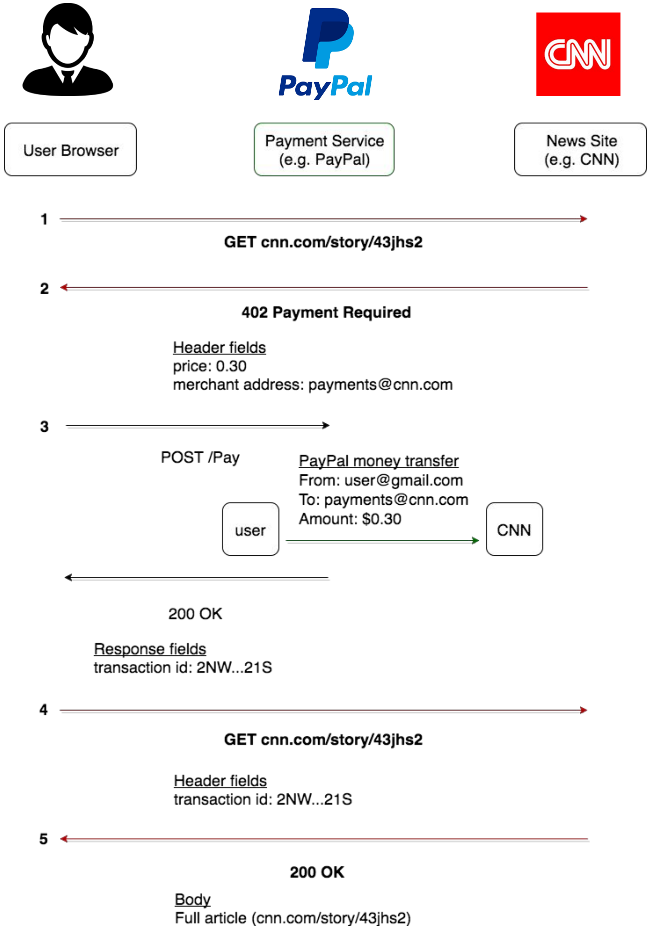
Approach

- Protocols
  - HTTP 402 Protocol
  - Payment verification (sub)protocol



HTTP 402 Payment Exchange

Using 21 BitRequest Library



Contributions

- Payment verification problem
  - User id verification - payment made **by this user**
  - Article id verification - payment made **for this article**

Article ids

User ids

	1	2	3	4
(A)lice		tx-3232	tx-2812	
(B)ob	tx-5283	tx-8404		
(C)arol				tx-1287
(D)avid			tx-4984	

Contributions

- Proof components
    - Public key certificate - $(U_{Alice}, PK_{Alice}, sig_{CA}(U_{Alice}, PK_{Alice}))$
    - User signature - sig_{Alice}(req id)

- Infrastructure
    - Key-value store of transactions
        - Key = transaction id T
        - Value = article id A, user id U_{Alice}

- Verification steps
    - SK_{Alice} correspond to PK_{Alice} (user signature check)
    - PK_{Alice} corresponds to U_{Alice} (certificate check)
    - U_{Alice} corresponds to T (KV-store lookup check)

Contributions

- Publish-Replay Attack
  1. Alice requests article **A** from NYT
     - a. Assigned request id **r**
  2. Alice purchases article **A** via PayPal
     - a. Assigned transaction id **X**
  3. Alice publishes **X**, $\mathbf{PKC}_{\mathbf{Alice}}$, and $\mathbf{sig}_{\mathbf{Alice}}\mathbf{(r)}$ on public forum
  4. Bob reads Alice's post
  5. Bob requests **A** from NYT
     - a. Assigned request id **r'**
     - b. Provides: **X**, $\mathbf{PKC}_{\mathbf{Bob}}$, and $\mathbf{sig}_{\mathbf{Bob}}\mathbf{(r')}$ in request
- Attack fails: X belongs to Alice, not Bob (KV-store check)

Contributions

- Publish-Replay Attack
  1. Alice requests article **A** from NYT
     a. Assigned request id **r**
  2. Alice purchases article **A** via PayPal
     a. Assigned transaction id **X**
  3. Alice publishes **X**, $\mathbf{PKC_{Alice}}$, and $\mathbf{sig_{Alice}(r)}$ on public forum
  4. Bob reads Alice's post
  5. Bob requests **A** from NYT
     a. Assigned request id **r'**
     b. Provides: **X**, $\mathbf{PKC=(U_{Alice}, PK_{Bob})}$, and $\mathbf{sig_{Bob}(r')}$ in request
- Attack fails: CA signature on cert doesn't check out (certificate check)

Contributions

- Publish-Replay Attack
    1. Alice requests article **A** from NYT
        a. Assigned request id **r**
    2. Alice purchases article **A** via PayPal
        a. Assigned transaction id **X**
    3. Alice publishes **X**, **PKC**$_{\textbf{Alice}}$, and **sig**$_{\textbf{Alice}}$**(r)** on public forum
    4. Bob reads Alice's post
    5. Bob requests **A** from NYT
        a. Assigned request id **r'**
        b. Provides: **X**, **PKC**$_{\textbf{Alice}}$, and **sig**$_{\textbf{Alice}}$**(r)** in request
- Attack fails: news site expects **sig**$_{\textbf{Alice}}$**(r')** from Bob (signature check)

Implementation

- Software components
  - Account service
    - https://payment-portal.herokuapp.com/
  - Browser extension
  - News site server
    - http://sample-news-site.herokuapp.com/

Evaluation

- Usability
  - User setup - create account, install Chrome extension
  - Use of public key certificates
- Privacy and security
  - Reads/modifies HTTP headers of requests
  - Requires payment credentials (PayPal login, credit card)
- Adoption
  - News sites must:
    - Unbundle content
    - Run verification code

Future Work

- Payment mechanisms
  - Support: credit cards, Stripe, Bitcoin
- Mobile devices
  - No browser extension on mobile
  - Purchase/read content from mobile phone

Thank you!