

SNAP2PASS:  
CONSUMER-FRIENDLY  
CHALLENGE-RESPONSE  
AUTHENTICATION WITH A  
PHONE

BEN DODSON, DEBANGSU SENGUPTA,  
DAN BONEH, MONICA S. LAM  
STANFORD UNIVERSITY

# Outline

- Web Security Overview
- Contributions
- Snap2Pass: User-Friendly Challenge-Response
  - ▣ Demonstration
  - ▣ Analysis
- Snap2Pay: Secure and User-Friendly E-Commerce
  - ▣ Demonstration
  - ▣ Analysis
- Related Work, Conclusion

# Web Security: How are we doing?

## FBI Hoaxes Boost Online Fraud

By [David Kravets](#)  March 12, 2010 | 5:38 pm | Categories: [Crime](#), [Threats](#)

Online fraud in the United States doubled to a reported \$560 million in losses last year as illicit phishing expeditions by thieves

[PCWorld](#) » [Web](#) » [Social Media](#)

## Your Facebook Profile May Be Sold by Russian Hacker

A spammer/scammer named Kirloss is selling 1.5 million Facebook accounts for a few pennies apiece. Yours might be one of them.

# Problems with Passwords

- Dictionary attacks ( $\sim 1\%$  choose “123456”)
- Phishing ( $\sim 0.4\%$  of users / year)
- Password reuse across the web (over 5 sites)

Source: Florencio and Herley,

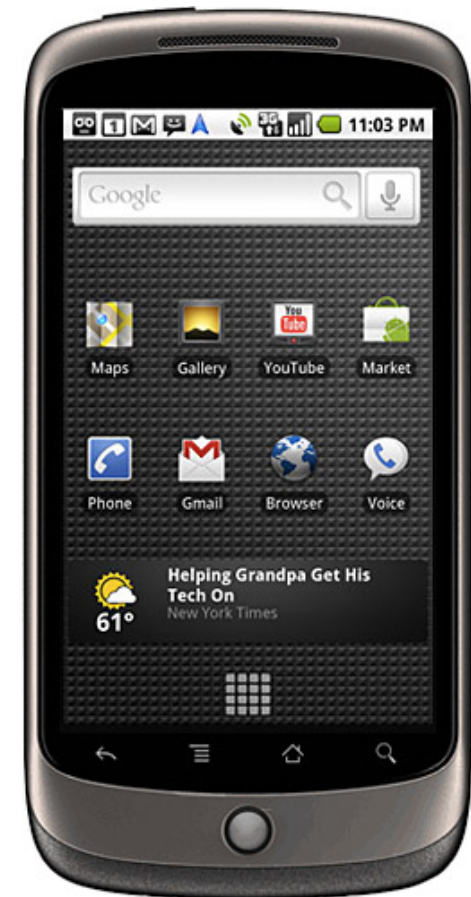
“A Large-Scale Study of Web Password Habits” (WWW ‘07)

# Can we do better?



# Snap2

- Use smartphones to enhance security & **usability**
- Phones are:
  - ▣ Always with us
  - ▣ Personal / individualized
  - ▣ Powerful
    - Internet-enabled, with adequate memory and CPU, and rich sensors

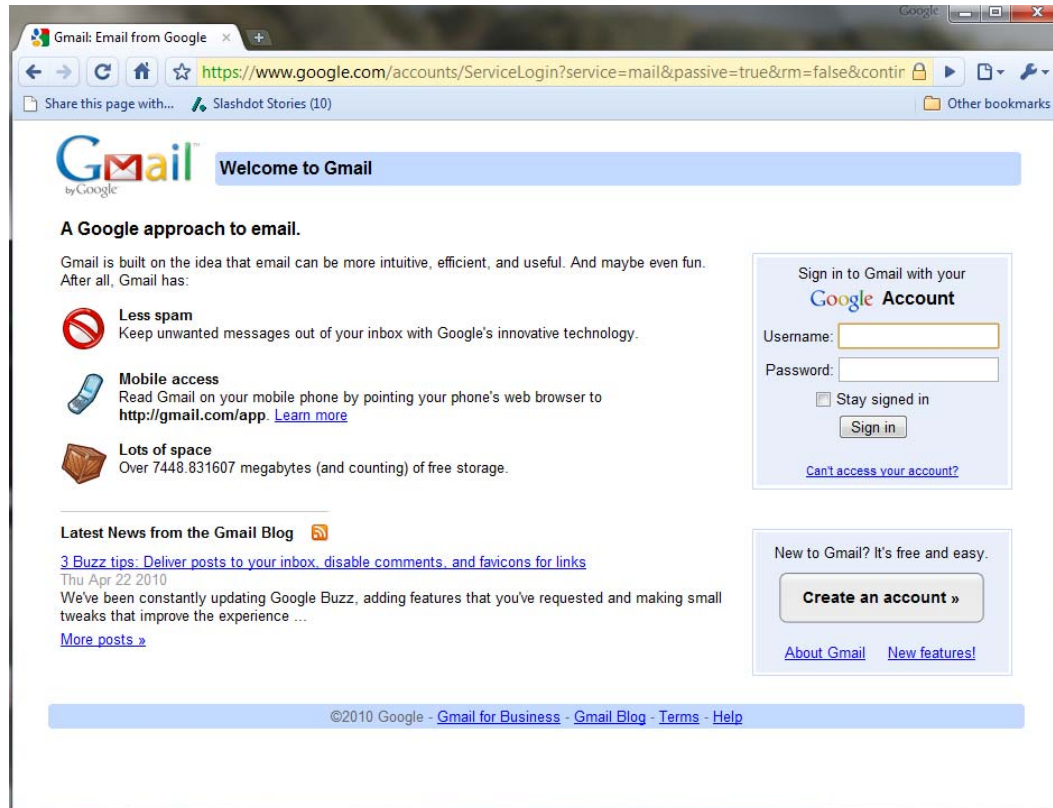


# Contributions

## **Security without loss of convenience.**

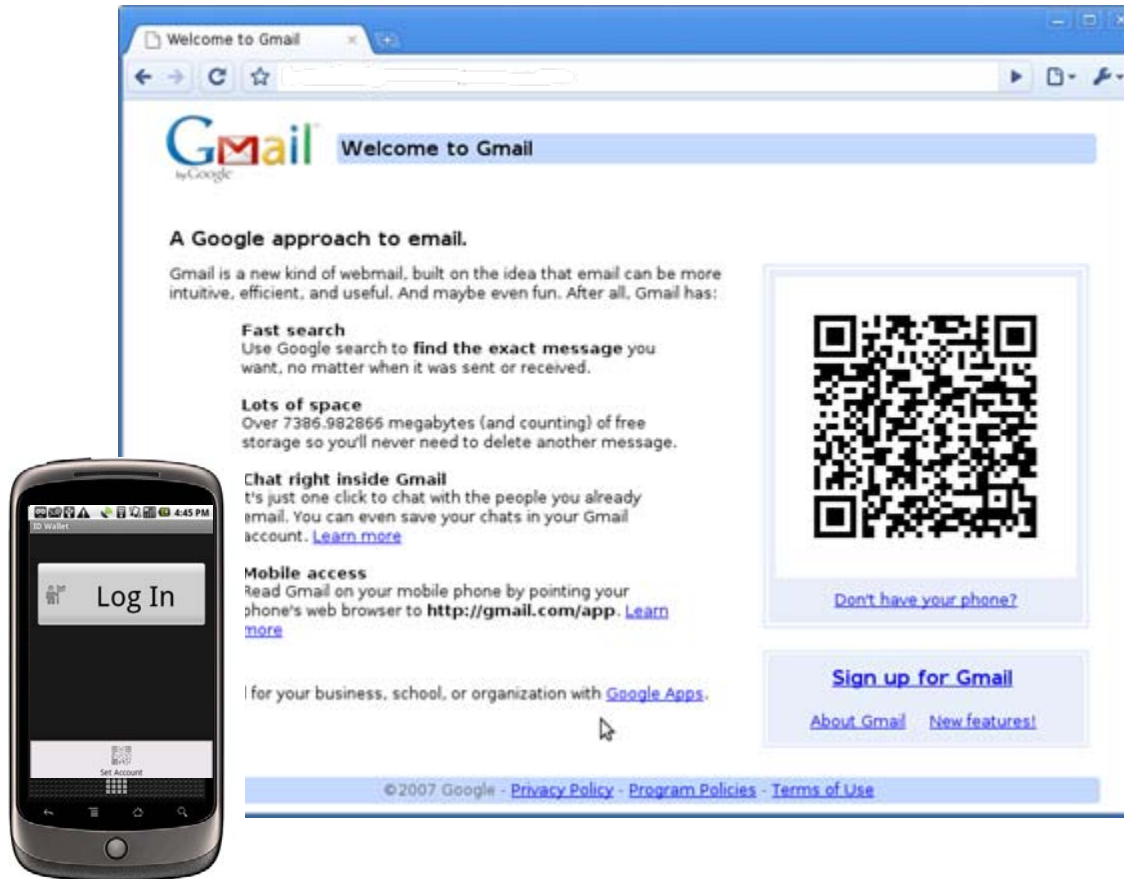
- Challenge/response authentication in a snap
  - ▣ Easy to learn, fun to do
  - ▣ No extra hardware\*, no change to web paradigm
- One-time-use credit cards in a snap
  - ▣ Leave no footprint

# Web Authentication (The usual way)





# Web Authentication (The Snap2Pass way)



# Account Creation

- Provider generates shared secret
  - ▣ Encode credentials in a QR code



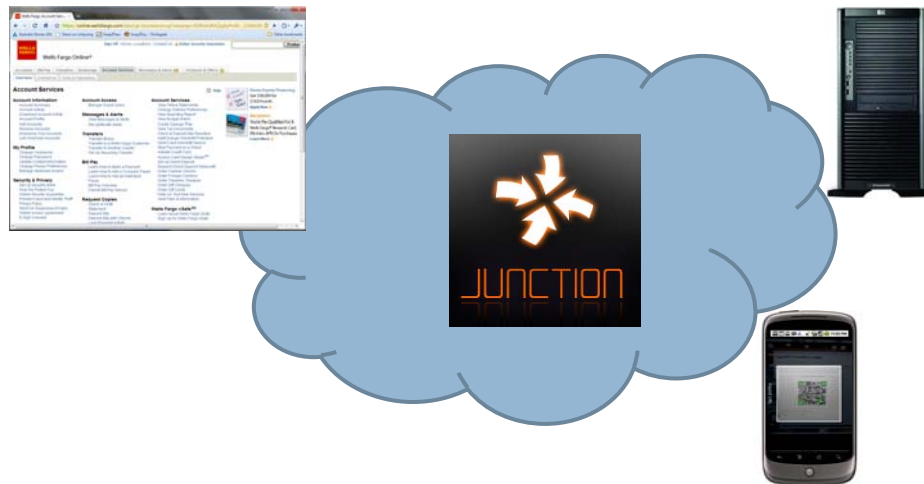
# Logging In

- QR encodes challenge and communication endpoint



# Aside: Junction

- Platform for multiparty interactions
  - ▣ Provider, browser, phone all communicate in one session
- Junction provides communication and connectivity
  - ▣ Generate and consume QR code with 1 line of code
  - ▣ Messaging in a few more



# Auth Transaction

- 3 Parties involved (phone, browser, provider)
  - ▣ HMAC challenge/response between phone/provider
  - ▣ Browser must know when session has been authenticated
- Implemented as a chat transcript
  - ▣ Chatroom name is the challenge
  - ▣ All devices actively listen for messages

!> *You have joined:*

*snap2pass.com/***CHALLENGE**

!> phone: {username: "letmein", response: "**RESPONSE**"}

!> provider: {status: "AUTH\_OK"}

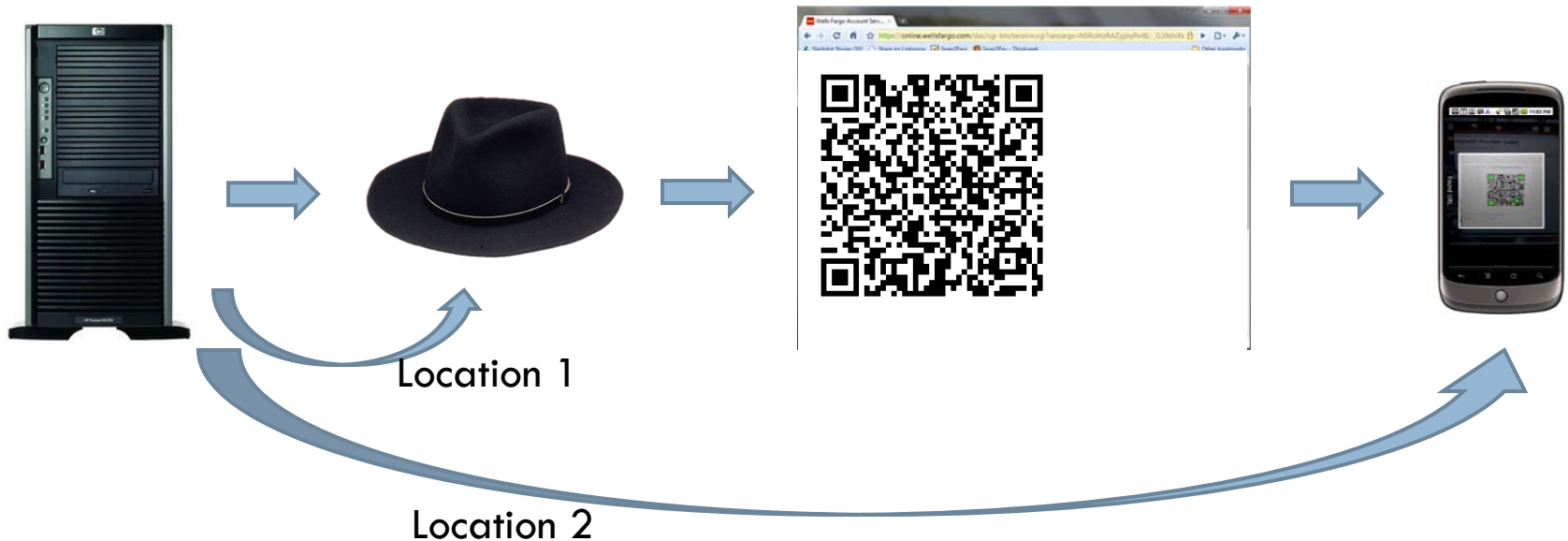
!> browser: /me refreshes web page

# Security Analysis

Criteria	Username / passwords	Snap2Pass
Offline phishing	Vulnerable	Secure
Online phishing	Vulnerable	Loss of session
Keylogging (client malware)	Vulnerable	Secure
Loss of device / theft	N/A	Revocable account
Malware on phone	N/A	Vulnerable
Passive network attack	SSL required	Secure w/o SSL

# Online Phishing

- A hard problem.
  - 1. Server uses geolocation to ensure browser/phone are near
  - 2. Verify sensitive transactions from phone



# Extending to multiple domains

- Multiple accounts for multiple domains
  - Single app, independent accounts
    - Account creation includes domain
  - User prompt helps prevent MITM



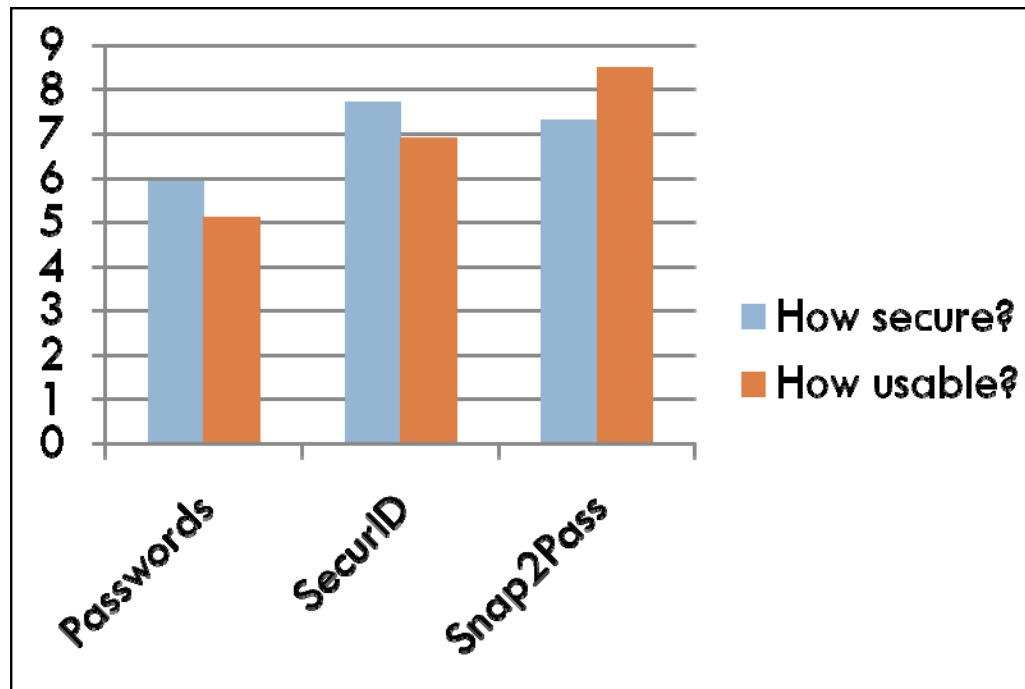


# Extending to multiple domains

- Single account, multiple domains
  - ▣ OpenID (implemented; requires username entry)
  - ▣ OpenPass (Reliant party generates challenge)
  - ▣ Public key cryptography

# Usability

- Comparison of SecurID and Snap2Pass
  - ▣ How 30 users feel using this system w/ bank



# Web Payments (The usual way)

The screenshot shows a web browser window with the URL `https://www.thinkgeek.com/brain/checkout/address.cgi?submit.x=33&submit.y=13`. The page title is "WarpSpeed Checkout!".


**Log into your account:**

Email:   
Password:  [Forgot your password?](#)

**Don't have an account yet?**

Enter a password after entering your addresses, and you'll get the automagical account benefits of:

- quicker checkout with saved addresses and carts
- shared Wish Lists with friends and family
- detailed order history and tracking
- earned Geek Points and exclusive discounts and freebies



**Checkout as a guest (or create new account):**

**Shipping Address:**

Country:  \* (required)  
First name:  \*  
Last name:  \*  
Company:   
Address:  \*  
Apt/Suite #:   
City:  \*  
State:  \*

**Billing Address:**

Same as shipping

Country:  \* (required)  
First name:  \*  
Last name:  \*  
Company:   
Address:  \*  
Apt/Suite #:   
City:  \*

A vertical "feedback" button is visible on the left side of the page.

# Problems with form-based e-commerce

- Tedious to enter billing, shipping information
- Risks associated with storing account in cloud
- Might not trust site with credit card number at all

(All are especially true for mom&pop sites)

# Web Payments (The Snap2Pay Way)



# Benefits

*“Should I let these guys save my credit card?”*

- Reduce time spent on checkout process
  - ▣ Without requiring per-site or centralized account mgmt.
- Enhanced security
  - ▣ Phone negotiates one-time-use credit card number
- Easily ship to anyone in your address book
- Integrated receipts, tracking

# Two Payment Modes

---

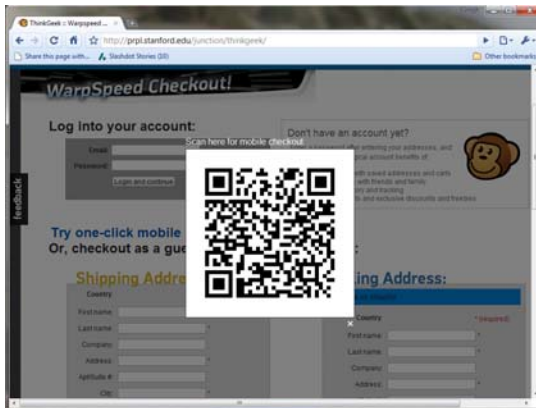
- FORMFILL provides easiest integration
  - ▣ Also allows user to modify submission
- PAYDIRECT provides enhanced security
  - ▣ Usable beyond the web, too

# Direct Payments with Snap2Pay





# PAYDIRECT Challenge



{ Domain: "thinkgeek.com"  
,challenge: "09a762c7de4df900da65b"  
,Price: "34.99 US"}

# Snap2Pay: Beyond the Web

The Meijer Team appreciates your business  
01/26/09  
Your fast and friendly checkout was provided by FASTLANE

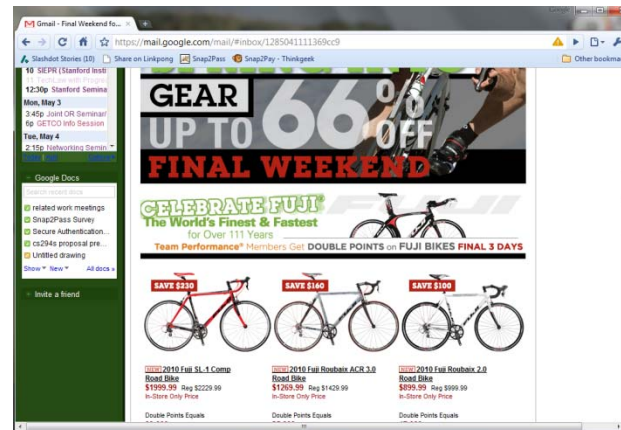
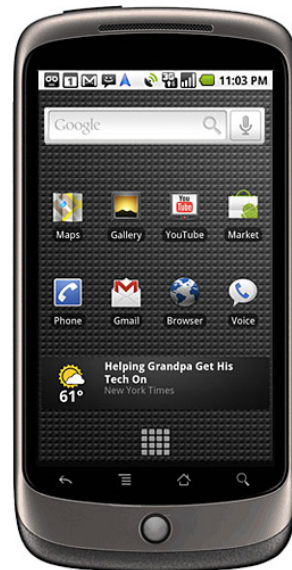
\*\*\*SAVINGS TODAY\*\*\*  
 \* TOTAL MEIJER PROMOTIONS 7.97 \*  
 \* TOTAL NON-COUPON SAVINGS 6.94 \*  
 \* TOTAL COUPON SAVINGS OF 8.50 \*  
 \*SAVINGS TOTAL 23.41\*

GENERAL MERCHANDISE  
 7301028010 TAMPONS 2.97 T  
 2270010065 LIP COLOR 7.97 CT  
 => FREE 1 item -7.97 CT  
 2270010074 LIPCOLOR 7.97 CT

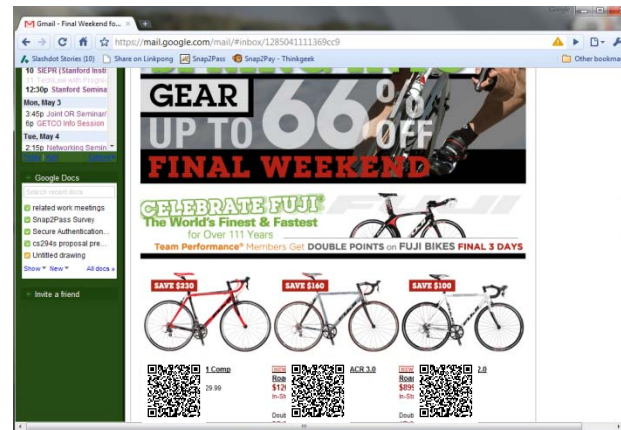
GROCERY  
 1254667304 GUM 1.99R FT  
 3700003866 FLOSS 3.69 T  
 \*4610000084 SHRED CHEESE 4.09  
 was 4.09 now 1.89 F  
 \*4400000013 SNK CRACKER 4.00  
 1 @ 2 2.75  
 was 2.75 now 2.00 F  
 \*4400000067 SNK CRACKER 4.00  
 1 @ 2 2.75  
 was 2.75 now 2.00 F  
 \*7192100765 FROZEN PIZZA 5.98  
 was 5.98 now 4.79 F  
 \*2100064592 MIR WIP LIGH 5.00  
 1 @ 2 2.55  
 was 2.55 now 2.50 F  
 \*4440015130 GRIN SCAMPI 7.99  
 was 7.99 now 5.99 F

COUPONS  
 54610012050 Vendor Coupon -.50 F  
 54610012050 EXTRA COUPON -.50 F  
 57301010050 Vendor Coupon -.50 N  
 57301010050 EXTRA COUPON -.50 T  
 51254622476 Vendor Coupon -1.00 F  
 52270099276 Vendor Coupon -1.00 N  
 53700065076 Vendor Coupon -1.00 N  
 54440020078 Vendor Coupon -1.50 F  
 54400020051 Vendor Coupon -2.00 F

TOTAL TOTAL TAX .97  
 TOTAL 28.26



# Snap2Pay: Beyond the Web



# Related Work

- Phoolproof (Parno et al.)
  - ▣ Use bluetooth + custom PC software
- OTP on phone (Aloul, Zahidi)
  - ▣ Move SecurID etc. to phone
- “Seeing Is Believing” (McCune et al.)
  - ▣ Use 2D barcodes for key exchange (unidirectional)

# Conclusions

- Phones are always with us, making them personal
  - ▣ Are also connected, have decent storage, and reasonable processing power
- QR codes allow cross-device communication without modifying standard software stacks
- Result: More security for web transactions, simplified user interaction.

# [Appendix]



# Usability

- Comparison of SecurID and Snap2Pass
  - ▣ How 30 users feel using this system w/ bank

