Digital Wallet

Challenges, Opportunities, and Solutions

Rajesh Krishna Balan

Joint work with folks at SMU (Narayan Ramasubbu and a team of students) and CMU (Nicolas Christin, Jason Hong, and Komsit)

Motivation

- My wallet is thick, bulky, falling apart, impossible to manage
- I already carry a cell phone wherever I go
  - Without it, I would have no idea what my next appt is!!

Grand Idea!



Roadmap

- What is a Digital Wallet?
- Scenario 1: Peer to Peer Payments
- Scenario 2: Point of Sale Transactions
- Future Directions / Interesting Questions
  - Research Opportunities

What is a Digital Wallet?

- Cash
- Payment Cards
  - Credit / Debit / Stored Value
- Loyalty / Reward Cards
- ID
- Name Cards
- Receipts
- Random other stuff
- Some parts have been done

Why do I think it is possible?

- Obligatory "Business" Case
  1. > 100% cell phone penetration rate in S'pore
  2. Highly savvy users
     - MMS / 3G / Video downloads etc.
     - Eager to try new technology
  3. Makes sense for businesses
     - Increase "cheap" online transaction volume
  4. Huge push to integrate everything here
     - Government driven in many cases

Required Tech Components

1. Secure Communication Medium
   - Needed to exchange information
   - Provided by NFC
     - Short range is a plus in this case
2. Fast Secure Authentication
   - Passwords are inherently broken
   - Biometrics have improved dramatically
3. Secure Tamper Proof Storage
   - To store money, ID, cards, etc.
   - Secure SIM chips are now available

Scenario 1

Peer-to-Peer Mobile Payments

Examples



Why Peer-to-Peer?

- Network access is not ubiquitous
  - Tunnels, underground, rain, etc.
- Infrastructure is expensive
  - Small operators will not pay for it
- Infrastructure solutions are a dime a dozen
  - No p2p solution yet!

Properties of Cash

- Easy to Understand and Use
- Anonymous
  - Our solution is not as good in this aspect
  - We trade anonymity for other properties
- Highly Available and Inter-Operable
  - Chicken and egg problem for our solution
  - Not something I can solve

Limitations of Cash

- Not Resilient to Theft
- Poor Accountability
- Poor Dispute Resolution
- Variable Accuracy
- Variable Cognitive Load
- Our solution corrects all of these limitations

Technical Challenges

- How do you store cash in a phone?
  - Digital cash requires a lot of support
- How do you make it a secure process?
  - Any bugs in security dooms the entire thing
- How do you make it fast and usable?
  - Cash Is trivial to use
  - This is replacing cash!

Solution: mFerio

- How do you store cash in a phone?
  - Use a stored value system
  - Existing protocols exist
- How do you make it a secure process?
  - 2 phase protocol
- How do you make it fast and usable?
  - Simple easy to use system

mFerio Success Criteria

- Fast
- Easy to Use
- Accurate
- Low Cognitive Load
- Secure

➡ Important that these criteria are both perceived and measured to be true

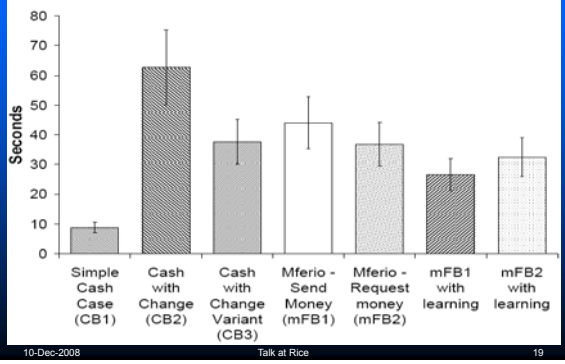
Two-Phase Evaluation

- Phase 1
  - Detailed user study of UI prototype
  - Fake authentication details
  - Test usability relative to cash
    - Get user input for various design choices
- Phase 2
  - Full system with real security / crypto
  - More focused in-depth stuff of cognitive load

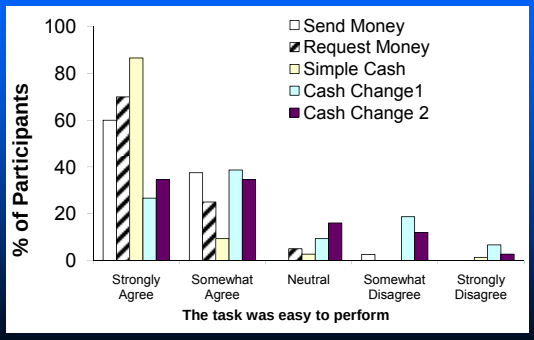
Phase 1 User Study Evaluation

Total Number	75
Gender	Male (35), Female (40)
Major	Accountancy (7), Economics (1), Business (29), Social Sciences (6), Information Systems (22)
Proficiency Level	Novice (22), Intermediate (30), Expert (23)
Importance of Phone	Low (8), Medium (36), High (31)

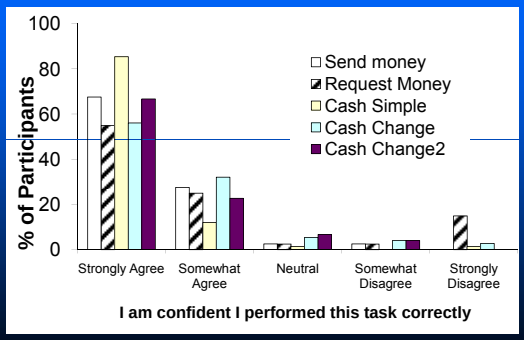
mFerio Results - Speed



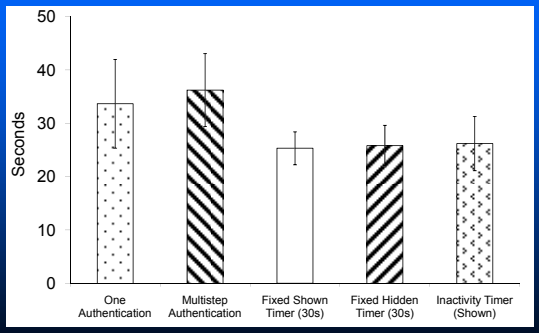
mFerio Results - Ease



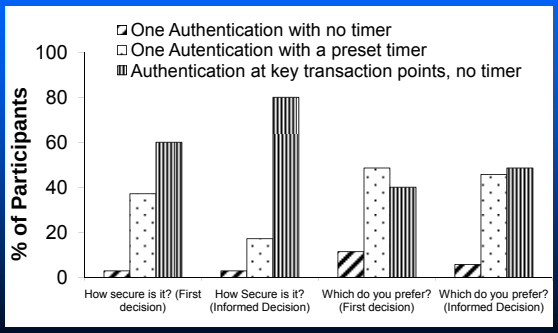
mFerio Results - Accuracy



mFerio Results – Authentication



mFerio Results – Auth 2



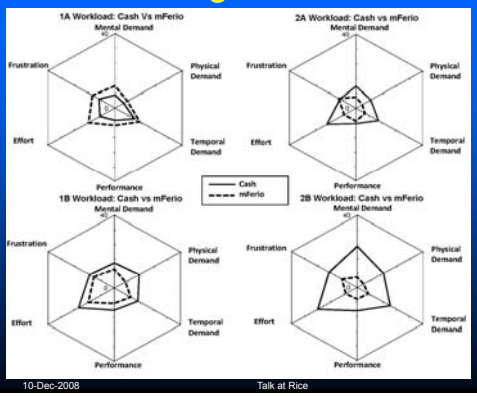
Phase 2 Study

- Added real security
  - Modified Even-Goldreich-Yacobi counter-based protocol
  - exchanges certificates and a symmetric key in the first touch
  - Exchanges payment in the second touch
- Performed NASA TLX cognitive load test

Phase 2 User Study Evaluation

Total Number	29
Gender	Male (19), Female (10)
Age	20 and below (2), 20 to 30 (13), Above 30 (4)
Proficiency Level	Novice (10), Intermediate (7), Expert (12)
Importance of Phone	Low (12), Medium (14), High (3)

Cognitive Load



1A: Simple No Change

1B: Complex No Change

2A: Complex Small Change

2B: Complex Large Change

Scenario 2

Point of Sale Card Overload

Motivation

- At the checkout counter at Bestbuy
  - You have X products from Y departments totaling Z dollars.
  - You have α payment cards, β reward cards, and θ loyalty cards.
- Q: What is the right combination of cards to maximize your net gain?

Current Solutions

- Guess
- Pick a decent "good enough" solution
  - Not maximal
- Perform detailed analysis
  - Fragile to change
  - Time consuming
  - Hard (Not novice friendly!)

Solution: pFerio PoS system

- Store all your card details in your phone
- Place phone on reader at store
- System matches store discounts with cards your have
- Best results are displayed on a LCD display
- Pick best option
- Profit!!!

Solution Requirements

1. Method to store cards in phone
2. Description of cards on phone
3. Description of retailer discounts
4. Mechanism to match discounts with cards
5. User interface to display results to user
6. Transfer chosen card details to store

Description of Cards / Discounts

- Created XML Schema for cards
  - Hideous multi-tiered XML monstrosity
    - Like most things XML
  - Due to complexity of real world
- Our schema supports
  - Discounts, rewards, loyalty
  - Specific retailers, categories
  - Time periods, stacking

Matching Mechanisms

- Two problems
  - Where to perform the match?
    - On phone => performance issues
    - At retailers side => privacy issues
  - How to perform the match
    - Needs to be a fast algorithm
    - General problem is hard. Very hard!
      - Probably NP-complete
    - Need to find a reasonable approximation
    - Still working on this

User Interface

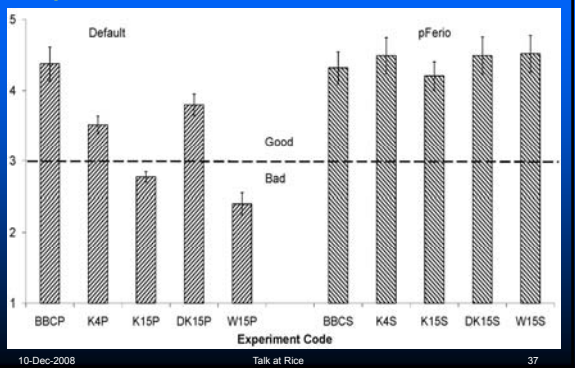
Evaluation Questions

- Is it better than the current process?
  - Speed (queue length increasing is a concern)
  - Accuracy
  - Ease of Use
- Under various scenarios
  - User has / does not have information
  - Cashier has / does not have information
  - User thinks they know something
    - But they are wrong!

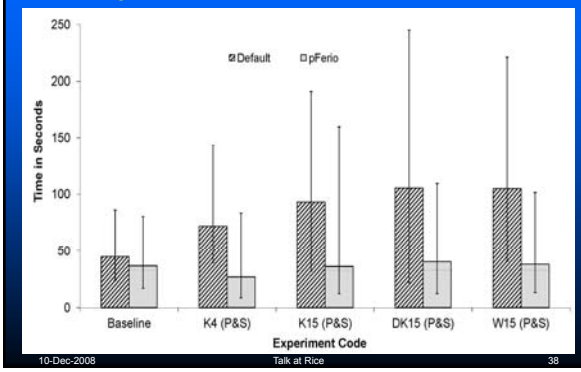
pFerio User Study Evaluation

Total Number	35
Gender	Male (19), Female (16)
Major	Accountancy (4), Economics (3), Business (18), Information Systems (10)
Number of Cards Normally Carried	1 – 3 (7), 4 – 6 (17), 7 – 9 (8), 10 or above (3)
I always look for the best deals	Strongly Agree (2), Somewhat Agree (20), Neutral (10), Somewhat Disagree (3), Strongly Disagree (0)
I know the best deals for my cards	Strongly Agree (2), Somewhat Agree (10), Neutral (14), Somewhat Disagree (7), Strongly Disagree (2)

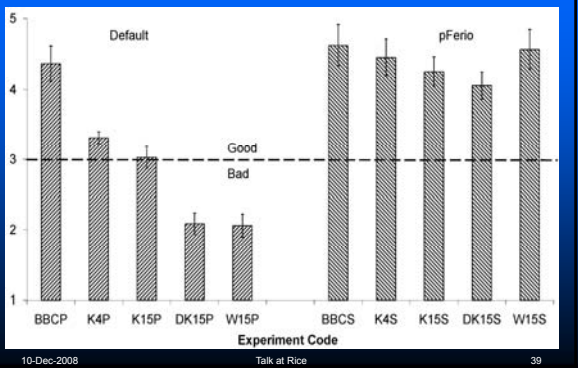
pFerio Perceived Quickness



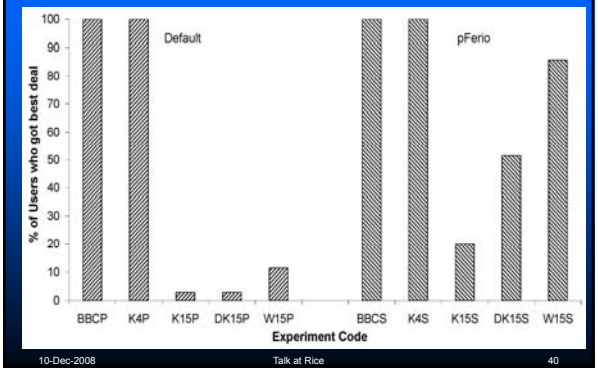
pFerio Measured Time



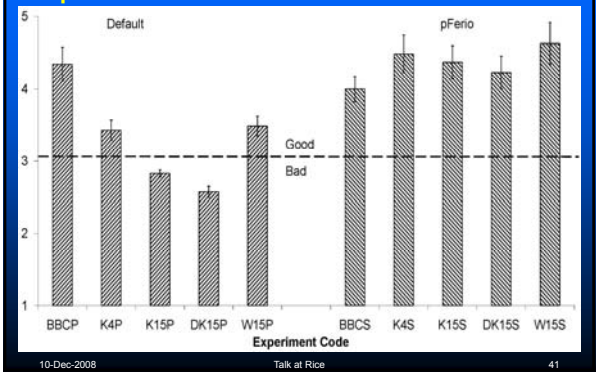
pFerio Perceived Accuracy



pFerio Measured Accuracy



pFerio Perceived Ease of Use



Future Directions

- Integrate mFerio with real systems / vendors
- Tackle the authentication / privacy issues
  - Planned for early next year
  - Develop good mobile authentication solution
  - Privacy mechanisms for PoS system
- Tackle Receipt tracking / Smart Apps / ID

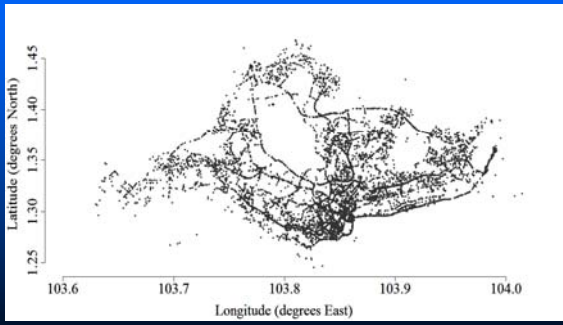
Big Finish!

- Migrating a physical wallet into the cell phone is possible
  - Can even be faster than established norms!
  - Solves many problems
  - Creates many others
    - Power, software crashes, etc.
- Full of interesting problems to work on
  - Spans many fields of CS / IS

Special Bonus – Traffic Analysis

- Real time GPS-enhanced taxi feeds?
  - Booking, trip, log information
- 250 million data points per month
  - ~ 40 updates per taxi per month
  - ~ 15,000 taxis per month
  - ~ 6 – 12 months of data
  - Don't use mysql as a back-end database!!
    - Good late night dinner rant

Accuracy of Data



What would be interesting?

- Traffic analysis?
  - Can GPS be used a sole traffic determinant?
  - Can a better traffic model be built?
  - Anomaly detection
  - Inefficiency analysis
- End-to-end system
  - Use LCDs in taxis with back-end analysis to improve system
- What else?