

Securing Interactive Sessions Using Mobile Device through Visual Channel and Visual Inspection

Chengfang Fang, Ee-Chien Chang

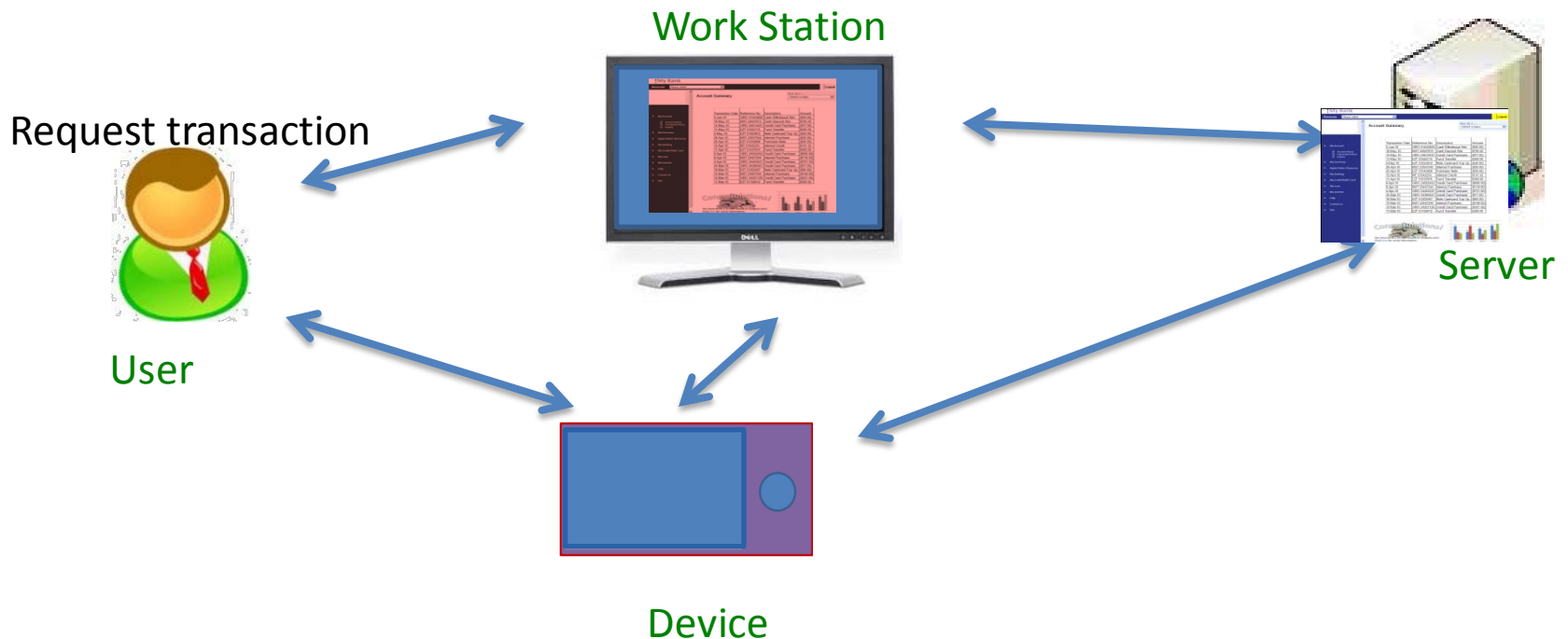
School of Computing

National University of Singapore

December 8, 2010

Authenticating a Message

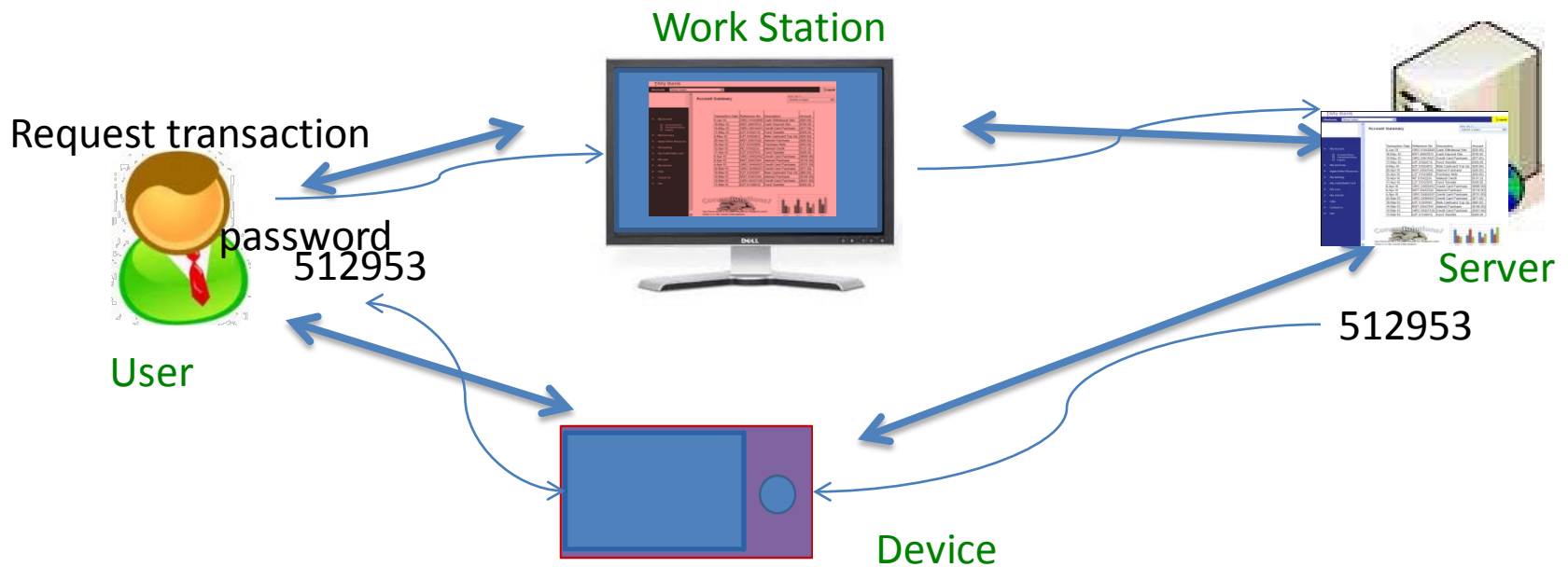
We are interested in securing interactions with a server via an work station using a mobile device.



Outline

- Background and related methods
- Our method
- Design Challenges
- Proof of concept demonstration
- Conclusion and future work

One Time Password



However, it does not verify the transaction content, thus the work station is able to modify the transaction.

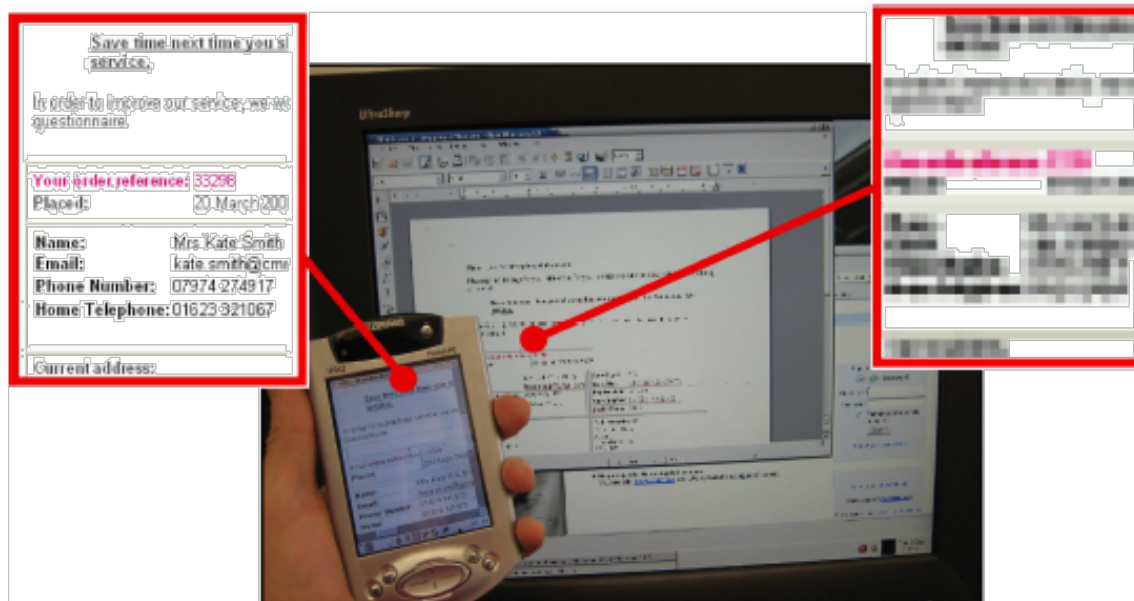
Related Work

- [Clarke2002] : Capture every pixel and verify the pixels (or perform OCR and verify the message) with a MAC barcode on the screen.

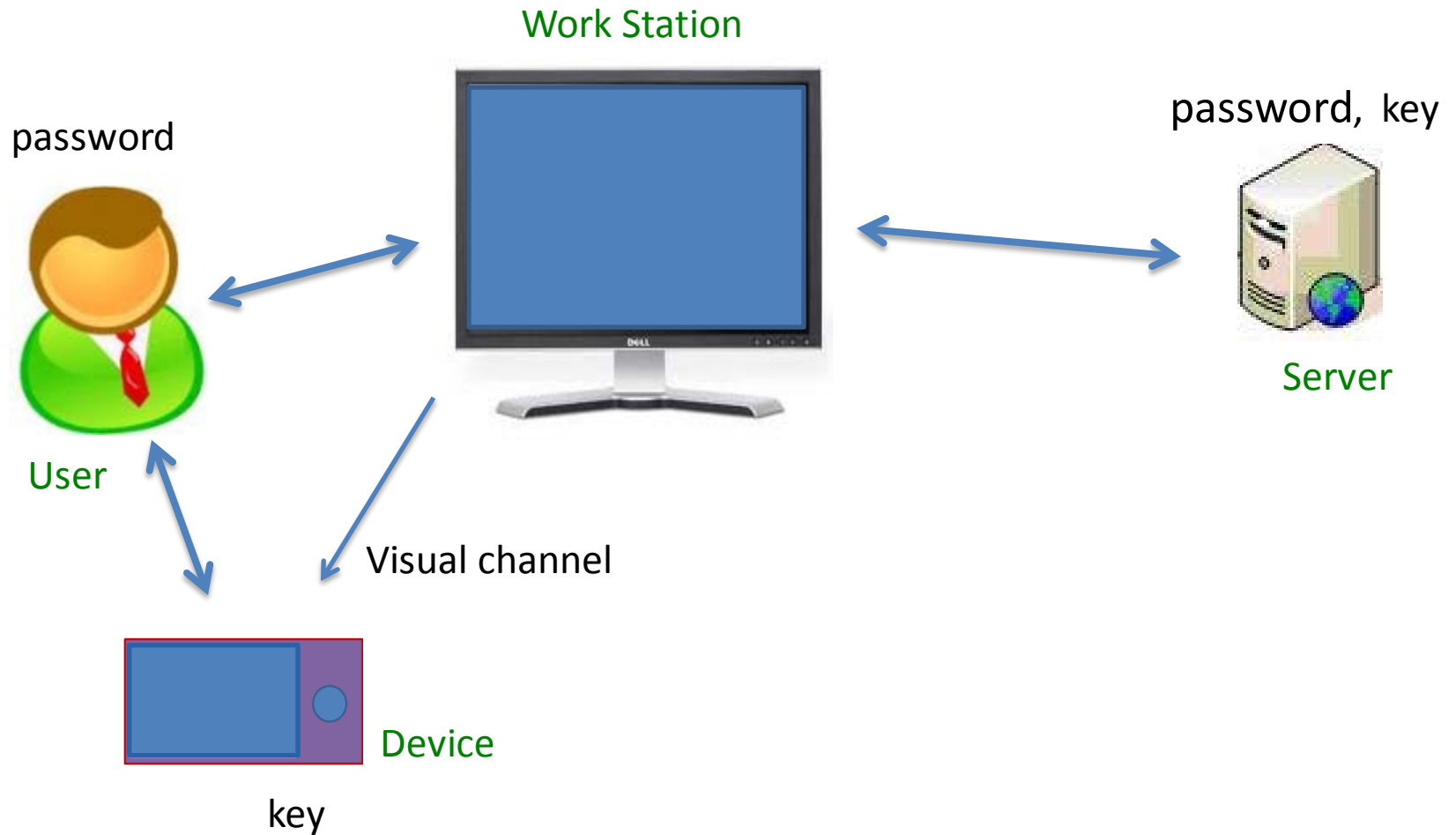


Related Work

- [Sharp2006]: Blur the sensitive information in the work station, display the region around the mouse pointer in mobile device.



Our Scheme: Setting



Two Adversary Models

- Model 1: the mobile device is honest the terminal is could be compromised, we want to achieve confidentiality and authenticity;
- Model 2: both the mobile device and the terminal could be compromised, but they cannot collude, we want to achieve authenticity.

Model 1 (Mobile Device is Honest)

My Bank

Shortcuts Please select Logout

Account Summary How do I ...
Select a topic

Transaction Date	Reference No.	Description	Amount
5-Jun-10	GIRO 51543858	Cash Withdrawal Atm	(\$30.00)
18-May-10	MST 24847813	Cash Deposit Atm	\$700.00
14-May-10	GIRO 24514421	Credit Card Purchase	(\$77.00)
11-May-10	EZT 51552115	Fund Transfer	\$300.00
5-May-10	EZT 51553812	Nets Cashcard Top Up	(\$30.00)
28-Apr-10	MST 23557542	Internet Purchase	(\$29.00)
25-Apr-10	EZT 51543858	Purchase Nets	(\$30.00)
12-Apr-10	INT 51542233	Interest Credit	\$131.32
11-Apr-10	EZT 51537815	Fund Transfer	\$300.00
8-Apr-10	GIRO 24502452	Credit Card Purchase	(\$699.99)
8-Apr-10	MST 23457244	Internet Purchase	(\$118.00)
4-Apr-10	GIRO 24454521	Credit Card Purchase	(\$721.50)
24-Mar-10	GIRO 24395451	Credit Card Purchase	(\$71.50)
18-Mar-10	EZT 51202457	Nets Cashcard Top Up	(\$60.00)
14-Mar-10	MST 23457244	Internet Purchase	(\$148.00)
12-Mar-10	GIRO 24321125	Credit Card Purchase	(\$321.95)
11-Mar-10	EZT 51158412	Fund Transfer	\$300.00

Sensitive information to be presented to the user.

Congratulations!
You have WON a \$5,000 rebate on myBank.com!
Click [here](#) for more information.

Model 1 Solution

The screenshot shows a web interface for 'My Bank'. At the top, there is a navigation bar with 'Shortcuts' and a dropdown menu, and a yellow 'Security and You | Logout' button. A left sidebar contains a menu with categories like 'My Account', 'My Summary', and 'Apply Online Resources'. The main content area features a table with four columns: 'Transaction Date', 'Reference No.', 'Description', and 'Amount'. Each cell in the table contains a 2D barcode. Below the table, there is a congratulatory message: 'congratulations!' with an image of stacks of money, and a bar chart showing data for four sessions.

Transaction Date	Reference No.	Description	Amount
[Barcode]	[Barcode]	[Barcode]	[Barcode]
[Barcode]	[Barcode]	[Barcode]	[Barcode]
[Barcode]	[Barcode]	[Barcode]	[Barcode]
[Barcode]	[Barcode]	[Barcode]	[Barcode]

congratulations!

You have WON a \$5,000 rebate on myBank.com!
Click [here](#) for more information.

Session	Blue	Red	Green
Session-1	4.3	2.4	2
Session-2	2.5	4.4	2
Session-3	3.5	1.8	3
Session-4	4.5	2.8	5

- (1) Non sensitive portions will be displayed as they are.
- (2) Sensitive information are replaced by specially designed 2D barcodes.

Model 1 Solution

The screenshot shows a web interface for 'My Bank'. At the top, there is a 'Shortcuts' dropdown menu and a 'Security and You | Logout' link. A left sidebar contains navigation links: My Account (Account History, Transaction History, Enquiry), My Summary, Apply Online Resources, My banking, My Credit/Debit Card, My Loan, My Interest, Help, Contact Us, and Site. The main content area features a table with columns: Transaction Date, Reference No., Description, and Amount. The table contains three rows of QR codes. A red-bordered box highlights a mobile device overlaying the second QR code, displaying a transaction list: 'Cash Withdrawal Atm (\$70.00)', 'Cash Deposit Atm \$ 790.00', and 'Credit Card Purchase (\$77.00)'. Below the table, there is a 'congratulations!' banner with an image of money and a bar chart showing data for four seasons.

Transaction Date	Reference No.	Description	Amount
[QR Code]	[QR Code]	[QR Code]	[QR Code]
[QR Code]	[QR Code]	[QR Code]	[QR Code]
[QR Code]	[QR Code]	[QR Code]	[QR Code]

congratulations!

You have WON a \$5,000 rebate on myBank.com!
Click [here](#) for more information.

Season	Blue	Red	Green
Season-1	4.3	2.4	2
Season-2	2.5	4.4	2
Season-3	3.5	1.8	3
Season-4	4.5	2.8	5

- (1) User verifies the order of the barcodes.
- (2) User moves the mobile device over the barcode.
- (3) Mobile device captures and verifies the barcodes, and displays the content.

Model 2 (Both Could Cheat)

My Bank

Shortcuts Please select Logout

Account Summary How do I ...
Select a topic

Transaction Date	Reference No.	Description	Amount
5-Jun-10	GIRO 51543858	Cash Withdrawal Atm	(\$30.00)
18-May-10	MST 24847813	Cash Deposit Atm	\$700.00
14-May-10	GIRO 24514421	Credit Card Purchase	(\$77.00)
11-May-10	EZT 51552115	Fund Transfer	\$300.00
5-May-10	EZT 51553812	Nets Cashcard Top Up	(\$30.00)
28-Apr-10	MST 23557542	Internet Purchase	(\$29.00)
25-Apr-10	EZT 51543858	Purchase Nets	(\$30.00)
12-Apr-10	INT 51542233	Interest Credit	\$131.32
11-Apr-10	EZT 51537815	Fund Transfer	\$300.00
8-Apr-10	GIRO 24502452	Credit Card Purchase	(\$699.99)
8-Apr-10	MST 23457244	Internet Purchase	(\$118.00)
4-Apr-10	GIRO 24454521	Credit Card Purchase	(\$721.50)
24-Mar-10	GIRO 24395451	Credit Card Purchase	(\$71.50)
18-Mar-10	EZT 51202457	Nets Cashcard Top Up	(\$60.00)
14-Mar-10	MST 23457244	Internet Purchase	(\$148.00)
12-Mar-10	GIRO 24321125	Credit Card Purchase	(\$321.95)
11-Mar-10	EZT 51158412	Fund Transfer	\$300.00

My Account

- Account History
- Transaction History
- Enquiry

My Summary

Apply Online Resources

My banking

My Credit/Debit Card

My Loan

My Interest

Help

Contact Us

Site

Congratulations!

You have WON a \$5,000 rebate on myBank.com!
Click [here](#) for more information.

Season	Blue Bar	Red Bar	Green Bar
Season 1	4.8	2.4	2
Season 2	2.5	4.4	2
Season 3	3.5	1.8	3
Season 4	4.5	2.8	5

Information which requires protection on authenticity.

Model 2 Solution

My Bank

Shortcuts Please select

Security and You | Logout

How do I ...
Select a topic

Transaction Date	Reference No.	Description	Amount
5-Jun-10	GIRO 51543858	Cash Withdrawal Atm	(\$30.00)
18-May-10	MST 24847813	Cash Deposit Atm	\$700.00
14-May-10	GIRO 24514421	Credit Card Purchase	(\$77.00)
11-May-10	EZT 51552115	Fund Transfer	\$300.00
5-May-10	EZT 51553812	Nets Cashcard Top Up	(\$30.00)
28-Apr-10	MST 23557542	Internet Purchase	(\$29.00)
25-Apr-10	EZT 51543858	Purchase Nets	(\$30.00)
12-Apr-10	INT 51542233	Interest Credit	\$131.32
11-Apr-10	EZT 51537815	Fund Transfer	\$300.00
8-Apr-10	GIRO 24502452	Credit Card Purchase	(\$699.99)
8-Apr-10	MST 23457244	Internet Purchase	(\$118.00)
4-Apr-10	GIRO 24454521	Credit Card Purchase	(\$721.50)
24-Mar-10	GIRO 24395451	Credit Card Purchase	(\$71.50)
18-Mar-10	EZT 51202457	Nets Cashcard Top Up	(\$60.00)
14-Mar-10	MST 23457244	Internet Purchase	(\$148.00)
12-Mar-10	GIRO 24321125	Credit Card Purchase	(\$321.95)
11-Mar-10	EZT 51158412	Fund Transfer	\$300.00

The transaction information is displayed together with their barcodes.

Congratulations!

You have WON a \$5,000 rebate on myBank.com!
Click [here](#) for more information.

Season	Bar 1	Bar 2	Bar 3
Season 1	4.3	2.4	1.8
Season 2	2.5	4.4	1.7
Season 3	3.5	1.5	2.8
Season 4	4.5	2.1	5.0

Model 2 Solution

The screenshot shows a banking website with a navigation menu on the left, a top bar with 'Shortcuts' and 'Security and You | Logout', and a main content area. The main content area displays a table of transactions, a mobile device overlay showing a transaction amount, and a congratulatory message.

Transaction Date	Reference No.	Description
5-Jun-10	GIRO 51543858	Cash Withdrawal Atm
18-May-10	MST 24847813	Cash Deposit Atm
14-May-10	GIRO 24514421	Credit Card Purchase
11-May-10	EZT 51552115	Fund Transfer
5-May-10	EZT 51553812	Nets Cashcard Top Up
28-Apr-10	MST 23557542	Internet Purchase
25-Apr-10	EZT 51543858	Purchase Nets
12-Apr-10	INT 51542233	Interest Credit
11-Apr-10	EZT 51537815	Fund Transfer
8-Apr-10	GIRO 24502452	Credit Card Purchase
8-Apr-10	MST 23457244	Internet Purchase
4-Apr-10	GIRO 24454521	Credit Card Purchase
24-Mar-10	GIRO 24395451	Credit Card Purchase
18-Mar-10	EZT 51202457	Nets Cashcard Top Up
14-Mar-10	MST 23457244	Internet Purchase
12-Mar-10	GIRO 24321125	Credit Card Purchase
11-Mar-10	EZT 51158412	Fund Transfer

Congratulations!
 You have WON a \$5,000 rebate on myBank.com!
 Click [here](#) for more information.

Bar chart showing data for Season 1, Season 2, Season 3, and Season 4:

Season	Blue	Red	Green
Season 1	4.3	2.4	2
Season 2	2.5	4.8	2
Season 3	3.5	1.8	3
Season 4	4.5	2.8	5

- (1) User verifies the order of the barcodes.
- (2) User moves the mobile device over the barcode.
- (3) Mobile device captures and verifies the barcodes, and displays the content.
- (4) User verifies the transactions are consistent in device and work station.

Rearrangement Attacks

My Bank

Shortcuts Security and You | Logout

How do I ...

Transaction Date	Reference No.	Description	Amount
5-Jun-10	GIRO 51543858	Cash Withdrawal Atm	(\$30.00)
18-May-10	MST 24847813	Cash Deposit Atm	\$700.00
14-May-10	GIRO 24514421	Credit Card Purchase	(\$77.00)
11-May-10	EZT 51552115	Fund Transfer	\$300.00
5-May-10	EZT 51553812	Nets Cashcard Top Up	(\$30.00)
28-Apr-10	MST 23557542	Internet Purchase	(\$29.00)
25-Apr-10	EZT 51543858	Purchase Nets	(\$30.00)
12-Apr-10	INT 51542233	Internet Purchase	(\$29.00)
11-Apr-10	EZT 51537815	Fund Transfer	\$300.00
8-Apr-10	GIRO 24502452	Nets Cashcard Top Up	(\$30.00)
8-Apr-10	MST 23457244	Internet Purchase	(\$29.00)
4-Apr-10	GIRO 24454521	Purchase Nets	(\$30.00)
24-Mar-10	GIRO 24395451	Interest Credit	\$131.32

Congratulations!

You have WON a \$5,000 rebate on myBank.com!
 Click [here](#) for more information.

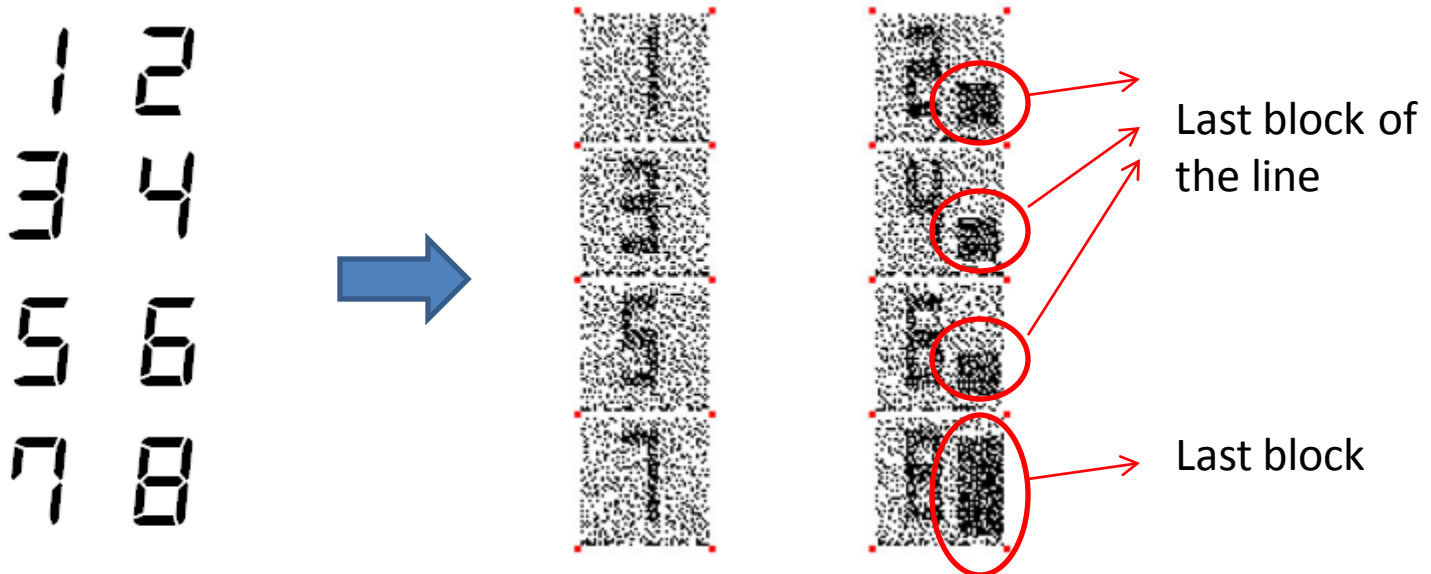
Season	Bar 1	Bar 2	Bar 3
Season 1	4.3	2.4	2
Season 2	2.5	4.4	2
Season 3	3.5	2.1	3
Season 4	4.5	2.8	5

Sub-Region Authentication

- Capture and decode one small region at a time.
 - It is subjected to rearrange/delete/duplicate attack
- Hardware limitation of mobile's camera
 - It cannot capture a whole screen with sufficient precision.
- Sub-region authentication problem:
 - how to authenticate the whole message using a device that can only verify one small region at a time.

Visual Inspection of Visual Cues

- Idea: bind the location information to the appearance of the barcodes.
- Example:



Our Design

2 bit message + 1 bit visual appearance + key \rightarrow 3 pixels

{00, 01, 10, 11}

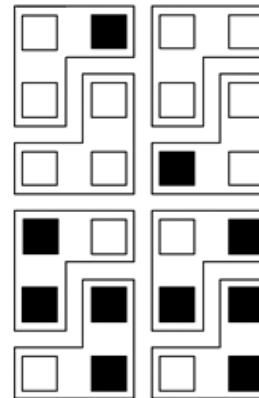
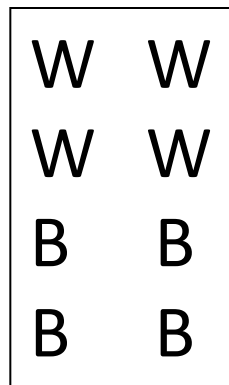
{W, B}

[1 ... 576]

$W = \left\{ \begin{array}{cc} \square & \square \\ \square & \square \end{array} \right\}$

$B = \left\{ \begin{array}{cc} \square & \blacksquare \\ \blacksquare & \square \end{array} \right\}$

L-blocks



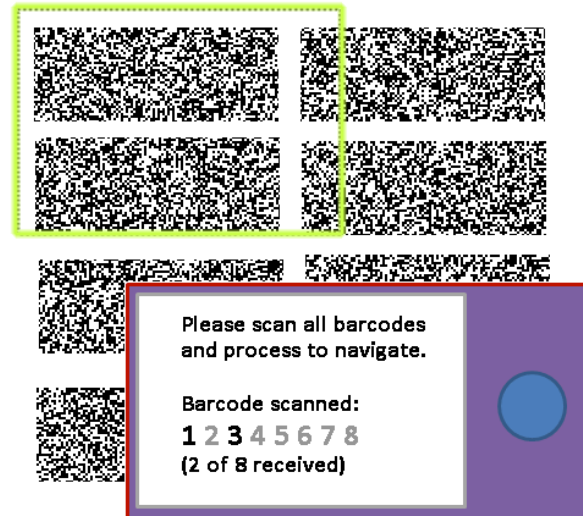
Our Design

- The arrangement is derived from session key. Hence, a malicious terminal who change a Black L-block to White L-block has $3/4$ chance of introducing error.
- To change the visual appearance, the adversary will need to change many L-blocks. This will destroy the barcode with high probability.

Alternative 1

- Use camera as a channel to send everything, then start browsing in mobile device.

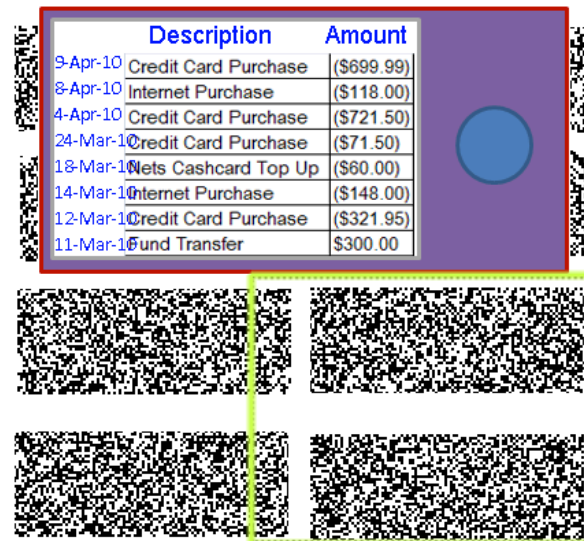
- (1) Less user-friendly to browse with small display.
- (2) Not easy to extend to cater dishonest mobile device.



Alternative 2

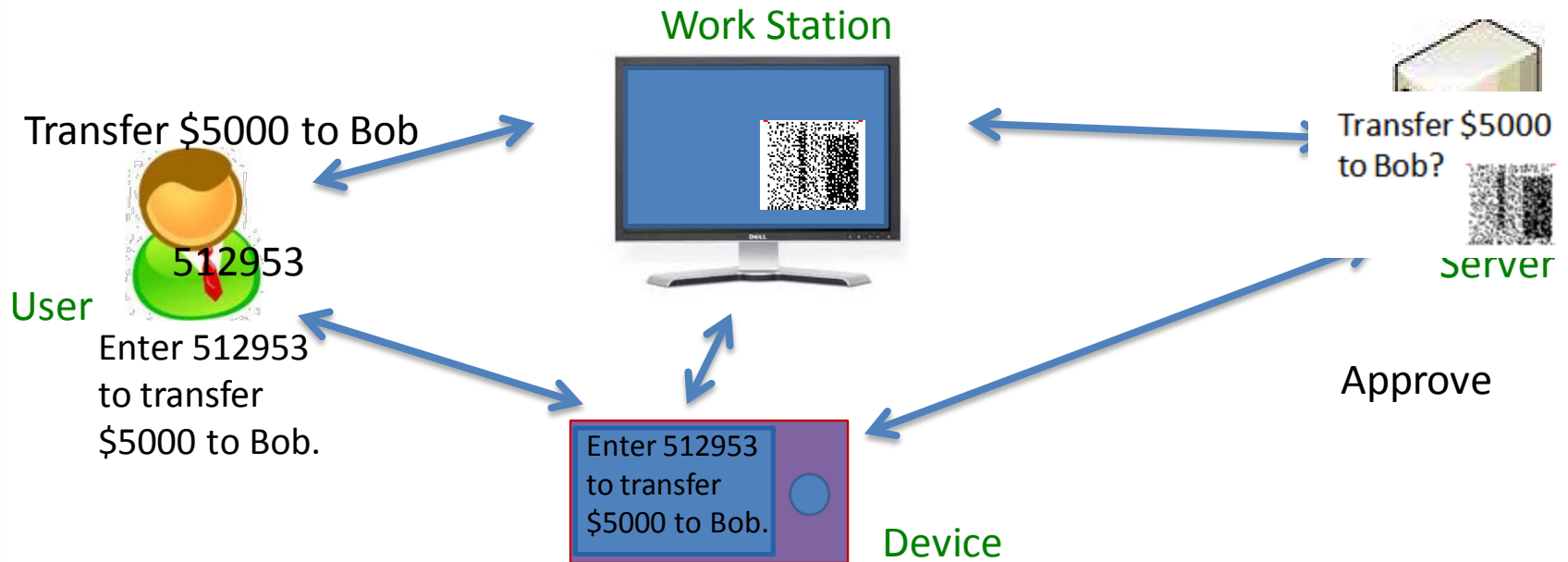
- Store location information (e.g. row names, column names) in the payload.

- (1) Not easy to prevent deletion and duplication attacks.
- (2) Only applicable for some table data.



	Description	Amount
9-Apr-10	Credit Card Purchase	(\$699.99)
8-Apr-10	Internet Purchase	(\$118.00)
4-Apr-10	Credit Card Purchase	(\$721.50)
24-Mar-10	Credit Card Purchase	(\$71.50)
18-Mar-10	Nets Cashcard Top Up	(\$60.00)
14-Mar-10	Internet Purchase	(\$148.00)
12-Mar-10	Credit Card Purchase	(\$321.95)
11-Mar-10	Fund Transfer	\$300.00

Send Message to Server



Comparison with Existing Work

- It can:
 - authenticate transaction content,
 - provide confidentiality when mobile is trusted.
- It requires:
 - mobile device has camera and display.
- It does NOT require:
 - installation in work station;
 - out-of-band channel;
 - mobile device to be trusted when confidentiality is not required.

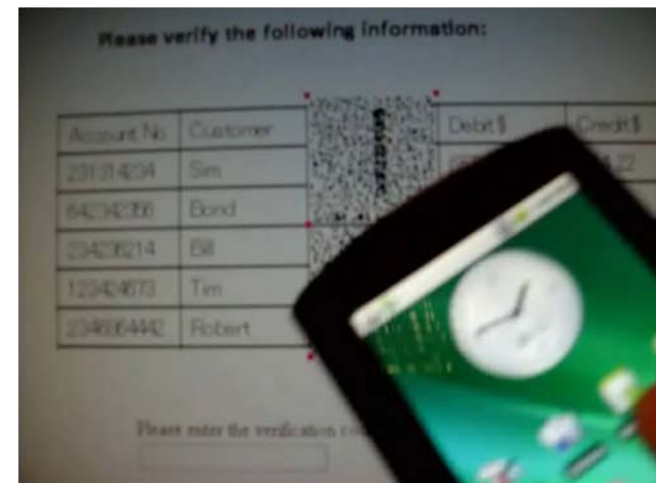
Proof-of-Concept Implementation

Programmed using Android API 1.6.

Tested on 3 phones: Acer Liquid, Motorola Milestone XT, HTC Legend;

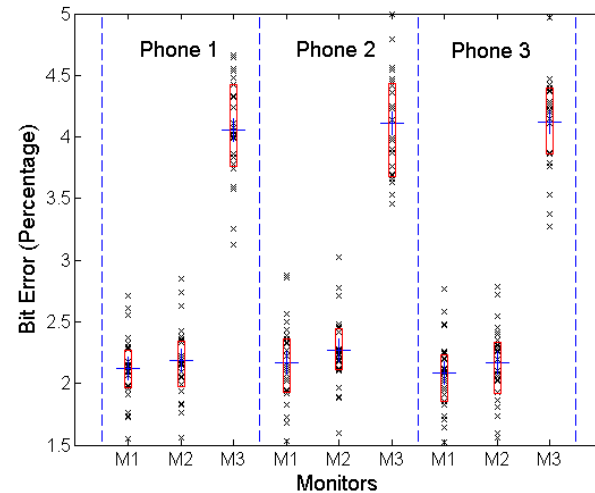
Tested on 3 monitors:

- An 19 inch TFT monitor in Dell model Optiplex 755;
- A 13.3 inches display of a Toshiba portege M900 laptop;
- A 15 inch Dell CRT monitor.



Performance

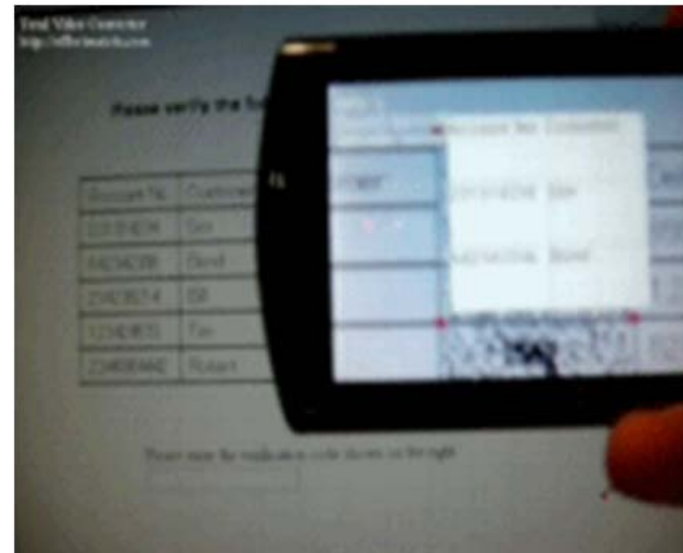
- Decoding rate: around 5 frames per second.
- Bit error rate:



- A barcode of 50 by 50 can carry around 952 bits message, and is able to correct 8% errors.

Proof-of-Concept Demo

- Proof-of-concept program running on Acer Liquid model,
- the webpage is rendered in a Dell model “Optiplex 755”, 19 inch TFT monitor.
- To improve user experience, we employ augmented reality framework, instead of requiring the user to manually take pictures.



Conclusions and Future works

- We designed a visual cue technique and show that this technique can help securing interactions.
- Our proof-of-concept implementation shows that such system is feasible to run in mobile devices.
- Our solution serves as an interesting example where authentication is carried out by coupling computer processing power and human perceptual system.
- The visual cue technique could potentially have other applications.



Thank you!