Usability and Security of Out-Of-Band Channels in Secure Device Pairing Protocols

Ronald Kainda, Ivan Flechais, and A.W. Roscoe

Oxford University Computing Laboratory

Concurrency Verification and Security Seminar

10 July, 2009

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

Introduction - Device Pairing

Scenario

Introduction - Device Pairing

Human-Interactive Security Protocols (HISPs)

(Nguyen and Roscoe, 2006)

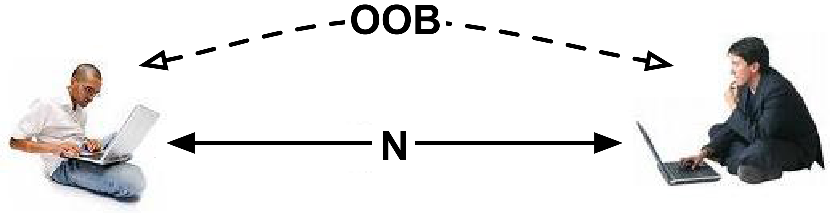
1. $\forall A \longrightarrow_N \forall A' : A, INFO_A, longhash(A, k_A)$
2. $\forall A \longrightarrow_N \forall A' : k_A$
3. $\forall A \longrightarrow_E \forall A'$:users compare *Digest(k*,INFOS)* where k* is the XOR of all the $k'_A s$ for A $\in$ G

Introduction - Device Pairing

Human-Interactive Security Protocols (HISPs)

(Nguyen and Roscoe, 2006)

1. $\forall A \longrightarrow_N \forall A' : A, INFO_A, longhash(A, k_A)$
2. $\forall A \longrightarrow_N \forall A' : k_A$
3. $\forall A \longrightarrow_E \forall A'$:users compare *Digest(k*,INFOS)* where k* is the XOR of all the $k'_A s$ for A $\in$ G



Introduction - HISPs

Security in HISPs

Technical security

- Security based on formal proofs
- Relates to the size of the digest/fingerprint—2^b bits for most protocols

Introduction - HISPs

Security in HISPs

Technical security

- Security based on formal proofs
- Relates to the size of the digest/fingerprint—2^b bits for most protocols

Effective security

- Secure systems are socio-technical (Sasse et al.)
- Security of a protocol may depend on human effort
- Humans forget, make mistakes
- These mistakes may result in security failures
- Human failures are not covered by formal proofs
- Increasing technical security (value of b) may reduce effective security

Introduction - Research Question

- Are proposed OOB methods usably secure to guarantee specified technical security?

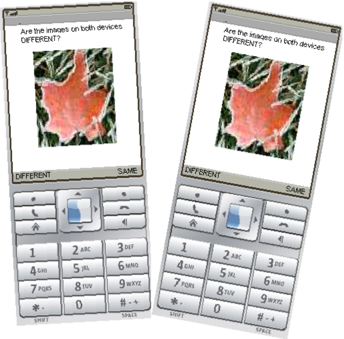
Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

HISPs - Proposed OOB Methods

Manual comparison

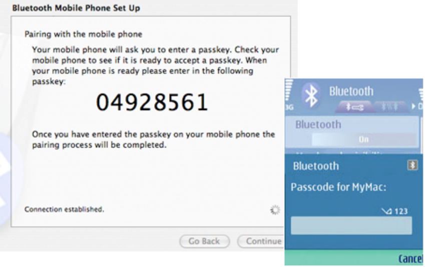
- Devices generate fingerprints
- Fingerprints displayed in appropriate format
- Users compare fingerprints and indicate on the device a match or lack of it
- Devices require display and some form of input method


Are the images on both devices DIFFERENT?
DIFFERENT
SAME
Are the images on both devices DIFFERENT?
DIFFERENT
SAME

HISPs - Proposed OOB Methods

Manual copying and entering

- One device displays a fingerprint
- User copies and types the fingerprint into one or more devices
- Requires display and keypad
- Efficiency of entry depends on affordances of devices involved



Bluetooth Mobile Phone Set Up

Pairing with the mobile phone

Your mobile phone will ask you to enter a passkey. Check your mobile phone to see if it is ready to accept a passkey. When your mobile phone is ready please enter in the following passkey:

04928561

Once you have entered the passkey on your mobile phone the pairing process will be completed.

Connection established.

Bluetooth

Passcode for MyMac:

HISPs - Proposed OOB Methods

Auxiliary devices

- Rely on secondary devices to transfer/compare information
- Proposed devices include
  - camera phone
  - external storage devices
  - data cable etc
- May require users to carry extra hardware

HISPs - Proposed OOB Methods

Short-range wireless channels

- Rely on short range wireless channels
- Require devices to be no more than a few centimetres apart
- Proposed methods include:
  - infra-red
  - light
  - distance bounding[1]
- Most methods lack human verification

[1] can also use normal channel

HISPs - Proposed OOB Methods

Timing methods

- Rely on transmission of information in well timed intervals
- Users coordinate the synchronisation
- Examples include
  - shaking devices (Saxena et al.)
  - pressing a button in response to some stimulus

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

Experimental Design - Methods

DEFINITIONS

Method

– refers to a specific mode of comparing/transferring information between devices by humans

Representation

– refers to specific format in which information is presented to users

Method-representation

– refers to a combination of a method and representation

Experimental Design - Method-representations

Compare & confirm

- Numeric
- Alphanumeric
- Words
- Sentences
- Country names
- Numeric & Sound
- Alphanumeric & Sound
- Melodies
- Images

Experimental Design - Method-representations

Compare & select

- Numeric
- Alphanumeric

Copy & enter

- Numeric
- Alphanumeric

Barcode

Experimental Design - Design

- A repeated measure design was used

Dependent variables

1. Time
2. Number of non-security failures
3. Number of security failures

Independent variable

1. Method-representation

Experimental Design - Participants

- 30 participants were recruited via online advertisement

Gender	Male: 47% Female: 53%
Age	18 - 25 40% 26 - 35 27% 36 - 45 13% 46 - 55 3% 56 - 65 13% 66 - 75 4%
Education	High School: 27% College: 27% Graduate: 26% Postgraduate: 20%

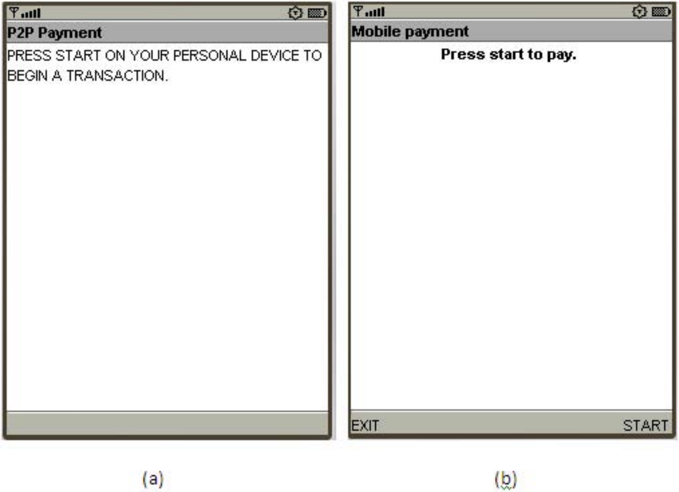
Experimental Design - Apparatus

- Devices: Nokia N95 and N73
  - Nokia devices are common
  - Bluetooth enabled
- Software:
  - P2P payment system
  - Device communication using Bluetooth
  - Software created a log of participant's actions
- Digital voice recorder
  - To record interviews
- Questionnaires
  - Enrolment
  - After scenario (AS)
  - After experiment/exit (AE)
- Written instructions

Experimental Design - Procedure

- Before study
  - Participants were sent an enrolment questionnaire
  - Sent brief description of the study and consent form
  - A day and time for the experiment was then agreed
- During study
  - Participants were presented with instructions on how to run the P2P
  - Participants thereafter followed instructions from the devices
  - The goal was to carry out a successful electronic money transaction
  - After each scenario, AS questionnaire was completed
  - After the experiment, AE questionnaire was completed and a short interview conducted

Experimental Design - Procedure: Tasks



P2P Payment

PRESS START ON YOUR PERSONAL DEVICE TO BEGIN A TRANSACTION.

(a)

Mobile payment

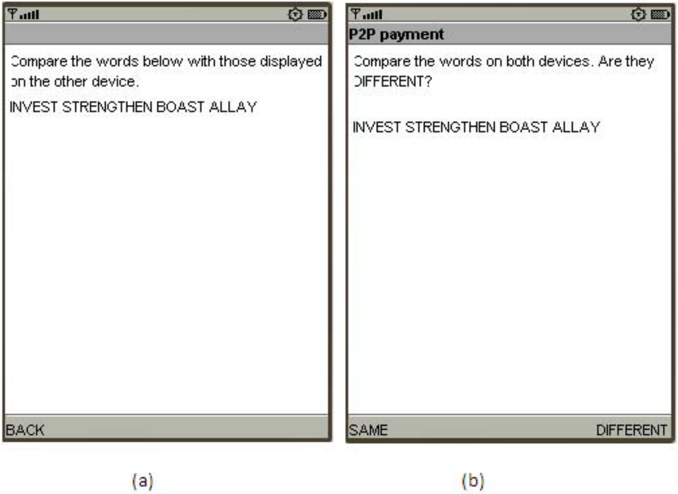
Press start to pay.

EXIT START

(b)

Figure: Step 1

Experimental Design - Procedure: Tasks



Compare the words below with those displayed on the other device.

INVEST STRENGTHEN BOAST ALLAY

(a)

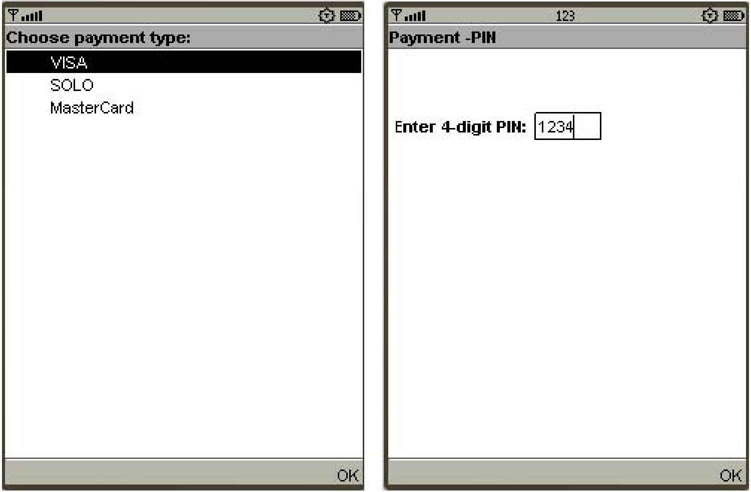
Compare the words on both devices. Are they DIFFERENT?

INVEST STRENGTHEN BOAST ALLAY

(b)

Figure: Step 2

Experimental Design–Procedure: Tasks



Choose payment type:

- VISA
- SOLO
- MasterCard

OK

123

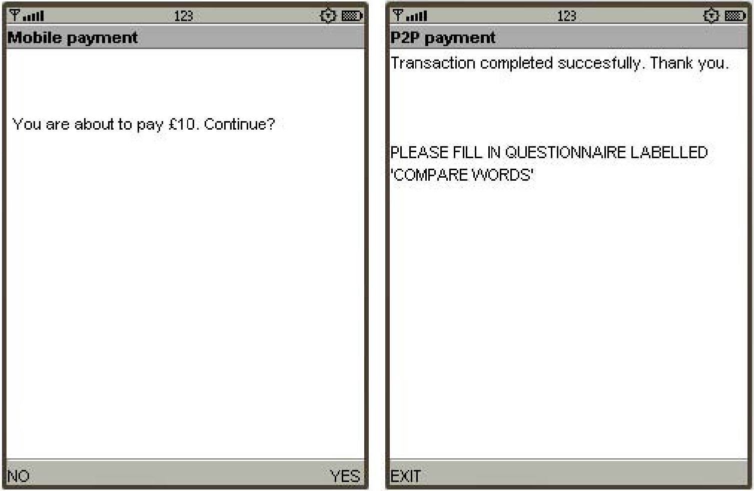
Payment -PIN

Enter 4-digit PIN: 1234

OK

Figure: Step 3 and 4

Experimental Design - Procedure: Tasks



Mobile payment

You are about to pay £10. Continue?

P2P payment

Transaction completed succesfully. Thank you.

PLEASE FILL IN QUESTIONNAIRE LABELLED 'COMPARE WORDS'

Figure: Step 5 and 6

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

Results - Compare & confirm: Errors and completion times

	Time (s)	Security failures	Non-security failures
	Mean	%	%
Numeric	6	0	3.3
Alphanumeric	6	13.3	16.7
Words	7	3.3	16.7
Images	8	0	3.3
Country/ City names	9	0	3.3
Sentences	11	0	16.7
Alphanumeric & sound	12	3.3	20
Numeric & sound	14	3.3	0
Melodies	24	6.7	36.7

Between-subjects: $p = 0.0007$ Within-subjects - time: $p =$

Results - Compare & select: Errors and completion times

	Time	Security failures	Non-security failures
	Seconds	%	%
Numeric	9	10	10
Alphanumeric	9	20	30

Between-subjects: $p = 0.0000$

Within-subjects - time: $p = 0.9255$

Results - Copy & enter: Errors and completion times

	Time	Non-security failures
	Seconds	%
Numeric	17	13
Alphanumeric	40	23

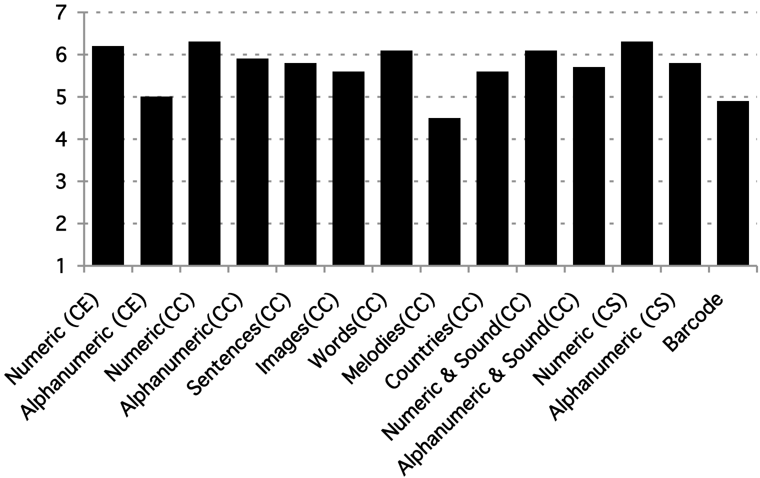
Beween-subjects: p = .7531

Within-subjects - time: p = .0004

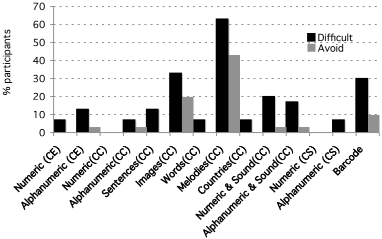
Results - Barcode: Errors and completion times

Time Seconds	Non-security failures %
37	53

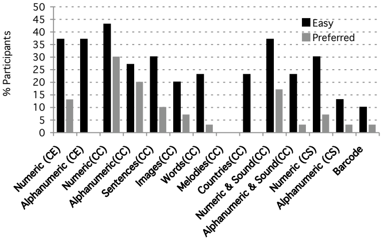
Results - ASQ scores



Results - Preferences



(a) Difficult

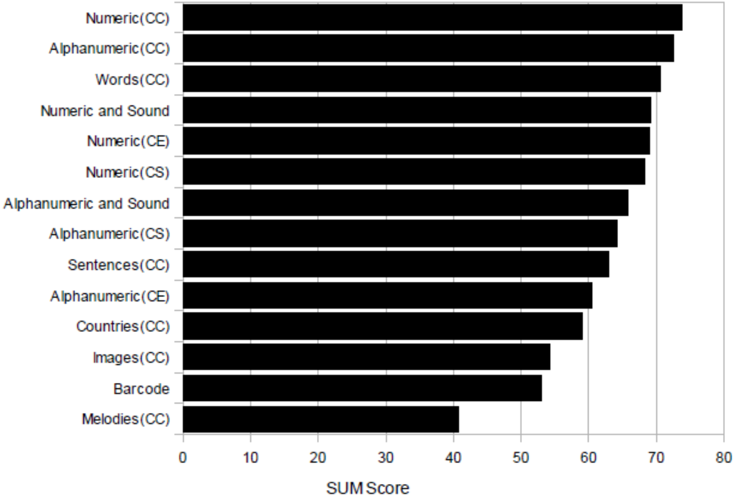


(b) Easy

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

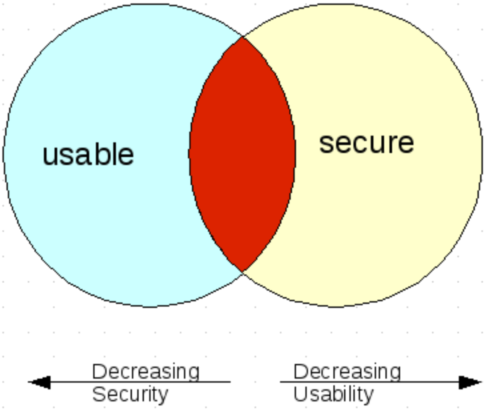
Analysis and Discussion – SUM Score Ranking



Analysis and Discussion – Ranking by Security Failures

	Subject to SF	SF	SUM Score
Numeric(CE)	No	0	69
Alphanumeric(CE)	No	0	60.4
Barcode	No	0	53
Numeric(CC)	Yes	0	73.7
Sentences(CC)	Yes	0	62.9
Countries(CC)	Yes	0	59.1
Images(CC)	Yes	0	54.3
Words(CC)	Yes	3.3	70.6
Numeric & sound	Yes	3.3	69.2
Alphanumeric & sound	Yes	3.3	65.8
Melodies(CC)	Yes	6.7	40.7
Numeric(CS)	Yes	10	68.3
Alphanumeric(CC)	Yes	13.3	72.5
Alphanumeric(CS)	Yes	20	64.2

Discussion and Discussion – Security Vs Usability trade-off



Analysis and Discussion – Security Vs Usability trade-off

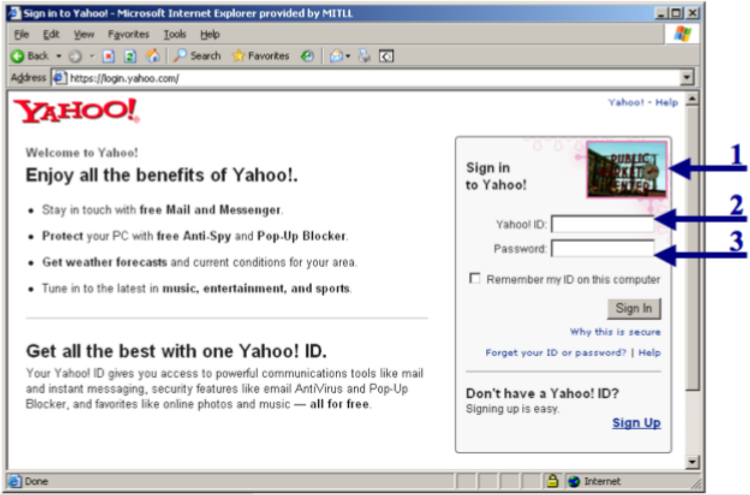
	Subject to SF	SF	SUM Score
Numeric(CE)[5]	No	0	69
Alphanumeric(CE)	No	0	60.4
Barcode	No	0	53
Numeric(CC)[1]	Yes	0	73.7
Sentences(CC)	Yes	0	62.9
Countries(CC)	Yes	0	59.1
Images(CC)	Yes	0	54.3
Words(CC)[3]	Yes	3.3	70.6
Numeric & sound[4]	Yes	3.3	69.2
Alphanumeric & sound	Yes	3.3	65.8
Melodies(CC)	Yes	6.7	40.7
Numeric(CS)	Yes	10	68.3
Alphanumeric(CC)[2]	Yes	13.3	72.5
Alphanumeric(CS)	Yes	20	64.2

Discussion – Security Vs Usability Considerations

- User conditioning

Discussion – Security Vs Usability Considerations

Example


Sign in to Yahoo! - Microsoft Internet Explorer provided by MITLL
File Edit View Favorites Tools Help
Back Search Favorites
Address https://login.yahoo.com/
YAHOO!
Yahoo! - Help
1
2
3
Done
Internet

Welcome to Yahoo!

Enjoy all the benefits of Yahoo!.

- Stay in touch with **free Mail and Messenger**.
- **Protect** your PC with **free Anti-Spy** and **Pop-Up Blocker**.
- **Get weather forecasts** and current conditions for your area.
- Tune in to the latest in **music, entertainment, and sports**.

Get all the best with one Yahoo! ID.

Your Yahoo! ID gives you access to powerful communications tools like mail and instant messaging, security features like email AntiVirus and Pop-Up Blocker, and favorites like online photos and music — **all for free**.

Sign in to Yahoo!

Yahoo! ID:

Password:

□ Remember my ID on this computer

Sign In

Why this is secure

Forget your ID or password? | Help

Don't have a Yahoo! ID?

Signing up is easy.

Sign Up

- (Schechter et al.)

Discussion – Security Vs Usability Considerations

- User conditioning
- User Motivation

Discussion – Security Vs Usability Considerations

- User conditioning
- User Motivation
- Security failures

Discussion – Security Vs Usability Considerations

- User conditioning
- User Motivation
- Security failures
- Attentiveness

Outline

1. Introduction
2. HISPs — Proposed OOB Methods
3. Experimental Design
4. Results
5. Analysis and Discussion
6. Conclusion

Conclusion

- Traditional methods are favoured by users
- Currently proposed methods need rethinking about their security/usability
- Security failures are not acceptable
- To achieve human compliance, enforcement is required
- Copy & enter is the best compromise
- There is a gap between formal proofs (technical security) and effective security

THANK YOU

Conclusion

Conclusion