PocketPIN

My Phone is my Keypad

Privacy-Enhanced PIN-Entry on Public Terminals

Bernhard Frauendienst

Betreuer: Dipl. Medieninf. Alexander De Luca
Verantw. Hochschullehrer: Prof. Dr. Heinrich Hußmann

Department of Media Informatics
Ludwig-Maximilians-University Munich

Oberseminar Sommersemester 2009
11.08.2009

Outline

Outline / Progress

What's wrong with the current situation?

Several ATM fraud methods:

- shoulder-surfing
  - "manually"
  - using a camera
- fake keypad overlays
- droplet (oil drops)

Cards are then copied or stolen using Skimming, a Lebanese Loop, or simply plain theft

$\Longrightarrow$ all attacks somehow rely on the ATMs keypad and its position

What's wrong with the current situation?

Several ATM fraud methods:

- shoulder-surfing
  - "manually"
  - using a camera
- fake keypad overlays
- droplet (oil drops)

Cards are then copied or stolen using Skimming, a Lebanese Loop, or simply plain theft

$\Longrightarrow$ all attacks somehow rely on the ATMs keypad and its position

What to do, what to do. . . ?

- Most approaches focus on making input harder to decipher
- *But:* if all attacks rely on the keypad, why not just take it away?
- Nearly everybody carries a mobile phone
  (which has a keypad just fine for PIN entry)
  $\Longrightarrow$ use the phone's keypad to enter the PIN

What to do, what to do. . . ?

- Most approaches focus on making input harder to decipher
- *But:* if all attacks rely on the keypad, why not just take it away?

- Nearly everybody carries a mobile phone
  (which has a keypad just fine for PIN entry)
  $\Longrightarrow$ use the phone's keypad to enter the PIN

What to do, what to do. . . ?

- Most approaches focus on making input harder to decipher
- *But:* if all attacks rely on the keypad, why not just take it away?

- Nearly everybody carries a mobile phone
  (which has a keypad just fine for PIN entry)
  $\Longrightarrow$ use the phone's keypad to enter the PIN

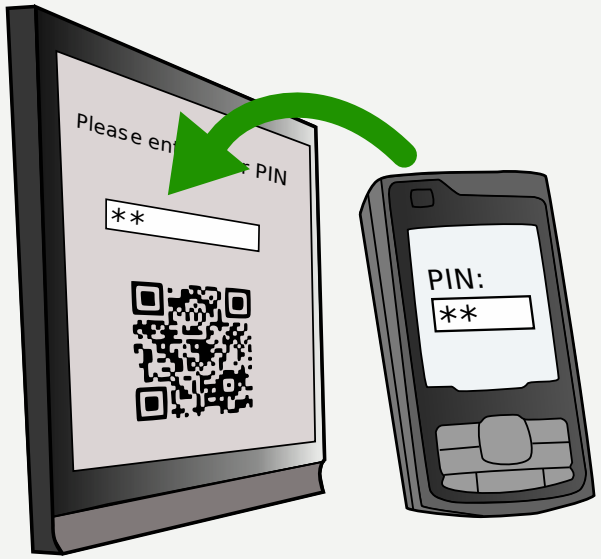
Outline / Progress

How does it work?

a. ATM displays a barcode
b. Mobile device captures/decodes the barcode and connects to the ATM
c. PIN is entered on the mobile and sent securely to the ATM

a.

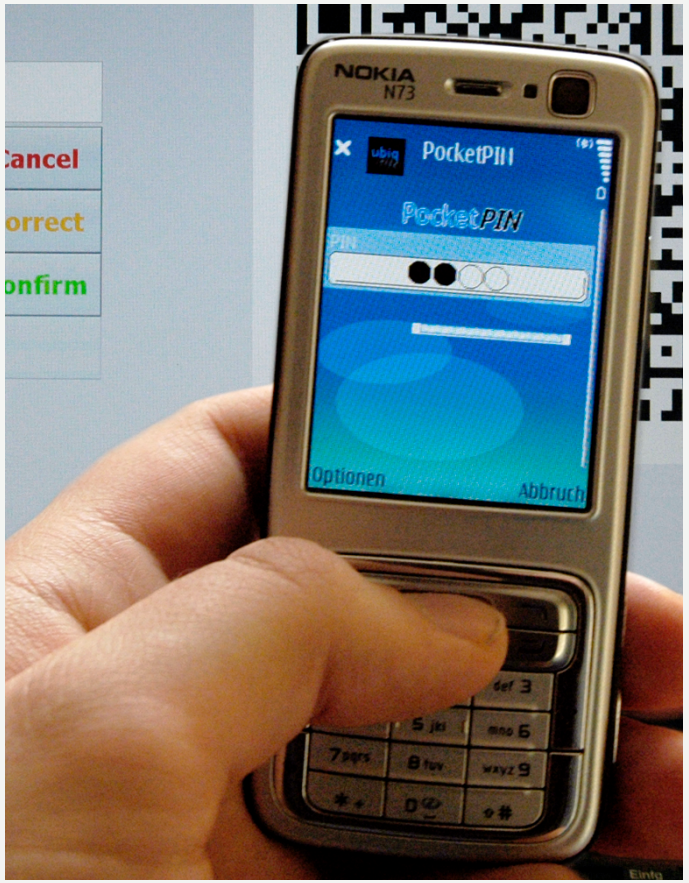
b.



c.

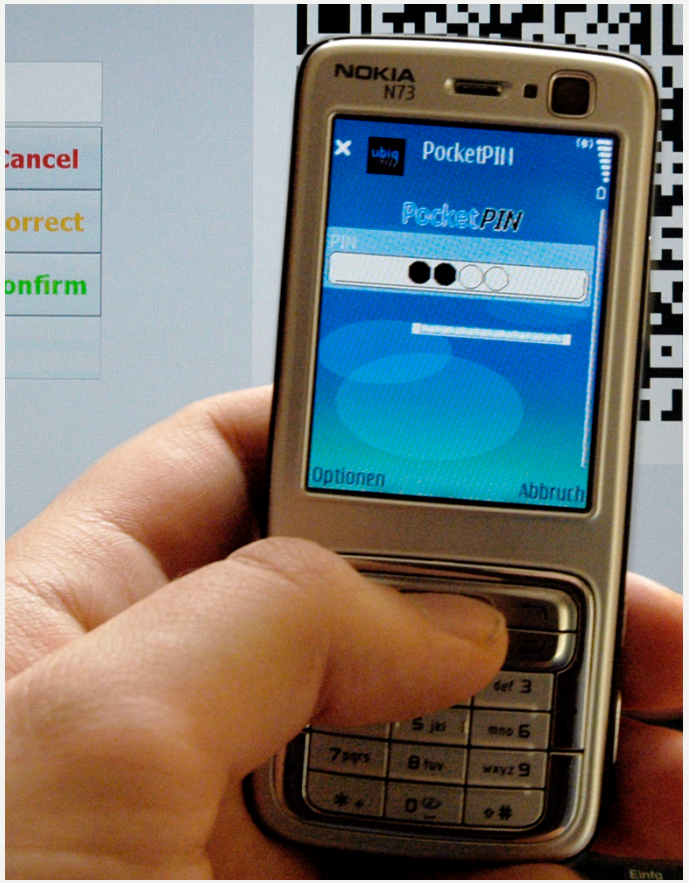
Prototype consists of two parts:

- a desktop application (JavaSE)
  - resembles the ATM (including a graphical keypad)
  - displays a 2D barcode
- a mobile application (JavaME)
  - uses the phone's camera to capture the barcode
  - decodes the barcode and connects to the ATM
  - lets the user enter the PIN number



Prototype consists of two parts:

- a desktop application (JavaSE)
  - resembles the ATM (including a graphical keypad)
  - displays a 2D barcode
- a mobile application (JavaME)
  - uses the phone's camera to capture the barcode
  - decodes the barcode and connects to the ATM
  - lets the user enter the PIN number

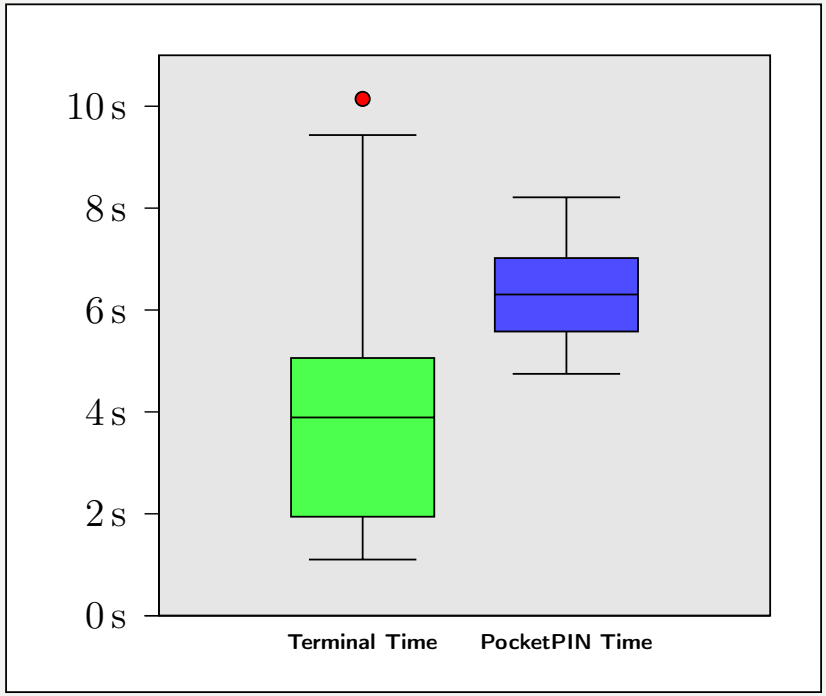


User Study

- 19 participants (avg. 25 yrs (min: 20, max: 32), 9 female/10 male)
- ATM usage: avg. 4.6 times/month (min: 1, max: 15)
- Repeated Measures – Factorial Design
- Independant variable: *input type*
  - PocketPIN
  - Keypad
- Dependant variables:
  - quantitative: *input speed*, *error rate* (automatically logged)
  - qualitative: *user satisfaction*, *experienced security* (questionnaire)
- Task: input 3 random PINs on the keyboard and the mobile device each

Results: Input Times

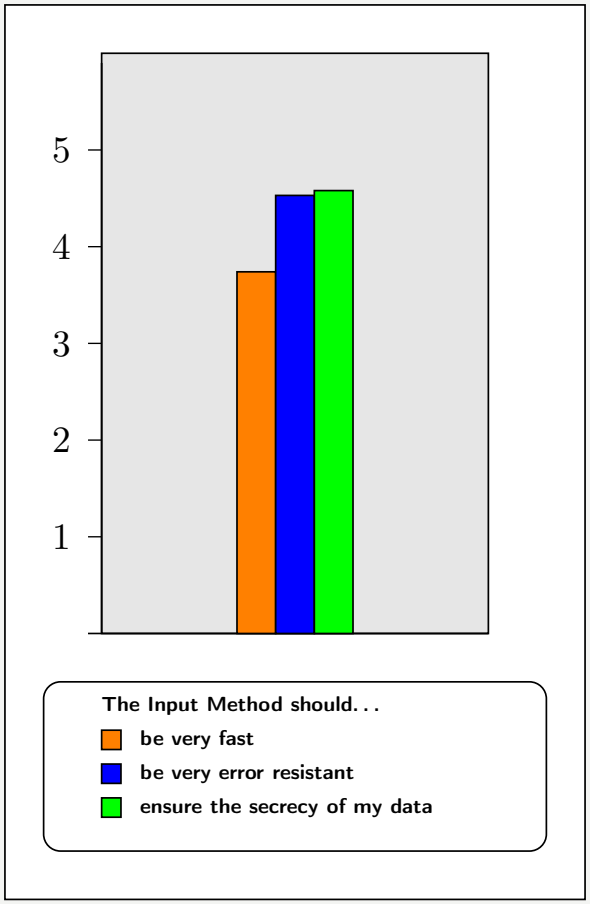
- Keyboard entry one third faster than MobilePIN (statistically significant)

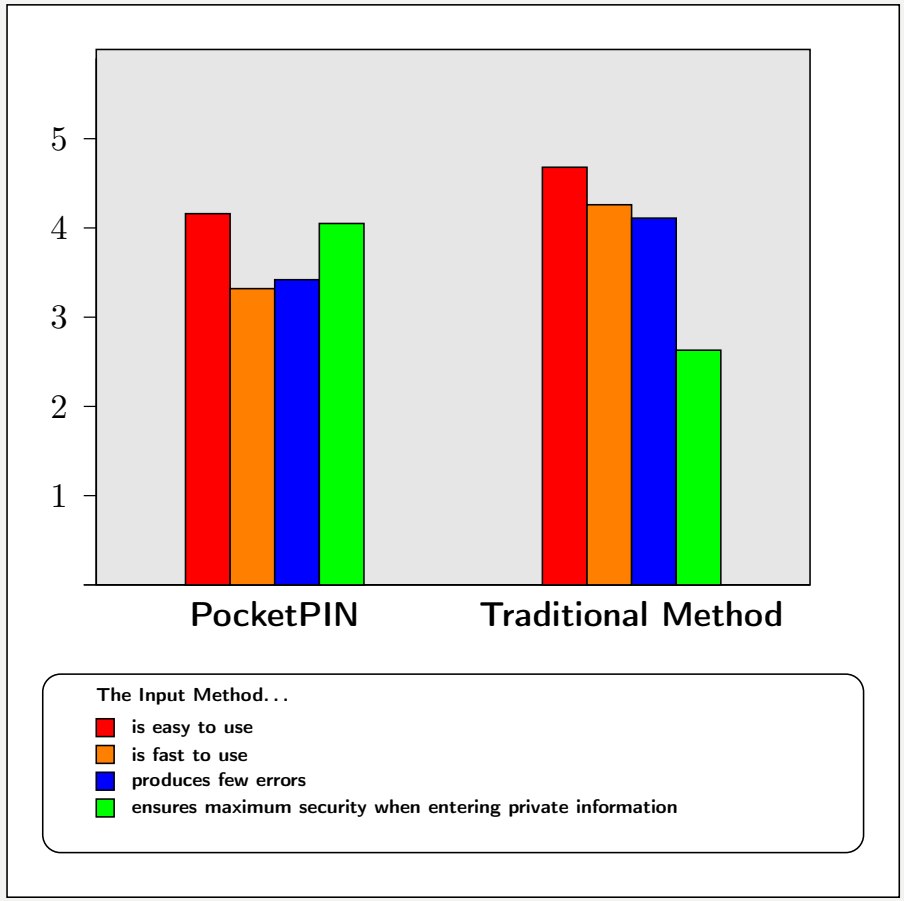


(Two extreme outliers removed for better overview)

- Unexpected result: error rates neglectably low on both input methods

Results: Usability and Privacy



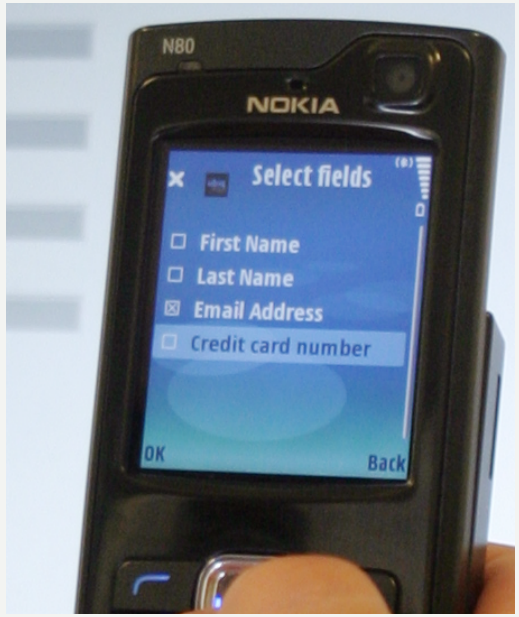


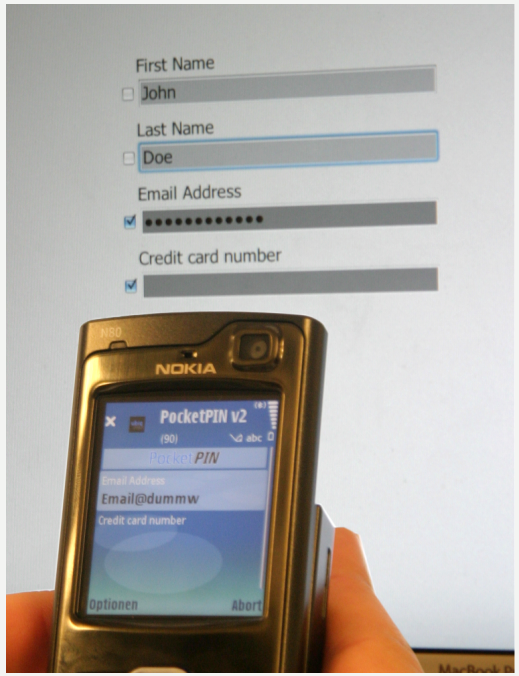
- Most users apply additional security measures when using ATMs
- Users can imagine using ATMs with PocketPIN (avg. score: 4.16)

Outline / Progress

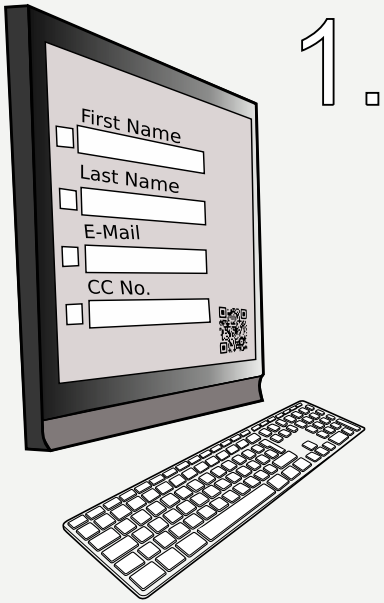
PocketPIN: A Privacy-Respectful Input Method for Public Terminals

- an extension of MobilePIN for private information input on public terminals
- allows not only PINs, but arbitrary content and fields
- users can choose which fields are deemed "private"
- "private" fields can be entered only on the mobile device and are obfuscated on the public display

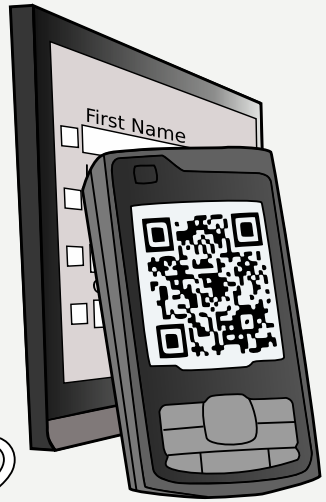




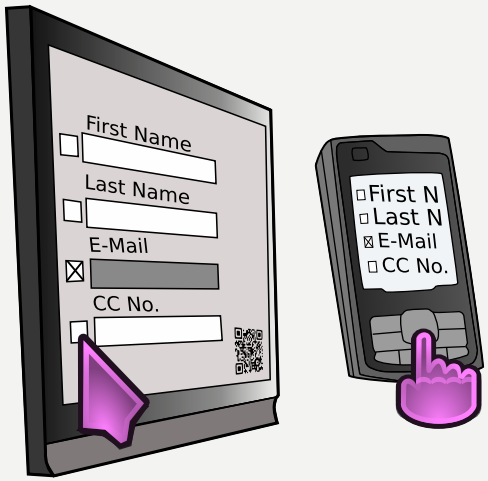
1.


First Name
Last Name
E-Mail
CC No.

2.


First Name

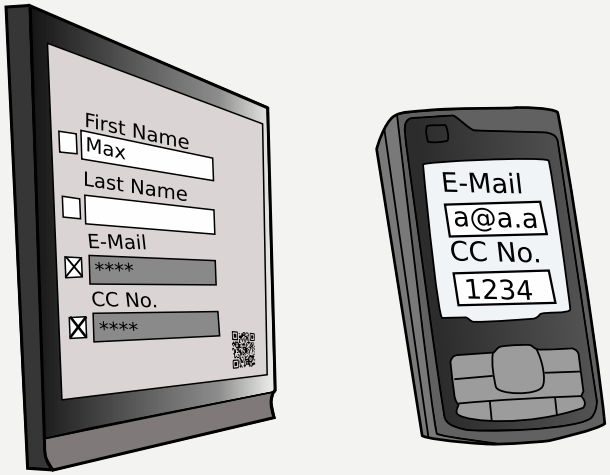
3.


First Name
Last Name
E-Mail
CC No.
First N
Last N
E-Mail
CC No.

4a.

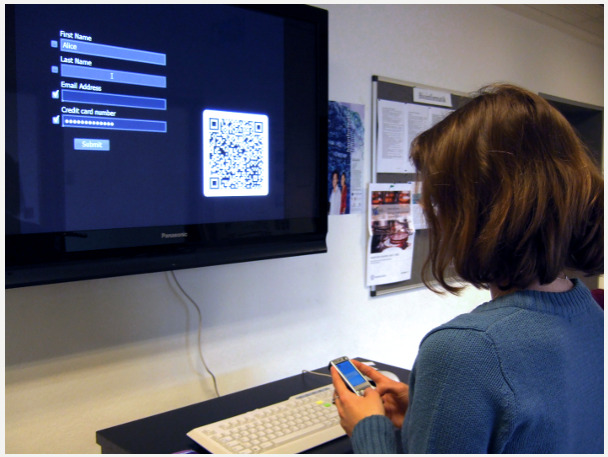

First Name
Max
Last Name
E-Mail
CC No.

4b.

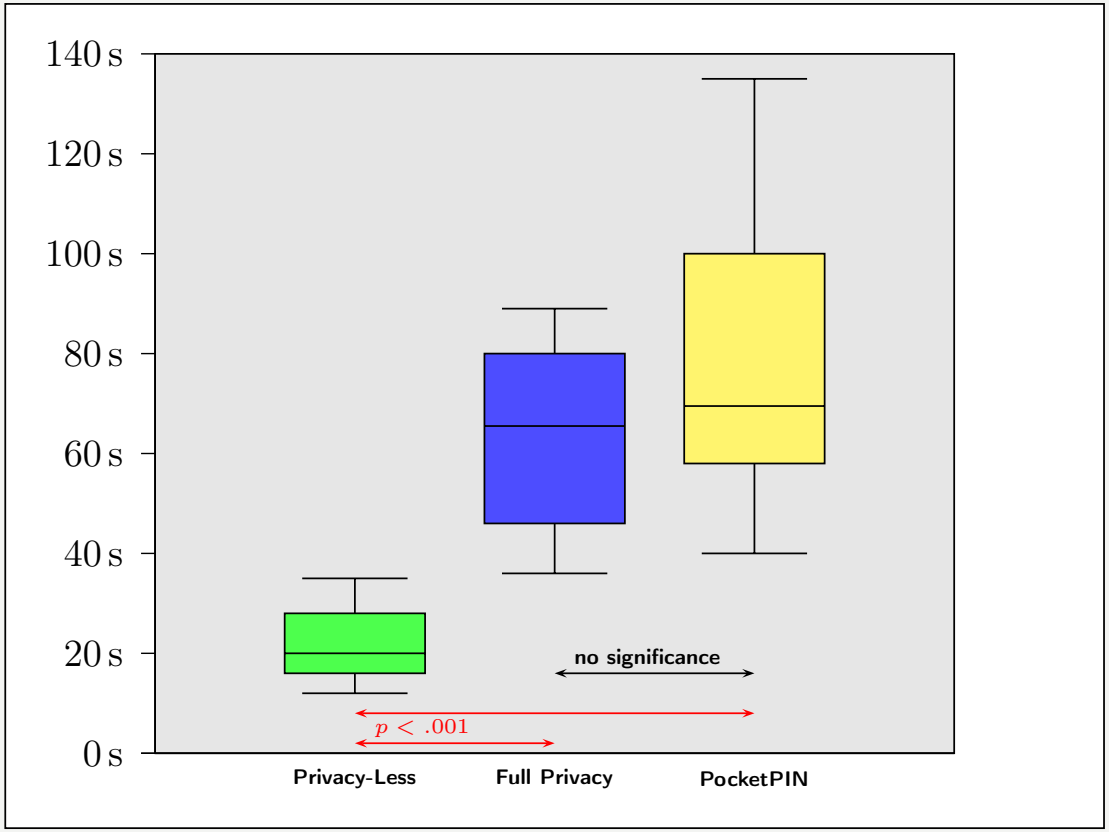

First Name
Max
Last Name
E-Mail
****
CC No.
****
E-Mail
a@a.a
CC No.
1234

User Study

- 12 participants (avg. 25 yrs (min: 21, max: 31), 4 female/8 male)
- all own a mobile phone and claim to have high experience
- Intra-Subject Factorial Design
- Independant variable: *privacy mode*
  - No Privacy
  - Full Privacy
  - Mixed Mode (PocketPIN)
- Dependant variables:
  - quantitative: *task completion time* (using a stop-watch)
  - qualitative: *user satisfaction*, *experienced privacy* (questionnaire)
- Order of modes was distributed uniformly amongst participants
- Task: enter First/Last Name, Email address and Credit Card Number in each mode (in PocketPIN mode the choice of "private" fields was left to each user)

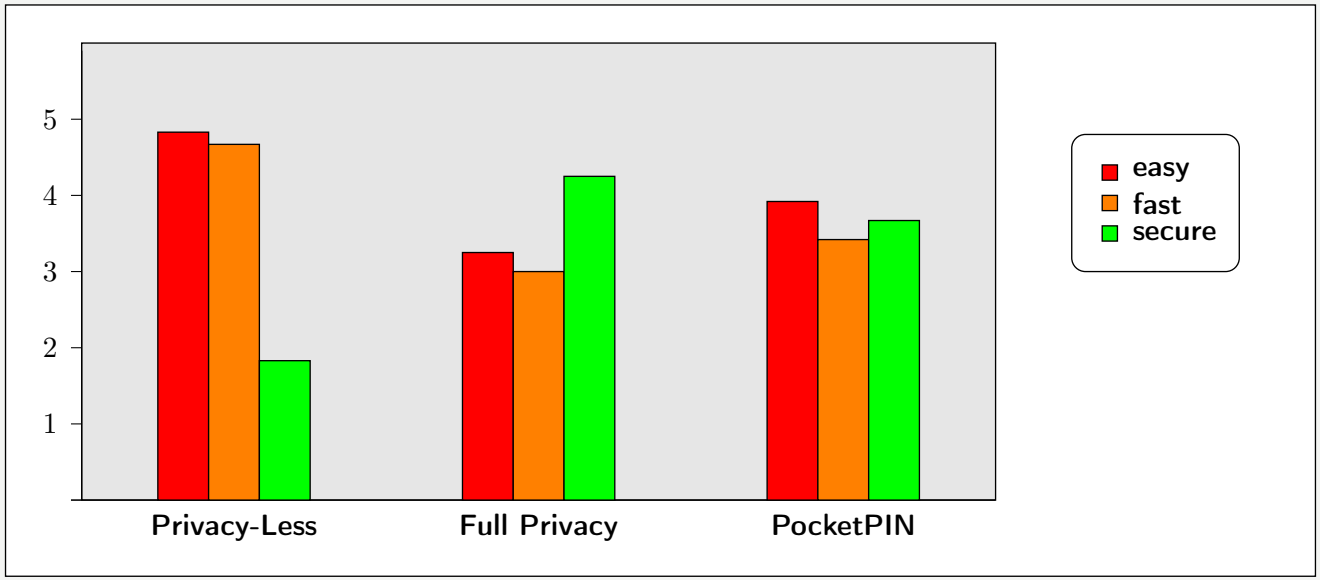


Results: Input Times



- Users starting with PocketPIN were faster in full private mode and vice versa (regardless of how many "private" fields they had selected)

Results: Usability and Privacy

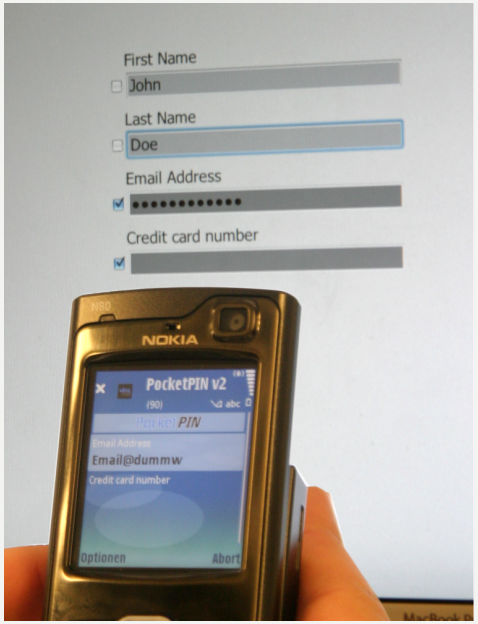


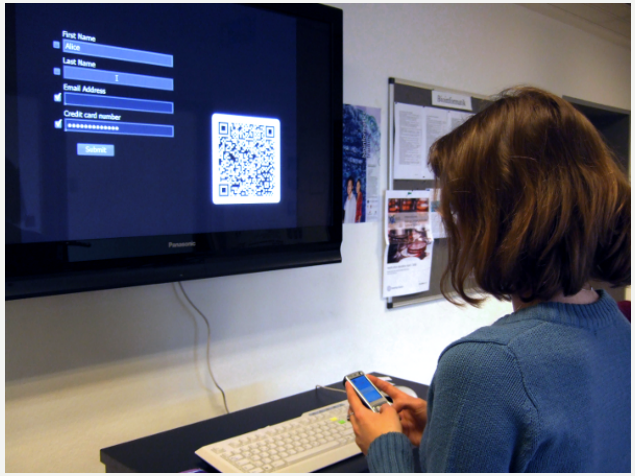
- 10/12 users would prefer to see *all* input fields (at least on short forms)

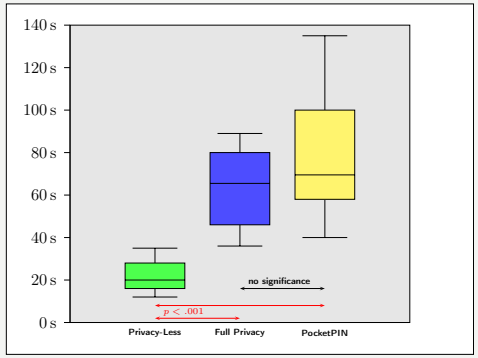
Outline / Progress

- 2D [QRCode™] marker contains:
  - [Bluetooth™] address of the ATM
  - [MD5] hash of the ATM's public [RSA] key
  - a challenge token

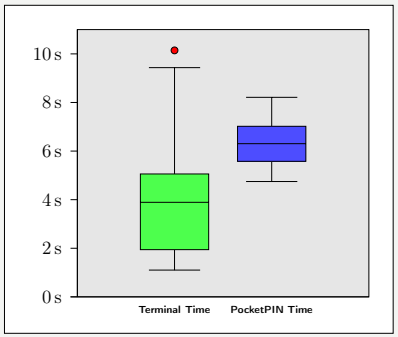
- after capturing, the mobile device connects to the given address
- the ATM sends its public key unencrypted, which the mobile compares to the given hashcode
- the mobile device sends the given challenge encrypted to the ATM
  $\Longrightarrow$ ATM knows the mobile read the marker
- the mobile sends a random challenge which the ATM decrypts and sends back
  $\Longrightarrow$ mobile knows the ATM actually has the right private key
- due to the low entropy (in MobilePIN only numbers 0-9 and some few control characters), messages are padded [using OAEP]

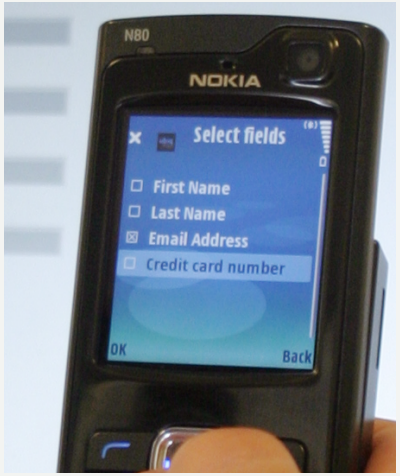

First Name
John
Last Name
Doe
Email Address
Credit card number
NOKIA
PocketPIN v2
Email@dummw
Optionen
Abort

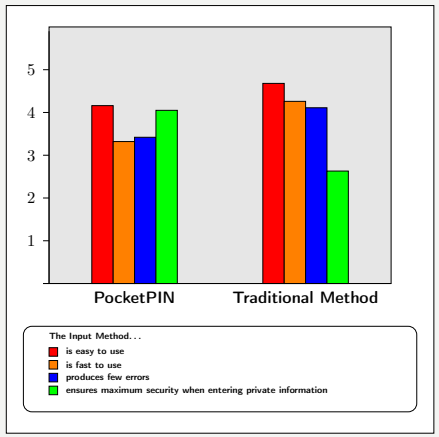



140 s
120 s
100 s
80 s
60 s
40 s
20 s
0 s
no significance
p < .001
Privacy-Less
Full Privacy
PocketPIN

Questions?


10 s
8 s
6 s
4 s
2 s
0 s
Terminal Time
PocketPIN Time


N80
NOKIA
Select fields
First Name
Last Name
Email Address
Credit card number
OK
Back


5
4
3
2
1
PocketPIN
Traditional Method
The Input Method...
is easy to use
is fast to use
produces few errors
ensures maximum security when entering private information


NOKIA
N73
PocketPIN
Optionen
Abbruch

Related Work

- Eye-Gaze based authentification/password entry (e.g. Kumar et al.; De Luca et al.)
- Increasing input complexity (e.g. Tan et al.: two-step character selection; Moncur et al.: graphical passwords; Roth et al.)
- Biometrics (e.g. Coventry et al.)
- Additional hardware (e.g. Patel et al.: accelerometer data; Deyle et al. or Sasamoto et al.: tactile feedback)
- Using mobile devices to display censored regions of the screen (Sharp et al.)