



a new perspective on  
user authentication on touch devices

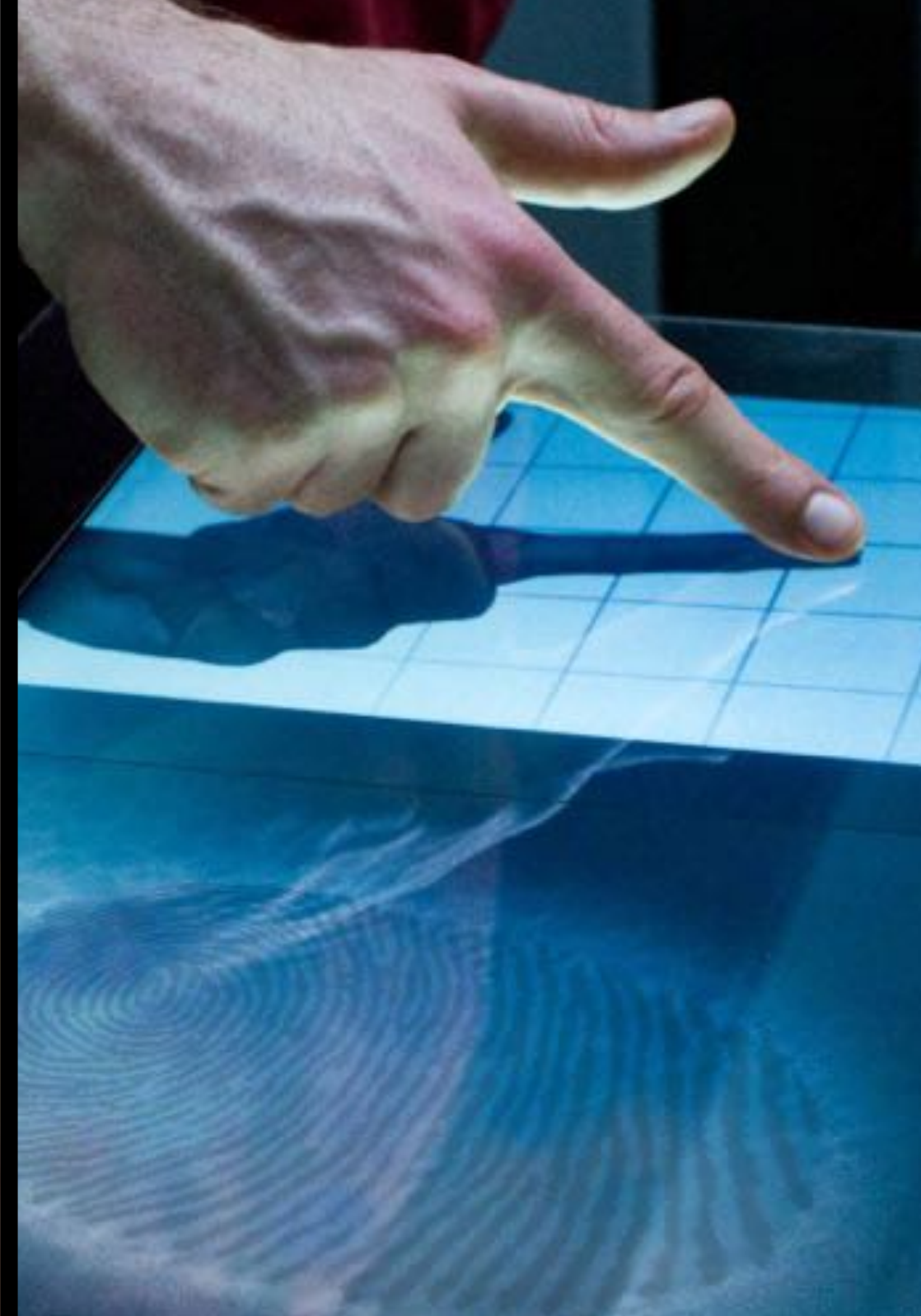
prof. dr. christian holz · department of computer science

**ETH** zürich  
sensing,  
interaction &  
perception lab





1 two factor authentication



2 touchscreens and fingerprints



3 a new model for authentication



AIX Version 4  
(C) Copyrights by IBM and by others 1982, 1996.  
login: \* /

INFO 5

LINK



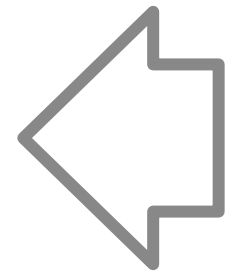
1) type in passcode

2) interact (start apps, access emails, ...)

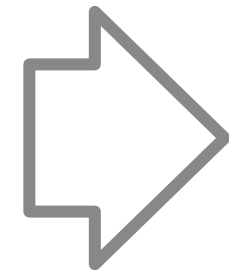
typical process



security



user  
authentication



convenience

something you know

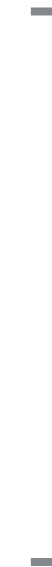
passwords

something you have

key, access token, ...

something you are

biometrics



+ combinations  
of these factors

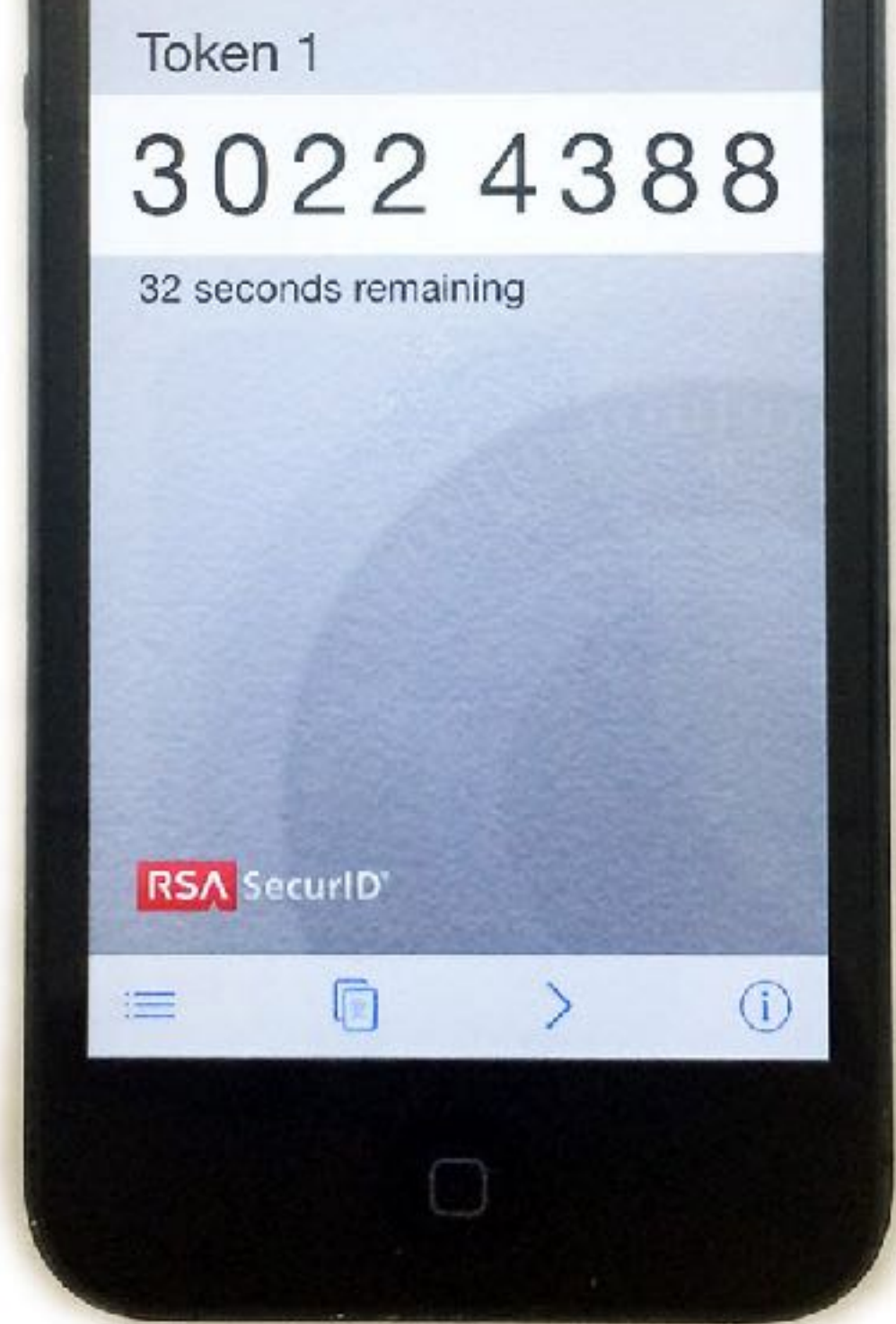
secure authentication

passwords...



keys and tokens





keys and tokens



two-factor  
authentication



## Enter code

Because you've turned on two-step verification, we need to verify your identity. Enter the code generated by your authenticator app.

I sign in frequently on this device. Don't ask me for a code.

If you can't use an app right now, [get a code a different way.](#)

Cancel

Submit

[Terms of Use](#)

[Privacy & Cookies](#)

## 2-step verification

Enter the verification code sent to your phone number ending in **65**.

Enter code:

Verify

Trust this computer

We won't ask you for a code again when we recognize one of your trusted computers. [Learn more](#)



Didn't receive the text message?

- [Call your phone ending in 65](#)  
In some cases, voice calls can work when SMS delivery is unreliable.
- [Don't have your phone?](#)

[Cancel](#)

additional login protection



only **6.4%**

two-step verification-enabled Google accounts  
of 900 million users

6.4%

two-step verification-enabled  
of 900 million users

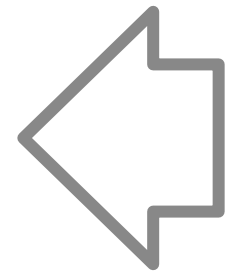
2014

10%

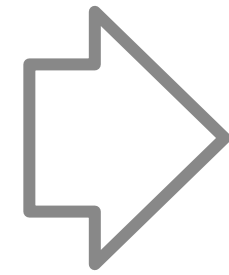
two-step verification-enabled  
of 1.5 billion users

2018

security



user  
authentication

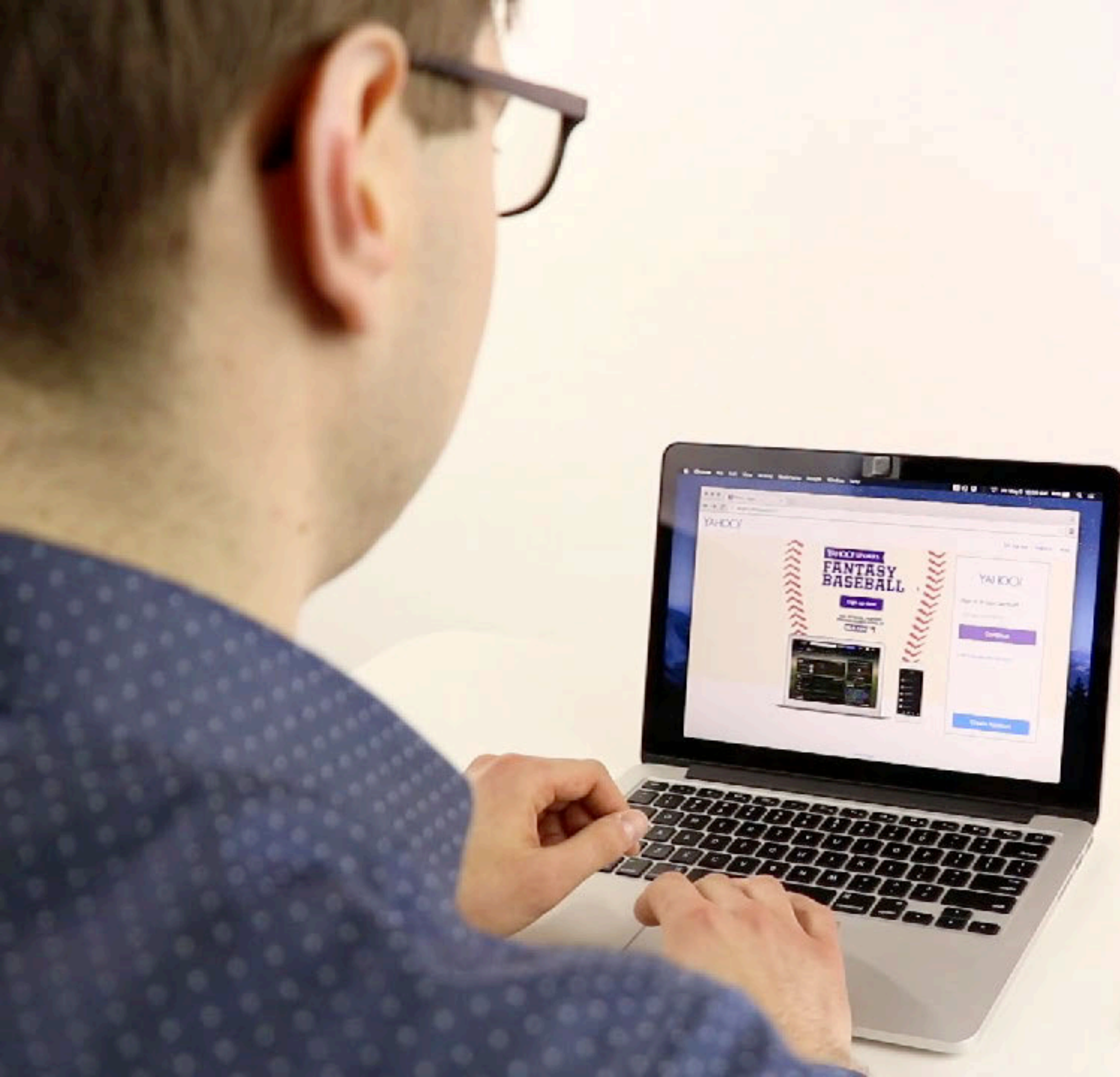


convenience

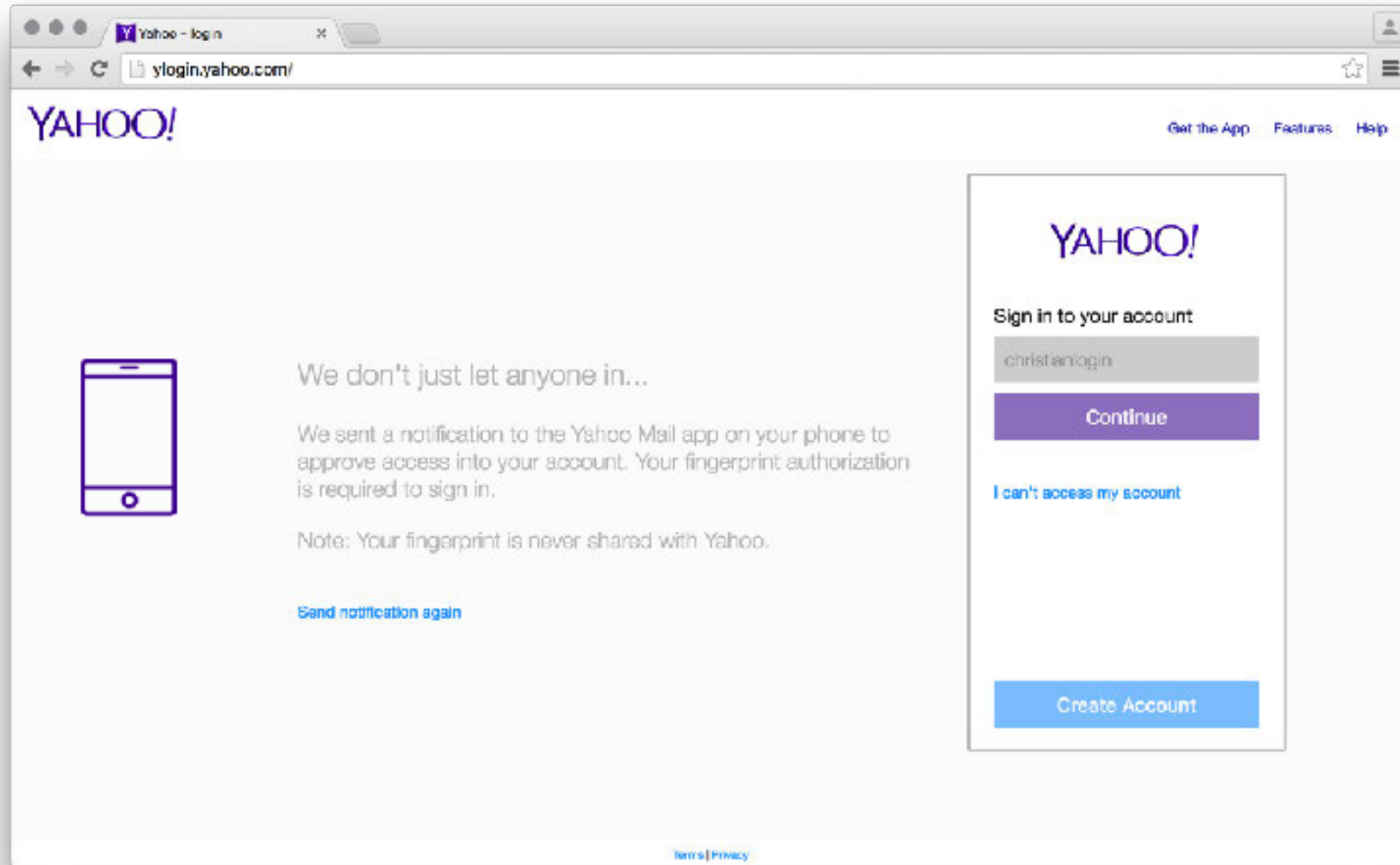


# 20 seconds

overhead of two-step verification



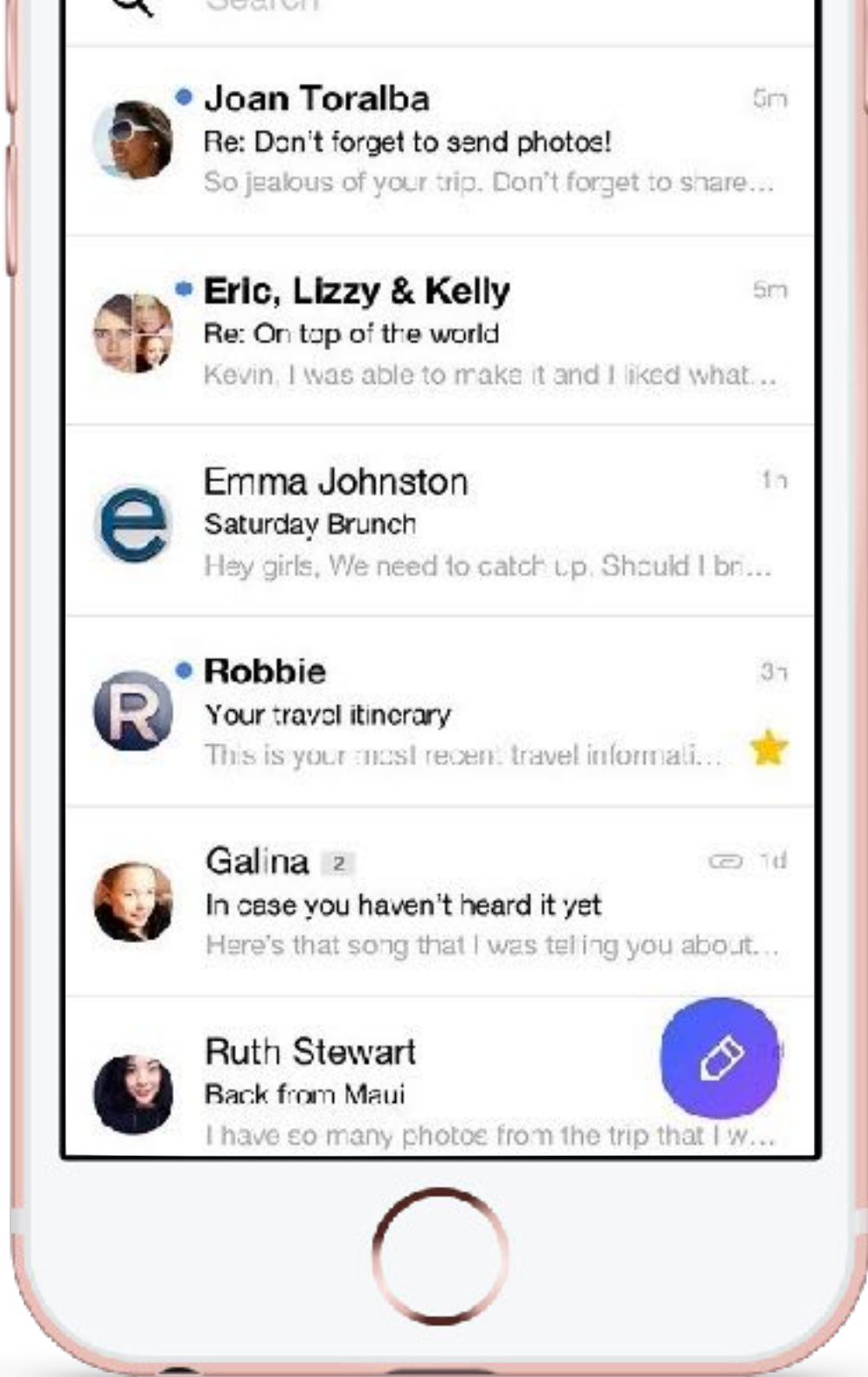
introducing  
**on-demand biometrics**  
fast, secure, and convenient web logins



on-demand biometrics

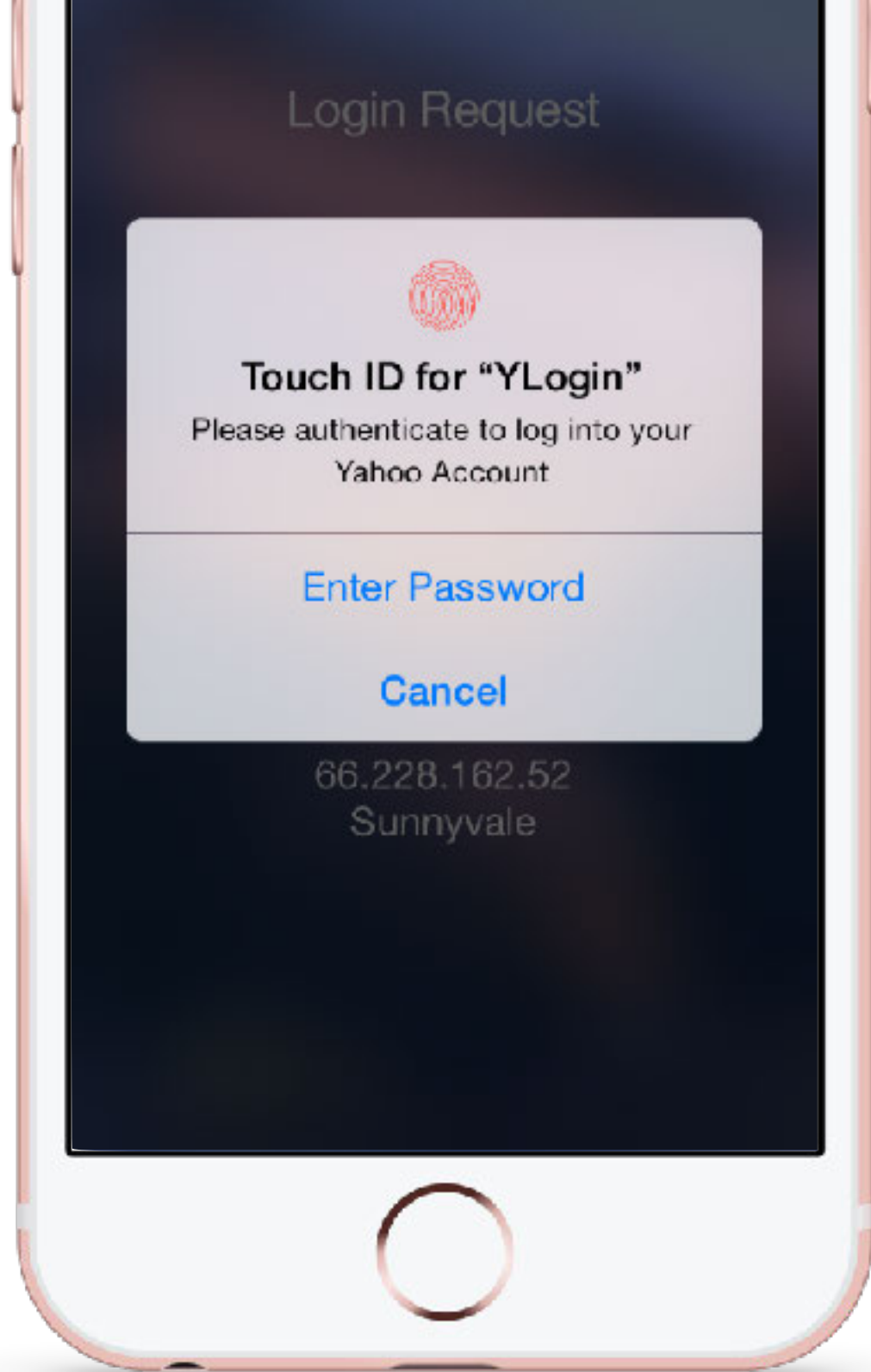
replaced login mechanism  
for Yahoo account on the web





on-demand biometrics

authentication integrated  
into Yahoo Mail on iOS



on-demand biometrics

authentication integrated  
into Yahoo Mail on iOS

email inboxes, social media, content apps contain sensitive data worth protecting

on-demand biometrics

**reduce effort** during login

are simple and **convenient**

result in **high acceptance** and **retention**

usability evaluation: resulting themes





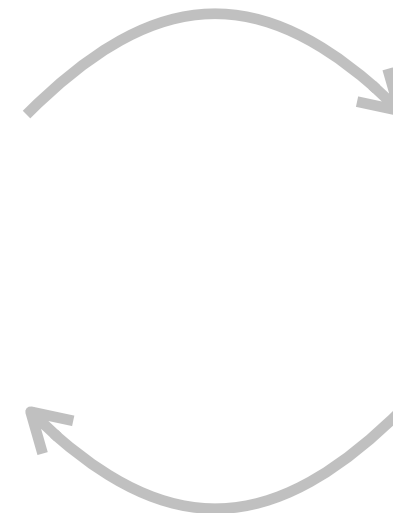
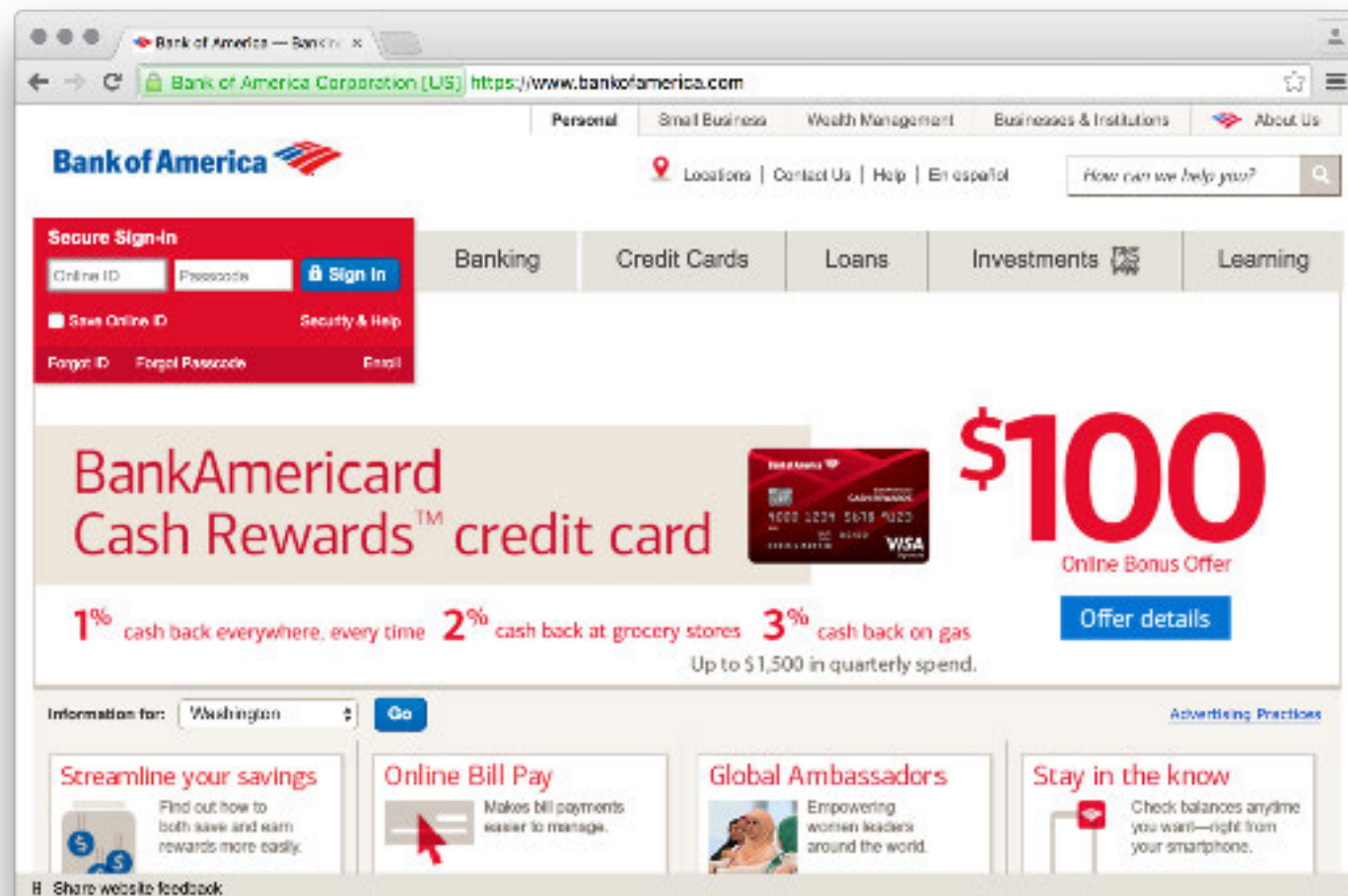
username + biometrics

fast and secure

convenient and usable

replacing password managers  
with biometrics


on-demand biometrics



**confined** web apps  
in the browser

**powerful** sensors  
on mobile devices

## payment options

 **Credit Cards**  


**Enter your credit card information:**

Card number

Select card type...

Name on card

Expiration date  
01  2010

credit card use

Inside the bank

Outside the bank

Please provide all of the following information to:

From:

To:

Amount: \$

Frequency:

bank transfer

## Beneficiaries

### Current Beneficiaries

Add, view, or change beneficiary designations for Last Check/Final Compensation, State 2X Employee Life, or Reduced Life below. For help, call 1-877-766-6447.

Manage Defined Contribution, 401K, and/or 457 beneficiary designations online at ING 401k/457 Plans Web Site. For help, call 1-800-748-6128.

Plan Type	Employee Life
Plan Name	LAST CHECK BENEFICIARY DESIGI
Name	<a href="#">Susie O Blank</a>
Type	Primary
Amount	100.00%
<input type="button" value="Add Individual"/> <input type="button" value="Add Trust"/>	
Plan Type	Employee Life
Plan Name	STATE 2X EMPLOYEE LIFE

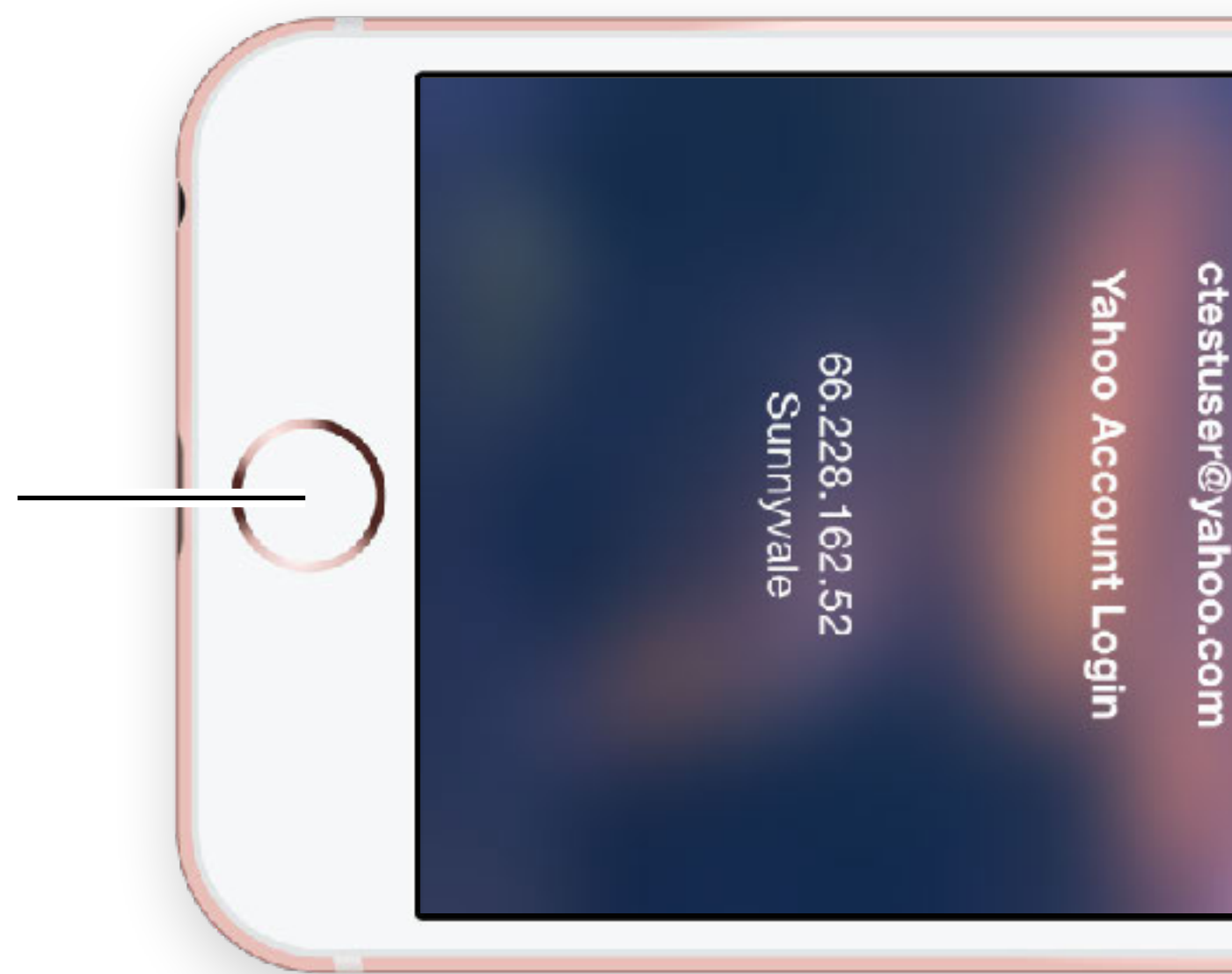
changes to HR details

more granular authentication





fingerprint scanner



on-demand biometrics





fingerprint  
scanner

face  
scanner



on-demand biometrics

89%

of iOS users actively use biometrics for authentication

vast potential for adoption

Apple Platform Security 2019: <https://support.apple.com/guide/security/welcome/web>

~80x

users unlock their devices a day on average

vast potential for adoption

Apple Platform Security 2019: <https://support.apple.com/guide/security/welcome/web>

- 1) type in passcode
- 2) interact (send emails, ...)

typical process





1) ~~type in passcode~~

use biometric authentication

2) interact (send emails, ...)

typical process

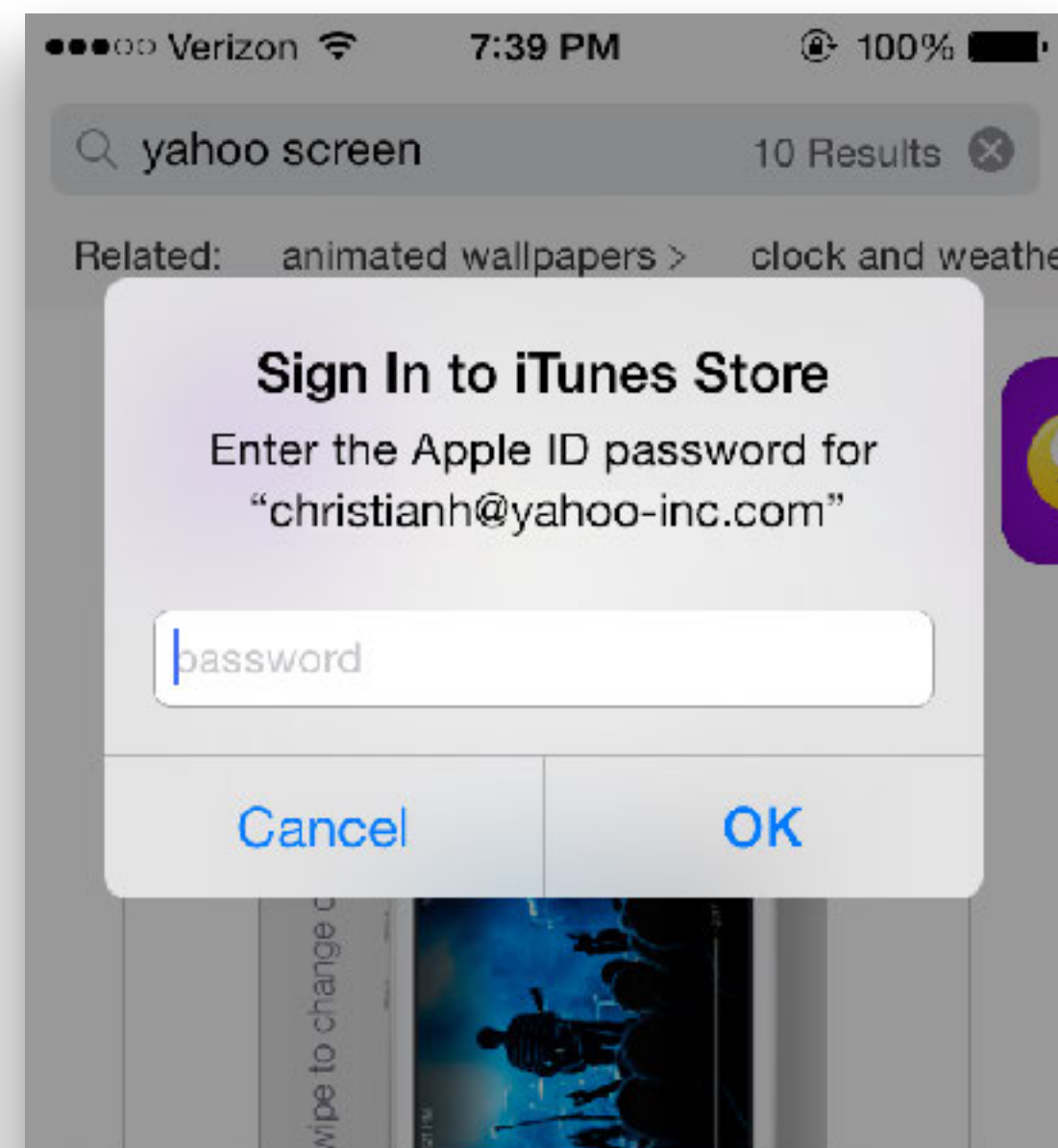
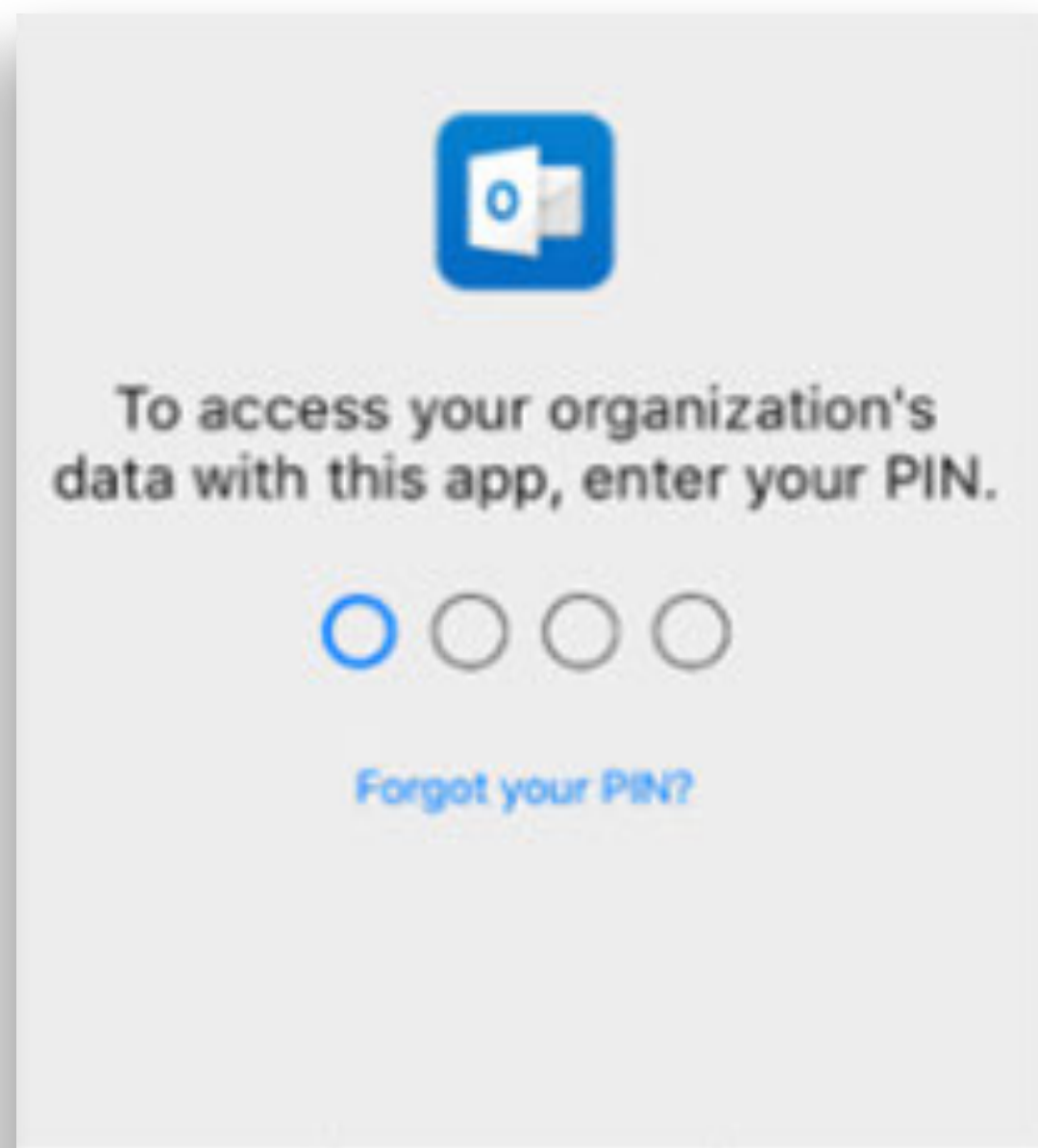
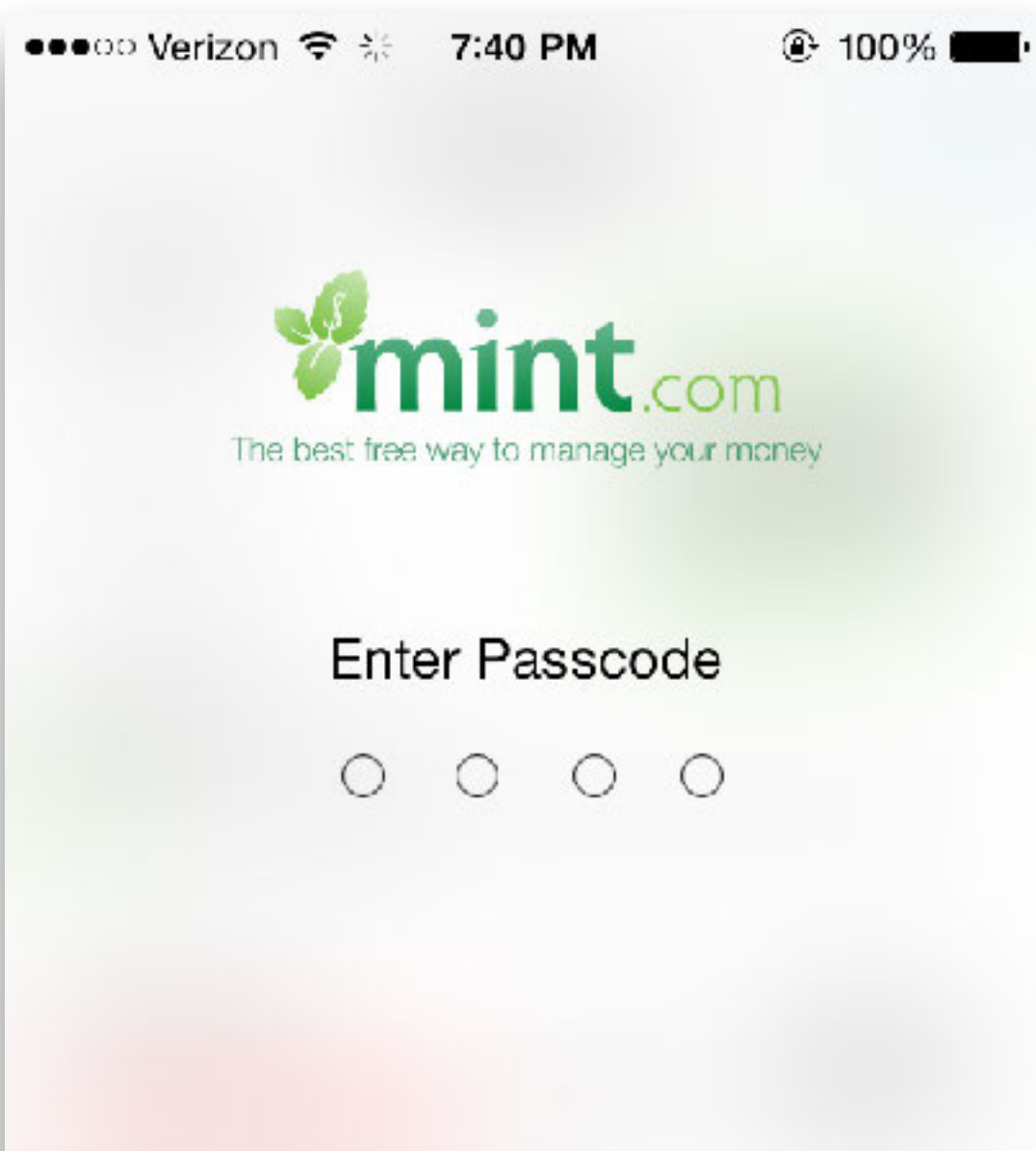


**wide-open** session  
access to all my data  
can we trust the user now?

is this secure now?



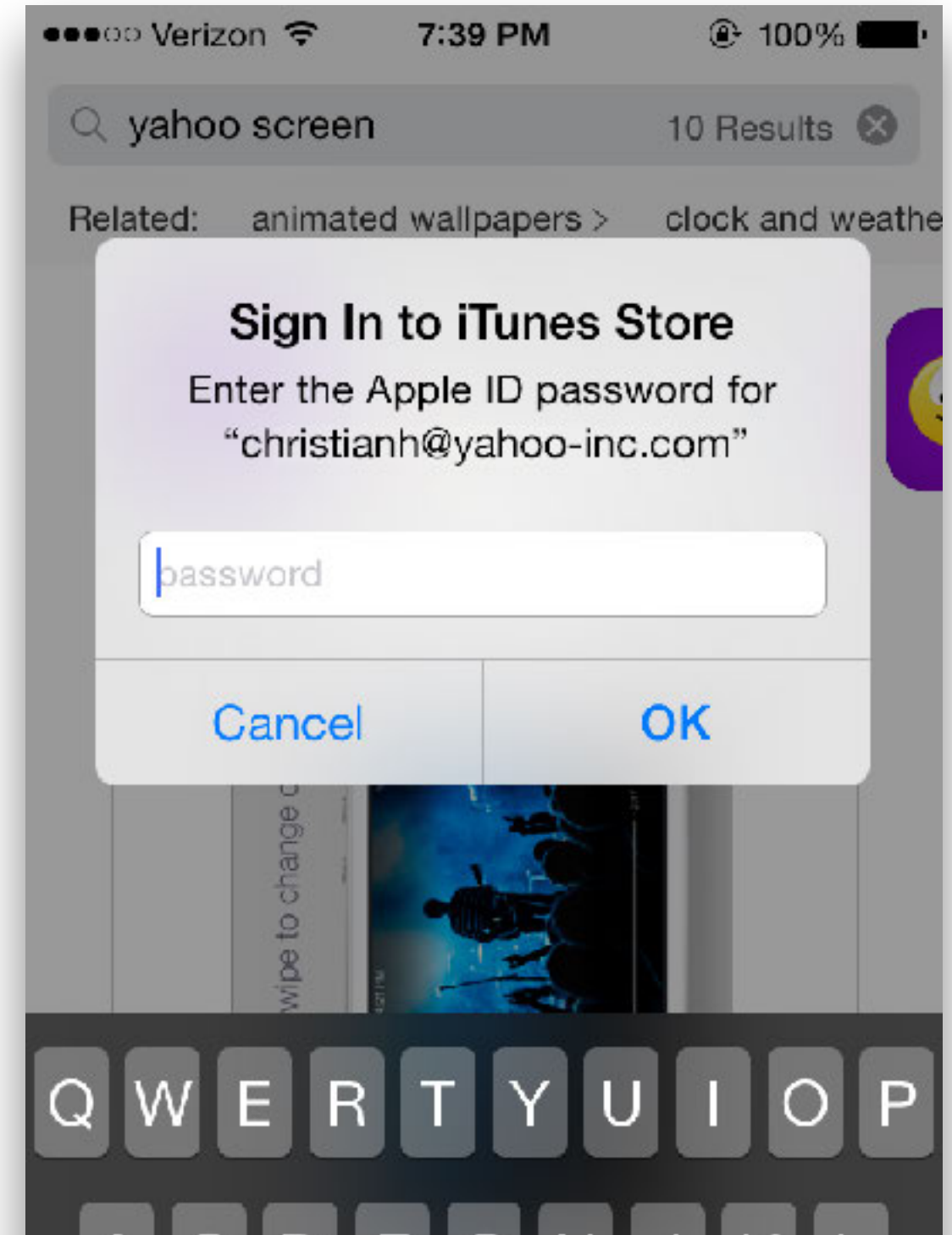
# some have decided "no"



# interaction flow

ideally we want this  
protection **all the time**

but it **disrupts** interaction

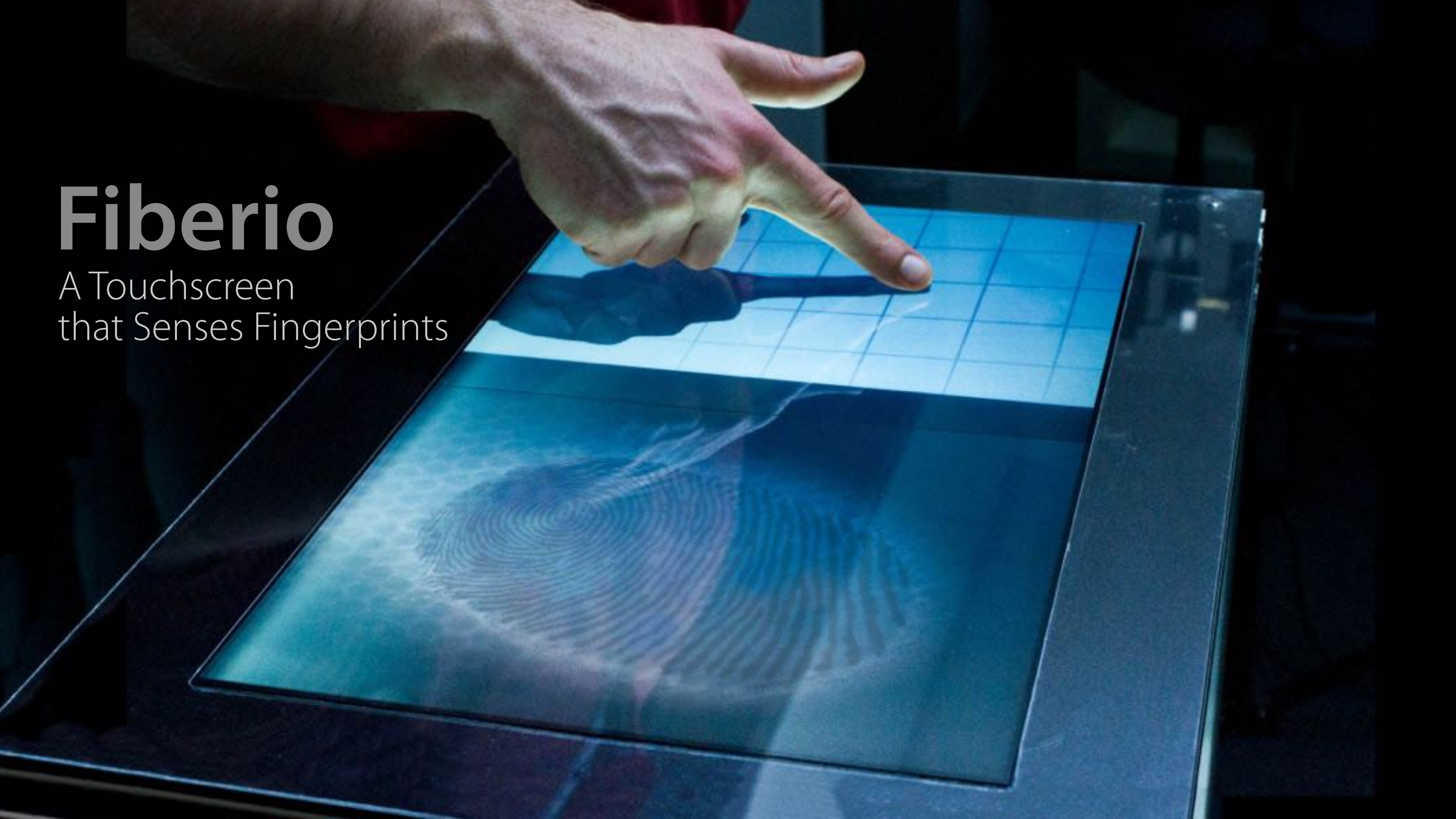




can we make this **part of the interaction?**

# Fiberio

A Touchscreen  
that Senses Fingerprints





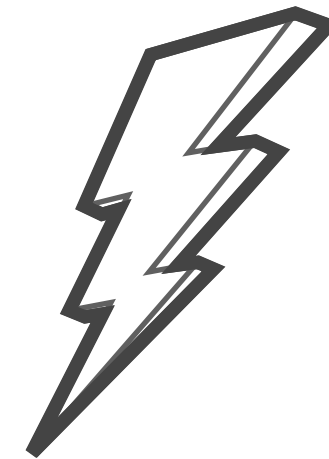


# challenge

such an **touchscreen** device requires

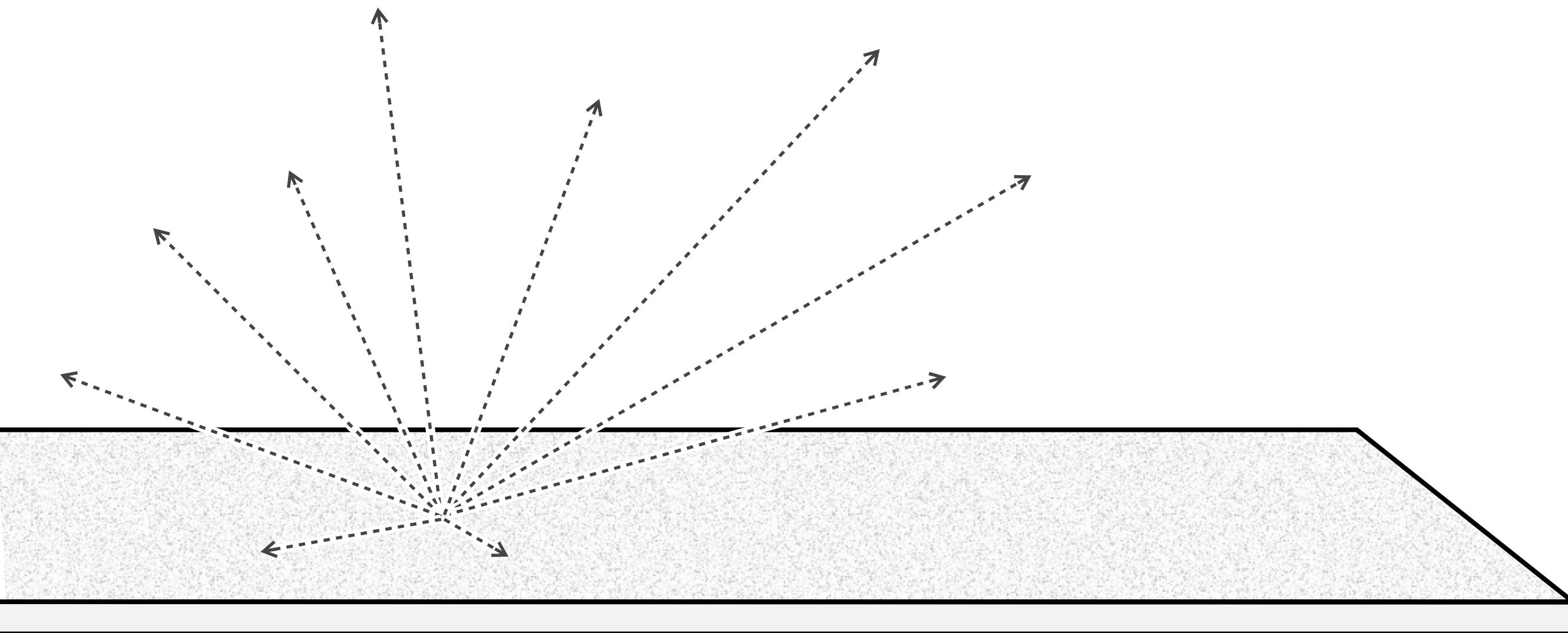
(1) output: display images

(2) input: capture fingerprints





# (1) display images

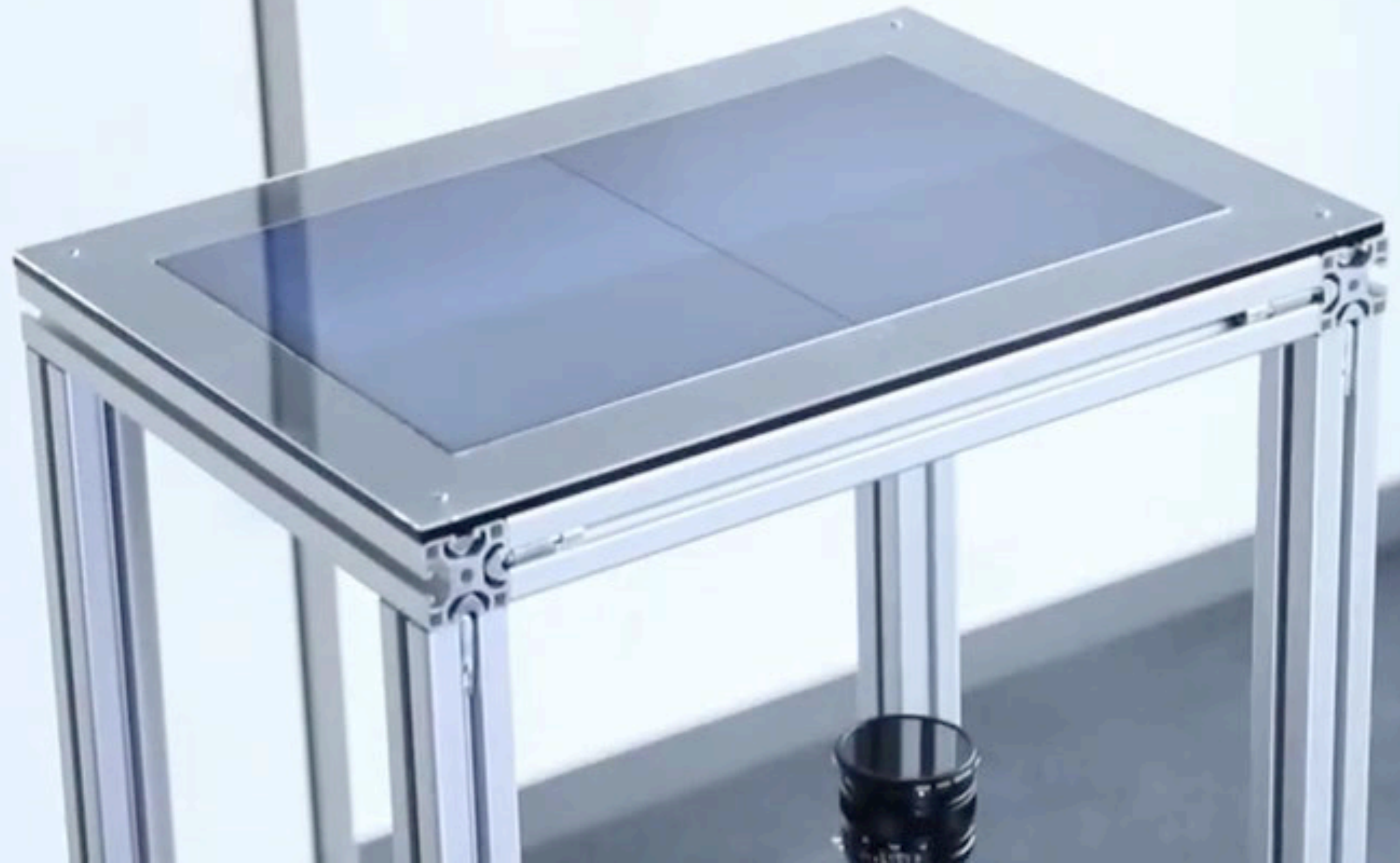


**scattered light**

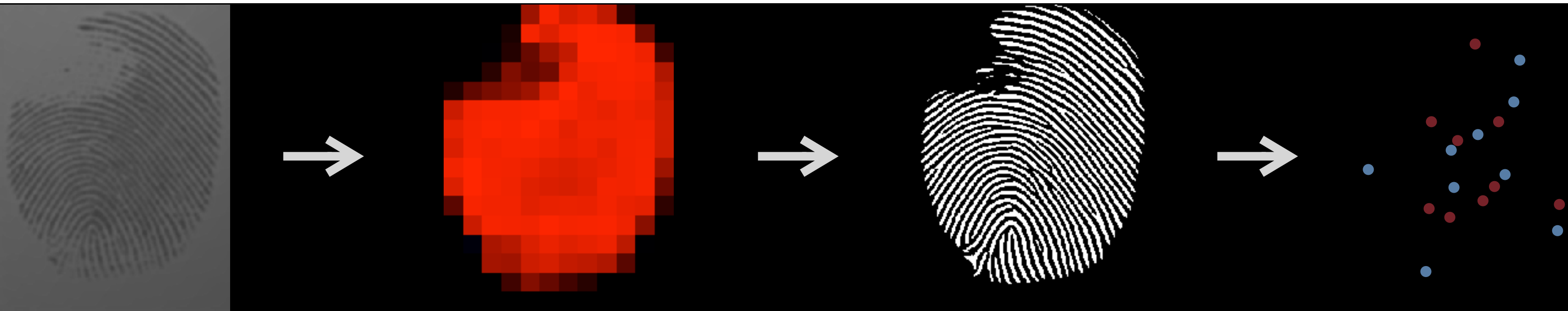
## (2) capture fingerprints



high **contrast**  
between ridges and valleys



# fingerprint processing pipeline



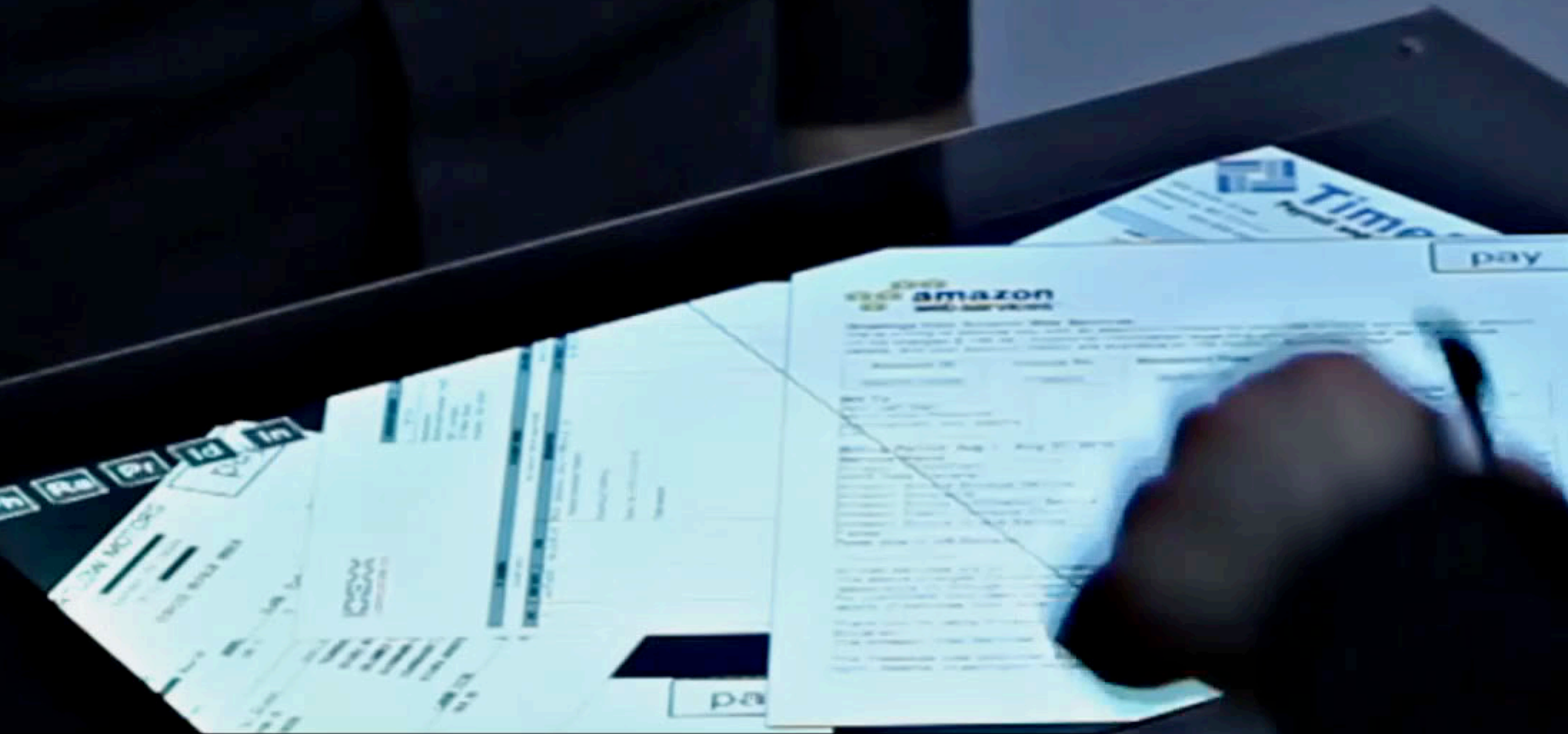
raw  
image

locate  
fingerprints

augment &  
extract features

match  
users





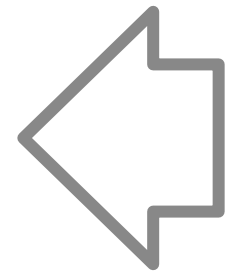
user authentication  
for **each** input event

realtime operation  
for **interactive** behavior

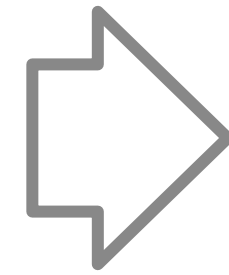
...integrating authentication  
into **regular** interaction



security



user  
authentication



convenience



2013





today



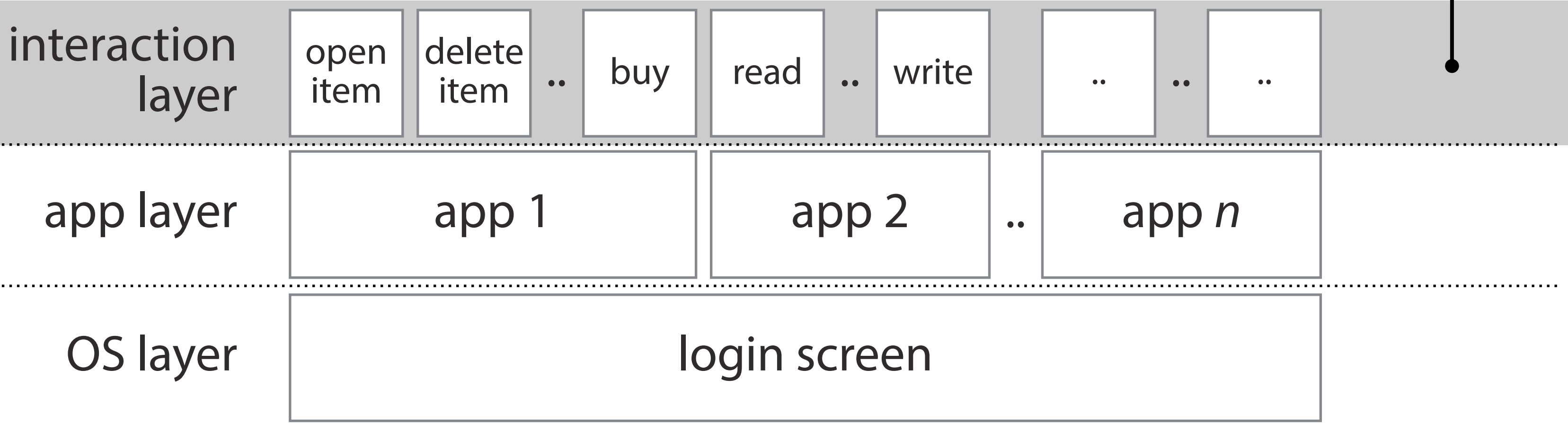


# Biometric Touch Sensing

a new model for authentication



authentication  
should happen here



moments of authentication



obtained directly  
from the touchscreen



```
touch event = (x, y)
session = {
  userID from initial login,
  running apps, ...
}
```

state of the art

```
touch event = (x, y, userID)
session = {
  running apps,
  ...
}
```

biometric touch sensing

continuous authentication during each touch

**seamlessly** integrated into regular interaction

**no password prompts** interrupt direct interaction

biometric touch sensing



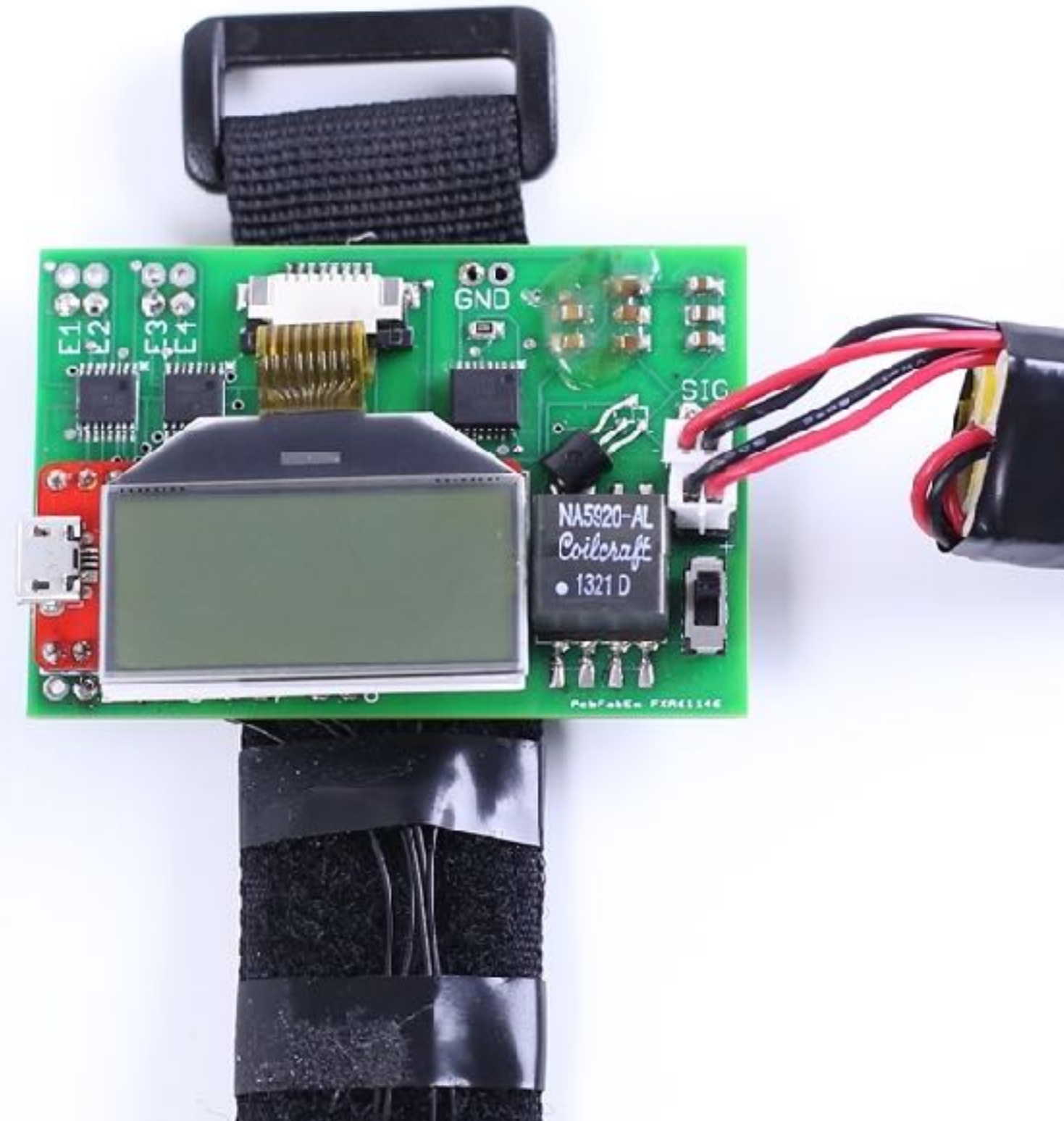
Bioamp  
a prototypical helper

# Bioamp

“watch” prototype for

1 biometric sensing

2 data transfer to the touchscreen





**bioimpedance** of the user's  
wrist as a unique feature



8 electrodes

1 biometric sensing



signal is transmitted  
through the body and finger  
touchscreen observes it  
**along with the touch event**  
no pairing necessary

2 data transfer to the touchscreen

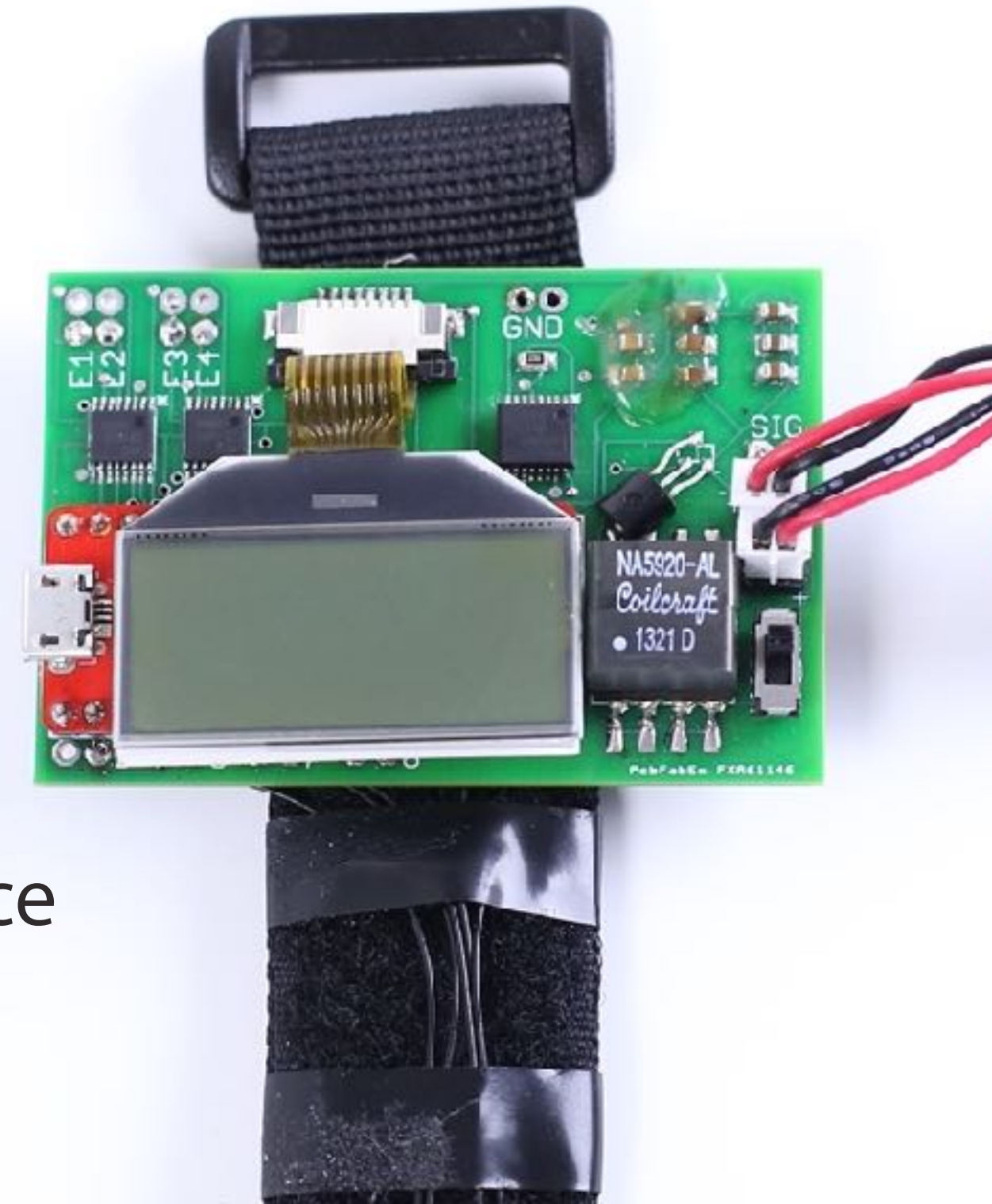
# Bioamp

“watch” prototype for

1 biometric sensing

2 data transfer to the touchscreen

3 authentication by the touchscreen device



touch := (x, y, userID)

integrated into the operating system



authentication during input  
access control for apps and personal data







authentication during output  
access control for displayed content







explicit logins  
for customized sessions and registration



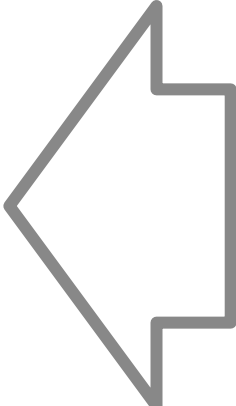




input event :=  $(x, y, \mathit{userID})$

wrap up

convenience



user  
authentication



security

# traditional process

1) ~~type in passcode~~

use biometric authentication

**disconnect**

---

2) use (interact, send emails, ...)

input event =  $(x, y)$



## traditional process

1) ~~type in passcode~~

use biometric authentication

2) use (interact, send emails, ...)

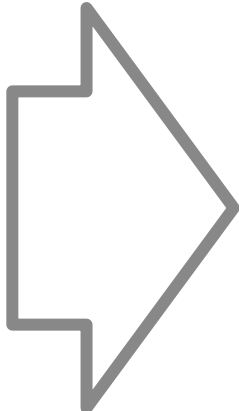
input event = (x, y)

## biometric touch sensing

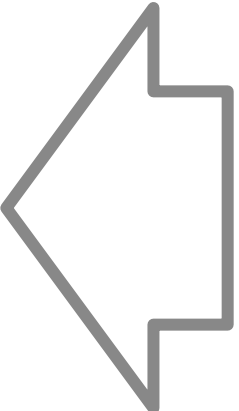
use & authenticate

input event = (x, y, *userID*)

convenience



user  
authentication

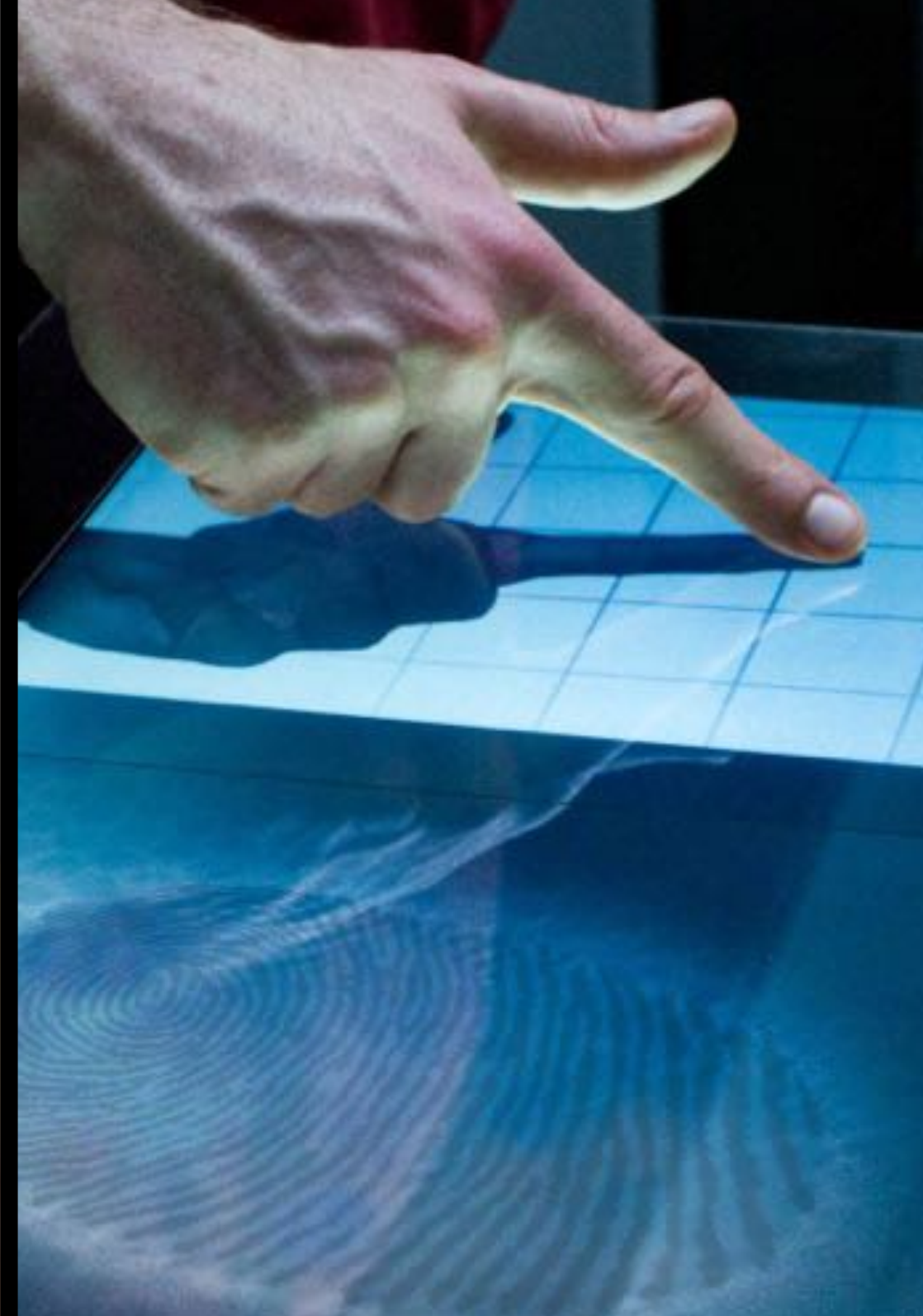


security

input event = (x, y, *userID*)



1 two factor authentication



2 touchscreens and fingerprints



3 a new model for authentication





a new perspective on  
user authentication on touch devices

prof. dr. **christian holz** · [christianholz.net](http://christianholz.net)

sensing,  
interaction &  
perception lab

[siplab.ethz.ch](http://siplab.ethz.ch)