On-Demand Biometrics
Fast Cross-Device Authentication

Christian Holz
Microsoft Research

Frank Bentley
Yahoo
on-demand biometrics
username and biometrics
traditional login: username and password, two-step verification
introduction
additional login protection
login request

user + password

two-step verification code

enter code
only 6.4% two-step verification-enabled Google accounts of 900 million users

[Petsas et al. '14]
security  user authentication  convenience
20 seconds

overhead of two-step verification

[Gunson et al. '14]
Duo Security

Authy OneTouch

Yahoo Account Key
security user authentication convenience

Duo Security
Authy OneTouch
(additional factor)

Yahoo Account Key
(no password)
on-demand biometrics

replacing passwords in the browser with biometric authentication on the mobile device
login request → authentication request → biometric authentication
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
study
interview
& observation
semi-structured interview-based study

think-aloud protocol

12 external participants
  6 female
  ages 18–49, M=34 years
  diverse backgrounds (manager, admin, photographer, clerk, student)

all were regular users of iPhone and TouchID

Yahoo Mail users, desktop and mobile
goal := testing the **usability** and **acceptance** of our new desktop authentication
BIOMETRICS interface
(biometric authentication)

BUTTON interface
(no mobile authentication)
tasks

1. “Find the invitation email we sent you!”
2. “Schedule a calendar appointment with a friend!”
3. “Look up the contact details of a friend!”

⚠ explicitly no mention of a login procedure
between tasks, participants put their phones back where they usually stored it
grounded-theory based affinity analysis
1. Email inboxes contain sensitive data worth protecting
2. On-Demand Biometrics reduce effort during login
3. On-Demand Biometrics are simple and convenient
4. On-Demand Biometrics alleviate the fear of impersonation
5. On-Demand Biometrics require good fallback design

main themes
email inboxes contain sensitive data worth protecting
all participants recognized the sensitive data in their emails

security of their email account important to them

P8: “Most people, when they think of their email, they don’t really think of security versus a bank account. But in my mind it’s the same, because if you could get into [the account], you can find a trove of information and that to me is worrisome. It could be shopping, it could be your account, your Paypal account, whatever it is, you can get to stuff from there.”
many embraced their inbox to manage credentials

P10: “Because I have so many passwords, I have a folder in my Yahoo email called ‘other important stuff.’ That’s where I send myself emails for everything, everything passwords and user IDs. For everything travel, financial, shopping, most banking.

P8: “Email is big. Once you get into someone’s email, basically the keys to the kingdom are in there.”
On-Demand Biometrics reduce effort during login
all participants immediately saw the difference to traditional logins

P4: “I have a lot of different passwords for different things. [Your system] makes things a lot easier.”

P2: “It seemed very easy to use, not much brain power needed to remember passwords” when logging in from a friend’s place.
all commented on the speed of login and ease of use
all appreciated the time and effort saved

P10 compared strong passwords and easy use:
„I really like the fingerprint. It’s awesome, because your password has special characters. You have caps lock. You have lowercase. You have numbers. **With your fingerprint, it’s just boom, done. It just makes things faster.** It just cuts down the time of waiting.”
On-Demand Biometrics are simple and convenient
all participants easily understood reaching for the phone to login

P4: “It was really simple to use. Even if you don’t know anything about computers or about your phone or anything, it’s just really easy.”

not one participant hesitated when approving the request

simple and convenient
on-demand biometrics require no typing of codes

P4: “Instead of sometimes they’ll email you a code or text you a code and you have to get the code and then put it in there. It will give you the letters to type in or to verify that it’s you. It just seems like a lot of processes, but this is really quick and easy.”

P5: “The message was loud and clear: We need to scan your finger to get to your mail.”
all mentioned the convenience over entering a password

P2: “I think it’s a time saver and it’s more of a natural movement to just use your fingerprint.”

eyes-free

they used their fingerprint to unlock the device eyes-free

P4, while being distracted nursing her baby, completed all tasks quickly “I could multitask at the same time. I could log into my Yahoo account while I’m doing something else.”
On-Demand Biometrics alleviate the fear of impersonation
most participants worried about compromised accounts due to leaked databases or attackers guessing weak passwords

on-demand biometrics increased participants’ perception of security

P1: “[This is] better than a password, because I can’t just tell someone my thumbprint […] Whereas with a password, someone else can guess it, and maybe they’re right. But nobody will be able to guess my thumbprint”

many mentioned that they felt an increased awareness of when someone would try to access their email accounts
all saw the extra level of control of biometrics over just ‘approve’
without additional effort

P9: “[the BUTTON] didn’t require my fingerprint, it just required me
to tap ‘approve’, actually. Then I feel like it’s better to have that extra step
of using your fingerprint. It’s not even a real extra step, it’s much easier.
It’s really convenient and it adds a level of security.”
On-Demand Biometrics require good fallback design
currently, the phone needs to be within reach during login

P5: “I have it with me almost all the time, except when I’m at home.”

✦ clear need for fallback options
  (e.g., backup codes or trusted family devices)
most said that they are permanently logged in at home

most use their browser’s password manager to store all credentials

P11: “Since it would be used with unrecognized devices, most likely that means you’re going to be in public or out somewhere, and then most likely I would have my phone with me.”

but all is good at home still
wet or dirty hands make scanning challenging

P11: “just dry it or wipe it off, then it will work”

fear of running out of battery

P4: “[I’d] click on ‘I can’t access my account.’ Maybe I’d have a password, like a default or security questions like they normally do when you forget your password.”

non-operational fingerprint scanner
conclusions
existing login methods: security vs. convenience

- user + password
- PIN through SMS
- PIN password
- approve/deny
- username
- approve/deny
- username
- PIN through SMS
username + biometrics
fast and secure
convenient and usable
replacing password managers with biometrics

on-demand biometricity
on-demand biometrics

fingerprint scanner
implications
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

Add your card

Inside the bank
Outside the bank

Please provide all of the following information to

From: Transfer money from
To: Transfer money to
Amount: $
Frequency: One time, immediately

Continue 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 1-877-765-6447.

Manage Defined Contribution, 401K, and/or 457 beneficiary designations online at ING 401k/457 Plans Web Site. For help, call 1-800-748-6126.

<table>
<thead>
<tr>
<th>Plan Type</th>
<th>Plan Name</th>
<th>Employee Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Check</td>
<td>Salary</td>
<td>State 2X Employee Life</td>
</tr>
<tr>
<td>$600.00</td>
<td>$100.00</td>
<td>State 2X Employee Life</td>
</tr>
<tr>
<td>Amount:</td>
<td>$600.00</td>
<td>State 2X Employee Life</td>
</tr>
</tbody>
</table>

Add Individual Add Trust

credit card use
bank transfer
changes to HR details

more granular authentication
promote authentication to the lock screen

biometric sensors on wearables?
61% of Yahoo Mail iOS app users have a TouchID-capable device (n > 1,000,000)
72% of users actively use TouchID for authentication.

Vast potential for adoption.
On-Demand Biometrics
Fast Cross-Device Authentication

Christian Holz
http://www.christianholz.net

Frank Bentley
Yahoo