On-Demand Biometrics: Fast Cross-Device Authentication

Christian Holz
Microsoft Research, Redmond, WA
cholz@microsoft.com

Frank R. Bentley
Yahoo, Sunnyvale, CA
fbentley@yahoo-inc.com

ABSTRACT
We explore the use of a new way to log into a web service, such as email or social media. Using *on-demand biometrics*, users sign in from a browser on a computer using just their name, which sends a request to their phone for approval. Users approve this request by authenticating *on their phone* using their fingerprint, which completes the login in the browser. On-demand biometrics thus replace passwords or temporary access codes found in two-step verification with the ease of use of biometrics. We present the results of an interview study on the use of on-demand biometrics with a live login backend. Participants perceived our system as convenient and fast to use and also expressed their trust in fingerprint authentication to keep their accounts safe. We motivate the design of on-demand biometrics, present an analysis of participants' use and responses around general account security and authentication, and conclude with implications for designing fast and easy cross-device authentication.

Author Keywords
Cross-device authentication; Login; Mobile Interaction; Biometric Authentication; Fingerprint scanning; Touch ID.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Webmail and social media services increasingly offer additional protection for users' accounts [31], such as linking phones to web accounts. When a user now logs in with their name and password in a browser, the provider will send a temporary code to their phone. The user then needs to enter this code into the browser to complete the login. This process is commonly called two-step verification or two-factor authentication and offered by several email providers (e.g., Microsoft Outlook [17], Yahoo Mail [34], Gmail [8]) and social networks (e.g., Facebook [7], Twitter [30], LinkedIn [15]).

While two-step verification protects user accounts from non-targeted attacks, it increases the effort required for users to login [32]. Users not only need to remember their passwords, but also need to receive and type in the temporary code, which can involve several swipes and taps on the phone, and additional text entry on the primary device. This added complexity may be one reason for the low adoption rates of two-step verification thus far (e.g., 6.4% of Google users [23]).

To simplify this process, some solutions have started to replace these temporary codes with an 'approve' and a 'deny' button on the phone to complete logins [3,6,35]. Alternatively, on-demand *passwords* discard users' own passwords and solely require typing in the temporary code sent to users' phones [33]. While both methods try to alleviate the user of some of the effort of two-step verification, neither method performs any user authentication on the mobile device.

In this paper, we explore the use of *on-demand biometrics*, a convenient way of cross-device authentication that replaces passwords in the browser with biometric authentication on the trusted mobile device users have linked to their accounts.

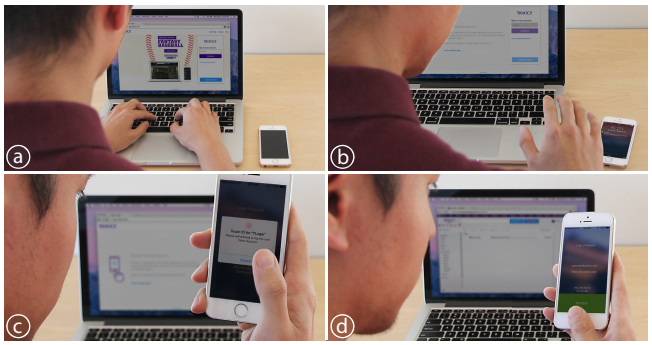

Figure 1: Login with *on-demand biometrics*: (a) A user enters their name into the login form in the browser, (b) receives the authentication request on their phone, and (c) approves it with their fingerprint, which (d) completes the login in the browser.

ON-DEMAND BIOMETRICS: REPLACING PASSWORDS
As shown in Figure 1, our login system uses the biometric sensors in today's mobile devices to authenticate a login request from a browser running on a computer. To log in, a user enters just their username in the login form in the browser and clicks 'continue'. The server then sends an authentication request to the trusted mobile device that is linked to the account and updates the browser page with instructions for the user to approve the request on the phone. Meanwhile, an app on the phone receives the request and prompts the user to authenticate through a *biometric sensor*, here a fingerprint scanner embedded in the home button. The app then forwards the result of the authentication to the server, which updates the browser page again, now logging the user into their email account after successfully authenticating on the phone.

Note that the user authenticates against the profile stored on the *trusted* phone, not that on the server. In our system, a user

CHI '16, May 07–12, 2016, San Jose, CA, USA

ACM 978-1-4503-3362-7/16/05…$15.00
DOI: http://dx.doi.org/10.1145/2858036.2858139

registers a phone as a trusted device when activating on-demand biometrics. The server then sends a one-time text with a code to the phone, which the user needs to enter into the browser. On-demand biometrics now replace the user's password-based login; browsers continue to maintain login sessions as before and do not require more frequent logins.

To explore the use of our system with real users, we integrated on-demand biometrics into the Yahoo email service, replacing the login backend and extending the mobile Mail app to perform biometric authentication. The Mail app was otherwise unmodified and only showed a separate view when receiving an authentication request from the server. A standalone app could accomplish the same, but we found it easiest for users to include this into their already-installed Mail app.

To study people's understanding of both the system and the benefits our login procedure provides in comparison to existing systems, we conducted a semi-structured interview-based study with 12 diverse participants and observed their use of the system. We discovered that participants were sensitive to the contents of their mail inbox, validating on-demand biometrics for authentication, and explored their perception of convenience as well as their concerns around our approach. We will discuss our findings and the implications for the design of new cross-device login implementations.

BACKGROUND

On-demand biometrics are related to two-step verification, mobile biometric authentication, and secure pairing methods.

Two-step verification for webmail and social media services

Petsas et al. found that only 6.4% of Gmail's 900 million active users (675 million on mobile [24]) had opted in to two-step verification as of late 2014 [23]. One explanation could be the interaction overhead and delay of two-step verification [13], which Gunson et al. compared to traditional password login [10]. On average, their participants took 20 seconds longer to login and rated the convenience of use of traditional passwords higher. The 141 participants in Peevers et al.'s evaluation also valued convenience and usability above the added security level of two-step verification [22].

Biometric authentication on mobile devices

Biometric authentication is typically faster and more convenient than password authentication [28]. On-demand biometrics currently use fingerprints as *one* possible biometric feature due to their wide use on iOS [2] and Android [19,26] today [4], but equally support other product approaches, such as face recognition as implemented by Android's Face Unlock [1] or Windows Hello [18]. On-demand biometrics could alternatively integrate mobile authentication proposed in the literature, such as detecting the biometrics of users' hands [25], voice [16], or scanning their ears or hands using the device's capacitive touchscreen (e.g., Bodyprint [12]).

Secure pairing of the mobile device and the user's browser

Our current implementation assumes that users respond to the same authentication request that they have issued from the browser. Securely pairing a user's phone once to the desktop system can prevent attacks from malicious login requests, such as by using inaudible audio signals [20,21,27] or Wifi [29], which requires virtually no interaction from the user. Kumar et al. presented an evaluation of such pairing methods, showing several that were secure and accepted by users [14]. As pairing requires minimal interaction, we did not include it as part of our usability evaluation, since it does not affect the everyday interaction, which is what we study.

STUDY METHODS: INTERVIEW AND OBSERVATION

To understand the use of on-demand biometrics, we conducted a semi-structured interview-based study in the Summer of 2015. We recruited 12 external participants (ages 18–49, *M*=34 years, 6 female) from the greater San Francisco Bay Area using professional recruiters to ensure diversity. Participants comprised a variety of ethnic backgrounds and had diverse occupations (e.g., office manager, system administrator, photographer, sales clerk, student) and received a gratuity of $75. All participants had been using TouchID on their personal iPhones and were regular users of Yahoo Mail, both on the web at home and the mobile app on their phone. We recruited participants who had already set up their fingerprint sensor, because they were the users who would be eligible to use on-demand biometrics in a production release. This allowed us to test the usability and acceptance of our new desktop authentication solution, not the particular user interaction for enabling fingerprint scanning using TouchID.

We installed an extended Mail app on participants' iPhones. The system was fully implemented to work in the wild, including push messages through Apple's service to the phone. In addition to the biometric authentication on the phone (BIOMETRICS interface), we integrated a separate approval interface to compare participants' impressions of using just an 'approve' and 'deny' button on the phone (BUTTON interface), but no form of mobile authentication (e.g., [3,6,35]).

We explicitly did not tell participants that this study was about logins. Participants performed three tasks on the Yahoo platform: finding the invitation email we had sent them, scheduling a calendar appointment, and looking up a contact. To accomplish each task, participants had to log in once, but received no explanation about how we changed their login process or login interfaces. Between tasks, we asked participants to put their phone back where they usually stored it (e.g., pocket or purse) if they did not do this on their own.

During the interview, we asked participants about the types of information that they had stored in their mail account and, related to information, such as bank accounts, how secure their email should be. Participants thought aloud during the interactive parts of the study and we explore their thoughts in the findings below. Sessions lasted one hour and participants were video and audio recorded. We analyzed all transcribed qualitative data from the interviews as a team (up to four people) through a grounded-theory based affinity analysis with 740 items, which were exact quotes from participants. Leaf nodes in the affinity were direct quotes from our interviews and we worked until all researchers were satisfied

with the themes. Each theme, which represents a subsection below, had support from multiple diverse participants.

FINDINGS

Overall, all participants were able to understand the concept of on-demand biometrics right away and successfully logged into their web-based email accounts using biometric authentication on their phones. During our analysis of the interview data, we found common themes and explore them below.

Email inboxes contain very sensitive data worth protecting

Showing the need for authentication beyond passwords, all participants were aware of the sensitive data in their personal email account and expressed that the security of their email account was important to them. P8 reflected: *"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 participants embraced their inbox as the place to actively manage access to other platforms. After once not having access to a password while on the go, P10 created an inbox folder with all of their login information: *"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. Today, I booked Southwest Airline tickets. I looked up under my 'other important stuff' folder, I have my Southwest account, my Chase passwords, everything passwords organized and user ID. For everything travel, financial, shopping, most banking."* P8 summed it up by saying, *"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

When logging in without a password, but using on-demand biometrics, all participants immediately recognized the difference to traditional logins. Participants' first responses typically contrasted our approach with the necessity of remembering passwords for traditional logins. P4 appreciated not having to remember passwords anymore, telling us that *"I have a lot of different passwords for different things. [Your system] makes things a lot easier."* P2 liked the feature for situations in which they previously had to login from a new computer, such as a friend's place: *"It seemed very easy to use, not much brain power need to remember passwords."*

In addition, participants mentioned that using biometric authentication in the place of passwords for their personal emails increased their sense of security. For example, P9 had experienced a compromised email account several times and said *"I don't know how they're getting the password, so I changed the password to get it back. I do like having more security, so people out of state or out of the country can't log into my email. I like it."* Many appreciated that biometric authentication uses the mobile device to gain access on the web. P1 explained *"It's like using the technology of another device to make other things more secure, which is pretty cool."*

All participants commented on the speed of login with on-demand biometrics. Instead of entering a password or receiving an additional code on their phone, they just placed their finger on the fingerprint scanner to approve the request from their browser. Participants appreciated the time and effort saved through our approach. P10 pointed out the tradeoff between a strong password and the convenience of using it: *"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."* Several others also mentioned their frustrations with caps lock or frequently mistyping passwords.

On-Demand Biometrics are simple and convenient

Participants generally commented on the simplicity of on-demand biometrics. Even though participants stored their phones in their pockets or bags, after entering their username and seeing the browser instructions to approve access on the phone, they promptly reached for their phones. P4 reflected, *"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. P11 spoke aloud while signing in: *"I just approved the login request that Yahoo sent me stating that my account was being signed in from another device, which is new to me. I'm opening the login request, […] 'Please use Apple Touch ID to sign in.' 'Success.' Oh that's so cool."*

Unlike typical two-step verification, our approach does not require users to type in a code that is sent to their phone. P4 found that *"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 stated, *"The message was loud and clear, we need to scan your finger to get to your mail."*

All participants also mentioned the speed of this type of login over entering a password or using two-step verification. P2 commented, *"It's just easier [than typing a password] and more convenient. I think it's a time saver and it's more of a natural movement to just use your fingerprint."* Participants also told us how they used their fingerprint to unlock the device *eyes-free*. P4 nursed her baby during the evaluation; while she was distracted, she still completed all tasks quickly and explained: *"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

Our system increased participants' perception of the security of their account. Most participants worried about compromised accounts due to leaked databases or attackers guessing weak passwords. P1 deemed our approach *"better than a password, because I can't just tell someone my thumbprint for them to draw it on and use it. Whereas with a password,*

someone else can know it, someone else can guess it, and maybe they're right. But nobody will be able to guess my thumbprint and put it on there." Most participants associated fingerprint scanning with accessing their accounts in a bank and seemed overly assured that, therefore, fingerprints are also much more secure in protecting their email accounts. P7 asserted, *"My fingerprint, there's only one in the world, one that exists is it, so usually no way that anybody could potentially log in to my bank account or log in to [my email] through my phone because they don't have my fingerprint."* No participant mentioned lifted or spoofed fingerprints, or expressed any concerns around exposed biometrics.

More importantly, we observed that participants recognized the potential of on-demand biometrics to prevent non-targeted attacks. Although most participants had not been using two-step verification for their accounts, many pointed out that breaking into their accounts becomes harder when using biometrics. P9 particularly appreciated this fact and told us, *"I'm assuming that someone from Africa wouldn't be able to get in, whereas for some reason some people have been able to get your password from out of the country."*

Comparing the BIOMETRICS and BUTTON interfaces, all participants understood the extra level of control that requiring their fingerprint has over a simple 'approve' button, and that it did not create any additional effort. For example, P9 explained that the BUTTON condition *"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."*

Finally, participants commented that they really felt in control when using on-demand biometrics. P7 said *"It's kind of like the phone alerts me if someone else is trying to use it. I can hit deny or I can [authenticate]."* Other participants also mentioned that they felt an increased awareness of when someone would try to access their email accounts.

On-Demand Biometrics require good fallback design

Our current implementation requires users to have their phones within reach during login, but participants revealed scenarios that challenge this assumption [5], showing a clear need for fallback options when a phone is out of reach, such as backup codes [9] or trusted backup devices from family. P5 said *"I have it with me almost all the time, except when I'm at home."* At the same time, most participants reported that they are permanently logged in at home and use their browser's password manager to store all credentials. P11 said *"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."*

Participants also recounted situations when their fingerprint scanner had refused access, such as when hands were wet or dirty. While some participants recommended to *"just dry it or wipe it off, then it will work"* (P11), P2 noted that *"when you put lotion on your hands and stuff, […] that's sometimes why my fingerprint doesn't work"*. A last concern participants had was a phone battery that had run out. Asked how they would approach this situation, P10 surmised *"I guess you would have to call Yahoo customer service."*, while P4 would *"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."*

DISCUSSION, IMPLICATIONS, AND CONCLUSION

Considering the space of existing implementations of two-step verification, we chose a new type of cross-device login that lies between one-time passwords sent to the phone [33] and just touchscreen controls to accept or decline a request [3,6,35], both of which require extra effort [10,22]. We have seen how on-demand biometrics strike a positive balance between the perceived security, convenience, and speed of use for users. Multiple studies in the related work have shown that usability trumps security for users, confirming the user's aversion to overhead in interacting with devices, and leading to low opt-in rates [23]. On-demand biometrics reduce the login process to just grabbing the phone and placing a finger on the home button, which participants often performed in a single motion during our evaluation, even while multitasking. On-demand biometrics thus reduce the overhead of one-time passwords, while providing the simple interaction of touchscreen buttons. We now distill two main implications for the design of cross-device authentication.

Extend the constraints of a web page with powerful sensors on mobile devices: Conceptually, on-demand biometrics replace the password manager in users' browsers with users' biometric features. Given the acceptance, speed, and convenience of use, on-demand biometrics can generalize beyond traditional logins and give users control over individual interactions on a more granular level [11]. Since biometric approval is fast, our feature could be used to authenticate and approve web-based requests to charge a user's credit card, change the address of an account, or delete personal records.

Promote authentication requests directly to the lock screen: Future implementations of on-demand biometrics should display requests on the lock screen, prompt for authentication right away, and render unlocking the phone redundant similar to a triggered alarm. Similarly, future wearable devices with integrated biometric sensors could be used to securely approve such requests across computers.

Overall, on-demand biometrics are a promising alternative to current implementations of two-step verification, addressing the challenges of convenience and speed of use that previous work has found to be responsible for low adoption rates. The themes in our analysis emerged across a diverse set of participants and thus provide a useful insight into the impression of everyday users. A quick look at the statistics of the usage of the mobile Yahoo Mail app ($n > 1{,}000{,}000$) shows that 61% of Yahoo's iOS users have a Touch ID-capable device and 72% of them actively use it—a vast potential for the adoption of on-demand biometrics for conveniently accessing accounts and interacting with sensitive information.

REFERENCES

1. Android Face Unlock. Biometric face recognition. Retrieved September 20, 2015 from https://support.google.com/nexus/answer/2781894
2. Apple Touch ID. Mobile fingerprint scanner. Retrieved September 20, 2015 from http://www.apple.com/iphone-6/touch-id/
3. Authy Two-factor Authentication. Retrieved December 31, 2015 from https://www.twilio.com/authy
4. Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 1411–1414. http://dx.doi.org/10.1145/2702123.2702141
5. Anind K. Dey, Katarzyna Wac, Denzil Ferreira, Kevin Tassini, Jin-Hyuk Hong, and Julian Ramos. 2011. Getting closer: an empirical investigation of the proximity of user to their smart phones. In *Proceedings of the 13th international conference on Ubiquitous computing* (UbiComp '11), 163–172. http://doi.acm.org/10.1145/2030112.2030135
6. Duo Security. Two-factor authentication. Retrieved September 20, 2015 from https://www.duosecurity.com/product
7. Facebook Login Approvals. May 12, 2011. Retrieved September 20, 2015 from https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920
8. Google 2-Step Verification. Retrieved September 20, 2015 from https://www.google.com/landing/2step/
9. Google Account Backup Codes. Retrieved December 31, 2015 from https://support.google.com/accounts/answer/1187538
10. Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* 30, 4 (June 2011), 208–220. http://dx.doi.org/10.1016/j.cose.2010.12.001
11. Christian Holz and Marius Knaust. 2015. Biometric Touch Sensing: Seamlessly Augmenting Each Touch with Continuous Authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology* (UIST '15), 303–312. http://dx.doi.org/10.1145/2807442.2807458
12. Christian Holz, Senaka Buthpitiya, and Marius Knaust. 2015. Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). 3011–3014. http://dx.doi.org/10.1145/2702123.2702518
13. Kat Krol, Eleni Philippou, Emiliano De Cristofaro, amd M. Angela Sasse. 2015. “They brought in the horrible key ring thing!” Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Network and Distributed System Security Workshop on Usable Security* (USEC '15). http://dx.doi.org/10.14722/usec.2015.23001
14. Arun Kumar, Saxena Nitesh, Tsudik Gene, and Uzun Ersin. 2009. Caveat emptor: A comparative study of secure device pairing methods. In *Pervasive Computing and Communications* (PerCom '09), 1–10. http://dx.doi.org/10.1109/PERCOM.2009.4912753
15. LinkedIn Two-Step Verification. May 31, 2013. Retrieved September 20, 2015 from http://blog.linkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/
16. Sébastien Marcel, Chris McCool, Pavel Matějka, Timo Ahonen, Jan Černocký, Shayok Chakraborty, Vineeth Balasubramanian, Sethuraman Panchanathan, Chi Ho Chan, Josef Kittler, Norman Poh, Benoît Fauve, Ondřej Glembek, Oldřich Plchot, Zdeněk Jančík, Anthony Larcher, Christophe Lévy, Driss Matrouf, Jean-François Bonastre, Ping-Han Lee, Jui-Yu Hung, Si-Wei Wu, Yi-Ping Hung, Lukáš Machlica, John Mason, Sandra Mau, Conrad Sanderson, David Monzo, Antonio Albiol, Hieu V. Nguyen, Li Bai, Yan Wang, Matti Niskanen, Markus Turtinen, Juan Arturo Nolazco-Flores, Leibny Paola Garcia-Perera, Roberto Aceves-Lopez, Mauricio Villegas, Roberto Paredes. 2010. On the results of the first mobile biometry (MOBIO) face and speaker verification evaluation. In *Proceedings of the 20th International conference on Recognizing patterns in signals, speech, images, and videos* (ICPR'10), 210–225. http://dx.doi.org/10.1007/978-3-642-17711-8_22
17. Microsoft Two-step verification. Retrieved September 20, 2015 from http://windows.microsoft.com/en-us/windows/two-step-verification-faq
18. Microsoft Windows Hello. Biometric face recognition. Retrieved September 20, 2015 from http://windows.microsoft.com/en-us/windows-10/getstarted-what-is-hello

19. Nexus Imprint. Retrieved December 31, 2015 from https://support.google.com/nexus/answer/6285273

20. Haojian Jin, Christian Holz and Kasper Hornbæk. 2015. Tracko: Ad-hoc Mobile 3D Tracking Using Bluetooth Low Energy and Acoustic Signals for Cross-Device Interaction. In *Proceedings of the 28th annual ACM symposium on User interface software and technology* (UIST '15), 147–156. http://dx.doi.org/10.1145/2807442.2807475

21. Ngu Nguyen, Stephan Sigg, An Huynh, and Yusheng Ji. 2012. Pattern-Based Alignment of Audio Data for Ad Hoc Secure Device Pairing. In *Proceedings of the 2012 16th Annual International Symposium on Wearable Computers (ISWC)* (ISWC '12). 88–91. http://dx.doi.org/10.1109/ISWC.2012.14

22. Gareth Peevers, Gary Douglas, Mervyn A. Jack, and Diarmid Marshall. 2011. A Usability Comparison of SMS and IVR as Digital Banking Channels. *Int. J. Technol. Hum. Interact*. 7, 4 (October 2011), 1–16. http://dx.doi.org/10.4018/jthi.2011100101

23. Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor authentication: is the world ready?: quantifying 2FA adoption. In *Proceedings of the Eighth European Workshop on System Security* (EuroSec '15), Article 4. http://dx.doi.org/10.1145/2751323.2751327

24. Sundar Pichai, Google I/O 2015, Active Gmail users. May 28, 2015. Retrieved September 20, 2015 from https://events.google.com/io2015/

25. Joanna Rokita, Adam Krzyżak, and C. Y. Suen. 2008. Cell Phones Personal Authentication Systems Using Multimodal Biometrics. In *Proceedings of the 5th international conference on Image Analysis and Recognition* (ICIAR '08), 1013–1022. http://dx.doi.org/10.1007/978-3-540-69812-8_101

26. Samsung Finger Scan. Mobile fingerprint scanner. Retrieved September 20, 2015 from http://samsung.com/us/support/answer/ANS00039905/997339939

27. Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2008. HAPADEP: Human-Assisted Pure Audio Device Pairing. In *Proceedings of the 11th international conference on Information Security* (ISC '08), 385–400. http://dx.doi.org/10.1007/978-3-540-85886-7_27

28. Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference* (ACSAC '12), 159–168. http://dx.doi.org/10.1145/2420950.2420976

29. Sacha Trifunovic, Bernhard Distl, Dominik Schatzmann, and Franck Legendre. 2011. WiFi-Opp: ad-hoc-less opportunistic networking. *In Proceedings of the 6th ACM workshop on Challenged networks* (CHANTS '11), 37–42. http://dx.doi.org/10.1145/2030652.2030664

30. Twitter Login Verification. May 22, 2013. Retrieved September 20, 2015 from https://blog.twitter.com/2013/getting-started-with-login-verification

31. Two Factor Auth (2FA). List of websites that support two-factor authentication. Retrieved September 20, 2015 from https://www.twofactorauth.org

32. Catherine S. Weir, Gary Douglas, Tim Richardson, Mervyn Jack. 2010. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*. 22, 3 (October 2009), 153–164. http://dx.doi.org/10.1016/j.intcom.2009.10.001

33. Yahoo On-Demand Passwords. A New, Simple Way to Log In. March 15, 2015. Retrieved September 20, 2015 from http://yahoo.tumblr.com/post/113708272894/a-new-simple-way-to-log-in

34. Yahoo Two-step verification. Retrieved September 20, 2015 from https://help.yahoo.com/kb/SLN5013.html

35. Yahoo Account Key. Retrieved December 31, 2015 from https://help.yahoo.com/kb/SLN25781.html