Goldilocks and the *Two* Mobile Devices:
Going Beyond All-Or-Nothing Access to a Device's Applications

Eiji Hayashi[1,*]   Oriana Riva[2]   Karin Strauss[2]   A.J. Bernheim Brush[2]   Stuart Schechter[2]

[1]Carnegie Mellon University
5000 Forbes Ave, Pittsburgh
PA 15213, USA
ehayashi@cs.cmu.edu,

[2]Microsoft Research
One Microsoft Way, Redmond
WA 98052, USA
{oriana, kstrauss, ajbrush, stus}@microsoft.com

ABSTRACT

Most mobile phones and tablets support only two access control device states: locked and unlocked. We investigated how well all-or-nothing device access control meets the need of users by interviewing 20 participants who had both a smartphone and tablet. We find all-or-nothing device access control to be a remarkably poor fit with users' preferences. On both phones and tablets, participants wanted roughly half their applications to be available even when their device was locked and half protected by authentication. We also solicited participants' interest in new access control mechanisms designed specifically to facilitate device sharing. Fourteen participants out of 20 preferred these controls to existing security locks alone. Finally, we gauged participants' interest in using face and voice biometrics to authenticate to their mobile phone and tablets; participants were surprisingly receptive to biometrics, given that they were also aware of security and reliability limitations.

Categories and Subject Descriptors

H.5.2 Information Interfaces and Presentation: Miscellaneous

General Terms
Human Factors and Security

Keywords
Access Control, Sharing, Mobile Devices

1. INTRODUCTION

Most smart phone and tablet operating systems offer optional locking mechanisms (*e.g.*, PINs) that restrict access to nearly all the device's functionality. The few exceptions, such as to allow users of a locked device to answer incoming calls, make emergency calls, or take photographs, are hard-coded into the devices' operating systems. We investigated how well all-or-nothing locks meet the access control needs of 20 smart phone and tablet users, and how receptive they might be to alternative access control policies and authentication mechanisms.

First, we examined how users would configure their phones if

given the opportunity to make additional functionality available when the phone is in the locked state. We asked participants to identify their 20 most important applications. For each application, we asked whether they would want some, or all, of the application's functionality to be available when the device was locked. All participants wanted at least one of their applications protected by a security lock. On average, our participants wanted roughly half of the applications available even in the locked state and half of the applications only available in the unlocked state. This means that our participants must currently opt for an access control model that is either "too hard", putting all applications behind the lock, or "too soft", using no lock at all. A device that was "just right" would allow them to lock roughly half their phone's functionality and make the other half available when the device is locked.

We also investigated solutions to the challenges users face when trying to share their devices under an all-or-nothing access control model, which we (and others) had observed in prior work [14]. We created paper prototypes of two alternative access mechanisms that could support safer sharing: group accounts and an activity lock. Configuring a *group account* to a device enables a device's owner to grant others access to a limited set of applications. A group-specific PIN unlocks the phone to login to the group account; alternatively, the owner can transition the phone from an unlocked state to the group account state without further authentication. Another access control mechanism to facilitate device sharing, the *activity lock,* requires no configuration but is activated by the device owner before handing the device to another user. As its name implies, the activity lock restricts the available functionality of the device to that associated with a specific activity (*e.g.*, playing a game). Both of these sharing controls appealed to a significant fraction of participants. In particular, we found several parents of young children to be quite interested in enabling safe sharing of devices with their children. However, when presented in the context of devices that allowed selected applications to be made available when locked, nearly a third of participants deemed these additional sharing mechanisms unnecessary.

While knowledge-based authentication methods (*e.g.*, passwords and PINs) are most commonly used on mobile devices, proponents of biometric authentication methods have argued that these technologies may provide a faster and more convenient way to unlock a device. However, it is not clear how users react to biometrics, especially when exposed to possible false rejects and

* Research done while interning at Microsoft Research.

false accepts. Thus, we investigated participants' reactions to the use of biometric authentication to unlock their devices. Participants tried five different authentication mechanisms. Three control mechanisms chosen from technologies that are ubiquitous today, *i.e.*, numeric PINs, passwords, and security questions (*a.k.a.* challenge questions). Two biometric authentication mechanisms, face recognition and a combination of voice and face recognition, were presented to participants as if they were working features, but were actually simulated using a Wizard-of-Oz approach. The researcher remotely (and discreetly) unlocked the device when the participant tried to authenticate under some conditions, but did not unlock the device when we dimmed the lights or introduced noise to illustrate the limitations of these forms of authentication to each participant. Participants were also warned that biometric authentication might falsely allow imposters who looked or sounded like them to access the device. Despite the disclosure of these limitations, and the potential privacy-invasiveness of biometric authentication, participants were surprisingly receptive to the technology as simulated.

When combined, our findings move us closer to a future in which devices require authentication less often, can be shared more safely, and offer additional choices for how to authenticate.

2. RELATED WORK

Most mobile devices are unlocked via numeric PINs, a form of knowledge-based authentication similar (but simpler) than the passwords common to desktop computer accounts. Mobile devices present a unique challenge in that these devices are commonly accessed when users' hands and attention may be engaged in other activities. Research on mobile authentication, such as that of Clarke and others [1,2,3,4], has been ongoing for a decade—since long before the advent of the modern smart phone.

PINs are still the most common form of authentication despite myriad research into other alternatives. Many researchers have investigated graphical passwords [7,13,20] for mobile devices under the assumption that choosing or drawing images may be easier than typing characters. For example, Hayashi et al. proposed using distorted pictures to authenticate users on mobile phones to prevent educated guess attacks [10,11]. Dunphy et al. tested multiple graphical password systems against shoulder surfing attacks and found that graphical passwords were more resilient against shoulder surfing attacks than PINs [6]. Yet, graphical passwords have seen little deployment. Only recently, Android phones adopted a version of Draw-A-Secret [13], though its security is suspect; prior results by Davis et al. has shown that users often behave too predictably when choosing a graphical password [5].

Using biometric sensing (*e.g.*, face, voice, or fingerprint recognition) to authenticate has been explored for mobile devices [1,12]. Of particular relevance to our study is research that explores trade-offs associated with biometric authentication. Prabhakar et al. discussed both positive aspects of using biometrics for authentication, such as a large key space, and negative aspects, such as mistaking biometrics measurements from two different people as the same person [16]. Woodward also discussed the trade-off between the privacy protection provided by the (potentially) higher security of biometrics and privacy violation caused by using biometric information [21]. Building on these types of trade-offs, we wanted to better understand users' receptiveness to biometric authentication and

their potential concerns about using it for authentication on their phones and tablets.

Prior work has suggested adding more nuanced access control in order to facilitate safer sharing of devices. Kraut et al. investigated how people share computers among family members at their homes. They found that most of the families share a single profile, and that, when one of the family members (usually children) created their own profile, they would get annoyed [9]. As a profile management system that facilitates sharing computers among trusted users (*e.g.,* family members), Egelman et al. proposed Family Account where all files are shared by default and some files are marked by the each user as private [8].

While the desktop computers are shared among relatively small numbers of people in well-known places (home, office, etc.), due to their portability, mobile devices can be shared among a wider variety of people in different contexts. This implies a different way of sharing mobile devices and fixed computers. Karlson et al. studied users' phone sharing behaviors and identified the need for a richer security model [14]. In particular, they found that participants wanted to be able to share their devices without allowing others to delete or modify data. Stajano proposed that PDAs could benefit from having both public and private modes, or "hats", that would "draw a security perimeter" around private data when users were compelled to hand their device to another person [19]. Seifert et al. proposed TreasurePhone which divides applications into multiple access 'spheres' and switches from one sphere to another based on the user's location [18]. This prior work inspired the group account mechanism that we offered to our participants in the study. In addition, our study highlighted a new potential security threat which has not been considered before by studies on sharing controls: many of our participants with young kids were concerned about their kids misusing their mobile phones and tablets.

One unique feature of our work is that we begin by measuring the impact of a relatively small change to today's most common model—adding the ability for users to make applications available even when a device is locked. We find this relatively small change could have a very significant impact. Finally, our examination of voice and face biometrics is unique in that, by using a Wizard-of-Oz deception, we were able to collect participants' responses to voice and face recognitions as we hoped they would work in the future, not as it existed in today's implementations.

3. METHODOLOGY

We conducted structured interviews in our lab to investigate users' perceptions about access control mechanisms. Each interview lasted 90 minutes. In the interviews, we asked for participants' opinions and preferences as well as their reasoning behind their choices. Although the lab study has its limitation in terms of the ecological validity, the interview format allowed us to investigate a wide variety of options in access control mechanisms before more costly implementations and field deployments take place.

We recruited 20 participants (9M, 11F) who owned both smart phones and tablets, using Microsoft's recruiting service to access a diverse population in the Seattle region. To ensure participants could speak to the problem of access control when sharing their phones, we required that participants live with others and had shared their smart phone at least once in the last month. Prior work (*e.g.*, [14]) suggested that sharing mobile devices was common practice among friends and/or family members. We
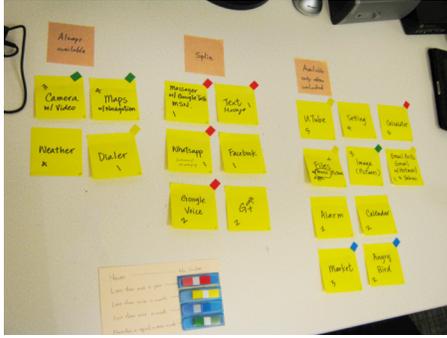
Figure 1. Participants categorized their applications by whether they wanted the application *always available*, available only *after unlocking,* or if the application's functionality should be *split* between those two categories.

| **(a) Tiles with padlock icons show applications that are inaccessible when device is locked** | **(b) Inaccessible applications are hidden when device is locked** | **(c) Baseline: all applications are inaccessible and hidden** |

Figure 2. Prototype UI designs for navigating a phone with applications available when the device is locked.

similarly found sharing was common and this requirement did not overly constrain our recruitment. To gather diverse opinions, we recruited both participants who currently use a security lock on their smart phone (11) and those who do not (9). Participants received a choice of Microsoft software and hardware gratuities (Max value $600 USD).

Our participants ranged in age between 23 to 54 years old (mean: 34). Participants used a variety of phone operating systems: iPhone (9), Android (8), Windows Phone (1), Symbian (1) and Palm Pre (1). Most participants had an iPad (17), with two participants having Android tablets and one a webOS tablet. Their occupations were diverse and included baristas, stay-at-home parents, engineers, wedding planers, business owners, and mechanics. None of the participants were Microsoft employees.

During the interviews, we first asked participants about how they would like to control access to their most important phone applications. Next, they tried multiple authentication methods including biometric authentication and then gave feedback on two mechanisms for limiting access while sharing: activity lock and group accounts. The study first focused on their phones, and then we repeated the same questions for their tablets. We now describe each section of the interview in more detail.

Figure 3. The prototype used to test the authentication methods.

3.1 All-or-Nothing Access to Applications

We asked participants to select from their installed applications the 20 that they would be least willing to give up. We then asked participants how frequently they used each application and how often they shared it with others. Next, we asked them to place each application into one of the following three categories (see Figure 1):

Always Available: Applications that would be available regardless of whether the phone was locked or unlocked.

After Unlock: Applications that could only be accessed when the phone was in the unlocked state.

Split: Applications to partition such that some functionality would be accessible when the phone was locked, and other functionality would be available only when the phone was unlocked. The example we gave of such an application was splitting the phone application into making local calls and making international calls.

After users categorized the applications, we interviewed them in more depth about their choices, and, in particular, about the applications in the Split category. We then asked them how they would prefer to manage the access to their applications and the visibility of which applications are not accessible when the device is in the locked state. To illustrate the options, we used the paper prototypes as shown in Figure 2. We offered them the choice of showing all applications with padlock icons indicating which applications are inaccessible when the device is locked (Figure 2(a)) or hiding applications that are inaccessible when the device is locked while showing all accessible applications (Figure 2(b)). We also included a baseline case which is common practice on most mobile devices. In the baseline condition, none of the available applications are shown and all applications are accessible only upon authentication (Figure 2(c)). We counter-balanced the presentation of the three designs to avoid the ordering effect.

3.2 Biometric Authentication Methods

To gauge participants' reactions to different forms of authentication, particularly biometric authentication, we had them try and rate five authentication mechanisms. We used a Samsung Focus Windows Phone 7 device, shown in Figure 3. We augmented the phone with additional Gadgeteer sensors [15] including a front camera and touch sensor on right side because there was no Windows phone that supported these sensors when we conducted the study. We tested three baseline authentication mechanisms that we expected any smart phone user would be familiar with: PINs, passwords, and secret questions (*aka* challenge question). We used a Wizard-of-Oz simulation to test

(a) PIN   **(b) Password**   **(c) Secret Question**

(d) Face Recognition   **(e) Automatic**
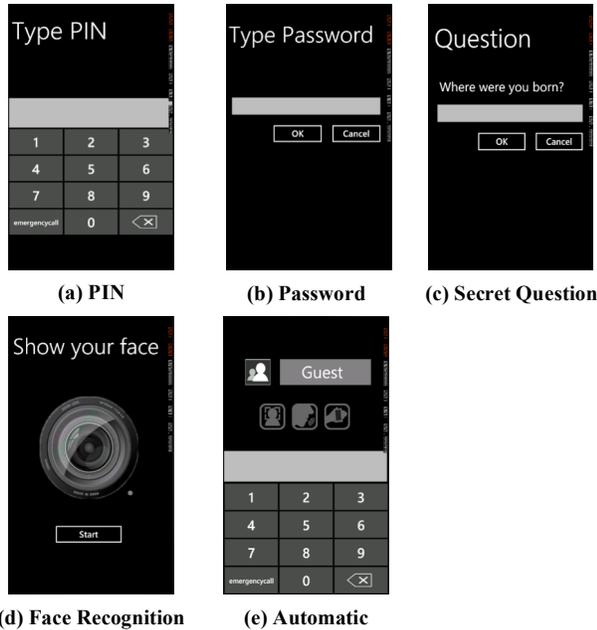
Figure 4. The screens presented in each of the five authentication methods we tested.

(a) Activity Lock   **(b) Group Account**

Figure 5. Paper prototypes of the two proposed sharing mechanisms. The blue padlock icon in (a) indicates that the access is limited to a specific e-mail and in (b) that is limited to a specific set of applications.

two biometric authentication mechanisms: one using face recognition and one using a combination of face and voice recognition, which we called *automatic* authentication [17] (see Figure 4). To describe this last mechanism, participants were told that they could use their voice, their face, or both to perform automatic authentication, so long as the biometric evidence was strong enough from whichever sensors were available. Furthermore, as long as the touch sensor on the phone sensed that they were holding their phone, the phone did not lock itself. We demonstrated that the two biometric authentication mechanisms could fail when there was noise (for voice recognition) or insufficient light (for face recognition). Participants were told to try to unlock the phone while we added noise and dimmed lights to confound participants' attempts to login via a biometric method. In these cases, participants were allowed to fall back to using the device PIN. For instance, the user interface in Figure 4(e) shows the case in which automatic authentication failed because none of the three signals (face, voice or touch) was present or detected with sufficient accuracy.

Participants locked and unlocked the phone five times using each method and we counter-balanced the order in which they were presented using the Latin square method. When participants were "using" the two biometric methods, the researcher remotely unlocked the phone as appropriate to simulate working biometrics. Participants were oblivious to this deception.

The primary purpose of showing multiple authentication schemes was to elicit our participants' qualitative opinions about using different authentication schemes. Testing the specific user interface designs was out of scope for this study. Hence, we adopted straightforward user interfaces for the authentication mechanisms.

3.3 Limiting Access when Sharing the Device
Finally, we exposed our participants to two optional add-on mechanisms for sharing their devices without granting access to
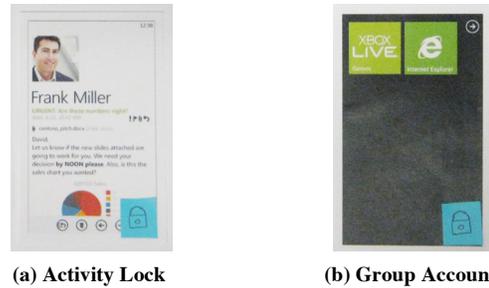
all functionality: *activity lock* and *group accounts* (see Figure 5). We told our participants that the activity lock restricted the phone such that the recipient would be limited to accessing only functionality available in the locked state and functionality associated with the device's current activity. We said that when an unlocked phone had its activity-lock activated (via a button press), only the current application would remain unlocked; for example, applying an activity lock when running the e-mail application would allow this application to remain accessible. Pressing the activity lock button one more time would lock the phone to a specific functionality *within* the application, such as reading a specific e-mail. Unlocking the activity lock would require the same authentication mechanism as the device lock.

Group accounts are similar to guest accounts in desktop operating systems and to the restricted mode approaches proposed by prior work [14,19]. One or more group accounts would provide access to some of the functionality that is normally available only when the phone is unlocked. Group accounts would be accessed via a group-specific PIN or, when the phone was unlocked, it could be put into group-restricted mode without a PIN.

We asked participants to think about how they shared their phone and whether they would prefer a simple lock/unlock mechanism (*i.e.*, current state-of-the-art), an activity lock, or group accounts. The phrasing of our question encouraged a single preference, but we allowed participants to choose more than one mechanism if they asked to do so.

4. RESULTS
In the following we present our main findings for the three parts of the study described above. To facilitate the comparison, we present results for phones and tablets together.

4.1 All-or-Nothing Access
Participants had between 12 to 103 applications on their phones (mean: 58, median: 51), and 20 to 167 applications on their tablets (mean: 72, median: 63). Out of these, each participant was asked to choose the 20 most important applications for her phone and tablet and then categorize them into the three categories of Always Available, After Unlock, and Split. Overall, our participants categorized 378 phone applications (five participants had fewer than 20 applications, and one participant chose more than 20 applications as he did not initially include phone-feature applications, such as calling) and 399 tablet applications (three participants had fewer than 20, and four participants categorized a few more than 20).

Used Phone Lock?	Participant ID	Always Available	Split	After Unlock
Yes	17	15 (71%)	3 (14%)	3 (14%)
	20	11 (55%)	3 (15%)	6 (30%)
	18	9 (47%)	4 (21%)	6 (32%)
	6	8 (40%)	4 (20%)	8 (40%)
	19	8 (40%)	3 (15%)	9 (45%)
	14	7 (35%)	5 (25%)	8 (40%)
	3	7 (35%)	0 (0%)	13 (65%)
	1	5 (25%)	5 (25%)	10 (50%)
	12	5 (26%)	5 (26%)	9 (47%)
	16	4 (20%)	6 (30%)	10 (50%)
	8	4 (20%)	4 (20%)	12 (60%)
	Subtotal	83 (38%)	42 (19%)	93 (43%)
	Median	35%	20%	45%
No	9	12 (60%)	1 (5%)	7 (35%)
	2	10 (50%)	7 (35%)	3 (15%)
	10	9 (39%)	6 (26%)	8 (35%)
	5	9 (45%)	3 (15%)	8 (40%)
	7	9 (45%)	2 (10%)	9 (45%)
	15	6 (35%)	3 (18%)	8 (47%)
	13	5 (25%)	7 (35%)	8 (40%)
	4	5 (42%)	2 (17%)	5 (42%)
	11	2 (29%)	4 (57%)	1 (14%)
	Subtotal	67 (41%)	35 (22%)	60 (37%)
	Median	41%	19%	40%
Total		150 (40%)	77 (20%)	151 (40%)
Median		39.5%	20%	40%

(a) Phones

Used Tablet Lock?	Participant ID	Always Available	Split	After Unlock
Yes	20	13 (59%)	4 (18%)	5 (23%)
	6	9 (45%)	2 (10%)	9 (45%)
	15	8 (36%)	5 (23%)	9 (41%)
	14	8 (40%)	4 (20%)	8 (40%)
	3	6 (29%)	0 (0%)	15 (71%)
	1	5 (25%)	6 (30%)	9 (45%)
	Subtotal	49 (39%)	21 (17%)	55 (44%)
	Median	38%	19%	42%
No	17	16 (80%)	1 (5%)	3 (15%)
	8	16 (76%)	0 (0%)	5 (24%)
	9	16 (84%)	0 (0%)	3 (16%)
	2	13 (65%)	5 (25%)	2 (10%)
	4	12 (63%)	4 (21%)	3 (16%)
	19	10 (50%)	0 (0%)	10 (50%)
	18	9 (43%)	6 (29%)	6 (29%)
	11	8 (62%)	3 (23%)	2 (15%)
	7	8 (40%)	2 (10%)	10 (50%)
	10	7 (33%)	4 (19%)	10 (48%)
	16	7 (35%)	3 (15%)	10 (50%)
	12	5 (25%)	7 (35%)	8 (40%)
	13	4 (20%)	8 (40%)	8 (40%)
	5	4 (20%)	0 (0%)	16 (80%)
	Subtotal	135 (49%)	43 (16%)	96 (35%)
	Median	46.5%	17%	34.5%
Total		184 (46%)	64 (16%)	151 (38%)
Median		41.5%	18.5%	40%

(b) Tablets

Table 1. Participants categorized phone (a) and tablet (b) applications into applications they wanted *Always Available*, applications that should be available only after the device is unlocked (*After Unlock*) and applications they wanted to *Split* such that only some application functionality would be always available and some would be available only after the device is unlocked. Participants who currently use their device's lock (*yes* in the leftmost column) appear above those who do not. Participants are ordered based on the number of applications placed in the Always Available category.

We found a surprisingly even division between the number of applications that participants wanted to protect with the lock and the number they wanted available. Participants wanted 35% (median) of applications on their phones to be Always Available, 45% (median) of applications to be available only After Unlock, and 20% (median) of four applications to be Split such that some functionality would be always available while other functionality was protected by the lock. The allocation of phone applications to categories for each participant is shown in Table 1(a).

For our 20 participants all-or-nothing access to applications appears to be a poor fit for every one of them, regardless of whether they currently use or do not use security locks on their devices. Overall, our participants put at most 71% of their categorized applications into a single category. The best case, as shown in Table 1, is that of P17 who could have 15 (71%) of her applications in the category she desired for them (Always Available) by deactivating her phone's security lock. Yet, even this is not a perfect solution—she currently uses the lock on her phone to protect six of the applications she did not want always available. Thus current locking mechanisms, which force users to choose between using the phone's lock for all applications or for none, do not match how participants told us they wanted to manage access control to their applications.

Simply allowing users to configure whether each application is available or unavailable when their phones are locked enables users to manage the applications in Always Available and in After Unlock according to their preferences. Although this simple modification does not help the applications in Split, it makes the access control system significantly closer to what users want compared to the current all-or-nothing approach.

The allocation of tablet applications to categories is shown in Table 1(b). The results are very similar to those for phones, with participants preferring to make a slightly (not significantly) larger fraction of applications Always Available. Six participants commented that they mostly kept their tablets at home, which might have made them less concerned about security and privacy on these devices.

We asked participants to explain the motivations behind their categorizations. Not surprisingly, the two main factors mentioned were privacy (for locking the application) and convenience (for making it always available).

Applications Types	Always Available	Split	After Unlock	*Type Total*
Utilities	31	6	32	69
Communications	4	27	21	52
Productivity	7	12	32	51
Photography	14	12	10	36
Entertainment	18	4	11	33
Social	5	4	19	28
Reference	10	7	9	26
Navigation	14	1	3	18
Games	12	0	2	14
Lifestyle	4	4	5	13
Weather	11	0	0	11
Travel	4	0	2	6
News	5	0	0	5
Music	3	0	1	4
Finance	1	0	3	4
Books	1	0	0	1
Others	6	0	1	7
Total	150	77	151	378

(a) Phones

Applications Types	Always Available	Split	After Unlock	*Type Total*
Entertainment	40	8	18	66
Productivity	10	9	27	46
Games	32	1	12	45
Utilities	9	7	29	45
Photography	16	7	12	35
Communications	1	9	15	25
Social	0	9	16	25
Reference	12	5	5	22
Lifestyle	15	2	1	18
Books	6	2	9	17
News	14	1	1	16
Travel	8	0	2	10
Music	6	1	1	8
Navigation	7	0	0	7
Finance	0	2	3	5
Weather	2	0	0	2
Others	6	1	0	7
Total	184	64	151	399

(b) Tablets

Table 2. Participants' classification of applications into Always Available, Split, and After Unlock shown by the type of application.

Most participants reported that they wanted applications containing personal data to be available only After Unlock (18 participants for phones and 13 for tablets). P6 said, "These all contain my personal information, which I don't want people to see." Conversely, several participants reported they wanted applications that did *not* contain personal data to be Always Available (13 participants for phones and 6 for tablets). P19 commented, "For always available [category], I put things that won't have direct connections to my private information."

Seven participants mentioned quick access as a reason to make phone applications always available, and ten did so for tablets. P15 said, "If you have this stuff available without unlocking it, it's just handier." P12 also said, "[Applications in always available are] stuff I want to access quickly." Furthermore, P12 had a particularly strong desire for quick access while driving. She told us: "I'm using my iPhone for navigation. But it locks. Then I have to type my password to unlock it while driving. So I disable the lock when I drive."

Some participants also reported that they wanted applications that could be used to make purchases available only After Unlock (6 participants for phones and 11 for tablets). P5 commented, "there are things where you can purchase things, which I don't want somebody to access."

4.1.1 Types of Applications
We hypothesized that certain types of applications would be more likely than others to be made Always Available. We classified applications into types, using the grouping taxonomy of the iTunes application store, to examine how different types of applications might have different security/accessibility tradeoffs. Three researchers manually classified other applications (*e.g.*, applications for other phones or applications distributed using different channels) working together to resolve any disagreements. The results are presented in Table 2.

Supporting participants' qualitative comments about how they categorized their applications, types of applications likely to require personal information (*e.g.*, communication) were likely to be made available only After Unlock or Split, whereas those unlikely to hold personal information (*e.g.*, entertainment) were more likely to be made Always Available.

Among the 378 phone applications, the most common categories were *utilities* (69, 18%), *communication* (52, 14%), and *productivity* (51, 13%). On the other hand, among the 399 tablet applications, the most frequent types were *entertainment* (66, 17%), *productivity* (46, 12%), *games* (45, 11%), and *utilities* (45, 11%). This difference suggests that our participants' tablets were primarily used for entertainment, while their phones were used for practical purposes. Participants' comments also suggest that these differences in types of installed applications may make them less conservative about sharing tablets than sharing phones. Table 3 shows how frequently applications on phones (Table 3(a)) and tablets (Table 3(b)) were shared. The distribution of the applications by sharing frequency shown in the rightmost columns indicates that applications on tablets were more frequently shared. P9 commented, "For the most of part we use this [tablet] for entertainment but we don't have any critical information saved. There may be some passwords, Pandora, YouTube, Netflix, Live Strong. But, they are not a big deal." P3 also commented, "My phone is more like my personal thing. This [tablet] is not a big deal because it's a shared device. It wouldn't affect me."

4.1.2 Application Usage and Sharing Frequency
We hypothesized that a desire for convenience might cause users to make their most frequently used applications always available. Contrary to our expectations, we found that the Always Available category contained a disproportionately small number of frequently-used applications (Table 4). The participants reported 101 phone applications to be used most frequently (*i.e.*, more than 10 times a day). However, they wanted only 22% of their most frequently used phone applications, and 29% of their most frequently used tablet applications, to be always available. Alas, the applications participants used most also contained the most sensitive information, such as e-mail.

Sharing Frequency	Always Available	Split	After Unlock	Total
5 (Weekly)	26	13	7	**46**
4	19	12	14	45
3	25	9	20	54
2	10	9	8	27
1 (Never)	70	34	102	206
Total	150	77	151	378

(a) Phones

Sharing Frequency	Always Available	Split	After Unlock	Total
5 (Weekly)	78	12	19	**109**
4	17	7	21	45
3	15	3	10	28
2	2	4	4	10
1 (Never)	72	37	97	206
Total	184	63	151	398

(b) Tablets

Table 3. Participants' classification of applications into Always Available, Split, and After Unlock shown by the sharing frequency of applications. The frequency metric (5 to 1) stands for, 5) more than or equal to once a week, 4) less than once a week, 3) less than once a month, 2) less than once a year, and 1) never.

Usage Frequency	Always Available	Split	After Unlock	Total
5 (10+ times a day)	22	33	46	101
4	49	21	43	113
3	37	12	27	76
2	24	4	17	45
1 (less than weekly)	18	7	18	43
Total	150	77	151	378

(a) Phones

Usage Frequency	Always Available	Split	After Unlock	Total
5 (10+ times a day)	10	9	15	34
4	46	23	40	109
3	47	16	43	106
2	31	8	23	62
1 (Less than weekly)	50	8	30	88
Total	184	64	151	399

(b) Tablets

Table 4. Participants' classification of applications into Always Available, Split, and After Unlock shown by the usage frequency of applications. The frequency metric (5 to 1) stands for 5) more than 10 times a day, 4) one to 10 times a day, 3) more than or equal to once in three days, 2) more than or equal to once in a week, and 1) less than once a week.

We also hypothesized that applications that were more frequently shared would be more likely to be made always available. We asked the participants to indicate how frequently they shared each application, using a scale with five options: *weekly*, *less than once a week*, *less than once a month*, *less than once a year*, *never*. Indeed, there does appear to be a correlation between applications that are frequently shared and those that participants wanted to be always available (Table 3). Applications that were shared weekly were made always available 57% (26 out of 46) of the time on phones, and 72% (78 out of 109) of the time on tablets.

4.1.3 Applications in Split Category
Perhaps most interesting are the applications our participants put in the Split category when they wanted some functionality to be Always Available and other functionality available only After Unlock. As the Total row in Table 1 shows, overall, participants wanted 20% of the phone applications and 16% of tablet applications to be split in this way. We asked participants to explain which functionality should be Always Available and which functionality should be available After Unlock. They described three different ways to split applications:

Feature sensitivity: Protecting a particular feature or set of features was the most common reason for splitting. Five participants wanted inbound communications (*e.g.*, receiving phone calls) to be always available while outbound communications (*e.g.*, making a phone call) available only after unlocking. Six participants also said that browsing existing entries or creating new entries in an application should always be possible, while modifying or deleting existing entries should be possible only after unlock. Furthermore, for the applications involving purchasing of goods, such as App Store or coupon applications (*e.g.*, Groupon), eight participants wanted browsing information to be always available while purchasing to require unlocking the phone.

Data sensitivity: Protecting some of the data in an application was another reason given for splitting. For example, three participants wanted emergency contacts to be always available, but access to most contacts to require unlocking the phone. Two participants mentioned they wanted some photos, such as those of their children, to be available only after unlocking. Lastly, in the calendar application, a participant wanted business appointments to be always available, and private appointments to be available only after unlocking.

Freshness: Splitting between showing the most recent data and older data was the final reason described to us. For the communication applications (*e.g.*, text messaging, instant messenger and e-mail), four participants wanted new incoming messages to be always available. In contrast, they felt old messages should be available only after unlocking.

4.1.4 User Interface for Unlocking Applications
Table 5 shows participants' preferences between the prototype user interfaces (shown in Figure 2) for showing or hiding inaccessible applications when the phone is locked. For phones, about half of the participants preferred showing inaccessible applications (*i.e.*, those requiring the device be unlocked) using a padlock icon to indicate that they were currently inaccessible. For tablets the trend was less clear, but 40% of participants preferred showing only the applications available while the tablet was locked, hiding the locked ones until after the user authenticates.

Participants' comments suggested that their choice of preferred user interface had a social explanation. Some participants did not want other users to see applications that were inaccessible to them. For example, P16 said that knowing these applications were not available to others might "piss them off". P5 said a user interface showing inaccessible applications might "tease" his daughter. In contrast, participants who preferred showing inaccessible applications with lock icons indicated it was for visibility and convenience. Participants liked the fact that they

Device	Showing Inaccessible	Hiding Inaccessible	PIN
Phones	**11 (55%)**	5 (25%)	4 (20%)
Tablets	6 (30%)	**8 (40%)**	6 (30%)

Table 5. Participants' preferences among designs for navigating a locked device. Most preferred method for each device is bolded.

Sharing	Showing Inaccessible	Hiding Inaccessible	PIN
Frequent	4 (20%)	**12 (60%)**	4 (20%)
Infrequent	**13 (65%)**	4 (20%)	3 (15%)

Table 6. Participants preferred hiding inaccessible applications on frequently shared devices and showing inaccessible applications on devices infrequently shared.

could see all applications. P1 said that the design "shows you what's there," even if it is not currently available. Another popular reason to choose this design was that it made clear when the PIN was necessary.

Given these comments, to understand if the amount a device was shared is a good predictor of which interface was preferred we categorized the devices into two groups based on sharing frequency. We categorized as *frequently shared* devices with five or more applications shared at least monthly. Other devices were categorized in *infrequently shared*. As Table 6 shows, many participants did favor hiding inaccessible applications on frequently shared devices (60%) and showing inaccessible applications on infrequently shared devices (65%).

4.2 Access when Sharing

Participants reported sharing a mean of 12% of their phone applications (median: 9%) more than once a week—primarily *photography* applications. Participants reported sharing a mean of 27% of their tablet applications (median: 25%) more than once a week—primarily *entertainment* applications. Similar to the informal and spontaneous types of sharing reported by Karlson et al. [12], our participants were more likely to mention focused, short-term sharing scenarios on their phone, such as sharing a photo, making a quick phone call, as compared to longer term-sharing scenarios on their tablet, such as watching movies or browsing the web.

At the top of many participants' security concerns were individuals with questionable judgment and frequent access to their devices—their children. Of the 11 participants with children, five referred to their children as one of the threats they wanted to protect against. Parents wanted to limit the access privileges of children because unintentional actions could cause unintended modification or deletion of data. Furthermore, they expressed concerns that children might, accidentally or purposefully, make purchases or perform other actions that cost money.

4.2.1 Activity Lock and Group Accounts Preferences

Participants were divided as to which sharing mechanism would work best for them, as illustrated in Table 7. Fourteen participants preferred to have Activity Lock (6) and/or Groups (9) on their phones over a lock alone. This included one participant who wanted both on her phone. Three participants wanted both on their tablets. For nine phones and ten tablets, participants chose group accounts. For six phones and six tablets, participants chose to have an activity lock. While we suggested that participants elicit a single preference, we allowed participants to choose more than one option if they chose to do so; the options are complementary as a phone could have both group accounts and an activity lock. On six phones and seven tablets, the owners prefer to have neither activity lock nor group accounts, if they can configure which applications are always available and which applications are available only after their devices are unlocked.

Participants who wanted the activity lock were more likely to describe ad-hoc or irregular sharing scenarios. P12 described using the activity lock "if I want to show you something, that's all I want." In contrast, those who expressed preferences for group accounts were more likely to discuss recurrent sharing scenarios.

Four participants expressed concerns configuring groups on phones would take too long. P11 said, "I just think it's interesting although I won't use it. It may be more hassle than worth… it takes too much time to configure". No participants raised the configuration time concern for tablets. P2 described his desired simple configuration in which he could tell his kids to "dial 1234 and you can use your applications".

While 70% of the participants preferred to have either the activity lock or the group accounts on their devices, 30% of the participants chose neither of the additional sharing mechanisms. Most of them reported that the extra effort was not worth the benefits, assuming the feature that allows them to categorize applications into the three categories (always available, split and after unlock) was available. For example, P7 said, "these offer a lot of granularity but I don't look for a lot granularity because we have always available and not available".

4.3 Receptiveness to Biometric Authentication

Participants had some applications for which they wanted to require a lock in both their own use and when sharing. While phones and tablet devices typically use a PIN lock, biometrics is

| Devices	Activity Lock	Group Accounts	Unlock Device
Phones	6 (29%)	9 (42%)	6 (29%)
Tablets	6 (26%)	10 (43%)	7 (31%)
Total	12 (27%)	19 (43%)	13 (30%)

Table 7. Preferred mechanisms to support sharing of phones and tablets. As we allowed participants to choose more than one option, each row does not sum up to 20.

Scheme	Overall		Convenience		Security	
	P	T	P	T	P	T
PIN	2	6	1	3	2	3
Password	1	1	0	0	**10**	**12**
Secret Question	0	0	0	1	0	0
Face Recognition	2	3	4	6	4	2
Automatic	**15**	**10**	**15**	**10**	4	3

Table 8. Participants' preferred authentication method overall and based on convenience and security for phones (P) and tablets (T).

another possible mechanism for authentication. In the study, participants authenticated five times with five authentication methods: a PIN, password, secret question, face recognition, and a method we referred to as "automatic" authentication, which combined face and voice biometrics. (Recall that, unbeknownst to our participants, the biometric authentications were only simulated—our researcher triggered the unlock mechanism remotely.) We asked participants their preferred method overall, which method they felt was most convenient and which method they felt was most secure.

Table 8 shows three quarters of participants preferred automatic authentication for their phone, using voice and face biometrics, despite recognizing that it might not be as secure as a password or PIN. Ten participants preferred automatic authentication for tablets, whereas six preferred using a PIN. Only two had preferred a PIN for their mobile phone. Participants who preferred using PINs for their tablets often liked the simplicity PINs offer when devices are shared. P19 said, "It's shared all the time. Simplicity is important considering how often it is shared." Another reason given by P3 for preferring PIN was that he did not need high security for the tablet. He said "I chose PIN because there is no reason for it to be super duper private. My phone comes with me everywhere, but my iPad stays at home. So there is no necessity for security."

Five participants mentioned that automatic authentication would work well when they drive. For example, P4 reported that his preference was influenced by not wanting to "push buttons" to authenticate while driving.

We were also surprised that only one participant mentioned privacy as a concern in using the two biometric authentication schemes. This surprised us as privacy is often cited as a concern with biometrics [21]. Once users register their biometrics information to an authentication system, the information could be easily replicated and shared among multiple parties to track the users. Furthermore, the users cannot change their biometrics information even if they noticed that their biometrics information is leaked. Although leakage is less of a risk when the biometrics information is stored in a local device, there is no clear way for users to distinguish whether the biometrics information is stored locally or sent to a server. Perhaps few participants expressed privacy concerns because they already speak into their mobile devices and use them to take photographs. It's also possible that participants would have felt uncomfortable expressing privacy concerns to researchers, as it might imply distrust.

Although overall the results are encouraging for using biometrics for authentication, participant preferences do come with some caveats. Once again, participants were not aware that the system they preferred was not real. Participants may have believed that the researchers had put great effort into perfecting a working

biometric authentication system and wanted to please the researchers by expressing a preference for that system. Also, real biometric authentications might not perform as seamlessly or inspire as much confidence as a Wizard-of-Oz simulation.

4.3.1 Multi-level Authentication

We initially asked participants to categorize their applications based on whether functionality should be Always Available or only After Unlock (or Split between those two options). However, there is no reason that users must be limited to only two authentication states. After participants had tried the five different authentication methods we asked them whether they wanted to add one or more additional authentication states in addition to locked and unlocked, and, if so, what method of authentication they wanted to use for that state. Note that additional authentication states could be accessible via authentication that was weaker than what a participant preferred for unlock, but stronger than no authentication at all. Or conversely, additional states could use methods more secure than what the participant preferred for unlock.

Ten participants expressed a preference for adding another authentication level. Four of these described using biometric authentication as a weak authenticator and using PIN or password for stronger authentication. For example, for applications such as banking, e-mail or social networking, they wanted to be more protected. Perhaps not surprisingly, most participants (8 of 10) that were interested in an additional authentication level were currently using security locks on their phone.

The decision to add additional authentication levels was more popular for phones than for tablets. Only three participants were interested in additional authentication levels on tablets. One participant classified tablet levels as "Always", "Kids", and "No kids", essentially using a third authentication level in place of a group account.

5. LIMITATIONS

The results of our study, like all studies, should be interpreted with a full understanding of the limitations of our methodology. Participants were asked hypothetical questions, and their self-reported responses may not match the choices they would make in reality. Unfamiliarity with Windows phones could have also caused confusion. On the other hand, all but one participant were unfamiliar with Windows phones and so they were equally inexperienced.

For all participants, we first asked questions about their phones and then repeated questions for their tablets. We did not randomize or counterbalance. Thus, statistical differences between what participants reported for their phones and what they reported for their tablets could be the result of changes in preference that occur over the progression of the study.

While one benefit of our lab study was the ability to gather qualitative data from participants about the reasons behind the choices they made, we want to acknowledge that our participants used the authentication mechanisms only in a laboratory environment. The mechanisms worked when they could reasonably be expected to and were never exposed to security attacks. Real biometric authentication systems may not be able to perform as seamlessly. By the time such systems become available, participants' preferences may have changed based on other experiences, the reports of others, or other factors.

Finally, for some participants the 20 applications we sampled might not be representative of the full set of applications on their devices. Regardless of this limitation, this subsample alone seems sufficient to disprove the assumption that all-or-nothing access to applications meets users' needs.

6. CONCLUDING REMARKS

For our participants, all-or-nothing access to applications does a remarkably poor job of meeting their self-reported preferences. Allowing applications to be made accessible in the locked state would go a long way to meeting our participants' needs, and likely mobile users in general.

Across both tablets and phones, we saw that the amount a device is shared has an effect on how users would like to manage access control including what user interfaces they prefer for showing which applications are accessible when the device is locked and the desire for additional sharing mechanisms. Since tablets are more likely to be shared by many users, all-or-nothing locks seem an even worse fit for these devices than they are for phones. Our participants' preferences suggest that some form of user or group accounts is overdue, especially for tablets. Participants were also interested in sharing devices using activity locks, especially in ad-hoc situations such as reading an e-mail or receiving driving directions. The results indicate potential usefulness of the access control systems, which could be further validated in field studies.

Whereas security designers often focus on highly malicious threats, we found that several parents of young children were most concerned about misuse by their kids. For instance, participants were concerned that small children (around five years old) could delete data on the devices by chance. Other participants were concerned that their children (around 10 years old) may purchase applications without their permissions. These children are legitimate users in some use cases (*e.g.*, parents let them play games on the devices). However, they could be a real threat in practice. A threat model for mobile devices that does not account for usage by the device owner's children is undoubtedly incomplete. Access control features designed with children in mind may serve the needs of these users better than more robust features. Allowing parents to make games accessible to children without a PIN, or with a simple group PIN, might actually make systems more secure—parents would no longer have to include their toddlers among the set of people who might reveal the PIN that guards access to their work e-mail application.

While the limitations of our study prevent us from knowing definitively whether participants' preference for biometric authentication would extend to real-world implementations and real-world situations, we were encouraged that few participants expressed concerns despite our attempts to disclose their limitations. Participants' lack of concern about biometric privacy may have simply been an acknowledgement that their device is already frequently trusted to collect the sound of their voice and the likeness of their face.

We believe these findings move us closer to a future in which devices require authentication less often, can be shared more safely, and offer additional authentication options for times when it may be unsafe or undesirable to enter a shared secret.

7. ACKNOWLEDGEMENTS

8. REFERENCES

[1] Nathan L. Clarke, Steven M. Furnell, Paul L. Reynolds. 2002. Biometric Authentication for Mobile Devices, In Proceeding of the 3rd Australian Information Warfare and Security Conference, 61-69.

[2] Nathan L. Clarke, Steven M. Furnell, L. B. Lines, Paul L. Reynolds. 2002. Subscriber Authentication for Mobile Phones through the Implementation of Keystroke Dynamics, In Proceeding of the 3rd International Network Conference, 347-355.

[3] Nathan L. Clarke, Steven M. Furnell, Paul L. Reynolds, Phillip L. Rodwell. 2002. Advanced Subscriber Authentication Approaches For Third Generation Mobile Systems, In Proceeding of the 3rd International Conference on 3G Mobile Communication Technologies.

[4] Nathan L. Clarke, Steven M. Furnell. 2005. Authentication of users on mobile telephones – A survey of attitudes and practices. Computers and Security. Vol. 24, Issue 7, 519–527.

[5] Darren Davis, Fabian Monrose, and Michael K. Reiter. 2004. On User Choice in Graphical Password Schemes. In Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13 (SSYM'04), Vol. 13. USENIX Association, Berkeley, CA, USA, 11-11

[6] Paul Dunphy, Andreas P. Heiner, and N. Asokan. 2010. A closer look at recognition-based graphical passwords on mobile devices. In Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS '10). ACM, New York, NY, USA, Article 3 , 12 pages. DOI=10.1145/1837110.1837114 http://doi.acm.org/10.1145/1837110.1837114

[7] Rachna Dhamija and Adrian Perrig. 2000. Déjà Vu: A User Study Using Images for Authentication. In Proceedings of the 9th conference on USENIX Security Symposium - Volume 9 (SSYM'00), Vol. 9. USENIX Association, Berkeley, CA, USA, 4-4.

[8] Serge Egelman, A.J. Bernheim Brush, and Kori M. Inkpen. 2008. Family accounts: a new paradigm for user accounts within the home environment. In Proceedings of the 2008 ACM conference on Computer Supported Cooperative Work (CSCW '08). ACM, New York, NY, USA, 669-678. DOI=10.1145/1460563.1460666 http://doi.acm.org/10.1145/1460563.1460666

[9] David M. Frohlich and Robert Kraut. 2003. The Social Context of Home Computing. Inside the Smart Home. R. Harper. London: Springer-Verlag, pp. 127-162

[10] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. 2008. Use Your Illusion: Secure Authentication Usable Anywhere. In Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08). ACM, New York, NY, USA, 35-45. DOI=10.1145/1408664.1408670 http://doi.acm.org/10.1145/1408664.1408670

[11] Eiji Hayashi, Jason Hong, and Nicolas Christin. 2011. Security through a Different Kind of Obscurity: Evaluating Distortion in Graphical Authentication Schemes. In Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11). ACM, New York,

NY, USA, 2055-2064. DOI=10.1145/1978942.1979242 http://doi.acm.org/10.1145/1978942.1979242

[12] Anil K. Jain, Ruud Bolle, and Sharath Pankanti. 1999. Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers.

[13] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. 1999. The Design and Analysis of Graphical Passwords. In Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99), Vol. 8. USENIX Association, Berkeley, CA, USA, 1-1.

[14] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones. In Proceedings of the 2009 Annual Conference on Human Factors in Computing Systems (CHI '09). ACM, New York, NY, USA, 1647-1650. DOI=10.1145/1518701.1518953 http://doi.acm.org/10.1145/1518701.1518953

[15] Microsoft .NET Gadgeteer,, http://www.netmf.com/gadgeteer/ (May, 31, 2012)

[16] Salil Prabhakar, Sharath Pankanti, and Anil K. Jain. 2003. Biometric Recognition: Security and Privacy Concerns. Security & Privacy, IEEE, vol.1, no.2, pp. 33- 42. DOI=10.1109/MSECP.2003.1193209. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1 193209&isnumber=26759

[17] Oriana Riva, Chuan Qin, Karin Strauss, Dimitrios Lymberopoulos. 2012. Progressive authentication: deciding when to authenticate on mobile phones. In Proceedings of the 21st USENIX Security Symposium, August 8-10, 2012.

[18] Julian Seifert, Alexander De Luca, Bettina Conradi, and Heinrich Hussmann. 2010. Treasurephone: Context-sensitive user data protection on mobile phones, In Proceedings of the 8th International Conference on Pervasive Computing, pp. 130-137, DOI=10.1007/978-3-642-12654-3_8.

[19] Frank Stajano. 2004. One user, many hats; and, sometimes, nohat–towards a secure yet usable PDA. In Proceeding of Security Protocols Workshop. 51-64.

[20] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. In Proceedings of the 1st Symposium on Usable privacy and security (SOUPS '05). ACM, New York, NY, USA, 1-12. DOI=10.1145/1073001.1073002 http://doi.acm.org/10.1145/1073001.1073002

[21] Woodward, J.D. 1997. Biometrics: Privacy's Foe or Privacy's Friend?. Proceedings of the IEEE, vol.85, no.9, pp.1480-1492, Sep 1997. DOI=10.1109/5.628723. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6 28723&isnumber=13673.