

Usage Profiles for the Mobile Phone

Amy K. Karlson

Microsoft Research, Visualization and Interaction Group
One Microsoft Way, Redmond, WA 98052
karlson@microsoft.com

Abstract. “Usage profiles” may offer an effective means to compartmentalize access to data and services to address privacy and security concerns that arise when users intentionally and unintentionally share their phones with others. I discuss the research questions I am exploring to inform the user-center design of usage profiles, such as how many profiles are appropriate, what data and services are accessible from each profile, and how users switch among profiles.

Keywords: Mobile phone, sharing, security, privacy.

1 Introduction

Mobile phones today exemplify personal computing. First, their rapid proliferation and adoption mean that in many markets, nearly every person has one. Second, phones’ small forms and high portability mean users can keep them within arm’s reach at all times. Third, by supporting a variety of text and voice communications, phones can satisfy a wide and important range of peoples’ social and data connectivity needs. At the same time, phones’ increasing processing capabilities elevate their utility as service, computing and entertainment platforms. Finally, phones’ expanding storage capacities allow users to keep larger volumes of personal data on the phone, such as communication histories (SMS, email, phone calls), calendar data, contacts, and even traditional media like documents, photos and music.

Given that phones are such personal devices, it is unsurprising that they typically support only a single-user model of security: either the phone is password-locked and none of its features are accessible, or the phone is unlocked and all of its features are accessible. Since typing a password every time you pick up your phone is tedious, this model of security often fails due to non-use. Although advances in low-overhead authentication solutions (e.g., fingerprint readers) may do much to encourage people to secure their devices between uses, the all-or-nothing approach to device security ignores the fact that it can be useful and natural to let others use our personal phones.

Indeed, while phones typically have a single owner, field studies have reported that phone sharing is commonplace [2,3]. Although the populations that have been studied (teenagers and communities in the developing world) have had economic incentives to share their phones, observations and interviews confirm that there are also a host of social and pragmatic motivations for phone sharing that are relevant across diverse user populations. Consider an example from my own life: *I am driving myself and my*

friend Jacquie to the movies, where we plan to meet up with our friend Lisa. During the drive, my phone rings and I see that it is Lisa who is calling. Assuming that Lisa's call is related to our plans, I pass my phone to Jacquie to field the call while I drive.

When I pass my phone to Jacquie, I am handing over all the personal data I have stored on it. Since Jacquie is a close friend, this does not particularly alarm me. Furthermore, since Jacquie is sitting next to me, it would be socially inappropriate for her to interact with my phone beyond the length of the phone call. But now imagine that I ask her to look up directions to the theater using my phone's web browser. In doing so, she may inadvertently see upcoming work appointments displayed on my home screen, the email messages displayed from my last interaction with the browser, and my previous web searches. Other than the fact that my employer might not appreciate a non-employee viewing a work-related appointment, the convenience of having Jacquie look up directions for me far outweighs the mild discomfort I have in her stumbling upon information she would not otherwise have access to.

If we instead put a coworker in my passenger seat, I now want to limit the exposure of my personal data and so am unlikely to encourage follow-up interactions. Unfortunately, with today's devices, the tradeoff is that I miss out on a favor because my options are limited to handing my device to someone (exposing all my data) or not (protecting my data). If I could instead put my device in "guest" mode, or better yet, my device automatically switches to guest mode when it detects that the person holding the device is not me, then I am freed from the burden of performing threat assessments at every sharing opportunity, *and* I get the favor I want – a double win!

2 Understanding User Profile Requirements

The idea of protecting private data from the eyes of others by enabling different usage modes for mobile devices is not new. Stajano [1] 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 otherwise compelled to hand their device to another person. In his discussion, Stajano theorizes about the data and services that might be assigned to the public and private "hats", flow-of-control requirements in switching between "hats", and the tradeoffs of alternative authentication methods and implementation models. Although usable security is his goal, Stajano's research focuses largely on the pragmatic implementation challenges.

As a complement to Stajano's system-level approach, I am interested in the human-centered requirements for multiple modes of operation. I call these modes "usage profiles" rather than "hats" since a "hat" is person-centric, and I believe it is an open question whether usage profiles are more appropriately centered on types of *people*, or types of *activity*. Ultimately, however, I am interested in understanding what constitutes a tractable, useful, and usable set of usage profiles for the phone.

Two fundamental and inseparable aspects of my exploration will be in investigating 1) *how many* profiles are appropriate; and 2) *what data and services* are available from within each profile. Stajano suggested a minimum of two profiles: public and private. But is this too simplistic? Perhaps I want my spouse to have access to everything on my phone except for my work calendar and email (the "spouse"

profile). But when my coworker's phone dies and she asks to use my phone to send an email, I would like to ensure she doesn't see my communications histories, calendar data, contacts, or even application access history (the "colleague" profile). And when my 5-year old nephew asks to play Pong on my phone, I am not so much worried about him seeing my personal data as I am concerned about protecting my data from accidental additions or deletions (the "child" profile).

The challenge of establishing an appropriate number of usage profiles is that offering too many profiles might confuse users, while offering too few might not provide users adequate flexibility. I propose that user confusion might be mitigated if profile definitions match the user's mental model of the sharing activity. For example, if a user's trust varies widely among the people in her life, it might be helpful for her to define profiles in terms her personal relationships (e.g., spouse, colleague, stranger). Alternatively, we might offer profiles around the *activities* that an owner allows others perform (e.g., calling, gaming, web browsing). Note that these approaches do not just differ in name, but imply different groupings of data and services; relationship-based profiles might have a hierarchical structure (a coworker is at least as trusted as a stranger), while activity-based profiles might be more disjoint.

I am currently designing a user study to understand how the characteristics of number, function, and structure of usage profiles impact their usability and desirability. I will also explore interface designs and user expectations for the mechanism(s) by which users switch among profiles. Since the success of a security scheme relies on an owner's willingness to use it, research must target both the system-level implementation as well as user-guided approaches that are flexible enough to match varying user preferences and mobile scenarios. I look forward to sharing my ideas, learning about the work of others, and engaging in the cross-disciplinary dialog that will help bring effective security to the mobile space.

3 Bio

Amy Karlson recently joined Microsoft Research's Visualization and Interaction (VIBE) Group as an HCI researcher. She is currently interested in the role that mobile devices play in spanning users' various information and communications networks, and addressing the usability and privacy challenges that arise from the boon of accessing limitless public and personal data from the palms of our hands.

References

1. Stajano, F. One user, many hats; and, sometimes, no hat—towards a secure yet usable DA. Security Protocols Workshop, Springer Verlag (2004), 51-64.
2. Steenson, M. and Donner, J. Beyond the personal and private: Modes of mobile phone sharing in urban India. In S. W. Campbell & R. Ling (Eds.), Mobile Communication Research Annual (Vol. 1), Transaction Books (in press).
3. Weilenmann, A. and Larsson, C. Local use and sharing of mobile phones. In B. Brown, N. Green and R. Harper (Eds.), Wireless World: Social and Interactional Aspects of the Mobile Age, Springer Verlag (2001), 99-115.