Secure Mobile Phone Access to Remote Personal Computers: A Case Study

Alireza P. Sabzevar and João Pedro Sousa

Computer Science Department, George Mason University
4400 University Drive 4A5, Fairfax VA, U.S.A.
apirayes@gmu.edu, jpsousa@cs.gmu.edu

Abstract. Cell phones are assuming an increasing role in personal computing tasks, but cell phone security has not evolved in parallel with this new role. In the class of systems that leverage cell phones to facilitate access to remote services, compromising a phone may provide the means to compromise or abuse the remote services. To make matters concrete, SoonR, a representative off-the-shelf product is used to examine this class of systems from a security point of view. This paper identifies the shortcomings of existing solutions, and explores avenues to increase security without compromising usability. The usability of two proposed techniques is evaluated by means of a user study.

The contribution of this paper is a set of guidelines for improving the design of security solutions for remote access systems. Rather than proposing a one-size-fits-all solution, this work enables end-users to manage the tradeoff between security assurances and the corresponding overhead.

Keywords: Mobile computing, Remote PC access, Security, SoonR, User studies, Visual cryptography.

1 Introduction

In recent years, cell phones have evolved spectacularly from supporting telephony only to supporting multiple features, ranging from capturing and playing digital media, to e-mail access, to e-banking [1, 2], to remote access to personal files [3, 4].

Cell phone security, however, has not evolved at the same pace. There exist recent examples of high-end phones which support sophisticated security features. For example, NTT DoCoMo in collaboration with Panasonic produces a phone equipped with face-recognition and satellite tracking, and that automatically locks down when the user moves beyond a certain distance [5]. However, the vast majority of phones supporting the estimated 4 billion mobile service subscriptions in 2008 offer only the same password mechanisms used a decade ago [6].

With explosive popularity, their rising role in supporting daily activities of end-users, and with limited security mechanisms, cell phones are increasingly appealing targets for attackers.

Because today’s phones are components of distributed software systems, a holistic view of security needs to be adopted: not only the phone and information it contains is at risk, but also is the information and services the phone has access to. Because an
attacker may obtain enough information to pose as the legitimate user to the remote services, physical protection of the phone is only part of the solution. These concerns are especially relevant for an emerging class of systems called remote control applications [7].

This paper focuses on a subclass of remote control applications where a cell phone facilitates access to files and services on a remote personal computer. To make matters concrete, we analyze and build on a commercial product, SoonR [3, 8], which is representative of this kind of solutions.

This work does not aim at improving the state of the art of security protocols, but rather at providing guidance for improving the engineering of solutions. For that, we analyze the threats and possible countermeasures for this class of applications.

A key principle for the work herein is to allow users to control the tradeoff between security and usability. Specifically, users may tailor the proposed security features to fit their needs: more concerned users incur more overhead in accessing services in a secure way, but reap greater assurances.

In the remainder of this paper, section 2 provides the background for remote access systems, and for SoonR in particular, while section 3 discusses the associated security issues. Section 4 proposes improvements to SoonR’s current security model, Section 5 presents the design of a multi-factor authentication schema, and Section 6 discusses its implementation.

Section 7 presents the results of a study for evaluating the usability and security perceptions of end-users. Section 8 compares with related work, while Section 9 summarizes the main points in this paper and points at future work.

2 Background

New technologies such as RFID, GPS, Bluetooth, pointing and touching sensors, digital cameras, and image and voice recognition offer new opportunities to take cell phones beyond voice communication. Advertisement, tourist and museum guidance, electronic key, payment, peer-to-peer sharing, remote control, and field force tracking [9] are among these new applications.

Cell phone interaction with other devices can be categorized as short-range and long-range. The short-range interaction uses technologies such as Bluetooth, WiFi or USB. In contrast, the long-range interaction is mainly based on a communication over a computer network such as Internet. Although the short-range interaction can complement our work, the fundamental of this work is based on the long-range interaction via an IP-based network.

SoonR employs a Mobile Web 2.0 solution, which provides access to applications and files residing on a PC connected to Internet. Using SoonR, standard mobile phones capable of running a mini-web browser can use some applications on PCs remotely. For example, Google’s Desktop Search, Outlook, Skype, and the files on a desktop computer become available at any location with cell phone network coverage. By using caching mechanisms, the files may be available even when the computer is turned off.