IMPROVING THE SECURITY OF MOBILE-PHONE ACCESS TO REMOTE PERSONAL COMPUTERS

Alireza P. Sabzevar and João Pedro Sousa
Computer Science Department, George Mason University, 4400 University Drive, Fairfax, Virginia 22030, U.S.A.
apirayes@gmu.edu, jpsousa@cs.gmu.edu

Keywords: Remote PC Access, Mobile Computing, Security, SoonR.

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 a 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. This paper presents the background to this class of systems, examines the threats they are exposed to, and discusses possible countermeasures. A concrete solution is presented, which is based on multi-factor authentication and an on-demand strategy for minimizing exposure. This solution is built on top of a representative off-the-shelf commercial product called SoonR. Rather than proposing a one-size-fits-all solution, this work enables end-users to manage the tradeoff between security assurances and the overhead of using the corresponding features. The contributions of this paper are a discussion of the problem and a set of guidelines for improving the design of security solutions for remote access systems.

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 (Hamilton 2007; Tiwari 2007), to remote access to personal files.

Cell phone security, however, has not evolved at the same pace. Some high-end phones recently started to 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 (Kageyama 2006). However, the vast majority of cell phones in use – now numbered in the billions, with over a billion units sold in 2006 alone according to the Semiconductor Industry Association – support only the same password mechanisms used a decade ago.

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. Physical protection of the phone is only part of the solution; because an attacker may obtain enough information to pose as the legitimate user to the remote services. These concerns are especially relevant for an emerging class of systems called *remote control applications* (Roduner 2007).

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), 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 analyzing the threats and possible countermeasures for this class of applications; and therefore at providing guidance for improving the engineering of solutions.

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 suit their needs: more concerned users incur more overhead in accessing services in a secure way, but reap greater assurances.

At this point we have implemented and analyzed the effectiveness of the proposed features, but gauging how a real user base perceives the

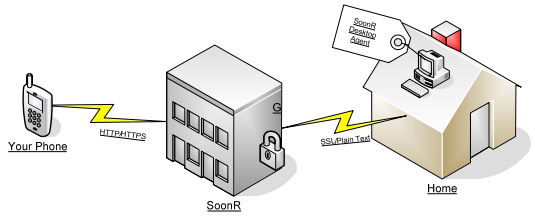

Figure 1: Conceptual model of SoonR.

usefulness and usability of these features is a matter for further research.

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 describes its implementation. Section 7 discusses the proposed solution and identifies points for further improvement of both the security and usability aspects. Section 8 compares this with related work, and Section 9 summarizes the main points being made in this paper.

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 (Enrico 2005) 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 (SoonR). Using SoonR, the 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 desktop computer(s) are made available anywhere with cell phone network coverage. By using caching mechanisms, the files may be available even when the computer is turned off. Any phone with data access and ability to run a web browser is capable of using the SoonR service. For that, the user needs to download and run the SoonR Desktop Agent. As part of the configuration process, the user defines the folders to be shared and which applications, the phone may access.

Figure 1 shows the key components of SoonR, according to SoonR's web site:

1. Cell Phone: with the wireless voice and data (Internet) and web browser.
2. SoonR Service: connection broker between the cell phone and SoonR Desktop agent, responsible for authenticates and storing meta-data of all shared resources.
3. SoonR Desktop Agent: a small client that links PC applications and data to the SoonR service and reports changes to the computers status.

3 SECURITY ISSUES

Although SoonR employs authentication or encryption, many security concerns are left with no clear answers. Specifically:

1. Encrypted Communication: optional encryption is provided through SSL, but unencrypted access is also supported. SoonR's privacy statement (SoonR-Privacy-Officer 2007) implies that this decision has been made because of the mobile phones without SSL support –particularly older mobile phones. This privacy statement relies on users to make their connection secure.
2. Device Authentication: In order to download the SoonR Software, a user must open an account on SoonR Website. The registration process asks for a cell phone number but access to the account is not limited to the registered cell phone. According to SoonR's privacy statement, when users login from their phone, the SoonR Software collects some information about the make and model of the user's mobile phone. However this information never plays any role in securing the service. A user is allowed to access the service from any web browser.
3. User Authentication: Authentication plays a major role in the security of SoonR. However, with cell phones' limited keyboarding, saving the SoonR username and password on the cell phone brings some convenience for user. As mentioned earlier, because of its mobility, the cell phone is a very easy target for people with bad intentions.

Having SoonR subscription on a cell phone means that the user's sensitive information is just a couple of key-presses away from the potential intruders. Cell phone password can be utilized to soften the unauthorized use of the cell phone. However it is fairly easy to compromise the cell phone passwords and the user has the ultimate responsibility for the appropriate use of the password system. The cell phone doesn't need to be stolen, with SoonR subscription, when the user leaves her cell phone at her desk in the office and rushes to a meeting; it is like forgetting the key on the car door.

4. Always-On issue: When the user is away from the computer, the SoonR Desktop Agent should be running, in case the user needs to access her data remotely. Such an Always-On connection gives intruders enough time to launch different attacks, may one succeed. In contrast, an On-Demand service can enhance the security level of the service by limiting the exposures.
5. Trust in SoonR Service: The users' files are cached on SoonR servers and the privacy statement does not reveal enough details about how and under what security circumstances the cached data is maintained. Instead, the privacy statement states that while the company strives to use commercially acceptable means to protect your information, they cannot guarantee its absolute security and some of the responsibility to prevent unauthorized access to data remains with the user.
6. Trust issue with SoonR Desktop Agent: The general security issue of malicious code is another problem. While user blindly installs an agent on his or her computer, there is no way to prove if the software is exactly doing what it advertises to do. A program, which opens a door to infinite world, may easily open a covert channel to transfer some sensitive data in the background. It gets even worse if the SoonR Desktop Agent is compromised by a virus or through buffer overflow exploitation. On the same note, the Always-On desktop agent doesn't show any warning if somebody is already connected to computer or if there is a flow of data between the server and the user computer.

Table 1: Security threads and possible countermeasures.

Security Issue	Solution
Always-On	Make it on-demand
Unauthorized use of phone	Authenticate the user
Using unauthorized device	Authenticate the cell phone
Saved SoonR password	Use one-time password
Caches on SoonR server	Clean up after the use
Trust on the SoonR agent	Monitor the agent's actions

Table 1 summarizes the security threats and proposed countermeasures. The next section describes a security model for addressing the identified issues.

4 PROPOSED SECURITY MODEL

In this section we propose improvements to the security model used by SoonR and other similar systems. We propose to combine multi-factor user authentication, one-time passwords, and device authentication to enhance intrusion deterrence. Additionally, we replace the always-on with an on-demand strategy, to reduce exposure.

The phone used in this work has three capabilities commonly found in today's devices:

- Voice with unblocked Caller ID
- Internet connection with SSL-enabled browser
- Short Text Messaging System (SMS) capability

We assume not only the cell phone itself is not physically secure but also a 3rd party can overhear the data and voice communication between the cell phone and the tower. At the same time, we assume the mobile service provider is trusted with the best-effort delivery of a secure voice and data service. We use Caller-ID to authenticate the device. However, a potential intruder can fool the Caller-ID into displaying arbitrary information. Therefore relying on the Caller-ID alone for authentication of the device is not the most secure way. Therefore we combine SMS with Caller-ID to authenticate the device.

User interaction with the system is partially based on speech. We believe speech input is a viable alternative for voce-enabled devices with limited keyboarding capability. At the same time, part of the user interface, inherited from SoonR itself, is inheritably based on key presses.

Not all the users and their security needs are the same. So our solution will provide the user with the choice to enable or disable some or all of our security mechanisms. However without a base for the security, any adds-on such as our security mechanism will be useless. So our next assumption is about the basic security of the user's computer: we assume the user's computer is connected to Internet and it is running in a physically secure environment such as the comfort of her home. Not only the computer is physically secured, we assume that all

the best security practices such as well-configured firewall, anti-virus with the latest virus definition, along with the latest operating system patches (here MS-Windows), etc. are installed. SoonR Desktop Agent is the only entrusted component of this computer.

In addition to the security assumptions, the user's computer is able to communicate and interact with some sort of telephony system. The telephony system can be a landline connected to hardware Modem or VoIP software running on the computer. Our only restriction is that the computer should be able to command the phone, pick up the line, play a message, receive a voice message and hang up. Also, the computer should be able to process the saved voice messages.

5 IMPROVING THE DESIGN

By design, the SoonR Desktop Agent is connected to SoonR Service all the time. However, would be safer if the agent connects to SoonR when the user really wants to use the service. However at such a moment, the user is away from the computer and cannot run or push the Connect button on the SoonR Desktop Agent program. In the other words, from the security standpoint an on-demand SoonR service is very desirable but hard to achieve.

This on-demand capability also should be password protected and capable of authenticating the device and user at the same time. In addition to that, a simultaneous authentication of the user and the device eliminates the danger of unauthorized use of the cell phone.

No matter if the cell phone is stolen or simply left at the desk in the office, unauthorized use of cell phone is a big threat to the SoonR solution and it can happen at any time. As mentioned before, this becomes worse when user can save her password on the cell phone. To overcome the unauthorized use of cell phone, which can be caused by lack of authentication on cell phone and the saved password, a simple one-time password is desirable. This one-time password can be an RSA token or a simple shared random number.

In our secure scenario, the user has the following installed on her computer:

- SoonR Desktop Agent
- A phone line with optional Caller ID detection capability, connected to the computer
- A program called SoonR Watchdog, which implements our suggested security model and controls the behavior of SoonR Desktop Agent.

When the user decides to connect to her PC via cell phone, first she is required to make an ordinary phone call to home. When this call takes place, SoonR Watchdog detects the Caller ID of the user, picks up the phone and prompts for a password. If the user says the correct password, thanks to speech recognition technologies, the SoonR Watchdog authenticates the user and cell phone both at the same time. However due to the possibility of the fake Caller-ID, the cell phone authentication is not finished yet.

To continue on authentication, SoonR Watchdog sends a text message containing 5-digit half-password to the cell phone. Trusting the mobile service provider with the best effort delivery of service and security, we are sure that the half-password will be delivered only to the cell phone of the user even though a potential intruder may overhear it.

The SoonR Watchdog and the user share a simple, yet secret formula, applied to the half-password by both side to generate the full password. SoonR Watchdog uses the interface of SoonR Desktop Agent to change the SoonR service password to the new password and at the same time the user will be able to login to her account via cell phone. Figure 2 shows this extended security model for the SoonR service.

After finishing her job, the user should make another call to home to disconnect the service. This disconnect call is necessary for maintaining the on-demand property and without it we fall back to SoonR's always-on nature. After receiving the disconnect order, the SoonR Watchdog will:

1. Change the SoonR password one more time
2. Disconnects the SoonR Desktop Agent
3. Cleans up the cache via SoonR web interface

We believe not every user needs the highest level of security. Therefore, in our model, the security level is an option for the user. To begin with, the user has option to use or not to use the SoonR Watchdog. If the user decides to use the Watchdog, Caller-ID authentication is mandatory but the user has an option to ignore the voice-password, deactivate the half-password or the secret formula. More explanation about the optional security comes in the next section, the implementation.

6 IMPLEMENTATION

The SoonR Desktop Agent is available for MS-Windows and Mac operating systems, and for practical considerations we implemented our

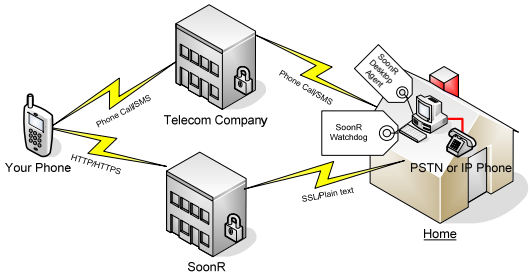

Figure 2: Proposed extensions to SoonR's security.

solution under Windows using Visual Studio 2005, although it would be possible to implement over Mac as well.

The user interaction with phone system is implemented by using the trial version of VTGO PC Soft phone, a product of IP blue Software Solutions . VTGO PC is a SCCP compliant soft phone for Cisco CallManager platform with programming API. This API exposes the phone functionalities to 3rd-party applications, allowing them to control the calls while VTGO is running in the background. During the implementation we had access to VoIP solution based on Cisco CallManager and that is why we chose the combination of CallManager and VTGO PC soft phone. Another possible commercial choice could be SkypeIn from Skype, which has its own API. In the open source world, the combination of Asterisk PBX (Van Meggelen 2005) and IDefisk soft phone can provide a similar environment.

At present, SoonR does not make an API publicly available. Therefore, to interact with SoonR Desktop Agent we used AutoItX ActiveX Control, a freeware that is designed for automating the Windows GUI by emulating human interaction (Flesner 2007). The issue of using this approach is that with a change in SoonR Desktop Agent GUI, the part of our experimental program, which interacts with SoonR Desktop Agent, should change. With lack of API, unfortunately at this point of time, this approach is the only way of interaction with SoonR Desktop Agent.

Windows Speech Recognition technology powers up the user voice interaction in our SoonR Watchdog. We use Microsoft's Speech API, SAPI 6.1, to analyze the user's recorded message and detect the password. SAPI is freely redistributable and can be shipped with any Windows application that wishes to use speech technology.

We also use Windows XP Text-to-Speech capability to generate a dynamic phone conversation with user. First we generate a 8kHz-16Bit-Mono '.wav' file and then we play it on the phone.

The Watchdog's voice recognition and text-to-speech behaviour is controlled by Speech Properties applet of Windows' Control Panel. Our grammar is basically limited to digits 0-9 and "start/finish" commands. The user can train the Windows Speech Recognition and in the same time, as the user uses the speech recognition, the system automatically adapts to the user's voice.

Another worth mentioning observation was the improvement of the recent version of Microsoft speech Recognition over the previous version. With having version 5.1 and 6.1 of Microsoft English Recognizer both installed on our experimental environment, during the tests, version 6.1 showed more accurate recognitions; although it was not 100 percent accurate.

As mentioned earlier, for a better security, we propose a one-time password mechanism in our authentication schema. Security tokens are an example of one-time passwords in practice. While using security token for performing two-factor authentication can provide a very satisfactory level of security, the cost of installation and maintenance is not affordable for many home users. In addition to that, user should always carry an extra item.

A cell phone-based token such as what has been presented in (Di Pietro 2005) is an alternative and replacement of the proprietary hardware tokens. Although, in the beginning the idea seems appealing, however, in case of stolen cell phone this method imposes a great risk to the security and privacy of the user. From the other hand, this method also needs a considerable amount of installation and maintenance, which is beyond ability of an average home user.

As mentioned before, for the purpose of this work we came up with a new idea for one-time password, which is basically a combination of a random number and a simple mathematical function. The system and user both know a simple yet secret mathematical function, which should be applied to the shared password to generate the final password. The shared password is nothing but a random number. When the system verifies the voice password of the user, it picks a random number and sends it to user via short text message. Both parties apply the secret function to generate the new SoonR password. For example the secret function can be something like:

```
SoonR Password ="Pi" + ((Random-
Number * 100) + 1) +"$"
```

Both user and the SoonR Watchdog calculate this new password. The result of this math function

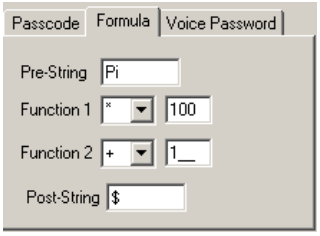

Figure 3: A sample of one-time password formula.

is the one-time password for the SoonR service, which will be set by the SoonR Watchdog and will be used by SoonR to authenticate the user. This method is not very convenient and might not be as strong as hardware token but it is easy to implement and it doesn't need extra hardware of software to generate the password. Figure 3 shows an example of the one-time password. Assuming the random number is 12345, the one-time password becomes Pi1234501$.

We assume the SoonR Desktop Agent and the cell phone both use SSL-enabled connection so this calculated password couldn't be overheard. Table 2 summarizes the one-time password mechanisms and their pros and cons.

Table 2: Different methods of one-time password generation and their pros and cons for our solution.

One time password	Pros & Cons
Security Token	User carry extra item; cost
Cellular Authentication Token	Doesn't help if cell phone is stolen; needs installation; cost.
Text message and simple math function	User needs to remember the function; calculation may not be easy to all users; free

As mentioned before, in our model, security is optional. If the user decides to use our SoonR Watchdog, only the Caller-ID check is mandatory and user can enable or disable the rest.

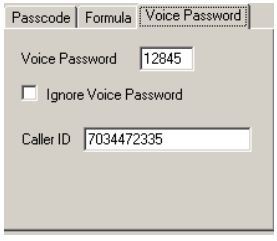

Figure 4: Caller-ID and voice password setting.

Figure 4 shows the Caller-ID and voice password in the configuration setting of SoonR Desktop Agent. As it can be seen, the user can easily avoid the voice password and its consecutive steps via configuration. In such a case the offline-password is going to be the all-time password and the SoonR desktop Agent never tries to change the service password.

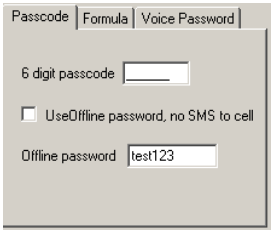

Figure 5: User's options for using regular password vs. one-time password.

Figure 5 shows how user can choose between one-time password and regular password for the SoonR Service. Even if the user decides to go with the one-time password, the formula and the calculation can be ignored. To do so, the user just needs to leave the Formula fields empty.

7 DISCUSSION

The proposed enhancements were implemented without accessing any API or the application's source code. Specifically, we proposed multi-factor authentication for validating the identity of both the user and the phone device. One-time passwords help us overcome some of the security shortcomings of cell phones.

Speech recognition technology is part of our authentication process. The Speech recognition is an exciting technology that promises to change the way we interact with computers in the future. Speaking is the easiest and the most widely used way of communication among humans. Considering the fact that in ubiquitous computing world, computers will be part of our daily life, it is not surprising if speech recognition technologies become a significant player of future ubiquitous computing world.

Recent advances in speech recognition technology coupled with the advent of modern operating systems and high power affordable personal computers have culminated in the first speech recognition systems that can be deployed to a wide community of users. Our simple speech-enabled application is a good example of such systems. A home user can use our SoonR Watchdog without being bothered with technical details of speech recognition. As mentioned before the user can train the speech recognition. During our

experiment we realized that when the grammar is so small, training the speech recognition profile doesn't enhance the voice recognition.

Although the mechanisms described in the previous sections considerably improve the security aspects of SoonR, further improvements are possible to both the security and usability aspects.

It is safe to assume that if the cell phone is in vicinity of the computer, the user prefers to use the computer rather than small-screen cell phone. Nowadays Bluetooth is an ordinary capability of many computers and cell phones both. Having Bluetooth detection capability, if the SoonR Watchdog detects the cell phone around, it shutdowns the SoonR Desktop Agent and all the other commands will be ignored. If the user still wants to use her cell phone in a short distance of her computer, she just needs to turn off the Bluetooth on the cell phone.

Watching the SoonR Desktop Agent by monitoring its system calls gives us another layer of security. A compromised agent will try to access areas of hard disk, which are not defined in the configuration file. SoonR Watchdog can monitor the disk read and write system calls to ensure that SoonR Desktop Agent is not doing any type malicious activity.

There are some known security practices including but not limited to event logging, password aging, strong password policy and maximum number of failed authentication attempts which can be added to our SoonR Watchdog.

8 RELATED WORK

In addition to SoonR, there exist other commercial solutions with similar security issues. For example, PocketView, which is GoToMyPC's handheld version. As with SoonR, the host PC initial communications are established through a TCP connection brokered by a provider's server. Because there is an assumption that the outgoing connections generally do not pose a security risk, most firewalls allow them without any configuration required and after establishing the channel, the connection remains open for virtually an unlimited time.

SoonR and PocketView are not the only examples. In early 2005, Toshiba announced the world's first software supporting remote operation of a personal computer from a mobile phone (Kallender 2005). According to Toshiba's press release, the Ubiquitous Viewer software provides access to any Windows home or office computer. It also allows users to open productivity software, such as the MS-Office suite, PC-based e-mail, Internet browser and other PC applications at any time, wherever they are. Unfortunately there is no public information about this application so we were not able to judge the security of the system.

(Makoto Su 2002) proposes a simple solution for using the joystick available in some phones to control a cursor and perform clicks on a remote display, but does not address security issues.

In other work, a user at an distrusted terminal utilizes a trusted device such as PDA to access the home PC securely through by remote desktop application such as GoToMyPC (Oprea 2004). The PDA as input device and distrusted terminal as display, create a secure environment that a possible Spyware on distrusted terminal cannot capture the user input on the distrusted terminal. (Jammalamadaka 2006) introduces a prototype of a proxy-based system in which the user must possess a trusted mobile device with communication capability such as a cell phone, in order to securely browse the net from distrusted terminal. In this system, the trusted proxy contacts the user through the trusted device to obtain authorization for requests from the un-trusted computer.

All the mentioned products, systems and projects assume the handheld devices are secure enough to be utilized for accessing other devices. However this assumption is far from reality. What makes our work different is that we don't trust the device and its holder. Instead of blindfolded trust, we try to authenticate the mobile device and the device holder to the best of our ability.

The closest to our work is (Tsai 2004) where the authors employ home-automation techniques to grant properly authenticated users, remote access to the their personal workstations at home. The solution uses web interface, short message text and phone call to authenticate the user. For example in short text message authentication schema, the user composes an SMS message by concatenating his account, password, the name of the personal workstation to be controlled remotely, and the interface address of the public terminal, in comma separated format. Then he sends the message to the phone number associated with his residential gateway. Upon receiving the message, the residential gateway parses it and performs validation on the authentication information. If nothing goes wrong, the residential gateway turns on the specified personal workstation, set up the temporary NAT and PATS port-mapping entries, and sends back another SMS message containing the corresponding URL.

The main difference between our system and Tsai et al. is that we never assume the SMS or phone calls are secure. With our one-time password mechanism the danger of eavesdropping is minimal.

As mentioned before, in the area of physical security, NTT DoCoMo, offers a phone that automatically locks itself down when its owner moves beyond a certain distance (Kageyama 2006). The cell phone comes with a small black security card, about the size of a movie-ticket stub, which the cell phone can sense its adjacent presence. If an owner keeps the card in a bag or pocket, the phone recognizes when the card moves too far away and locks automatically to prevent someone from making a call. Face recognition, satellite tracking are other security feature in this type of cell phone, which can also be used as a credit or a prepaid cash card. Having such a phone makes the SoonR experience safer, but it doesn't eliminate the need for on-demand connection and one-time password mechanism. From the other hand, not only this solution has its own shortcomings, there are many cell phones out there without this type of protections. However the idea of distance detection in this cell phone is close to what we suggest for disabling SoonR Desktop Agent when the cell phone is in vicinity of the computer.

9 CONCLUSIONS

This paper demonstrates that it is feasible to improve the deterrence against security threats in an off-the-shelf product. The product chosen to make this point, SoonR, is representative of an emerging class of commercial products for accessing remote PCs using a cell phone. Specifically, the proposed enhancements consist of:

- Reducing the window of exposure to threats by granting remote access to the user's PC only when required, instead of supporting the current always-on policy.
- Reducing the likelihood of impersonation by using multifactor authentication:
  a) Verifying the phone's caller id,
  b) Asking a one-time password from the user,
- Reducing the risk if devices are stolen by having the one-time password being generated by "something the user knows," rather than "something the user carries."

An important feature of the proposed solution is that it enables users to manage the tradeoff between security assurances and the associated usability overhead. Users with stringent requirements may use more sophisticated mechanisms, such as generating complex one-time passwords, while users more concerned with ease of access can reduce the overhead by using simpler flavours or skipping such mechanisms.

Future work includes studies to evaluate how end-users perceive the usability and usefulness of the proposed security features.

REFERENCES

Di Pietro, R., Me, G., Strangio, M. A. (2005). "A two-factor mobile authentication scheme for secure financial transactions." International Conference on Mobile Business: 28-34.

Enrico, R., Wetzstein, S., Schmidt, A. (2005). A Framework for Mobile Interactions with the Physical World. Wireless Personal Multimedia Communication Conference (WPMC'05). Aalborg, Denmark.

Flesner, A. (2007). AutoIt v3: Your Quick Guide O'Reilly Media

GoToMyPC. http://www.gotomypc.com.

Hamilton, A. (2007)." Banking Goes Mobile." TIME Magazine, http://www.time.com/time/business/article/0,8599,1605781,00.html.

Jammalamadaka, R. C. v. d. H., T.W. Mehrotra, S. Seamons, K.E. Venkasubramanian, N. (2006). "Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine." Computer Security Applications Conference: 57-66.

Kageyama, Y. (2006). Cell Phone Takes Security to New Heights. The Associated Press.

Kallender, P. (2005). Toshiba software will remotely control PCs by cell phone. COMPUTERWORLD: Today's top stories, http://www.computerworld.com/softwaretopics/software/story/0,10801,99012,00.html.

Makoto Su, N., Sakane, Y., Tsukamoto, M., Nishio Rajicon, S. (2002). Remote PC GUI operations via constricted mobile interfaces. 8th annual international conference on Mobile computing and networking, Atlanta, Georgia, USA, ACM Press.

Oprea, A., Balfanz, D., Durfee, G., Smetters, D. (2004). "Securing a remote terminal application with a mobile trusted device." Computer Security Applications Conference, 2004. 20th Annual: 438-447.

Roduner, C., Langheinrich, M., Floerkemeier, C., Schwarzentrub, B. (2007). Operating Appliances with Mobile Phones - Strengths and Limits of a Universal Interaction Device. Pervasive 2007, Intl Conference on Pervasive Computing. Toronto, Ontario, Canada.

SoonR-Privacy-Officer. (2007). "Privacy Policy " from http://www.soonr.com/web/front/security.jsp.

SoonR. "SoonR - In Touch Now, The Company."

Tiwari, R., Buse, S.,and Herstatt, C. (2007). Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage. Intl Research Conference on Quality, Innovation and Knowledge Management, New Delhi.

Tsai, P., Lei, C., Wang W. (2004). A Remote Control Scheme for Ubiquitous Personal Computing. IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan.

Van Meggelen, J., Smith, J., Madsen, L. (2005). Asterisk: The Future of Telephony, O'Reilly Media, Inc.