Do You Trust Your Phone?[⋆]

Aniello Castiglione[⋆⋆], Roberto De Prisco, and Alfredo De Santis

Dipartimento di Informatica ed Applicazioni *"R. M. Capocelli"*,
Università di Salerno,
Via Ponte don Melillo, I-84084 Fisciano (SA), Italy
Tel.: +39089969594
castiglione@acm.org, robdep@dia.unisa.it, ads@dia.unisa.it

Abstract. Despite the promising start, Electronic Commerce has not taken off mostly because of security issues with the communication infrastructures that are popping up threateningly undermining the perceived trustworthiness in Electronic Commerce.

Some Internet security issues, like malware, phishing, pharming are well known to the Internet community. Such issues are being, however, transferred to the telephone networks thanks to the symbiotic relation between the two worlds. Such an interconnection is becoming so pervasive that we can really start thinking about a unique network, which, in this paper, we refer to as the Interphonet.

The main goal of this paper is to analyze some of the Internet security issues that are being transferred to the Interphonet and also to identify new security issues of the Interphonet. In particular we will discuss about mobile phones malware and identity theft, phishing with SMS, telephone pharming, untraceability of phone calls that use VoIP and Caller ID spoofing. We will also briefly discuss about countermeasures.

Keywords: VoIP security, SMS security, identity theft, mobile malware, telephone phishing, telephone pharming, untraceability, caller ID spoofing, SMS spoofing, NGN.

1 Introduction

The Internet is a fertile ground for dishonest people: Electronic Commerce, online banking transactions and any other online operations involving confidential information give opportunities to perform fraudulent actions whose goal is mainly to steal money. The Internet poses many well known threats. One of them is that of malware (malicious software), like, for example, computer viruses. Phishing is another well known Internet threat: an attacker elicits the disclosure of private information from the victim.

[⋆] This work has been partially supported under the project *"Framework for Advanced Secure Transactions - Definizione di un'architettura di riferimento per la realizzazione di sistemi di micropagamenti"*, developed in collaboration with Telepark S.r.l. and funded by Regione Campania (Italy), in the framework of the POR Campania 2000/2006 Misura 3.17.

[⋆⋆] Corresponding author.

T. Di Noia and F. Buccafurri (Eds.): EC-Web 2009, LNCS 5692, pp. 50–61, 2009.

A more recent threat, which goes side by side with phishing, is that of pharming. Pharming refers to techniques that bring the user to a web server (or more generally to an Internet server) which is not the one that the user wants. Such a redirection is usually accomplished by exploiting vulnerabilities in the DNS. In a well orchestrated pharming attack, the web server to which the user is redirected looks exactly as the real one. In this situation, it is very easy to induce the victim to disclose private information. Malware can be used to perform a pharming attack. Phishing can be used, for example, to lead a victim to visit a fake bank web site. Hence, these attacks are powerful tools for dishonest people to steal money or perform other fraudulent actions. The above threats are only some of the security issues that the Internet poses to its users. It goes beyond the scope of this paper to extensively analyze Internet related security issues. Here we are only emphasizing the ones that are more relevant for the problems analyzed in this paper and that we think may threaten the spread of Electronic Commerce.

What we have said so far is fairly well known to the Internet community since these threats have been around for awhile. What people seem unaware of is that many of such issues are being transferred to the telephone networks. Nowadays, indeed, the Internet and the telephone networks are becoming more and more interconnected. This implies that many of the problems that we have discussed before also apply to the telephone networks. Furthermore, the interconnection with the Internet creates even new security issues for the telephone networks, such as identity theft and untraceability, which did not exist before (or at least were much more difficult to achieve). Since the interconnection is becoming so pervasive we like to think about a unique network, which include the Internet and the telephone networks. Such a unified network is commonly known as Next Generation Network (NGN) and we like to call it the *Interphonet*. The interconnection itself is not the unique cause of the problem. Newer mobile phones (usually called smart-phones) resemble more and more to small personal computers. This allows the possibility of spreading malware also on mobile phones. By taking advantage of all these possibilities, dishonest people can perform fraudulent actions over the Interphonet and threaten the pervasiveness of the Electronic Commerce that often rely on such new technological tools. For example, it is relatively easy to send an SMS impersonating any person or organization of which one knows the mobile telephone number. Phishing can be performed via SMS, and with SMS bulk services it is easy to reach a multitude of mobile devices. Fraudulent actions involving SMS sent via the Internet are becoming common. In particular [16] reports a successful phishing attacks. Moreover, it is possible to place a call and forge the source telephone number impersonating whoever we want. Pharming can be applied to telephone calls: a user types a telephone number on his smartphone but the call is deviated somewhere else (this requires that, before the call, the mobile device has been the target of a malware attack).

Some related work. There are a number of papers that have recently addressed several emerging security issues in the Internet. Very few of them specifically consider the Interphonet. In [2], Enck *et al.* analyze some aspects of the connection between the Internet and the mobile telephone networks showing how to launch a Denial of Service attack by sending a huge volume of SMS via web-based messaging portals to mobile telephone networks. Another paper [1] also consider the Denial of Service problem in the GSM network in a more general way. Security problems related to the Voice over IP service are tackled in [11] where confidentiality, integrity and availability issues are considered.

2 Technologies

The communication infrastructures that we are interested in are the Internet and the telephone networks (both mobile and PSTN). Until few years ago these two network infrastructures were completely separated. Nowadays, however, the interconnection is increasingly growing.

2.1 GSM and SMS Architecture

The *Global System for Mobile Communications* (GSM) is a standard adopted worldwide. Such a standard offers a variety of services, which, beside the obvious one of voice call, include voice mail, call handling facilities and messages. The basic one is the Short Message Service (SMS) which allows to exchange short alphanumeric messages among users, located anywhere in the world, connected to any digital cellular network. Mobile phone users can use the service by simply typing the message on the phone keypad. A message is usually delivered within few seconds if the recipient is reachable. Otherwise, a “spooling” system keeps the message until the recipient becomes available. The messages are handled, maintained and transmitted, by SMS Centers (SMSCs). SMS are injected into the mobile network essentially by submitting the message text and associated information to an SMSC. Normally a user would just compose the message text on the keyboard of the mobile device and send it to the recipient (on behalf of an SMSC) via the mobile device itself. However it is possible to inject an SMS into the network from a connection outside the wireless carrier’s network. For example, one can use a web-based messaging portal using several different protocols such as SMPP (created by SMS Forum/Logica) or CIMD (created by Nokia). Since these communications are not encrypted it is possible to intercept and modify them. Once the SMSC has received the request, the content of the request is inspected and, possibly, modified in order to make it compliant with the format used by the SMSC. At this point the message becomes indistinguishable from an SMS sent by a mobile device and it is queued in order to be forwarded and delivered. Personal use of SMS is normally limited to single point-to-point messages. However it is becoming increasingly widespread the use of SMS for commercial purposes (e.g., advertising). Clearly, to have an effective impact, it is necessary to have services that allow sending a large number of messages in automated ways. Spurred by such a necessity, a number of companies are starting to provide Internet services that allow sending bulk SMS. This feature facilitates (or at least increases the chances of) phishing with SMS (see Section 3.2 and Section 3.3).

2.2 Voice Over IP (VoIP)

VoIP is the technology that allows “voice” to be transported over the Internet Protocol. It consists of software, hardware and industry standards. VoIP can be used to make phone calls between “something” connected to the Internet (PC, ATA, etc) and a traditional phone. In some cases, even a phone call between two traditional phones can actually use VoIP but only among “carrier” operators. For the scope of this paper, we are interested only in the fact that using VoIP one can make and receive phone calls using a PC connected to the Internet. Using VoIP, a user can get a regular phone number, with country and area codes. In order to use that number it is enough to be connected to the Internet. This implies that for VoIP is not true that a phone number tells where the user is geographically located. Currently there are many companies that, in order to foster the use of VoIP, offer VoIP numbers free of any charge and to obtain such a number it is enough to surf to an appropriate web site; registration to such web sites requires only undocumented information (like name, date of birth and address). Recently in [12] has been coined a new term (“vishing”) to address the term “VoIP phishing”.

3 Security Issues

In this section we discuss how the increasing interaction between the Internet and the telephone networks creates, makes simpler, or transfers from the former to the latter network, opportunities for dishonest users to perform fraudulent actions. Emerging Internet threats (e.g., malware, phishing, pharming) are being transferred to the telephone networks. Many of such issues are strongly interconnected and, thus, it is difficult to discern the borders between some of them.

3.1 Mobile Phones Malware

Malware (spyware, adware, malicious software, e.g. viruses, Trojan horses) is a widespread threat to computers connected to the Internet [8]. Less known is the analogous risk for mobile equipments. Mobile equipments can be considered safer than computers connected to the Internet because on one hand the operating systems are less known and less vulnerable and, on the other hand, the connectivity may be limited. However, newer phones increasingly resemble to computers and they run complex operating systems (e.g., Symbian OS, Windows Mobile, Apple iPhone OS, BlackBerry OS, etc.) allowing for more vulnerabilities. Newer phones can be reached through a variety of ways (e.g., Bluetooth, IrDA, Wi-Fi, GPRS, UMTS) and thus the exposure to malware is increasing. However, even with classical ways of reaching a mobile equipment (e.g. the SMS) it is possible to spread malware. Malicious SMS could be constructed to contain executable malicious code. Most SMS centers are supporting the Enhanced Messaging Service (EMS) developed by the Third Generation Partnership Project (3GPP) [10]. Such a standard extends the SMS standard to include a User Data Header (UDH) which allows to include binary data in the SMS (e.g. [3]). Mobile telecommunication companies are starting to use SMS to send executable code to their users for various reasons, such as minor phone upgrades and new applications. A user that receives an SMS from a telco has no reason not to trust the message and not to execute the code. Furthermore, using a simple WAP-Push SMS it is possible to deliver URL from which a user can download an application or a patch. However, as we will discuss in Section 3.2, it is possible to fake the identity of the sender of an SMS. Hence, the threat of receiving malware through SMS is concrete.

3.2 Identity Theft

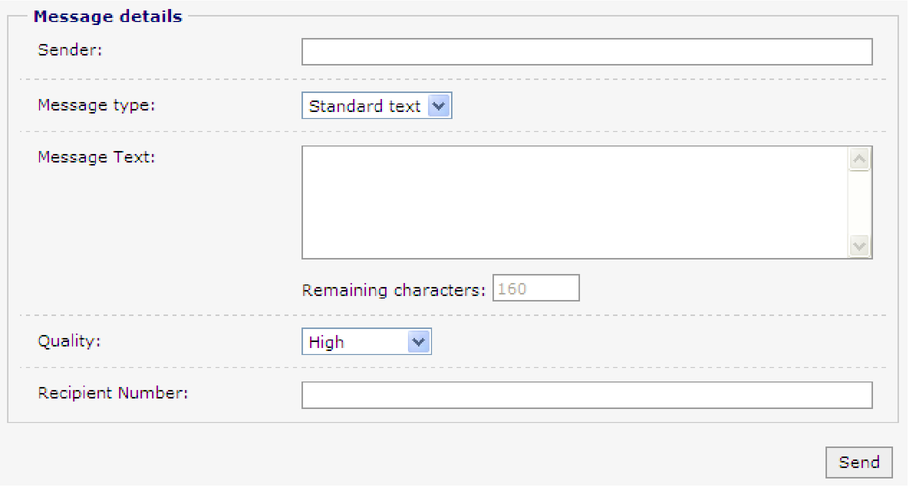
In the GSM networks the identity is provided by the *International Mobile Subscriber Identity* (IMSI) and the *International Mobile Equipment Identifier* (IMEI) codes. The first one identifies the SIM card and the second one the mobile device. We remark that these two codes are not correlated and often the IMEI code is not bound to the user. The IMSI code instead, usually, is bound to the individual or organization which has bought the SIM card.

There are several degrees of identity theft. The highest level of identity theft is when one can clone both the IMSI and the IMEI codes. Cloning the IMSI codes requires physical access only for a few seconds to the user's SIM card to discover with a brute force attack the private key stored in the SIM card. Luckily, this attack is not easy to perform because on one hand it requires physical access to the user's hardware and, on the other hand, newer SIM cards are not vulnerable to brute force attacks.

In [15] it is shown how to build a private GSM network in order to impersonate an official Base Station and steal all the information needed to make a perfect clone of a GSM SIM card simply by interacting with the mobile equipment of the user under attack. We remark that it is easy to get cheap hardware to assemble a Base Station or to buy it on the Internet.

Talking about SMS, the simplest form of identity theft is to fake the real user phone number. This is possible by setting the sender field in the message header. As we have already pointed out (see Section 2.1), this is easy to do by contacting an SMSC. For example, it is possible to inject an SMS into a SMSC via a web-based messaging portal. A typical service offers a form that allows to set all the parameters of the SMS (see Figure 1). In particular, it allows to set the sender phone number to any desired string, which, obviously, can be a regular mobile phone number. Notice that, in this case, the malicious attacker is using the stolen identity only in the sense that the sender phone number appears to be the stolen one.

There exist other ways of delivering an SMS to an SMSC that can be easily found on the Internet. Another way of delivering an SMS to a SMSC is to contact it via a direct data call (e.g. with a modem). In this case the entire message needs to be correctly formatted in order to comply with the SMS standard (task that, in the previous case, is done by the web-based service). This is possible only when the SMSC accepts the incoming data call without authentication. Not long ago this was the default behavior of the SMSCs. Nowadays, however, most data calls



Message details

Sender:

Message type: Standard text

Message Text:

Remaining characters: 160

Quality: High

Recipient Number:

Fig. 1. Example of a typical web-based service for sending SMS

to SMSC are filtered and permitted only for management reason. Nevertheless, in some countries where there are old telecommunication infrastructures, all incoming calls to an SMSC are accepted.

Thanks to caller ID spoofing it is possible to mount a similar attack by placing a normal (spoofed) call (see Section 3.5).

3.3 Phishing with SMS

Among all the above possibilities, the one that is currently most usable is to fake the identity phone number using web-based messaging portals offered by bulk SMS service providers. This kind of identity theft can be used to perform a new kind of phishing attack [17]. This emerging problem attracts the attention of both the scientific and the economic communities. The interest of the former community is to provide technical solutions while the latter is concerned with financial losses (usually suffered by customers). Regarding possible countermeasures, many organizations, like banks, suggest not to trust any email message requesting confidential information. Phishing can be accomplished with SMS in the same way. Even expert users that would normally not trust an email message coming from a known sender, might accept the authenticity of an SMS coming from a known source. Moreover some institutions (like banks), warn their customers not to trust email, but to trust phone calls or SMS. This makes phishing with SMS easier and opens the doors to caller ID spoofing attacks. Moreover with bulk SMS services an attacker can easily reach many mobile devices. As we have pointed out before in Section 3.2, the identity of the sender of an SMS can easily be forged.

3.4 Telephone Pharming

Another risk connected to malware is that of pharming. The word "pharming" refers to techniques that exploit vulnerabilities of the Domain Name System in order to redirect a user to a forged Internet server that looks like the authentic one. Pharming techniques are well known for computer systems. The newest telephone technologies allow for "telephone pharming" too. For example, it is possible to hijack a mobile equipment and forge its software so that outgoing calls or messages are redirected somewhere else. Indeed, with recent phones most of the functionalities are implemented via software, hence once an attacker is able to manipulate the phone (e.g. via a malware attack), it can replace/modify the software. Such attacks are made easy by the fact that most phone operating systems do not have a "kernel mode" that protects access to the system at low level. We remark that it is possible also to attack a user by operating a "reverse pharming": the caller ID of an incoming phone call can be changed to any wanted number. With this attack, for example, a malicious user can call the victim masquerading the actual phone number (the one the attacker is using) by letting the malware change such an incoming number to any desired number. Alternatively, and quite simply, it may be used a caller ID spoofing attack to reach the same goal.

3.5 Caller ID Spoofing

It is interesting to show that caller ID spoofing has been around from the initial introduction of it. Such a feature was mainly used by companies accessing a Primary Rate Interface (PRI) phone line provided by carriers. Caller ID spoofing has been used, in its basic form, by changing the telephone number of all outgoing calls in order to show outside the "general" (e.g. PBX) number. Many websites that provide Caller ID spoofing are popping up on the scene. Some of them implement even other "services" that go beyond the simple spoofing of the number: call recorder, voice changer, unmasking private numbers (makes useless the caller ID blocking *67#), corporate plan, and others. There exist some implementation of spoofing software (SpoofApp) running on Apple iPhone, Google Android and RIM BlackBerry mobile platforms. The VoIP server Asterisk may also be used to forge the outgoing number of a call using a very simple PHP script (see [13]). A good compendium of the state of the art for the caller ID spoofing world is given in [14].

3.6 Untraceability

When talking about traceability in the Interphonet, we mean the identification of the digital equipment involved in the execution of the action. If we confine the discussion only to the classical wired telephone networks (PSTN), then traceability is not so difficult: the networks indeed know where the originating phone is located (and plugged to the wall) and telecommunication operators are required to maintain logs of all phone activities, and supply them, if required, to the law enforcement agencies. With the introduction of mobile phones, traceability of phone calls has become slightly more complicated. This is due to the fact that while in the PSTN the phone number is sufficient to identify both the customer and the physical location of the phone, with mobile networks this is not true anymore. Indeed, on one hand the mobile equipment is not bound to a physical location and on the other hand the identity of the individual who buys the service, in most cases, is not strongly verified or even not verified at all. For example, in some countries in order to buy a SIM card it is not necessary to show an identification document (e.g. driver license, passport, identification card). Even when one has to provide some proof of identity it is very easy to provide a fake one (especially considering that the documents do not have to be shown to a public officer).

With Internet, traceability means to determine an IP address. Roughly speaking an IP address is the equivalent of a phone number in the telephone networks. However there are substantial differences between these two addressing systems that render the association between the equipment and the person using it even more complicated. There are several Internet anonymizer tools which mask the real IP address. More sophisticated techniques can be used. For example, a malicious user who has physical access to a network could steal an IP address. Another possibility for malicious user over the Internet is that of performing an intrusion into someone else system and use that system to perform the wanted action. To all extents, the IP address of the violated system will appear as the originating IP address. Hence, the Internet offers much more opportunities to hide the identity behind an IP address. Using VoIP one can make phone calls from (and to) the Internet. So, the identity hiding opportunities offered by the Internet extend to the telephone networks: it is enough to make the phone call from an IP address conveniently hidden with one of the above discussed, or similar, techniques.

3.7 Putting Everything Together

In the previous section we have outlined several security issues by classifying them into separate kinds of attacks. We have also remarked that these attacks are strongly interconnected and malicious users exploit them together in order to perform fraudulent actions. In this section we provide an hypothetical example which involves many of the discussed security issues.

A malicious user, connected to the Internet with an IP address that cannot be tied to his real identity, subscribes, with a fake identity, to a VoIP service which provides him a telephone number. Moreover, the malicious user buys from an SMS bulk service provider the possibility of sending SMS. Notice that, even if buying such services requires a payment, in most cases the payment can be easily done without revealing the identity of the payer (e.g., with an anonymous money transfer). Mr. Bill Sphigath receives a message from his telephone mobile operator. Apparently the message contains a security patch and Mr. Bill, trusting the identity of the sender, executes the code contained in the message. However the message has been actually sent by the malicious user and the

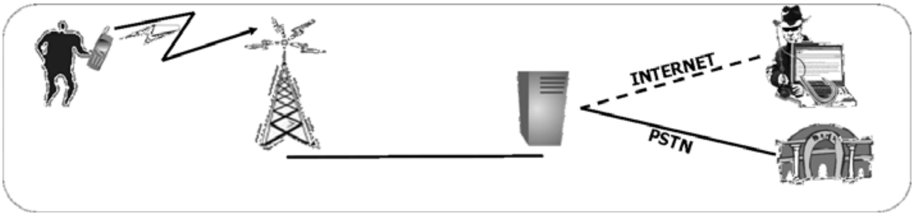


Fig. 2. Telephone pharming. Mr. Bill calls his bank but the call is deviated somewhere else.

attached code has installed a software module capable of deviating some outgoing phone calls (pharming); in particular, phone calls directed to Bill's bank Customer Care center. After a couple of weeks Mr. Bill receives an SMS from his bank (or a call from the telephone number of his bank). The SMS asks Mr. Bill to call the bank Customer Care because the bank needs to verify some information about his bank account. Although Mr. Bill believes the truthfulness of the message, the message has been sent by the malicious user (as well as the spoofed call apparently coming from the number of his bank). Mr. Bill, worried by the fact that the bank needs information about his account, immediately calls the Customer Care number. Because the calls to such a number are redirected to the number provided by the malicious user in the pharming attack, although Mr. Bill dials and sees on the phone display the number of the Customer Care, the call is actually redirected to the other number (see Figure 2). Such a number is the VoIP number created by the malicious user and can be physically located anywhere. Behind the VoIP number the malicious user has setup an IVR (*Interactive Voice Response*) which is used by most Customer Care, including Mr. Bill's bank, to receive customer phone calls. The IVR has been setup to "look and feel" as that of Mr. Bill's bank. The IVR service, in order to identify the user, asks Mr. Bill his bank account number and the associated personal access code. Moreover, to justify the request made to Mr. Bill, the system will inform him that he has been contacted because he should change his personal access code in order to improve the security of his account. Clearly, at this point the malicious user has both Mr. Bill's bank account and personal access code.

4 Countermeasures

As we have pointed out before, giving countermeasures is not the focus of this paper. Such countermeasures must rely on well-known cryptographic tools. However in this section we briefly discuss some of the actions that we can take to defend ourselves from the security threats of the Interphonet. On a non-technical side, the first and simplest countermeasure is not to trust messages (both email and SMS), especially when they require the disclosure of private information and reveal such information only after having gained a sufficient level of confidence about the interlocutor. On a technical side, we can identify two basic issues that, if solved, would address most of the security problems that arise in the Interphonet: authentication and encryption of the communication. Both are well studied and cryptographic techniques are widely available. The problem is to devise viable methods to implement them in the Interphonet in order to minimize the impact on the existing infrastructures and overcome interoperability problems.

Security issues can be tackled either solely from the endpoints or involving the network. Involving the network, however, would imply a bigger impact on the network infrastructure while a solution involving only the endpoints is entirely transparent to the network [18]. Moreover, if two users wish to achieve security goals without the help of the network cannot do otherwise. Guaranteeing security poses different problems depending on whether we are targeting SMS security or voice call security. However in both cases the endpoints must be capable of running specialized applications that use of cryptographic algorithms. This is not feasible with standard mobile equipments, whose computing capabilities are limited. However newer devices are equipped with enough powerful hardware that allows to run software that can use advanced cryptographic algorithms. For SMS, the encryption software must assure that the encrypted data should be in a form compliant with the SMS message body standard and the size of the resulting encrypted data should not be too big. The simplest authentication method is to share a secret key. Secret keys, however, have a number of well known drawbacks. Public key authentication is more suitable, although more expensive in terms of communication overhead. For SMS, the use of public key algorithms introduces the necessity of sending more than a single message between the source and the destination requiring interaction between them. It also implies charges for the recipient of the message which, for regular SMS, does not exist. If one can use (one-time) secret keys, then clearly this is the simplest solution. In such a case it is possible to include an HMAC, for example, with MD5 or SHA, using 128 or 160 bit. Another possibility is to use digital signatures schemes. A public key infrastructure and its concrete implementation for securing SMS has been presented in [21].

For voice calls it is easier to use public key cryptography because the end users must anyway interact. So, assuming that end users would have enough computing power on the mobile device, it is viable to authenticate the parties and encrypt the call [18]. Regarding the concrete security issues that arise from the use of caller ID by means of an authentication factor, a reasonable solution has been presented in [7]). Palmieri and Fiore in [9]) developed a novel hybrid framework for enhanced end-to-end security in VoIP environments by using digital signatures and encryption to enforce calling party identification, privacy, no-replay attack and non-repudiation.

It is worth noting that, even when the mobile operating system has a “kernel mode” or uses cryptographic protection to restrict certain functionality by checking digitally signed excecutable, often it is possible to bypass such constraints (see for example [20]) allowing the user to install any kind of (dangerous) software.

5 Conclusions

In this paper we have analyzed some new security issues that arise from the interconnection of the Internet and the telephone networks. Such security threats derive both from the interconnection of the telephone networks and the Internet and from new mobile devices which resemble more and more to small but powerful computers. We have shown how to perform several fraudulent attacks that are possible in the Interphonet. We believe that the Interphonet gives new possibilities for fraudulent attacks and thus everyone should be aware of them. The GSM standard provides three algorithms for authentication and encryption. However the solutions proposed eventually proved to be insecure. Moreover such standards were designed to protect only the communication between the Mobile Equipment and the Base Station. The remaining part of the communication is transmitted without any protection. Since in the Interphonet this communication can flow even through the Internet, privacy concerns are amplified. There are many other issues that are not discussed in this paper. We have however outlined several possible attacks that involve many of the security issues arising in the Interphonet. We believe that these problems, while well pondered for the Internet, are still undervalued for the Interphonet. It is quite obvious that the technical countermeasures must make use of cryptographic tools. At the same time, we are not sure that cryptography may overcome the intrinsic and (probably) insurmountable weaknesses deriving from the use of an open system which may be considered the Internet.

Recently [19] , the U.S. Secret Service has determined that the BlackBerry of the U.S. President did not provide the requisite security required for its continued use. Secret Service raised special concern because potential attackers could gain access to government confidential information. Although President Obama persuaded his security staff to let him keep using his smartphone, it is not clear how, exactly, the device was modified to ensure extra security.

References

1. Bocan, V., Cretu, V.: Security and Denial of Service Threats in GSM Networks. Periodica Politechnica, Transactions on Automatic Control and Computer Science 49(63) (2004) ISSN 1224-600X
2. Enck, W., Traynor, P., McDaniel, P., La Porta, T.: Exploiting Open Functionality in SMS-Capable Cellular Networks. In: Proc. of CCS 2005, Alexandria, VA, USA, November 2005, pp. 7–11 (2005)
3. Kim, S.h., Leem, C.S.: Security Threats and Their Countermeasures of Mobile Portable Computing Devices in Ubiquitous Computing Environments. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3483, pp. 79–85. Springer, Heidelberg (2005)
4. Lawton, G.: E-mail Authentication Is Here, but Has It Arrived Yet? IEEE Computer 38(11), 17–19 (2005)
5. Peersman, G., Cvetkovic, S., Griffiths, P., Spear, H.: The Global System for Mobile Communications Short Message Service. IEEE Personal Communications, 15–23 (2000)

6. Salam, A.F., Rao, H.R., Pegels, C.C.: Consumer-Perceived Risk in E-Commerce Transactions. Comm. of the ACM 46(12), 325–331 (2003)
7. Fujii, H., Shigematsu, N., Kurokawa, H., Nakagawa, T.: Telelogin: a Two-factor Two-path Authentication Technique Using Caller ID, NTT Information Sharing Platform Laboratories, NTT Technical Review, Vol. 6(8) (August 2008), https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200808le3.html
8. Thompson, R.: Why Spyware Poses Multiple Threats to Security? Communications of the ACM 48(8), 41–43 (2005)
9. Palmieri, F., Fiore, U.: Providing True End-to-End Security in Converged Voice Over IP Infrastructures. Journal of Computer & Security (in press) (January 2009), http://dx.doi.org/10.1016/j.cose.2009.01.004
10. 3rd Generation Partnership Project, Technical realization of the Short Message Service (SMS), Rel. 5.1.0, 3GPP Technical Specific Group Terminals (2001)
11. Internet Protocol Telephony and Voice Over the Internet Protocol, Security Technical Implementation Guide, Defense Information Systems Agency (DISA) for the U.S. Department of Defense (DOD), Version 2, Rel. 2 (April 2006), http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R2.pdf
12. Griffin, S.E., Rackley, C.C.: Vishing. In: Proc. of the ACM InfoSecCD '08: Proceedings of the 5th annual conference on Information Security Curriculum Development, pp. 33–35 (2008)
13. Caller ID spoofing with PHP and asterisk (last updated 14 February 2006), http://www.nata2.org/2006/02/14/caller-id-spoofing-with-php-and-asterisk/
14. The definitive resource on Caller ID spoofing (last updated, 20 February 2009), http://www.calleridspoofing.info/
15. Running your own GSM network, 25th Chaos Communication Congress (last updated, 29 December 2008), http://events.ccc.de/congress/2008/Fahrplan/events/3007.en.html
16. SMS phishing, Computer Crime Research Center, September 04 (2006), http://www.crime-research.org/news/04.09.2006/2221/
17. SMiShing: SMs phISHING, Wikipedia, the free encyclopedia (last updated, 1 May 2009), http://en.wikipedia.org/wiki/SMiShing
18. Castiglione, A., Cattaneo, G., De Santis, A., Petagna, F., Ferraro Petrillo, U.: SPEECH: Secure Personal End-to-End Communication with Handheld. In: Proc. of ISSE 2006, Securing Electronic Business Processes (Information Security Solutions Europe), October 2006, pp. 287–297. Vieweg Verlag (2006)
19. Harauz, J., Kaufman, L.M.: A New Era of Presidential Security: The President and His BlackBerry. IEEE Security & Privacy 7(2), 67–70 (2009)
20. Jailbreak (iPhone), Wikipedia, the free encyclopedia (last updated 29 April 2009), http://en.wikipedia.org/wiki/Jailbreak_(iPhone)
21. Castiglione, A., Cattaneo, G., Cembalo, M., De Santis, A., Petagna, F., Ferraro Petrillo, U.: An Extensible Framework for Efficient Secure SMS". Technical Report - University of Salerno