Smart-Phone Attacks and Defenses

Chuanxiong Guo
xguo@ieee.org
Microsoft Research

Helen J. Wang
helenw@microsoft.com
Microsoft Research

Wenwu Zhu[*]
wenwu.zhu@intel.com
Intel Corporation

ABSTRACT

Internet has been permeating into every corner of the world and every aspect of our lives, empowering us with anywhere, anytime remote access and control over information, personal communications (e.g., through smart-phones), and our environment (e.g., through the use of sensors, actuators, and RFIDs). While enabling interoperation with the Internet brings tremendous opportunities in service creation and information access, the security threat of the Internet also dauntingly extends its reach. In this paper, we wish to alarm the community that the long-realized risk of interoperation with the Internet is becoming a reality: Smart-phones, interoperable between the telecom networks and the Internet, are dangerous conduits for Internet security threats to reach the telecom infrastructure. The damage caused by subverted smart-phones could range from privacy violation and identity theft to emergency call center DDoS attacks and national crises. We also describe defense solution space including smart-phone hardening approaches, Internet-side defense, telecom-side defense, and coordination mechanisms that may be needed between the Internet and telecom networks. Much of this space is yet to be explored.

1. INTRODUCTION

The first proof-of-concept smart-phone worm, *Cabir* [14], has recently appeared. This is among the first signs of the expansion of the Internet security threats into other networks like telecom networks by the means of interoperating devices, e.g., smart-phones that are endpoints to both networks. These threats are especially alarming because as smart-phones become prevalent (according to market forecast [25], 30 millions smart-phones will be shipped in 2004, and more than 100 millions in 2007), and as their powerfulness and functionality reaches that of PCs [23], a fast- and wide-spreading smart-phone worm or virus could cause the large cohort of compromised smart-phones to cripple the telecom infrastructure and jeopardize critical call centers, such as 911, resulting in national crises.

In fact, telecom networks are not the only reach of the Internet security threats. Many have long realized that as we bridge home networks, sensor networks, and RFID-based inventory systems to the Internet for more flexible service creation and integration, we also give opportunities to Internet-based intrusions into those networks. Sometimes these intrusions could even be transformed into physical attacks — for example, actuators could be maliciously instructed to turn on the oven and cause a fire accident.

In this paper, we want to bring attention to the imminent dangers that Internet-compromised smart-phones can bring to telecom networks. We first give some background on smart-phones and discuss their trend of having common development platforms for the ease of service creation and deployment in Section 2. In Section 3, we describe various attack vectors for compromising smart-phones; then enumerate attacks launched by compromised smart-phones against the telecom networks, including radio channel consumption attacks, DDoS attacks against call centers, spamming, identity theft, and wiretapping. We give guidelines and potential strategies on protecting the telecom infrastructure as well as smart-phones in Section 4 and discuss other interoperating devices and the causes for such attacks in Section 5. Finally, we conclude in Section 6

2. SMART-PHONES

Smart-phone is the trend of unified communications which integrate telecom and Internet services onto a single device because it has combined the portability of cell-phones with the computing and networking power of PCs. As illustrated in Figure 1, smart-phones, as endpoints of both networks, have connected the Internet and telecom networks together.

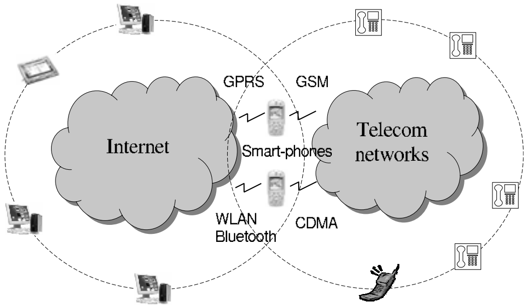

Figure 1: Smart-phones become end-points of both the Internet and telecom networks.

Another key reason for this trend is the ease and low cost of introducing new integrated Internet and telecom services. Easy service creation demands common operating systems (OSes). Because smart-phones are typically as powerful as a

[*]This work was performed while Wenwu Zhu was affiliated with Microsoft Research Asia.

few year-old PCs, their operating systems have evolved to be rather full-fledged. Smart-phone OSes today include Symbian OS [25], Microsoft Smart-phone OS [6], Palm OS [12], and embedded Linux. Although the detailed design and functionality vary among these OS vendors, all share the following features [23]:

- Access to cellular network with various cellular standards such as GSM /CDMA and UMTS.
- Access to the Internet with various network interfaces such as infrared, Bluetooth, GPRS/CDMA1X, and 802.11; and use standard TCP/IP protocol stack to connect to the Internet.
- Multi-tasking for running multiple applications simultaneously.
- Data synchronization with desktop PCs.
- Open APIs for application development.

While common OSes, open APIs, and sophisticated capabilities enable powerful services, they also create common ground and opportunities for security breaches and increase worm or virus spreading potentials. Given the PC-like nature of smart-phones and the trend of full-fledged OSes, software vulnerabilities seem inevitable for their OSes and applications. Moreover, with the Internet exposure, smart-phones become ideal targets for Internet worms or viruses since smart-phones are always on, and their user population will likely exceed that of PCs, observing from the prevalence of cell phone usage today.

3. THE SMART-PHONE ATTACKS

In this section, we first describe various ways that smart-phones could be compromised, then we illustrate how compromised smart-phones may attack telecom networks.

3.1 Compromising Smart-Phones

There are three venues for a smart-phone to be compromised:

1. **Attacks from the Internet**: Since smart-phones are also Internet endpoints, they can be compromised the same way as the PCs by worms, viruses, or Trojan horses. The first Symbian based Trojan [19] has recently been discovered in a popular game software.
2. **Infection from compromised PC during data synchronization**: Smart-phone users typically synchronize their e-mails, calendar, or other data with their desktop PCs through synchronization software like ActiveSync [6]. There exists trust relationships between smart-phones and their respective synchronization PCs. Therefore, to ultimately infect a smart-phone, attackers can first infect its synchronization PC, and then the smart-phone will be infected at the next synchronization time.
3. **Peer smart-phone attack or infection**: A compromised smart-phone can actively scan and infect peer smart-phones through its Wireless Personal Area Networks (WPAN) interface such as Bluetooth or UWB (ultra wideband). Since smart-phones are mobile devices, they can infect new victims at different locations. The first smart-phone worm, Cabir [14], uses this method.

It is also possible that a cellular phone can be crashed by a malformed SMS text message [9]. Nonetheless, due to the limited services provided by the telecom networks, the attack surface at the telecom side is much smaller than that of the Internet side. Therefore, we believe that the risk that a smart-phone to be compromised on the telecom side is minimal.

3.2 Smart-Phone Attacks against the Telecom Networks

Once a smart-phone is compromised from the Internet, it also becomes a source of malice to the telecom networks that it has access to. Before we describe the attacks, we first give a brief description of the GSM cellular network [20], as an example of telecom networks against which smart-phone attacks can be launched. Nevertheless, the attacks we describe here can be applied to other cellular networks, such as CDMA, as well.

3.2.1 Background: GSM

GSM consists of three sub-systems: the Mobile Equipment (ME), the Base Station Subsystem (BSS), and the Network Switching Subsystem (NSS). ME has a Subscriber Identity Module (SIM) for storing identities, such as the International Mobile Subscriber Identity (IMSI). BSS consists of two elements: the Base Transceiver Station (BTS) which handles radio interfaces between BTS and MEs and the Base Station Controller (BSC) which manages radio resources and handovers. NSS uses mobile switching center (MSC) for routing phone calls and connecting the GSM system to other public networks such as PSTN.

Besides voice communications, GSM also offers Short Message Service (SMS) [18], Multimedia Message Service [7], and GPRS general packet radio service [4] for Internet access.

The radio spectrum is limited resource in any cellular systems. GSM uses a combination of Time and Frequency Division Multiple Access (TDMA/FDMA) to time-share or space-share the radio resources. FDMA divides the (maximum) 25 MHz bandwidth into 124 carrier frequencies of 200 KHz bandwidth each. One or more carrier frequencies are assigned to a base station. Each of the carrier frequencies is then divided into 8 time slots, with the TDMA scheme. Suppose a base station has n carrier frequencies, then the maximum number of voice users it can support is at most $C = 8n$. The value of n depends on the traffic volume of a base station. Typically, $n = 3$ or 4. In CDMA-based or next generation cellular networks [3, 11], logical “channels” are used for voice and data traffic, which, at a high level, are similar to time slots.

Telecom networks operate under the following two assumptions: 1. Its traffic is highly predictable. 2. User identities are tightly coupled with their telephone numbers or SIM cards. With the first assumption, telecom carriers plan their network capacity according to the predicted traffic model. With the second assumption, telephone numbers or SIM cards are used for accounting purposes. These assumptions have been held (mostly) up to now. However, with the prevalence of smart-phones in the near future, these assumptions could be easily violated by attackers through subverting smart-phones from the Internet, which we describe in detail next.

3.2.2 Attack I: Base Station DoS

Compromised smart-phones can easily make phone calls, say using Microsoft Smart-phone SDK API *PhoneMakeCall* [6], to call other phone numbers obtained from sources like yellow pages.

The radio channel of a GSM base station with n carrier frequencies can be completely exhausted by $8n$ well-coordinated smart-phone zombies in the same cell initiating calls and using up all the time slots of a base station. The zombies can hang up as soon as their call setups complete and then re-initiate new calls, and so on. In the case that a callee is also subverted, the callee smart-phone can be configured deliberately not to answer the phone, occupying the time slot at both the caller and the callee side for about one minute in each call attempt. Since the callee does not accept the call, the caller would not even need to pay for this unfinished call, despite the fact that valuable radio resource has been allocated and wasted.

The impact of this type of attacks on the availability of the cellular network can be significant. In telecom networks, *call blocking rate* is the metric for measuring the availability of the network. Typically, the availability requirement for telecom network is a call blocking rate of less than 0.01%. Telecom carriers plan for the network capability according to call volume statistics and obey the call blocking rate requirement. The call blocking probability is calculated with the Erlang B formula [1]: $B(C, \alpha) = \frac{\alpha^c/C!}{\sum_{i=0}^{C} \alpha^i/i!}$ where C is the number of radio channels in our context, α represents the planned call volume to support for, and B is the call blocking probability. Typically the planned call volume is an average of 15-16 simultaneous users (i.e., $\alpha = 15.63$ Erlang) and since the call blocking rate is expected to be less than 0.01% ($B < 0.01\%$), a base station typically needs 4 carrier frequencies and a total of 32 voice channels (8 time slots $\times$ 4), so $C = 32$. Erlang B formula assumes the common telephone behaviors – they are idle most of the time and the traffic aggregation from many phones is highly predictable. These assumptions, however, can be easily violated by compromised smart-phones. With 8 compromised smart-phones occupying 8 out of 32 channels, the blocking probability rises to 1.2%; if 16 and 24 channels are occupied, the blocking rates will be as high as 16.4% and 53.6%, respectively; when all 32 channels are taken, the system will simply be out of service. This shows that even a handful of subverted smart-phones can jeopardize the availability of a base station.

Similar attacks can be launched against GPRS. In GPRS, at most 8 time slots can be assigned to GPRS users in a base station. The maximum data rate is at most 171 Kbps. Such a small bandwidth capacity can be easily saturated. GPRS networks may assign private addresses to smart-phones due to IPV4 address shortage and use NAT or NAPT to communicate with the rest of the Internet. In this case, compromised smart-phones can actively initiate connections first, thereafter, both sides are free to send packets to each other.

3.2.3 Attack II: DDoS Attack to Call Centers

This attack is similar to the previous one, but the goal is not to exhaust radio resources, but to put call centers to a halt. This is in the same spirit as the Internet DDoS attacks to web servers.

Such attacks are not possible in the past with traditional telephones because one would have to manually dial call center numbers. This requires attackers to be physically co-located with many phones. Consequently, the attackers can be easily traced back, caught, then legally prosecuted.

For the case of smart-phone zombies, their owners are most likely the victims rather than the attackers themselves. Therefore, tracing back to the true attackers becomes a much more difficult task.

Similar DDoS attacks can be launched against PSTN and cellular switches, which are designed for a limited Busy Hour Call Attempts (BHCA). These switches may collapse once the BHCA value is out of the designed range. For example, right after terrorists' attacks on September 11, 2001, the phone switches were under such a heavy load that it was hard to call a New York resident. Similarly, a large cohort of smart-phone zombies could create the same flash-crowd effect.

Not only smart-phone DDoS attacks can cause service disruptions and heavy financial losses, they can also jeopardize national security by attacking the critical 911 service, leaving emergency patients not saved and accidents, crimes or terrorists' acts not reported.

3.2.4 Attack III: Spamming

Attackers can manipulate smart-phone zombies to send junk or marketing messages through SMS. In the case that the charging model is flat, a compromised smart-phone can spam for "free"; and therefore its owner may not even notice its bad behavior. Free SMS spamming gives attackers good incentives to compromise smart-phones.

3.2.5 Attack IV: Identity Theft and Spoofing

Telephone numbers or IMSIs stored on SIM cards are difficult to spoof, which is the basis of authentication and accounting mechanisms in telecom networks.

In the past, researchers have attempted and successfully spoofed SIM cards [21]. However, the procedure involves physical access to a SIM card, and requires about 150,000 queries to the stolen card, which could last as long as 8 hours. Mass cloning with attacks in this nature is hard.

However, this is not the case with smart-phones. Identity theft with smart-phones is trivial — once a smart-phone is compromised, the attacker literally possesses its owner's identity for any activities in her name. This is especially alarming since in many countries, one's SIM card serves as her identity card for voting, ordering goods, or accessing her finance. Further, call center services evolve to be completely automatic, which enables attackers to carry out automatic response.

With the possession of an identity, an attacker can even achieve impersonation. For example, an attacker can use Voice-Over-IP from the Internet and then use a smart-phone zombie as a relay point in pretending to be the smart-phone owner for both incoming and outgoing phone calls.

3.2.6 Attack V: Remote Wiretapping

A smart-phone zombie can also passively record the conversations of its owner with others; and then stealthily report back to some spies. Such attacks could be hard to detect since recording and reporting can be two asynchronous steps; the report traffic can even be encrypted and tunneled along with other legal Internet traffic to further evade detection. It is even difficult for the smart-phone owner to notice the spying activity.

Such easy and stealthy remote wiretapping could easily become means of blackmailing and espionage activities from insider-trading to classified information extraction.

4. DEFENSE

We address defense for smart-phone attacks from four angles: How we may harden smart-phones themselves to be less vulnerable; Internet-side defense; telecom-side defense; and what coordinations between the Internet and telecom networks may be needed. We don't intend to give full-fledged or bullet-proof solutions, but rather to layout the landscape of the solution space, and point out interesting and challenging topics of research in this area.

4.1 Smart-Phone Hardening

People have long favored functionality over security and are unwilling to pay the price and inconvenience incurred by security schemes [15]. Functionality demands extensibility, and extensibility invites malicious extensions. Given the current trend, unless legislature can effectively mandate limited extensibility for smart-phones, we don't see the hope of reducing the powerfulness and functions of a smart-phone. Nevertheless, there are some strategies that we'd like to point out for hardening smart-phone which we discuss as follows:

- **Attack surface reduction:** One simple defense is to reduce the attack surface as much as possible. This defense mechanism has also been applied to PCs [5], but with limited success because it is disruptive to popular applications like file-sharing and network printer. Nevertheless, this mechanism may be more effective for smart-phones because the smart-phone usage model is different from that of PCs. Although a smart-phone is always on, most of its features need not be active. For example, when users make an outgoing phone call or compose a SMS message, the PC part of the smart-phones can be turned off (unless instructed otherwise, say, when a user is downloading a movie).

- **OS hardening:** Smart-phone OSes can enforce some security features, such as always displaying callee's number and lighting up LCD display when dialing. This can be achieved by only exporting security enhanced APIs to applications. With hardened OSes, unless attackers can subvert the smart-phone OS without being noticed, attacking actions from malicious user-level code can be more easily detected by the smart-phone user.

- **Hardware hardening:**

  We believe one advantage we can leverage for smart-phone hardening is that smart-phone already has an embedded smart-card, the SIM card. The SIM card has evolved to incorporate the use of the SIM Toolkit (STK) — an API for securely loading applications to the SIM. STK allows the mobile operator to create or provision services by loading them into the SIM card without changing anything in the GSM handset. One interesting approach therefore is to combine STK card and TCG's Trusted Platform Module (TPM) [10] for smart-phone hardware harding. This way, no additional security chips will be needed.

4.2 Internet Side Protection

The malware defense mechanisms that have been deployed or proposed for the Internet can be readily applied to smart-phones. For example, more rigorous process in software patching or vulnerability-driven network traffic shielding [24] will certainly strengthen the defense for smart-phones for known vulnerabilities, though not unknown ones. It would be desirable for smart-phone Internet service providers to ensure that devices that access them are properly patched or shielded — unpatched or unshielded ones should not be exposed to the wild Internet. Currently, majority of smart phones access the Internet through telecom data networks such as GPRS or CDMA1X. In this scenario, base stations can first check whether smart-phones have been properly patched or shielded and they will be forced to patch or shield if not. Alternatively, base stations could even perform shielding on behalf of the smart-phones. This kind of strategy, however, faces challenges when smart-phones use 802.11 access points for Internet connectivity: many 802.11 access points have already been deployed, it would be very difficult, if possible at all, to upgrade all the access points to enforce patching or shielding. Further, such quarantining makes seamless handoff between access networks very challenging. This is an open research question.

In any case, the weakest link points to smart-phone users, who may be fooled to download a piece of malicious code (masquerading as a pirated movie) that takes the advantage of the interoperability feature of smart-phones to attack telecommunication networks.

4.3 Telecommunication Side Protection

There will always be some subverted smart-phones no matter how much Internet-side protection there is. Telecom networks must introduce misbehavior detection and reaction mechanisms to sustain its normal operation.

Fortunately, unlike the Internet traffic, telecom traffic is highly predictable and well managed since they can only be voice or SMS traffic. Therefore, it is not difficult to identify abnormal behaviors. To detect smart-phone attacks, telecom carriers can collect and analyze the following information from its networks:

1. Abnormal blocking rate of a base station or a switch: Normally the call blocking rate should be below a threshold (e.g., $< 0.01\%$). A sudden rise in the blocking rate is a good indication of an on-going attack. Similarly, abnormal data packet drop rate at the GPRS or CDMA Internet access networks is also such an indicator.

2. Call center load information: If a call center experience unexpected flash crowd and client behaviors are abnormal (see the next point), then the call center is very likely to be attacked.

3. Abnormal end user behaviors: Such as endless call initiations followed by abortions, connected calls without voice traffic, non-interactive bi-directional traffic; prolonged data packet transmissions from or to a single user, and spamming.

Most statistics demanded here can be obtained from the network management units of telecom networks. For abnormal end user behavior detection, message content will need to be examined and analyzed. For junk SMS messages, techniques developed for email spam filtering can be applied here.

When abnormal behaviors are observed at the telecom side, telecom networks can perform rate limiting, call filtering, or put the zombie smart-phone IDs into a black list — it is much easier to trace back misbehaving smart-phones in telecom networks. All the building blocks such as rate limiting, filtering, and caller ID are already available in current telecom infrastructures. Therefore, building an effective defense system in telecom networks seems hopeful. Nonetheless, it will be very expensive to put these defense mechanisms into various parts of the telecom infrastructure.

Another advantage in telecom networks is that there are only a handful telecom carriers, unlike tens of thousands of Autonomous Systems we have seen in the Internet. Therefore, it will be easier for telecom carriers to coordinate their defense effort.

4.4 Cooperations between the Internet and Telecom Networks

Solutions proposed in the previous sections can hardly be bullet-proof. Effective coordination between the Internet and telecom networks would be desirable. In this section, we discuss the opportunities and difficulties in coordinating the Internet and telecom networks for defending against smart-phone attacks.

Known vulnerability and attack information can be exchanged between the Internet and telecom networks. Then, attack surface on smart-phones can be further reduced by not using vulnerable services as much as possible. If specific attack target information, such as which call center will be attacked, becomes known from the Internet side, it can help the call center prepare for the attack and put its rate limiting and call filtering mechanisms in place.

With the black list of smart-phone zombies from a telecom carrier, Internet access points (AP) could potentially reject those zombies from getting on the Internet. This means that SIM ID-based authentication needs to be in place for the APs. If GPRS is used for Internet access, this authentication is trivial. However, for 802.11-like APs, this is very challenging in that these APs are not just for smart-phones but general-purpose for all wireless Internet endpoints; state-of-the-art APs cannot recognize which devices are smart-phones, and which are not, since a smart-phone can always claim not being one. We identify the following approaches in addressing this issue:

1. Since it is hard to differentiate between smart-phones and other endpoints, we could assign unique IDs to all Internet wireless endpoints, then create the mapping between SIM IDs and Internet wireless IDs. This solution faces significant backward compatibility issues with the existing devices and 802.11 infrastructure.

2. We could design smart-phone OSes to submit SIM IDs to APs for authentication when accessing the Internet, as part of the OS hardening (see Section 4.1). This solution raises the bar for attackers significantly. To make OS tamper-proof, we could further harden the smart-phone hardware for OS authentication, as described in Section 4.1.

5. DISCUSSIONS

5.1 Modem-Equipped or VoIP-Enabled PCs

Modem-equipped or Voice-Over-IP-enabled PCs are also interoperating devices which are capable to launch some of the attacks described in Section 3. Nonetheless, there are some subtle differences between such PCs and smart-phones. PCs and phones are loosely coupled devices in Modem-equipped PCs and users can only access one network at a time in this context; so attacks that take advantage of simultaneous access to both networks, such as remote wiretapping (Section 3.2.6), are not possible. VoIP-enabled PCs do not have SIM cards; therefore identity theft-based attacks (Section 3.2.5) are not possible. Also, VoIP-enabled PCs are not direct telecom endpoints, but proxied over IP-to-PSTN gateways. Simple rate-limiting at such gateways could easily contain attacks from VoIP-enabled PCs. Moreover, smart-phones are more ideal attack targets than these interoperating PCs because of its popularity.

5.2 Interoperation breaks design assumptions

Despite telecom carriers' wishes, some intelligent Internet end-points are becoming end-points of telecom networks. The Internet and telecom networks, however, are inherently different in nature. The telecom networks are well-planned and engineered, which were mainly designed for telephone calls, and hence the design choice of dumb terminals and intelligent network core.

On the other hand, the Internet was designed to be general-purpose, with future unknown applications in mind, and hence the design choice of the best effort data delivery model which offers the minimal of what any applications may need. Additional guarantees or features must be achieved through higher layer customizations at respective endpoints. As a result, the Internet is a relatively "dumb"[1] network with intelligent endpoints.

Both networks have been successful in fulfilling their design goals: Telecom networks have been serving our voice communications with high reliability and availability for more than a century; the flexibility of the Internet has revolutionized information exchange and service creation and begotten the whole e-commerce industry. However, when the two networks are connected with smart-phones, the assumption of dumb terminals in telecom networks no longer holds. Consequently, the attacks described in Section 3 become possible in telecom networks.

While the risk of interoperation with the Internet has long been realized, as smart-phones are gaining popularity, this risk is materializing into extremely dangerous and realistic threat.

Other networks or systems that are on the way of being bridged into the Internet include sensor networks, RFID-based inventory systems, and home networks. The Internet offers the flexibility and easy service integration for connecting these systems or networks. But the other side of the coin is that the security level of these systems then reduces to that of the Internet. Since these systems are designed for specific functionalities, specific attacks targeted for those functionalities can then be designed. It is alarm-

[1] Functionalities such as routing and traffic engineering provided by the Internet core are by no means "dumb". However, the complexities are transparent and unknown to end applications.

ing that these attacks can even be transformed into physical attacks. For example, if sensor networks were controlled by Internet-based attackers, the actuators could be controlled to increase the room temperatures, or open the security gate! Since these attacks often take advantage of the violated assumptions (such as the dumb terminal assumption of the telecom network) in specific targeted systems, it will be difficult to design general defense mechanisms. Therefore, it is important to consider the Internet security issues at the design time for such interoperating systems.

6. CONCLUSION

In this position paper, we wish to alert the community on the imminent dangers of potential smart-phone attacks against telecom infrastructure, the damages caused by which could range from privacy violation and identity theft to emergency center outage resulting in national crises. We have outlined a number of defense strategies, many of which demand much further research. We also urge system architects to pay close attention to the insecurity of the Internet when bringing new peripherals to the Internet.

7. ACKNOWLEDGEMENT

We thank Zihua Guo for providing materials about cellular networks. Nikita Borisov, David Brumley, John Dunagan, Jon Howell have provided us insightful critiques and comments on the first draft of our paper. We are thankful to their input.

8. REFERENCES

[1] Ian Angus. An Introduction to Erlang B and Erlang C. *Telemanagement*, July-August 2001.

[2] Andrey Belenky and Nirwan Ansari. On IP Traceback. *IEEE Communications Magazine*, July 2003.

[3] Live Bos and Suresh Leroy. Toward an All-IP-Based UMTS System Architecture. *IEEE Network*, January and February 2001.

[4] Jian Cai and David J. Goodman. General Packet Radio Service in GSM. *IEEE Communications Magazine*, October 1997.

[5] Microsoft Corporation. New Security Technologies in Windows XP Service Pack 2 (SP2). http://msdn.microsoft.com/security/productinfo/xpsp2/default.aspx?pull=/library/en-us/dnwxp/html/securityinxpsp2.asp.

[6] Microsoft Corporation. Windows Mobile-based Smartphones. http://www.microsoft.com/windowsmobile/smartphone/default.mspx.

[7] Stéphane Coulombe and Guido Grassel. Multimidia Adaptation for the Multimedia Messaging Service. *IEEE Communications Magazine*, July 2004.

[8] David Dagon, Xinzhou Qin, Guofei Gu, Wenke Lee, Julian Grizzard, John Levine, and Henry Owen. Honeystat: Local Worm Detection Using Honeypots. In *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID)*, 2004.

[9] F-Secure. SMS Killer. http://www.f-secure.com/v-descs/sms.shtml.

[10] Trusted Computing Group. TCG TPM Specification Version 1.2: Design Principles . https://www.trustedcomputinggroup.org/home.

[11] Harri Honkasalo, Kari Pehkonen, Markku T. NieMi, and Anne T. Leino. WCDMA and WLAN for 3G and Beyond. *IEEE Wireless Communication Magazine*, April 2002.

[12] PalmOne Inc. Treo smartphones. http://www.palmone.com/us/products/smartphones/.

[13] Christian Kreibich and Jon Crowcroft. Honeycomb - Creating Intrusion Detection Signatures Using Honeypots. In *Proc. HotNets*, 2003.

[14] Kaspersky Labs. Viruses move to mobile phones, 2004. http://www.kaspersky.com/news?id=149499226.

[15] Butler W. Lampson. Computer Security in the Real World. *IEEE Computer*, June 2004.

[16] David Moore, Geoffrey Voelker, and Stefan Savage. Inferring Internet Denial-of-Service Activity. In *Proceedings of the 2001 USENIX Security Symposium*, 2001.

[17] Vern Paxson. Bro: a system for detecting network intruders in real-time. *Computer Networks*, 31(23-24):2435–2463, 1999.

[18] Guillaume Peersman, Srba Cvetkovic, Paul Griffiths, and Hugh Spear. The Global System for Mobile Communications Short Message Service. *IEEE Personal Communications Magazine*, June 2000.

[19] Cyrus Peikari, Seth Fogie, Jonathan Read, and David Hettel. Summer Brings Mosquito-Borne Malware. http://www.informit.com/articles/article.asp?p=327994&seqNum=1.

[20] Moe Rahnema. Overview of the GSM System and Protocol Architecture. *IEEE Communications Magazine*, April 1993.

[21] The ISAAC research group. GSM Cloning. http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

[22] Martin Roesch. Snort-lightweight intrusion detection for networks. In *Proceedings of LISA'99*, Seattle, Washington, November 1999.

[23] S.J. Vaughan-Nichols. OSs battle in the smart-phone market. *IEEE Computer*, 36(6), 2003.

[24] Helen J. Wang, Chuanxiong Guo, Daniel. R. Simon, and Alf Zugenmaier. Shield: vulnerability-driven network filters for preventing known vulnerability exploits. In *Proc. SIGCOMM*, August 2004.

[25] Symbian white paper. Symbian smartphones for the enterprise. http://www.symbian.com/technology/smartphone_enterprise.html.