ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Review of Smart Phone Attacks

Pratyush, Prince, Punit Anand

UG Students, Department of ECE , Aarupadai Veedu Institute of Technology, Payanoor, Chennai, India

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. 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.

I.INTRODUCTION

The first proof-of-concept smart-phone worm, 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 end points to both networks.

These threats are especially alarming because as smart-phones become prevalent and as their powerfulness and functionality reaches that of PCs , 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, 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 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 discuss other interoperating devices and the causes for such attacks in Section 4.

II.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.

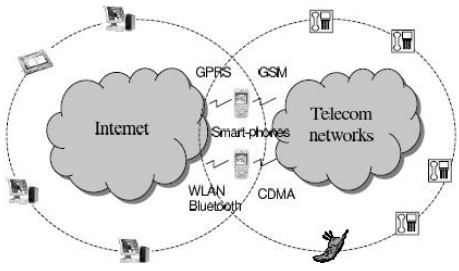

FIGURE:1 Smart-phones become end-points of both the Internet and telecom networks

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

As illustrated in Figure 1, smart-phones, as endpoints of both networks, have connected the Internet and telecom networks together.

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

• 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.

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.

III. THE SMART-PHONE ATTACKS

In this section, we first describe various ways that smartphones 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 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 [5]. There exist trust relationships between smart-phones and their respective synchronization PCs. Therefore, to ultimately infect a Smartphone, attackers can first infect its synchronization PC, and then the smart-phone will be infected at the next synchronization time.

3.It is also possible that a cellular phone can be crashed by a malformed SMS text message. 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, as an example of telecom networks against which Smartphone 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, GSMalso offers Short Message Service (SMS) , Multimedia Message

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Service [6],and GPRS general packet radio service [3] 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 [2, 9], 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 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.

IV.DISCUSSIONS

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.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 are not possible. VoIP-enabled PCs do not have SIM cards; therefore identity theft-based attacks are not possible. Also, VoIP-enabled PCs are not direct telecom endpoints, but proxied over IPto-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.

V.CONCLUSION

In this 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 also urge system architects to pay close attention to the insecurity of the Internet when bringing new peripherals to the Internet.

REFERENCES

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

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

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

[4] Microsoft Corporation. New Security Technologies in Windows XP Service Pack 2 (SP2).