www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1018 -1022

Study of Smartphone Attacks and Defenses

Bhavya Chojar, Divya Lal, Kunal Gandhi, Kshitij Salariya
Computer Science Department, Dronacharya College of Engineering,
Greater Noida, Uttar Pradesh India
bhavya_1992@ymail.com, dl_3792@yahoo.co.in, kunal_gandhi_91@yahoo.co.in,
kshitijsalariya@yahoo.co.in

Abstract

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 enlighten 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 propose techniques to generate solution space that includes smart-phone hardening approaches, Internet-side defense, telecom-side defense, and coordination mechanisms that may be needed between the Internet and telecom networks.

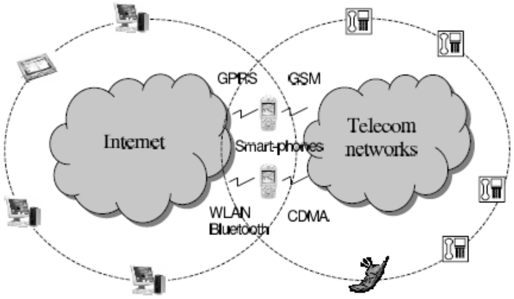
KEYWORDS-- Spamming, Identity Theft, Wiretapping, Internet, Telecommunication Side Protection, vulnerability.

I. INTRODUCTION

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 and discuss other interoperating devices and the causes for such attacks.

I. 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.



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.

II. THE SMART-PHONE ATTACKS

A. *Telecom Design Assumptions*

Traffic is highly predictable

- Telecom carriers plan network capacity according to the predicted traffic model
- Radio spectrum sharing schemes includes TDMA, FDMA, or logical “channels”

User identities are tightly coupled with their telephone numbers or SIM cards

- Telephone number or SIM (*Subscriber Identity Module*) cards are used for accounting purposes

B. Motivation

Telecom network was relatively safe
Smart-phone worms, viruses, Trojan horses appeared

- Cabir, June 14, 2004 (worm)
- Duts, July 17, 2004 (virus)
- Mosquito dialer, August 6, 2004 (trojan horse)

The source code of the Cabir has been posted online by a Brazilian Programmer
Various attacks to telecom infrastructures and users become reality

C. 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. There exists 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. *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, uses this method.

D. Attack I: Base Station DoS

Compromised smart-phones can easily make phone calls, say using Microsoft Smart-phone SDK API PhoneMakeCall [5], 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 con-
figured 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. It 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.

E. 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 colocated 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 sameflash -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.

III. DEFENSES

A. *Internet side protection*

Protection techniques like more intensive software patching and vulnerability-driven network traffic shielding will definitely be useful protection for smartphones against well-Known vulnerabilities. It would be desired for smartphone Internet service providers to guarantee that devices which access them are shielded or patched. It means that unshielded devices should not be granted access to the Internet.

B. *Telecom side protection*

In order to detect the smartphone attacks described, analyzing the following information from telecom networks can be helpful for telecom carriers:

- Anomalous blocking rate of a base station or a switch: Commonly the call blocking rate must be under a threshold (< 0.01%). So a sharp increase in the blocking rate can be a conspicuous sign of an ongoing attack.
- Call center load information: if a call center experiences a sudden flash crowd and user behaviors are anomalous then the call center is susceptible to attack.
- End user's misbehavior: A normal behavior such as connected calls with no voice traffic; lengthy data packet transmission from a single user or to a single user and transmitting the same message to many different users (spamming).

.

C. Protection against spoofing

A simple defense technique that only works for simple ARP spoofing attacks is the use of static IP-MAC mappings. In order to be protected against IP spoofing, the solution is to apply ingress filtering and have all internal routers to disable source routing. It can be further prevented by educating users to be conscious about the address window in a web browser that shows the web address they are directed to. In addition, DNS spoofing can be prevented by securing the DNS servers and by adding anti-spoofing measures to the filter-list to check site ratings for URLs by their name and IP address. DNS lookups are supported to filter-list information for improved IP address lookups.

D. Protection against DDoS attacks

The following countermeasures can be taken as precautionary techniques against DDoS attacks:

- Filtering the packets with broadcast address as a destination address which are coming into the networks.
- Turning off directed broadcast address on all internal routers.
- Blocking any packet with the source addresses which contain address space 10.0.0.0, 172.16.24.0, 192.168.0.0 and loop back address 172.0.0.0 to enter.
- Setting rules in the firewalls to block any packet that apply a port or protocol which is not for Internet communication in the local area network.
- Preventing packets with a source address belonging to the inside to enter the network.
- Applying DoS detection tools like Air Magnet and Air Defense
- Scanning the computer systems and network to ensure that they contain no publicly known vulnerabilities

.

E. Hardening the Smartphones

Smartphone hardening is one of the recommended solutions to make smartphones less vulnerable. Some techniques can be:

- Operating system hardening(OS hardening):

Some security issues can be enforced by Smartphone operating systems like always showing the callee's phone number and also brighten LCD display when dialing. This can be achieved by only using security modified APIs to applications. There are also further policies for hardening operating systems such as using security patches and bug patches to software and limiting user privileges and disabling unnecessary processor

- Hardware hardening:

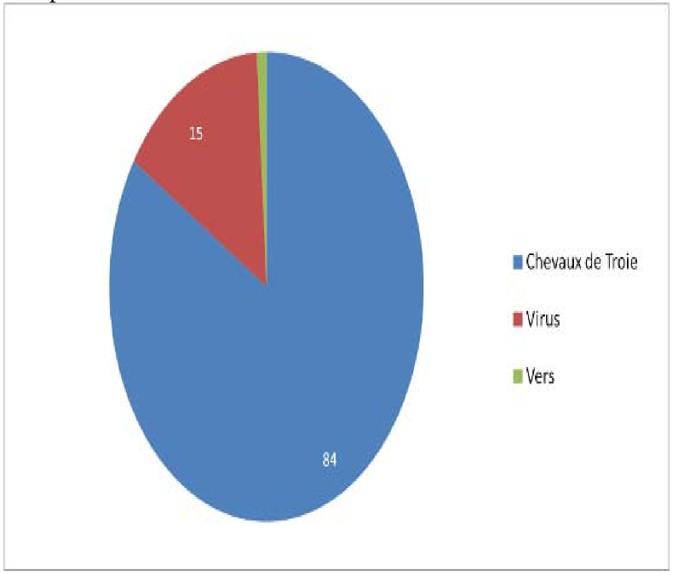
Smartphone already has an embedded smart-card(the SIM card)which has evolved to incorporate the use of the SIM Toolkit (STK)

1. STK allows the mobile operator to provide services by loading them into the SIM card without modification of the GSM handset .One intriguing method is merging the STK card and TCG Trusted Platform Module (TPM) for smartphone hardware hardening without additional security chips

- Feature reduction: one simple protection technique is to reduce inactive features as much as possible. Although Smartphones are always on, most of their features are not necessary to be active. For instance, Bluetooth and WiFi should be turned off when not in use.

F: Malicious Software (Malware)

As smartphones are a permanent point of access to the internet (mostly on), they can be compromised as easily as computers with malware. A malware is a computer program that aims to harm the system in which it resides. Trojans, worms and viruses are all considered malware. A Trojan is a program that is on the smartphone and allows external users to connect discreetly. A worm is a program that reproduces on multiple computers across a network. A virus is malicious software designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel. However, it must be said that the malware are far less numerous and important to smartphones as they are to computers.



1) *The three phases of malware attacks*

Typically an attack on a smartphone made by malware takes place in 3 phases: the infection of a host, the accomplishment of its goal, and the spread of the malware to other systems. Malware often use the resources offered by the infected smartphones. It will use the output devices such as Bluetooth or infrared, but it may also use the address book or email address of the person to infect the user's acquaintances. The malware exploits the trust that is given to data sent by an acquaintance.

Infection

Infection is the means used by the malware to get into the smartphone, it can either use one of the faults previously presented or may use the gullibility of the user. Infections are classified into four classes according to their degree of user interaction:

Explicit permission

The most benign interaction is to ask the user if it is allowed to infect the machine, clearly indicating its potential malicious behavior. This is typical behavior of a proof of concept malware.

Implied permission

This infection is based on the fact that the user has a habit of installing software. Most Trojans try to seduce the user into installing attractive applications (games, useful applications etc.) that actually contain malware.

Common interaction

This infection is related to a common behavior, such as opening an MMS or email.

V. IMPACT OF COMPROMISE

An attacker who has fully compromised a device which remains in use (whether a smartphone or a PC) can effectively impersonate the user of that device. This includes access to all data and network resources available to the user. This is because a sophisticated attacker can elevate privileges to that of the device's operating system, and carry out any activity from the device that the user would (and without the user knowing). This includes making use of any credentials stored directly on the device, or those which are accessible from it. Storing credentials on hardware tokens provides a mitigation, as the attacker is then required to connect to the compromised device in order to make use of these credentials. This requires an attacker to expend more effort and engage in more-visible network activities. Any credentials stored directly on the device's main storage, however, can be collected by an attacker during the initial compromise and then used to impersonate the user and access resources from another location at the attacker's leisure. As malicious email or web pages can be used by an adversary to make a successful initial intrusion into either a smartphone or desktop, little stands in the way of an attacker making further use of such techniques to compromise other systems (and gather privileged credentials) once inside an enclave. This can be enabled by using contacts listed in the address book of the user's device. For outdated desktop systems which are most vulnerable to this kind of attack, it is notable that applying the limited configuration guidance available for browsers, email clients, or PDF readers is a very weak mitigation when compared to updating to newer software.

Although modern smartphones are more resistant to fully remote compromise when compared to outdated desktop systems, their array of hardware features provides an attacker with much greater capabilities for information gathering and remote communications. This includes a microphone for listening to conversations, GPS for location tracking, cameras for visual surveillance, and cellular or WiFi radio for non-enterprise controlled or monitored network communications. Such capabilities may be of little consequence on a compromised device that belongs to a rank and file soldier or civilian, but may betray significant sensitive information from a senior leader.

Effective detection of compromise remains a high priority, and this is dependent on platform vendor cooperation. On some platforms, detection is currently hindered by security features themselves. App sandboxing, for example, limits the capabilities of any security-enhancing software that is not provided by the platform vendor as part of the device's operating system. Even mobile devices with a "trusted" or "secure" boot process – a valuable feature – often prevent independent access of the device's main storage area for verification purposes. Should vendors choose to provide it, low level hardware support for integrity checking could address this problem. Such a design permits confidence that a compromised operating system is not providing false integrity information.

VI. CONCLUSION

The new generation of smartphones is more resistant to some types of cyber-attacks that have proven extremely damaging to DoD, such as spear phishing and user-installed malicious software. At the same time, their use involves acceptance of other risks such as attacks via the cellular network, and a greater likelihood of data loss due to lost or stolen devices. Overall, vast numbers of obsolete desktops are likely to continue to be attackers' front door to DoD networks, although smartphones do permit highly motivated adversaries to carry out highly-targeted attacks against senior leaders. NSA continues to partner with industry to develop technological enhancements that prevent and detect such attacks. Hence 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.

VII. REFERENCES

[1]. www.google.com/smartphones attacks and defenses.

[2]. en.wikipedia.org/wiki/Mobile_security

[3].research.microsoft.com/en
us/um/people/helenw/papers/smartphone

[4].http://www.nsa.gov/ia/_files/factsheets/mobilerisks.pdf