5-31-2015

A Covert Channel in the Worldwide Public Switched Telephone Network Dial Plan

Bryan Harmat

Jared Stroud

Daryl Johnson

A Covert Channel in the Worldwide Public Switched Telephone Network Dial Plan

Bryan Harmat, Jared Stroud, and Daryl Johnson
Department of Computing Security
Rochester Institute of Technology
Rochester, NY 14623
Email: {bjh7242, jxs1261, daryl.johnson}@rit.edu

***Abstract*—The worldwide dial plan proposed by the International Telecommunication Union recommendation E.164 reserves multiple country codes for future use. These unused codes present an opportunity for a potential covert channel over the public switched telephone network utilizing a spoofed source phone number of a call to send information to a mobile device. The reserved country codes can act as a delimiter indicating that a secret message is being sent. By spoofing a call using a reserved country code number, the application listening on the mobile device will be able to intercept the call and extract information from the remaining digits based on ASCII encoding in a decimal format. The purpose of using a reserved country code number is so that there will be no denied service to the user with a call from a legitimate phone number.**

Keywords*—*Covert channel; Public Switched Telephone Network; Dial plan; Android; Phone number

I. Introduction

The public switched telephone network "refers to the worldwide voice telephone network accessible to all those with telephones and access privileges," as defined by Newton [15]. A dial plan (also commonly referred to as a numbering plan) is "a numbering scheme used in telecommunications to allocate telephone number ranges to countries, regions, areas, and exchanges, and to nonfixed telephone networks such as mobile phone networks." [17]. This is essential for call routing and is the central component of how phone numbers are allocated to different regions. By taking a subset of a dial plan, and converting the numeric values to ASCII characters; it is possible to embed hidden messages from a spoofed calling source number.

A. Legality

In the United States, the Truth in Caller ID Act of 2009 prohibits caller ID spoofing if the caller has "the intent to defraud, cause harm, or wrongfully obtain anything of value." [2]. However, during the development of this channel, there were no malicious intents as the tests during development were utilizing the authors' own devices.

B. North American Numbering Plan

The ITU E.164 recommendation [10] reserves multiple country codes such as 0 and 999. There should be no valid phone call from a phone number beginning with values such as these since they are "reserved for future use." [10]. Due to this, a covert channel can be created by taking advantage of the worldwide public switched telephone network dial plan. For the purposes of simplicity in order to elaborate on proposed methods of extensibility, this covert channel will follow the standards set forth by the North American Numbering Plan Administration to adhere to one format as opposed to attempting to combine multiple regional dial plans, which may differ.

All phone numbers with the assigned country code of 1 fall under the authority of the North American Numbering Plan Administration [3]. NANPA further breaks down 10 digit phone numbers by a 3-digit Numbering Plan Area (NPA) commonly referred to as the area code followed by a 7-digit local number. The format of phone numbers that fall within the authority of NANPA is NXX-NXX-XXXX where N is any digit 2-9 and X is any digit 0-9 [3].

C. Define Covert Channel

Although the field of covert channels is in an embryonic stage, there have been multiple proposed definitions for covert channels. In 1973, Butler Lampson introduced the concept of a covert channel and describes it as "[a channel] not intended for information transfer at all." [11]. Gligor reenforced this definition by describing covert channels as, "[a] communication channel that allows a process to transfer information in a manner that violates the system's security policy." [8]. Covert channels have been broken down into three categories: storage, timing, and behavioral-based channels [5]. The channel proposed in this paper can be classified as a storage channel. Millen explains that, "Research in covert channels split up into four disciplines: explaining them, finding them, measuring them, and mitigating them." [13]. Further analysis can be performed on the following three factors: detection, mitigation, measuring. Considering that the proposed channel has been explained, the remaining three categories will be discussed further.

D. Detection and Mitigation

This covert channel can be mitigated and potentially prevented at the network layer where the backbone infrastructure of the PSTN can examine the source phone number of a call. If the number is reserved in accordance with the ITU E.164 recommendations, then the call can be blocked and dropped. However, this can reduce system performance of the PSTN below acceptable levels since every call would be examined for potentially spoofed numbers.

Additionally, it is possible for a transcription of all calls made to or from a mobile device to be obtained from a wireless provider. Excessive calling in a short period of time could raise suspicion.

E. Measuring Throughput and Robustness

When discussing covert channels, it is important to recognize the *throughput* and *robustness* of the channel. Throughput is defined as "the amount of data the channel is able to transmit over a given period of time," [7] and robustness is defined as "the survivability of a given channel." [7].

The channel can send three ASCII characters through the first six digits of the local number. Although there are 127 ASCII values, the printable characters have decimal values between 32 and 127 [4]. This leaves 95 characters that can be sent. Since 95 is only two digits, each character in the secret message will only require two digits. Thus, three characters can be sent with each call. This can be accomplished by taking the ASCII value of the character being sent, subtracting 32, sending the message, and then adding 32 back on the other end to determine the original value. For example, the decimal value for a capital A using ASCII encoding is 65. Subtracting 32 will result in 33. A phone call from the source address of 999-200-3333335 will send "AAA" since the receiving device will add 32 to 33 resulting in 65, which is the original message being sent. Further functionality will be discussed later in this paper.

The formula for encoding the data on the sending device is as follows:

$$M = p - 32$$

where M is the actual message (the digits) being sent and p is the ASCII value of the plaintext character. The receiving device calculates the following formula to determine the original message sent:

$$p = M + 32$$

This covert channel is highly robust since the PSTN is a core part of the world's critical infrastructure, and it is not likely to be removed or shut down.

F. Extensibility

The proposed method of extensibility uses the area code of a phone number as a pre-shared secret codebook to send a command code to the device. This code can represent a command that tells the device what information the sender is looking for. For example, code 200 may tell the device to send data via an HTTP POST request to a web server. The URL of the web server may be a pre-shared secret or it can be conveyed in the data portion of the number. The former can potentially become a single point of failure because if a domain name becomes blacklisted, the phone will not be able to communicate with that server. However, if the domain can be conveyed in a secret message to the phone, this will allow for more flexibility with having a command and control server for relaying data back to.

If a device receives a phone call from a number beginning with a reserved value, it should examine the following digits that may contain a hidden message. This phone call should be intercepted and terminated before being passed to the application that receives calls.

II. General Procedure

The proposed channel will adhere to the standard created by the North American Numbering Plan Administration. This means that following the country code is a three digit Numbering Plan Area (NPA) followed by a seven digit local number. The following example is a general method intending to serve as an outline for potential methods to implement a covert channel based on the Public Switched Telephone Network dial plan. An example phone number for this channel is 999-200-3333335. Upon examining a phone number, three fields initially stick out: the country code (one to three digits), the area code (three digits, according to NANPA's standard), and the local number (seven digits, according to NANPA's standard). This channel breaks up the local number into two parts - the first six digits, and the last digit.

Value	Purpose
999	Country Code
200	Area Code
333333	First six digits of local number
5	Last digit of the local number

This channel uses each of the three fields for a different purpose. The purpose for each is as follows:

- **Country code** - In this channel, the country code serves as the delimiter indicating whether there is a hidden message contained in the digits following. The application residing on the mobile device looks for specified reserved country codes or spare codes. For example, country codes 0 and 999 are both reserved, and codes such as 280, 424, and 890 are all "spare codes." [10]
- **Area code** - The intention of this field is to provide the opportunity for the user to send "command codes" to the mobile device. This will provide a feature for extensibility and create the opportunity to develop a framework for users to develop their own commands.
- **First six digits of the local number** - The first six digits of the local number are used for sending the actual covert message using ASCII encoding.
- **Last digit of the local number** - This value is used in a method similar to the More Fragment IP header.

The country code is used as a delimiter because it will look for phone calls from specified reserved country codes without service as a denial of service to legitimate phone calls (since it would not pass them up to the dialer). The ITU E.164 recommendation can be examined to determine a country code to use.

A. Potential Command Codes

1) Remote Wipe: A remote wipe functionality could have multiple implications. There are currently some commercial solutions available to remotely wipe a device [12], but a remote wipe functionality of this channel could prove to be useful for wiping sensitive data off of a device if it is misplaced or stolen.

2) HTTP POST: The application can be configured to send a POST request to a specific server containing information such as applications installed, a list of contacts, or contents of text messages.

B. "More Fragments"

According to RFC 791 [6], the "More Fragments" (MF) flag in the Internet Protocol header is used to indicate "datagram is not the last fragment." Similar to the MF flag in the IP header, the last digit in the seven digit local number serves to indicate the end of the transmission of a covert message. The value will be a predetermined set of values to allow the sender to inform the receiver when the message is done transmitting. Instead of relying on just one value to indicate whether the message is done or if there is still more to come, there should be multiple values in order to increase the variety of phone numbers calling. This will increase the covertness of the channel since there will be less of a pattern of phone numbers to decrease the detectability. For example, all even numbers could indicate the end of the transmission and all odd numbers could indicate that there are still more parts of the message that the receiver should wait for.

III. Proof of Concept

A. Android Application

An Open Source Android application titled 'Call Code' [14] was originally designed as a tutorial for developers to detect incoming and going calls. By modifying the source code of "Call Code" [14], it was trivial to derive the last seven digits of a incoming caller's number (with the first 6 containing the secret message). The application is given a higher priority for changes to the phone state by declaring a higher integer value for an intent filter in the application's manifest file. An intent is "an abstract description of an operation to be performed," [1] which can include launching applications. This allows the application first access to execution upon any change to the Android phone's state, including incoming and outgoing calls. When a call is detected, the application segments the phone number into "chunks." These "chunks" contain a country code, area code, city code and six unique digits where our ASCII message is derived. After the number is obtained, if it matches a pre-defined reserved country code value of 999, the call is dropped never making it to the phone's dialer application. The use of the reserved country code 999 is made possible through third party services that allow spoofing of phone calls. During testing, the Android application "Mask My Number" [18] was used. The first six of the last seven digits of the incoming number are then segmented into three, two digit values that are converted to their ASCII representation via the method described in the introduction. In the source of the application, a hash table is constructed with numeric values associating with alphabetic characters. If the incoming number contains a pair of digits that do not have a corresponding value in the hash table, they are replaced with a null value. If successful, the character is then written to a file on the external storage of the Android phone.

B. Forensic Analysis

Considering the method described, if forensic analysis of the device is performed, the text file can be discovered - even if it is deleted [9]. Upon examining call logs, the spoofed number is logged; there is no trace of the number of the original caller. This is beneficial because the sender can remain anonymous. However, should the channel be discovered, the information being relayed can be easily discovered if someone performing the forensic analysis is able to aggregate all of the spoofed phone numbers and parse out the digits containing the message.

IV. Future Work

OpenBTS is "an open source software project dedicated to revolutionizing mobile networks by substituting legacy telco protocols, and traditionally complex, proprietary hardware systems with Internet Protocol and a flexible software architecture." [16]. Potential future work includes determining whether spoofed phone numbers are logged at the base station as the actual originating source number or whether they are logged as the spoofed number. As noted previously there are pros and cons for both options. If the legitimate number is logged, there will be a lot of short phone calls logged between the two devices, which may raise suspicion. However, if the spoofed phone number is logged, it would be possible for someone with access to the logs to reconstruct the message if the person is able to determine the encoding scheme being used. A spoofed phone number may also stick out more if there are logs that say there is a number that has an unused country code (such as 999). By simulating a base station utilizing the OpenBTS software, it would be possible to test this.

Another method which could potentially send more information to a mobile device would be to treat the listening application as a call center application. This would allow a caller to send a message by pressing buttons similar to pressing buttons at a menu before waiting to speak with a representative for a company. This would allow an established connection to be able to send more data at a single point in time. However, a drawback of this is that it would most likely cause a denial of service to the phone since it would not be able to receive phone calls while that application is listening and connected with another caller.

V. Conclusion

This paper examines the North American Numbering Plan Administration's dial plan format and proposes a covert channel based on the source phone number of a call. Although the NANPA standard is used in this example, the covert channel can be extended to use dial plan formats of other regions. By waiting for a phone call from a number with a specified value in the country code as the delimiter to indicate the start of a message, an application listening on the receiving device can parse the number of the incoming call and determine the corresponding ASCII characters for the expected message.

References

[1] Intent. Online. [Online. http://developer.android.com/reference/android/content/Intent.html].

[2] Truth in caller id act of 2009. Online. [Online. http://www.gpo.gov/fdsys/pkg/BILLS-111s30enr/pdf/BILLS-111s30enr.pdf].

[3] North American Numbering Plan Administration. About the North American Numbering Plan, 2014. [Online. Accessed 20-October-2014].

[4] American Standards Association. *American Standard Code for Information Interchange*, June 1963. [Online. Accessed 19-October-2014].

[5] Daryl Johnson, Bo Yuan, Peter Lutz. Behavior-Based Covert Channel in Cyberspace. pages 311–318, June 2009.

[6] Defense Advanced Research Projects Agency Information Processing Techniques Office, 1400 Wilson Boulevard Arlington, VA 22209. *RFC 791 - Internet Protocol - DARPA Internet Program Protocol Specification*, September 1981.

[7] Erik Brown, Bo Yuan, Daryl Johnson, Peter Lutz. Covert channels in the HTTP network protocol: Channel characterization and detecting Man-in-the-Middle attacks. In *The Proceedings of the 5th International Conference on Information Warfare and Security*. The Air Force Institute of Technology, Academic Conferences Limited, April 2010.

[8] Virgil D Gligor. *A guide to understanding covert channel analysis of trusted systems*. The Center, 1994.

[9] Jaromir Horejsi. Android forensics, part 1: How we recovered (supposedly) erased data. https://blog.avast.com/2014/07/09/android-foreniscs-pt-2-how-we-recovered-erased-data/, 2014.

[10] International Telecommunication Union. List of ITU-T Recommendation E.164 Assigned Country Codes, November 2011. [Online. Accessed 13-October-2014].

[11] Butler W. Lampson. A note on the confinement problem. *Commun. ACM*, 16(10):613–615, October 1973.

[12] McAfee. *Security for Military-Grade Google Android Devices*. [Online. http://www.mcafee.com/us/resources/solution-briefs/sb-security-military-grade-android.pdf].

[13] Jonathan Millen. 20 Years of Covert Channel Modeling and Analysis. Computer Science Laboratory, SRI International, May 1999.

[14] Andrew Moskvichev. Detecting incoming and outgoing phone calls on android. Online, March 2013. [Online. http://www.codeproject.com/Articles/548416/Detecting-incoming-and-outgoing-phone-calls-on-And].

[15] Harry Newton. *Newton's Telecom Dictionary*, page 578. Flatiron Publishing, March 1998.

[16] OpenBTS.org. A platform for innovation. Online. [Online. http://openbts.org/].

[17] Kevin Wallace. *Implementing Cisco Unified Communications Voice over IP and QoS (Cvoice) Foundation Learning Guide: (CCNP Voice CVoice 642-437), 4th Edition*, chapter 4. Cisco Press, May 2011.

[18] Zantive. Mask my number. Online. [Online. https://play.google.com/store/apps/details?id=app.maskmynumber.com&hl=en].