

Rapid Release Report

Unauthorized Remote Access, Privacy Leak, Call Interception and Eavesdropping

Google Voice, Beta

30-Mar-2009, v1.0

A [Secure Science Corporation](#) Preliminary Security Review

In Partnership with:

[SpoofCard.com](#)

Jay Beale, [InGuardians.com](#)

J.A. Simmons V, [RedKeep.com](#)

**Secure Science Corporation
7770 Regents Rd.
Suite 113-535
San Diego, CA 92122**

**(877) 570-0455
<http://www.securescience.net/>**

Table of Contents

Rapid Release Report	1
1 Rapid Release Report.....	3
1.1 Findings	3
1.2 Exploit Method	3
1.2.1 Privacy Leak	4
1.2.2 Unauthorized Remote Access	5
1.2.3 Incoming Call Interception	5
1.2.4 Incoming Call Snooping	6
1.3 Risks	6
1.4 Next Actions	6

1 Rapid Release Report

Multiple Secure Science Corporation Clients¹ posed interest in using the Google Voice system for business purposes and had requested our professional opinion regarding the product as it stands today. SSC's External Threat Assessment Team (ETAT) along with assistance from [SpoofCard.com](#)², [InGuardians](#)³, and [RedKeep](#)⁴ underwent a preliminary glance at the existing setup of [Google Voice](#) (Beta), formerly <http://www.grandcentral.com>. Uncovered was trivial (and likely known) access to Google Voice Subscribers' Dial-in Interactive Voice Response (IVR) system, which maintains settings for Voicemail⁵, Initiated Outbound Calls⁶, Goog-411, and Temporary Settings, such as enabling "Do-Not-Disturb" and Temporary Forwarding Numbers.

Initially it was thought to be unlikely that a successful attack could be widespread, being that the attacker would require knowledge of the mobile number connected to the Google Voice (GV) account. According to GV's "[Securing your privacy](#)" help page, one of the specific designs of GV phone numbers was to secure your privacy by hiding your "phone locations" from your callers. Thus in essence, there shouldn't be a situation where your mobile phone number is revealed. An application flaw within the SMS system can enable an attacker to take advantage of a privacy leak that will divulge mobile numbers directly connected to GV numbers.

1.1 Findings

A multi-step process equips an attacker with the capabilities of remotely exploiting GV subscribers:

- ✓ Enumeration of private Mobile Numbers connected to GV (privacy leak)
 - GV to GV initiated SMS can reveal mobile phone associated (MPA) with GV subscriber
- ✓ Unauthorized remote access
 - Dialing the GV target number with spoofed MPA forwards directly to GV IVR settings⁷
 - Access to Voicemail (options and messages), Outbound Calls, and Temporary Settings
- ✓ Incoming Call Interception
 - Temporary Forwarding Numbers (TFN) can be added by attacker within IVR
 - Additionally, attackers' TFN number will receive GV subscribers' calls
- ✓ Incoming Call Snooping
 - "Switching phones" feature enables monitoring⁸ of received calls

1.2 Exploit Method

Recently it was discovered that SIP devices could be used to spoof a phone number attached to a GV number, giving the spoofed number access to greetings and voicemail⁹. According to the headline, it was also very obvious that one could spoof a number by setting the "Caller-ID"¹⁰ (CPN) of a PBX extension (such as [asterisk](#), a free PBX) to a mobile number attached to the GV subscriber, essentially gaining the exact same access to the voicemail settings, and outbound calls¹¹.

SSC safely makes the assumption that the reason a pin request was not required by default for **all** types of communication into the IVR is that the difficulty of obtaining a known mobile number of a GV subscriber required significant effort¹². In the case of GV, the private mobile number is acting analogous to a secret key, and the GV number is behaving similarly like a public key.

¹ Identities will remain anonymous

² Provided complimentary access to SpoofCard CPN Spoofing services and research attribution

³ Testing & research

⁴ Testing & research

⁵ Includes new voicemail message access

⁶ Both US and International

⁷ When IVR reached by GV connected mobile number, pin number is not requested by default

⁸ Also known as "eavesdropping" or "wiretapping"

⁹ <http://it.slashdot.org/article.pl?sid=09/03/25/2219231>

¹⁰ Calling Party Number (CPN)

¹¹ Secure Science has issued [advisories](#) introducing similar problems in 2004

¹² Specifically targeted pretext attacks are not usually scalable with voice communication

1.2.1 Privacy Leak

A very favorable feature with Google Voice is the ability to send and receive SMS. If you have a mobile phone attached to a GV number, the received SMS message will forward to your mobile phones:

Quote from Google's '[SMS Forwarding Basics](#)'

Anyone can send a text message to your Google number and the message will be forwarded only to the phones you've marked as **Mobile** in the **Phone Type** section of your **Phones** tab.

If you reply to the message, your replies display your Google number as the caller ID and the whole conversation is stored and searchable from your inbox.

The SMS messages that are sent to your Google number will also be displayed on the website. You can reply to the SMS from the Web as well.

This effect is produced by a SMS bridge using the "406" area code.

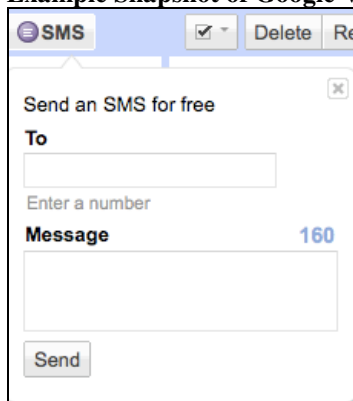
Quote from Google's '[Receiving SMS on phone from 406 numbers](#)'

When you send an SMS through Google Voice, the SMS appears to be sent from your Google number. When someone sends an SMS to your Google number, and it's forwarded to your mobile phone, it won't appear as from the sender's actual number (e.g., the SMS may appear from 1-406-xxx-xxxx). This is so that when you reply to the 1-406-xxx-xxxx number from your phone, the SMS you send appears to be sent from your Google number and will be saved in your Google Voice inbox.

Essentially this feature is to protect your originating private mobile number from being revealed and maintains state with Google Voice.

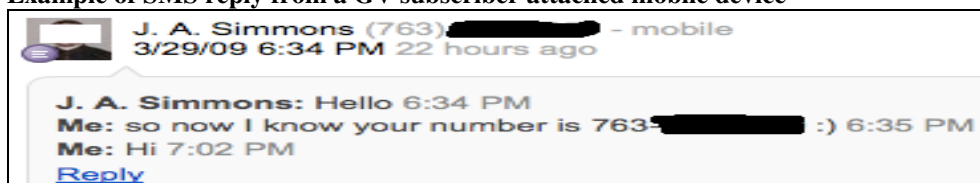
Google Voice subscribers can also initiate (or reply) to SMS messages within your browser via the "SMS button".

Example Snapshot of Google Voice '[SMS Button](#)'



When sending with the "SMS Button", the GV subscribers' number will appear to the mobile recipient. They can reply as normal from their mobile phone. Unfortunately, GV does not distinguish between a mobile device and another GV number. When sending a web-initiated SMS message to another GV subscriber that has an attached mobile device, the "406" bridge is not present. Thus the reply the initiator receives will contain the private mobile number.

Example of SMS reply from a GV subscriber attached mobile device



A malicious attacker can target GV subscribers using this method to successfully enumerate attached mobile numbers. This privacy leak is the first step for gaining full-privileged access to the targets' Interactive Voice Response (IVR) settings.

1.2.2 Unauthorized Remote Access

It is starting to become common knowledge amongst security researchers that Calling Party Number (CPN) verification alone cannot be used to validate credentials within phone systems. Ever since the onset of personal VOIP systems and open-source PBX systems such as asterisk, it has been trivial to fake the CPN and disguise your calls. This technique is not limited to tech-savvy VOIP users, but is now available by an online service known as SpooferCard.com. SpooferCard.com assisted our researchers with testing by providing us an account so that we may not only spoof, but also record the calls in an effort to log our results.

Along with concealing calls, CPN spoofing can bypass authentication methods previously thought to be secure by the phone providers¹³. Known examples of exploitable voicemail IVR systems are AT&T and T-Mobile wireless telecommunication providers. By merely spoofing the mobile number of the voicemail subscriber, the default system will permit access without requesting any form of authentication. The reason this occurs is that the IVR's default security model is to trust the incoming mobile device and provide the convenience of readily accessing the mobile voicemail account. We'd like to point out that Verizon Wireless and Sprint request a PIN be entered in by default, and so far no complaints from customers have been publicly made about this specific and consistent request when they access their voicemail from their mobile device.

With the above section (1.2.1) it was demonstrated that enumeration of GV attached private mobile numbers (PMN) could be ascertained. By spoofing the acquired PMN to the targets' GV public number, the default mechanism enables access to the IVR system without any further authentication requests¹⁴. Some of the highlighted settings that are of concern are:

- ✓ Voicemail Access
 - New messages, PIN Code modification, and Greetings
- ✓ Outbound Dialing
 - US and International¹⁵ calls
- ✓ Temporary Settings
 - Temporary Forward Number (TFN)
 - Do-Not-Disturb¹⁶

1.2.3 Incoming Call Interception

While an attacker has access to the IVR "Main settings" menu, a specific feature becomes apparent within the "Temporary Settings" menu:

"Temporary call Forwarding"

If you're heading to the mountains for the weekend and want Google Voice to forward your calls to your cabin, you can add a temporary number to Google Voice. Here's how:

1. Call your Google number. Press the * key and enter your PIN if you're not calling from one of your forwarding phones that connects directly to your voicemail and account system.
2. Press 4 to access the main settings menu.
3. Press 4 again to access your temporary settings.
4. Press 2 to set a temporary number to forward your calls to. You'll have the option to add the number you're calling from or any other number. Keep in mind that you can't select a number you already have on your Google Voice settings as a temporary number to receive calls.

¹³ Prior to VOIP technology

¹⁴ It is possible to turn this feature off and we recommend off should be the default setting

¹⁵ Revenue leakage occurs if pre-paid credits are available

¹⁶ Send all calls to voicemail (essentially a Denial-of-Service)

A malicious attacker can add a destination phone number to the targets' GV account¹⁷ enabling incoming call interception¹⁸ and passive incoming call log analysis¹⁹. Additionally, all other attached phone numbers will ring simultaneously so the target will not be readily aware of any changes made to the account.

1.2.4 Incoming Call Snooping

Another choice aspect of Google Voice is the “switching phones” feature:

Switching phones during an incoming call

To switch phones in the middle of an incoming call, just press * while you're talking, and your other phones will ring. Then, for example, you can pick up the call from your mobile phone (if you're about to head out), or from your desk. There are no passcodes or PINs to enter and, best of all, your caller won't even hear the switch.

This feature enables an attacker to intercept²⁰ and resend a parallel call channel to the GV target all while maintaining a continuous open-line. The target is likely unaware of the 3rd party, and the only caveat is that the resending of the call causes the phone devices to display the CPN of the targets' GV number²¹.

1.3 Risks

This new attack vector has the following potential risks:

- ✓ Denial of Service
 - Automated answer supervision²² performed by the attacker can lead to loss of service against GV subscribers
 - Unauthorized Do-Not-Disturb modification can lead to denial of anticipated direct communications²³
- ✓ Unauthorized Remote Access
 - CPN Spoofing bypasses authentication within GV subscribers IVR settings
 - Permits remote modification of critical settings
- ✓ Electronic Intelligence Gathering
 - Interception of Voicemail
 - Interception and monitoring of incoming voice calls
 - Passive monitoring of incoming call logs

1.4 Next Actions

Secure Science Corporation suggests two primary actions to take that will remedy the vulnerabilities outlined within this report.

- ✓ Strict Requirement of PIN code for IVR login
- ✓ In-network SMS recognition
 - Initiate “406” bridge for SMS device forwarding

CPN verification is not a valid method for authentication and Secure Science encourages strict PIN code use no matter what type of device calls into the Google Voice IVR. When initiating SMS from the browser session, GV should recognize in-network subscribers and offer the “406” bridge when forwarding to an attached device.

¹⁷ Tests show that one destination phone number can be added to multiple GV accounts

¹⁸ Denial of Service and Incoming call hijacking

¹⁹ Identification of incoming callers

²⁰ Upon pickup, all other devices cease ringing

²¹ This is similar to the warning message within a SSL/TLS cert when a Man-in-the-Middle attack occurs, usually going unnoticed

²² http://en.wikipedia.org/wiki/Answer_supervision

²³ Unacceptable for excepted business calls