

# **Google Voice Unauthorized Remote Access, Privacy Leak, Call Interception and Eavesdropping**

**SSC  
Rapid Release Report (3R™)  
Preliminary Security Review v1.0  
30-Mar-2009**

**Secure Science Corporation**

In Partnership with:

Jay Beale, [InGuardians.com](http://InGuardians.com)

J.A. Simmons V, [RedKeep.com](http://RedKeep.com)

TelTech systems, [SpoofCard.com](http://SpoofCard.com)

# *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 (3R™)

Google Voice (GV) is the latest offering in Unified Communications from Google. The service features a collective of telephony objectives including the consolidation of multiple phone contact numbers, simplified voicemail features (modeled after a principle email user format) and additional selections such as voicemail sharing, SMS, block calls, screening and preview options.

This technology originates from Google's purchase of UC provider [Grandcentral.com](http://Grandcentral.com) in 2007. As an ideal communication management tool for utilization within corporate/business infrastructures, a broadening interest in GV has developed amongst SSC clientele. In response to numerous requests for a comprehensive security and compliance review of Voice in its current stage, ETAT<sup>1</sup> initiated layered analysis of the technology in partnership with [SpoonCard.com](http://SpoonCard.com), [InGuardians](http://InGuardians), and [RedKeep](http://RedKeep).

Preliminary examination of GV revealed several considerable flaws significant to the functionality of the service as a whole. The axis for these major vulnerabilities stem from a single known exploit concept first (publicly) identified<sup>2</sup> in a general advisory posted in 2004. Google maintains a premise of overall safety based on the commonly accepted, yet controversial theory of "security by obscurity". According to GV's "[Securing your privacy](#)" help page, a specific design virtue highlights the security of user privacy by cloaking "phone locations" from callers. Despite this promise, Voice calls are easily hijacked through the attainment of readily available tools and services which allow these exploits to occur. In order to execute and take advantage of the outlined flaws inherent within GV (1.1 Findings), a progressive skill set is not essential. Much like spamming, the tools required to compromise this system are readily available online for all who choose to obtain them. These congenital inconsistencies generate a particularly high level of concern for current and potential users.

## 1.1 Findings

A multi-step process equips attackers with the capabilities to remotely exploit 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 Interactive Voice Response (IVR) settings
  - When IVR is reached by GV connected mobile number, pin number is not requested by default
  - 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 subscribers' calls
- ✓ Incoming Call Snooping
  - "Switching phones" feature enables monitoring of received calls (also known as "eavesdropping")

## 1.2 Exploit Method

A recent posting revealed the manner in which SIP devices could be adapted in an effort to spoof phone numbers affixed to a GV number. This equips the spoofed request with the ability to access user greetings and voicemail<sup>3</sup>. The desired execution manifests by setting the "Calling Party Number" (CPN)<sup>4</sup> of a PBX extension (i.e. [asterisk](#), a free PBX) to a mobile number associated with the Voice subscriber, consequently gaining identical access to the voicemail settings and outbound calls.

Specifically targeted pretext attacks are not typically scalable with voice communication. Therefore, it is safe to presume that as a result of this reasoning a pin request is not required by default for all IVR communication

---

<sup>1</sup> External Threat Assessment Team, division of Secure Science Corporation

<sup>2</sup> SSC Advisory [TSA-051](#)

<sup>3</sup> <http://it.slashdot.org/article.pl?sid=09/03/25/2219231>

<sup>4</sup> Caller ID

modalities for this reason. With respect to Voice, the private mobile number is analogous to a secret key. The (GV) number behaves similar to a public key. In consideration of this, malicious attackers targeting subscribers may appropriate the process in an effort to successfully enumerate associated mobile numbers. This privacy leak is the primary entry point required in order to gain replete admission into the targets' IVR settings. Admittance into subscribers' Dial-in IVR system encompasses the structures maintaining Voicemail (including new voicemail message access), Initiated Outbound Calls (US and International), Goog-411 and Temporary Settings (allowing "Do-Not-Disturb" and Temporary Forwarding Numbers).

## 1.2.1 Privacy Leak

GV features the ability to send and receive SMS. If a subscriber has a mobile phone attached to a Voice number, the received SMS message will forward to the users' mobile phones:

### Excerpt 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.

The effect is produced by an SMS bridge appointed to a "406" area code.

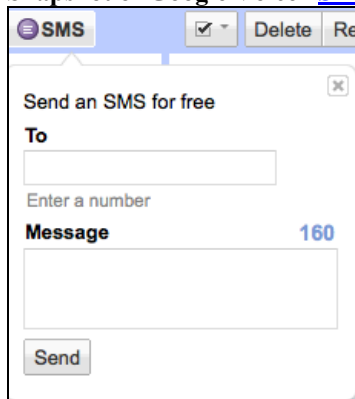
### From Google's ['Receiving SMS on phone from 406 numbers'](#)

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.

This feature protects the originating private mobile number from being revealed by GV.

Subscribers can initiate (or reply to) SMS messages within the browser via the "SMS button".

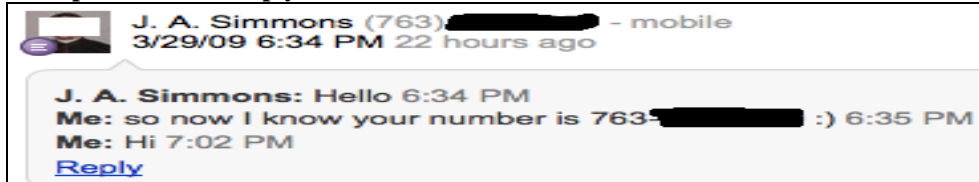
### Snapshot of Google Voice ["SMS Button"](#)



The screenshot shows a web interface for sending an SMS. At the top, there is a blue header with the text "SMS" and a checkmark icon, followed by "Delete" and "Re" buttons. Below the header is a form titled "Send an SMS for free" with a close button (X) in the top right corner. The form has a "To" field with the placeholder text "Enter a number" and a "Message" field with a character count of "160". A "Send" button is located at the bottom left of the form.

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

### Example of an SMS reply from a GV subscriber attached mobile device



## 1.2.2 Unauthorized Remote Access

CPN verification alone cannot be used to validate credentials within phone systems. Since the onset of both personal VOIP and open-source PBX systems such as asterisk, it has been commonplace to fake the CPN and disguise calls. This technique is not limited to tech-savvy VOIP users as it is now available via an online service; [SpooferCard.com](http://SpooferCard.com). SpooferCard.com assisted researchers with testing by providing an account to execute the spoof, also allowing the recording of calls for entry into the logs.

CPN spoofing allows attackers to conceal the source of calls and also bypass authentication methods previously thought secure by phone providers<sup>5</sup>. Historic cases of vulnerable IVR voicemail systems implicate wireless telecommunication providers AT&T and T-Mobile. By spoofing the mobile number of the voicemail subscriber, the default system grants access without requesting any form of authentication. This occurs since the IVR's default security model is to trust the incoming mobile device and provide readily accessible voicemail entry. Verizon Wireless and Sprint request that a PIN be entered by default, in kind providing appropriate user protection and relatively convenient account access.

The preceding section (1.2.1) validates how the enumeration of GV attached private mobile numbers (PMN) affiliated with Voice can be ascertained. By spoofing the acquired PMN to the targets' public GV number, the default mechanism provides access to the IVR system with no additional authentication requests.

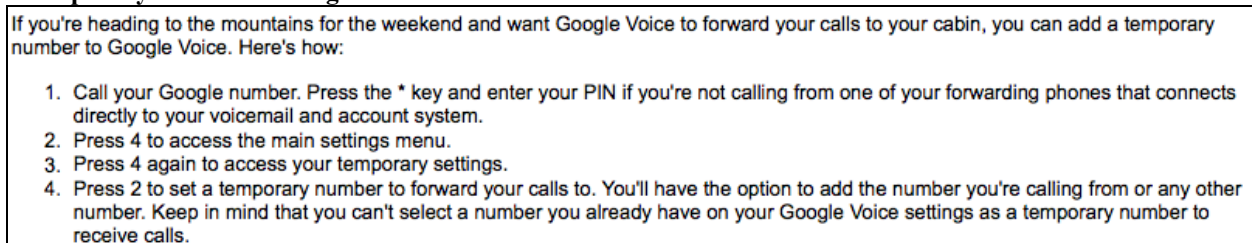
Acute setting defects include:

- ✓ Voicemail Access
  - New messages, PIN Code modification, and Greetings
- ✓ Outbound Dialing
  - US and International calls (revenue leakage occurs if pre-paid credits are available)
- ✓ Temporary Settings
  - Temporary Forward Number (TFN)
  - Do-Not-Disturb (send all calls to voicemail/Denial-of-Service)

## 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"



<sup>5</sup> Prior to VOIP technology

Malicious attackers simply need to add a destination phone number to the targets' account. Testing indicates that one destination number can be added to multiple accounts. This action permits the interception of incoming calls (denial of service, incoming call hijacking) as well as passive incoming call log analysis/identification of incoming callers. All other attached phone numbers will ring simultaneously. The target will not be readily aware of any changes made to the account.

## 1.2.4 Incoming Call Snooping

Another aspect of GV 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 attribute empowers attackers to intercept and resend a parallel call channel to the target while maintaining a continuous open line. Upon pickup, all other devices cease ringing. As a result, the target is unaware of the 3<sup>rd</sup> party. A potential but unlikely caveat for the attackers occurs when the call is resent; the phone devices will display the CPN of the targets' number. This is similar to the warning message within an SSL/TLS certificate when "Man-in-the-Middle" attacks occur, usually going unnoticed.

## 1.3 Risks

The attack vector contains the following potential risks:

- ✓ Denial of Service
  - Automated answer supervision<sup>6</sup> performed by the attacker can lead to loss of service against GV subscribers
  - Unauthorized Do-Not-Disturb modification may lead to denial of anticipated direct communications (unacceptable for business calls)
- ✓ Unauthorized Remote Access
  - CPN Spoofing bypasses authentication within 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

CPN verification is not a valid method for authentication. Strict PIN code use is encouraged no matter which type of device calls into the 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.

Preliminary steps necessary to remedy the identified vulnerabilities:

- ✓ Strict Requirement of PIN code for IVR login
  - Change IVR mobile CPN authentication default setting to off
- ✓ In-network SMS recognition
  - Initiate "406" bridge for SMS device forwarding

Prior to release of this publication, Google/GV was notified of all vulnerabilities outlined herein. A complete repair of these flaws has since been reported.

---

<sup>6</sup> [http://en.wikipedia.org/wiki/Answer\\_supervision](http://en.wikipedia.org/wiki/Answer_supervision)