

# Chatter Bug: VoIP Solution with a Problem



**Chatter Bug™**  
Personal Long Distance  
Patent Pending

**\$9.95** /Month

Introducing ...



**Chatter Bug™**  
Patent Pending

**AS SEEN ON TV**

- ❖ Economical
- ❖ Convenient
- ❖ Full Service Features

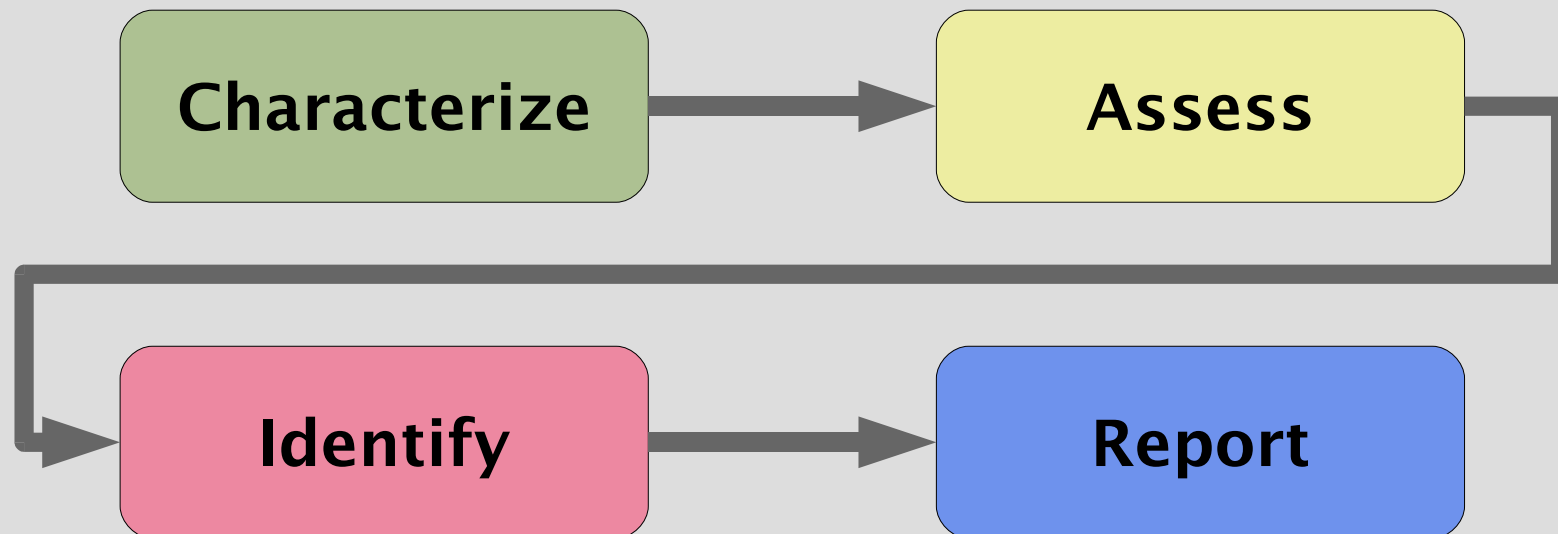
*The latest revolution in communications!*

dual\_parallel  
November 2006  
Phoenix 2600 Meeting



# Objectives

- Characterize the Chatter Bug
- Assess its functions
- Identify any vulnerabilities
- Report findings



# Chatter Bug Overview

- A plug- n- play, retail VoIP solution for those with a PSTN connection
- Lagunawave, Inc. in Tucson
- \$24.95 on the web, ~\$20 at Kmart
- \$9.95/ month unlimited toll calling in US and Canada



# Registration

- Toll-free at 866-690-3919, M-F 7-7 and Sat 8-5
- Requisites
  - Name, address, phone number, email
  - Credit card
  - Serial number
  - Minimum five-character password
- Login is email or phone number and password



# How does it work?

- Purchase
- Register
- Plug it in
- Dial your party
- Call is connected
- Credit card is billed monthly
- Wait, did you hear that?



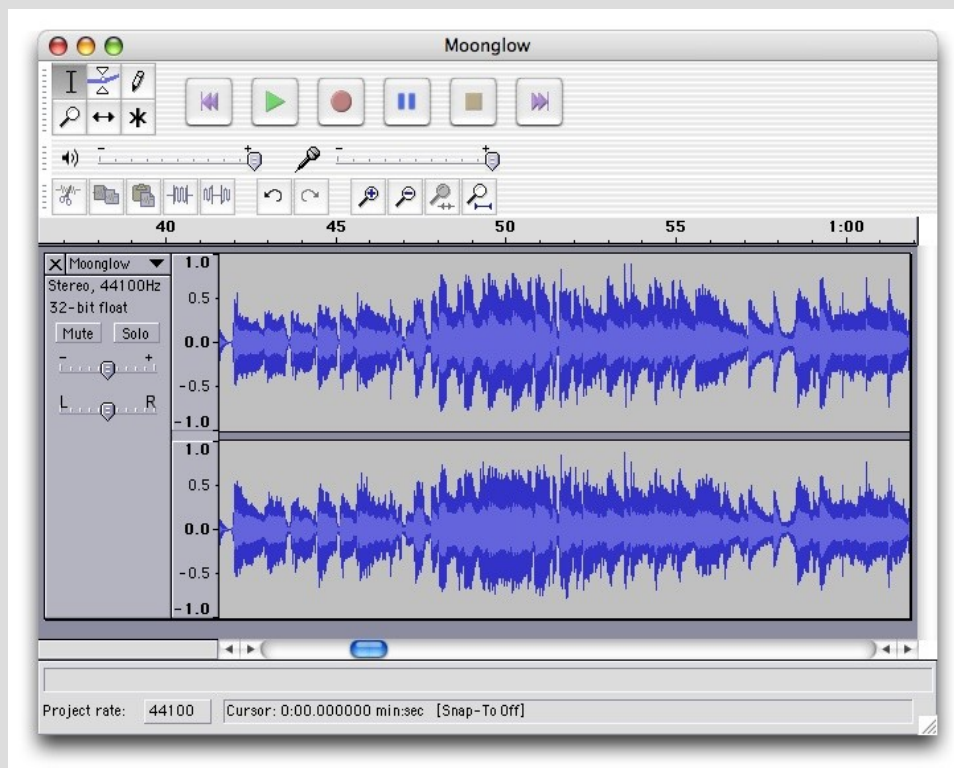
# How does it really work?

- <http://www.chatterbug.com/faqs.do#47>
- “The tones will be repeated in your ear very softly...”
- Can hear faint dial tone and DTMF
- Carrier Access Code (CAC)?
- Extender?



# New- meets- Old Solution

- Audacity, which pwns
- Pager, which is handier than you might think



# Digit Analyzer

- First, Chatter Bug checks for 1
  - If 1, then check next three digits (NPA)
- If not toll-free or pay-per-call, then...
- Dial Lagunawave access number
- Replay captured digits
- Capture and replay remaining digits
- Pound completes dialing or disconnects
- If toll-free, release line at timeout
- CACs, like 101-0288, do not work



# What does it dial?

- 800- 381 - 3967
- Lagunawave's extender
- Then simply the number dialed and #
- That's it, no access code, no serial number...
- The hardware does nothing.
- In fact, it adds vulnerability.



# Spoof Charge Number

- Lagunawave verifies Charge Number (CN)
- Spoofing CPN/ CID does not work
- Spoofing Charge Number by greyarea
- If you can spoof CN, you don't need Chatter Bug.

The logo for Telespoof, featuring a stylized 'i' composed of four orange squares stacked vertically, followed by the word 'telespoof' in a lowercase, orange, sans-serif font.



# Leverage Hardware

- Obtain a, sequential, serial number
- Set up from and for a pay phone
- With prepaid credit card and fake info
- Lost sale of \$20 unit
- Unlimited anonymous toll calling



# Mitigation

- Use non-sequential serial numbers
- Obscure the serial number
- Activation at retail outlets
- Or better yet...
- \$5 “calling” card
  - Environmentally friendly
  - Larger market



**SELL PHONE CARDS  
FOR USE IN 190 COUNTRIES**

ONE ACCESS NUMBER. ONE PIN  
SMS TRIGGER. WEB TRIGGER.  
CALLER ID TRIGGER

10-DAY FREE TRIAL

The advertisement features a man in a suit looking at a laptop. The background is a blurred city street at night.



# Conclusions

- Wish there was more to it
- Leet
  - Easy to use
  - Reasonable rate
  - It's a great idea that works well.
- Noob
  - Breaks CACs
  - Waste of \$20
  - Vulnerable serial numbers
- Thanks!



# Addendum

- Natas asked if it's possible to place multiple calls simultaneously using Chatter Bug's extender from a single CN. I placed a three-way call and affirmed his hypothesis.
- I also found that you can divert to 8s with Chatter Bug's extender. 305-000-0000 or 305-728-6200 is passed, revealing that Lagunawave uses VarPhonex as its provider.

