Chatter Bug: VoIP Solution with a Problem
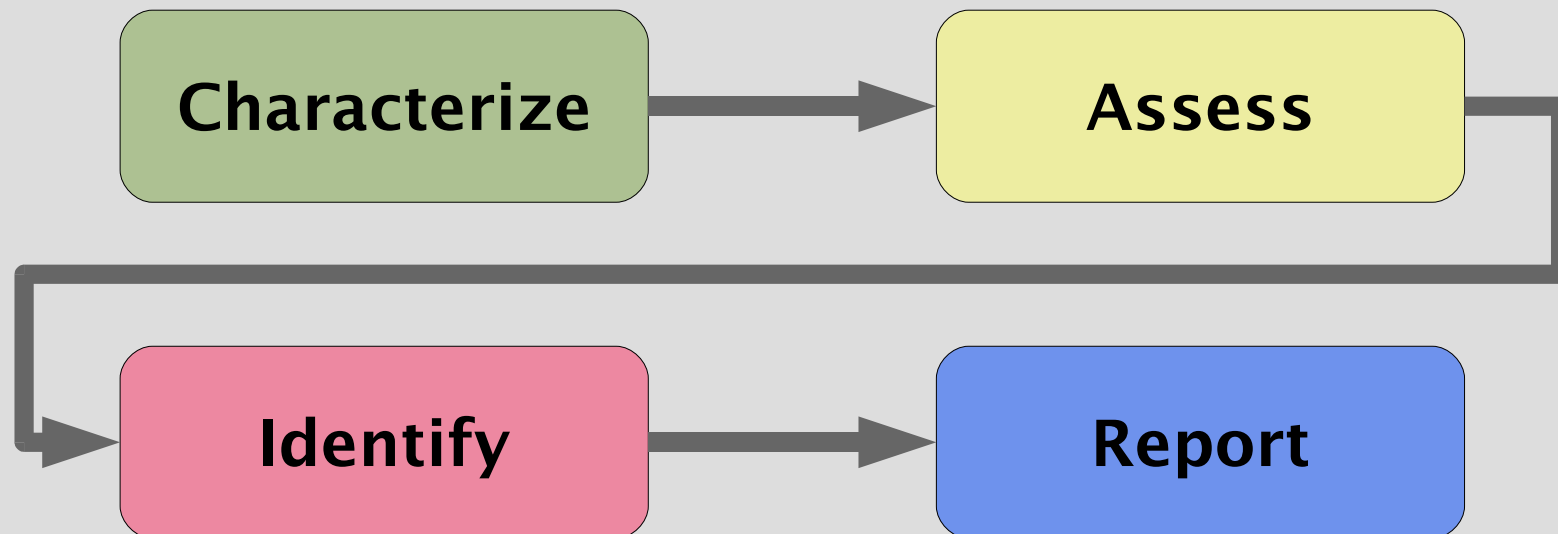

dual_parallel
November 2006
Phoenix 2600 Meeting

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
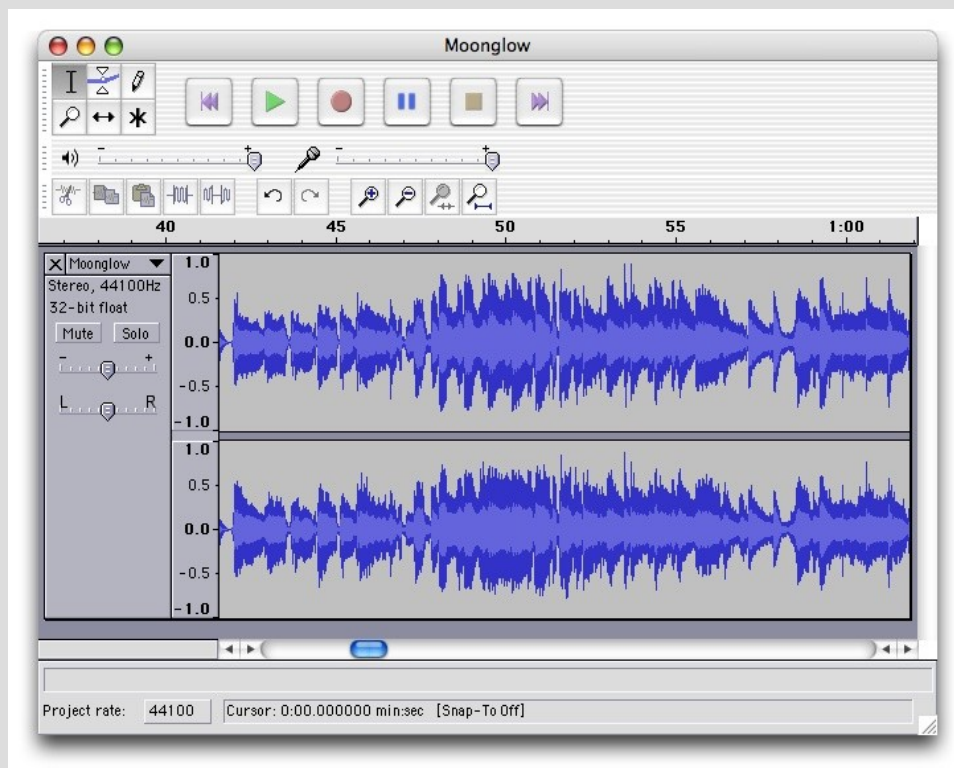- Wait, did you hear that?

?

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 <u>nothing</u>.
- 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.

Telespoof

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

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!

Chatter Bug™

Patent Pending

http://www.dualisanoob.com/