



# “Vishing”

Slade Griffin

Sword and Shield Enterprise Security

**Sword & Shield**  
ENTERPRISE SECURITY

# Vishing

- What is it?

- New threat vector. People have become attuned to standard phishing techniques, this method adds a “twist.” No more clicking an obfuscated link, now your “bank” calls you.

- How does it work?

- Compromise 1 internet facing host.

- How difficult is it?

- Fast, simple, and effective.

# What is needed?

- Access to one internet facing computer.
  - Method of compromise is inconsequential.
  - Software is available for Linux, MacOSX and Windows.
- Intermediate networking knowledge.
- A phone number
  - SIP to PSTN (Public Switched Telephone Network) converter.
    - ( e.g. Sipura SPA-1000)
  - ITSP (Internet Telephony Service Provider)
    - <http://www.voip-info.org/wiki/>
- The ability to record the call
  - This functionality is built into most digital PBX software.

# Required Software

- Any digital Private Branch Exchange (PBX)
  - The PBX software allows the compromised machine to accept multiple incoming calls on the same phone number.



# Attack Framework

- Identify one host computer that faces the internet.
  - Although the method of compromise is inconsequential the attacker must be able to install and run software. If the compromise does not result in Administrator, Root, or System level access, privilege escalation would also be needed.

# Attack Framework (2)

- Install your VoIP/PBX software
  - Several programs exist that are both commercial and open source. Examples include:
    - Asterisk <http://www.asterisk.org/>
      - Trixbox is a packaged OS for Asterisk - <http://www.trixbox.org/>
        - Asterisk is an Open Source hybrid TDM and packet voice PBX and IVR platform with ACD functionality. Moreover, Asterisk is quite possibly most powerful, flexible, and extensible. Its name comes from the asterisk symbol, \*, which in UNIX (including Linux) and DOS environments represents a wildcard, matching any filename. Similarly, Asterisk the PBX is designed to interface any piece of telephony hardware or software with any telephony application, seamlessly and consistently.
    - Skype <http://www.skype.com/>
      - Free version has limited functionality.

# Attack Framework (3)

- Configure your outbound caller ID number.
  - These programs can “spoof” any number.
    - Your local bank.
    - The White House
- Install and configure an SMTP daemon.  
(optional attack vector)
  - Used for the SPAM attack.

# Attack Framework (4)

## ■ Attack Vectors:

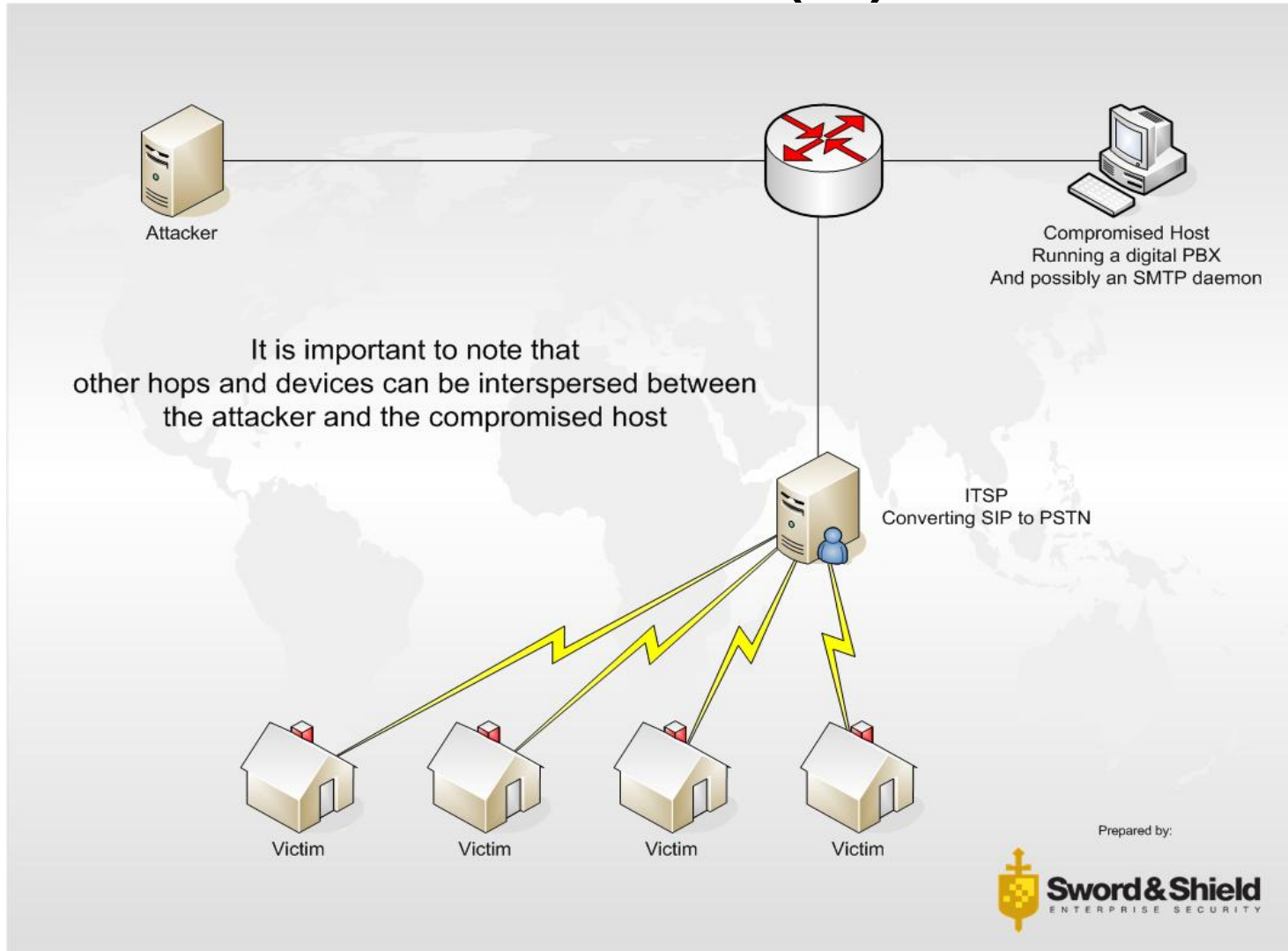
### □ War dialing:

- With this option the attacker configures the VoIP software to dial a pre-set group of phone numbers.
- The Victims receive a scripted phone call that induces them to enter information.
  - Asterisk functionality allows for both incoming and outgoing calls to be recorded, and allows the recordings to be e-mailed upon completion.

### □ Spam attack:

- With this option victims receive a standard phishing type e-mail that can include obfuscated links and a phone number.

# Attack Framework (5)



# Sample e-mail



[Home](#) [About SunTrust](#) [Contact Us](#) [Customer Service](#) [ATM/Branch Locator](#)

## Personal Finance

[Business Banking](#) [Corporate & Institutional](#)

???

Dear  
Thank you for banking online at suntrust.com. Our records indicate that you recently added or made a change to one of your email address(es). This notification is to confirm that you initiated this change.  
If you feel you have received this email in error and did not add or change your email address(es), please [click here](#)  
If you need additional assistance, email us or speak with a SunTrust representative 24 hours a day, 7 days a week at 718-536-0001.  
Sincerely,  
Krista Massey  
Director of Customer Advocacy  
SunTrust Banks, Inc.

# Evolving threat

## ■ What if:

- Attackers began doing better research.
  - Base the phone/spam attack on locality instead of relying on the larger banks.
- Attackers collaborate.
  - If attackers begin sharing data like they do when they find hosts that function as an open proxy or mail relay.

# Asterisk

- It is also important to point out that the software mentioned during the presentation has several valid uses.
  - Road warriors using soft-phones or Wi-Fi handsets while traveling.
  - Open source voicemail and office PBX allowing you to not only control the system but the actual software



# Current events

- <http://www.internetnews.com/security/article.php/3619086>
- [http://www.usatoday.com/tech/news/internetprivacy/2006-07-12-vishing-scam\\_x.htm](http://www.usatoday.com/tech/news/internetprivacy/2006-07-12-vishing-scam_x.htm)
- <http://www.pcmag.com/article2/0,1895,1981797,00.asp>



# Prevention

- User “re-education”



<http://www.sses.net>