A Reality Check on Security in VoIP Communications

Rick Robinson
CISSP ISSAP
IEEE Sr. Member

Agenda

- Background
- Overview of Threats – "Top Ten"
  - With Reality Checks
- Trends
- Actions
- Pearls
- Questions

Background

Historical Communication Threats

- Phone Phreaking
- Toll Fraud
- Eavesdropping

…but the threats are different today…

Why is VoIP Security Important Today?

- Users and Providers
  - Never practiced security before (but don't want to tell anyone)
  - Penalties for Executives are greater (SOX, HIPPA, GLB, etc.)
    - go to jail
  - Result: Fear of the Unknown

- Attackers
  - "Space" now has a lot more bad guys
  - They want Fame, Fortune, Car, Girls, beer, etc.
  - They are bolder – destroy and tell
  - They are organized (e.g. identity and credit card theft)

- "Experts"
  - Make fame, glory, and money over selling fear and uncertainty
    - *The Sky is Falling: 10 Easy ways to Protect you and your Family*
    - Snake-Oil Salesmen

Hype in the Media

CMP

Part of the TechWeb Business Technology Network

networkingpipeline

SEARCH search advanced search Free Newsletter Glossary

NEWS | TRENDS | HANDS ON | BLOG | PRODUCT FINDER | SECURITY | WIRELESS

June 13, 2006

Big Security Flaws Found In Asterix PBX, IAX VoIP Client

NETWORKWORLD

Hype vs. reality in VoIP security

IP telephony threats

Study: Identity theft keeps climbing

By Caroline McCarthy
Staff writer, CNET News.com
Published: March 6, 2007, 10:19 AM PST

c|net NEWS.com

TalkBack E-mail Print del.icio.us Digg this

The rate of identity theft-related fraud has risen sharply since 2003, a report from research firm Gartner suggests.

Gartner's study, released Tuesday, shows that from mid-2005 until mid-2006, about 15 million Americans were victims of fraud that stemmed from identity theft, an increase of more than 50 percent from the estimated 9.9 million in 2003.

January 31st, 2007

Microsoft confirms Vista Speech Recogniti remote execution flaw

Posted by George Ou @ 1:42 pm

MSNBC

Newsweek Hor

New

Stealing Minute

By Benjamin Sutherland
Newsweek International

March 19, 2007 issue - The telephone industry has been in an upheaval ever since upstarts began competing with the big telecoms by sending voice calls over the Internet. Now even big firms use so-called voice over Internet protocol. But VoIP is not as secure as the old-fashioned phone lines—as carriers that rely on the Internet are finding out. They are

abcNEWS

MONEY

All Sections ABC News Home > Money

Miami Man Arrested for Thef of VoIP Calls

Miami Man Arrested for Theft of VoIP Calls; 15 Internet Phone Companies Victimized

Cisco IP phone flaws discovered

By Marguerite Reardon
Staff Writer, CNET News.com
Published: February 21, 2007, 1:59 PM PST

c|net NEWS.com

Trojan horse targets Skype users

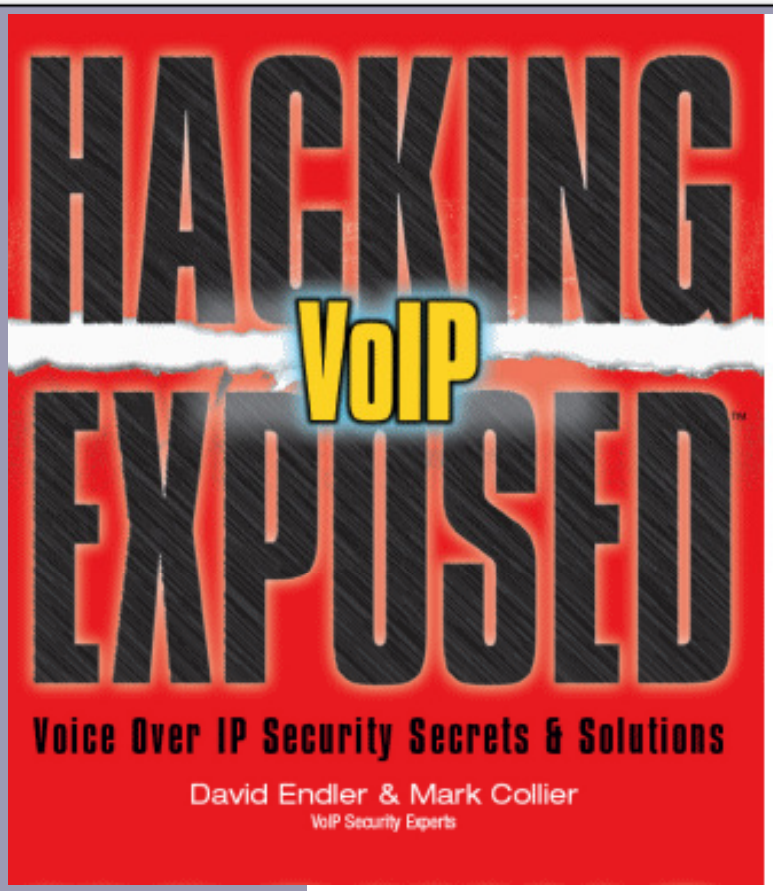
Cisco flaw could invite hackers

By Kevin McLaughlin, CRN 20 June 2006 10:06 AEST

iTnews

Vulnerabilities in Cisco's Call Manager software could open the door for hackers to reconfigure VoIP settings and gain access to individual users' account information, according to researchers at US-based solution provider FishNet Security.

Publications Highlight Fears



- Introduction
- PART I: Casing the Establishment
  - Chapter 1: Footprinting
  - Chapter 2: Scanning
  - Chapter 3: Enumeration
- PART II: Exploiting the VoIP Network
  - Chapter 4: VoIP Network Infrastructure Denial of Service
  - Chapter 5: Network Eavesdropping
  - Chapter 6: Network and Application Interception
- PART III: Exploiting Specific VoIP Platforms
  - Chapter 7: Cisco Call Manager
  - Chapter 8: Avaya Communication Manager
  - Chapter 9: Asterisk
  - Chapter 10: Emerging Softphone Technologies
- PART IV: VoIP Session and Application Hacking
  - Chapter 11: Fuzzing VoIP
  - Chapter 12: Disruption of Service
  - Chapter 13: VoIP Signaling and Media Manipulation
- PART V: Social Threats
  - Chapter 14: SPAMMING/SPIT
  - Chapter 15: VoIP Phishing

Additional VoIP Attack Tools

October 30th, 2006 by mark

David Endler and I posted several new tools on our "Hacking Exposed" website, www.hackingvoip.com. We also provided updates and better README files for some of the existing tools. Here is a quick summary of the new tools:

Overview of Threats

- Signaling Tampering
- Directory Tampering
- Feature and Function Tampering
- SPIT
- RTP Attacks
- Caller ID Spoofing
- Eavesdropping
- - System Robustness / Product Maturity -

Reference: Gary Audin – VoIP Security Threats – The New World, 4-16-07, www.searchvoip.com

Signaling Tampering:1

- Description:
  - Modify contents of data exchanged between source and destination IP devices – by a "Man in the Middle"
    - E.g. Packets too large, small, new elements, old elements, etc.
    - A.K.A "fuzzing"
- Reality:
  - Not *really* a VOIP problem
  - Software Deployment problem
  - Improve robustness of Software with Input Checking
  - Filtering is well-known practice

Signaling Tampering:2

- Description:
  - Act as a call server – man in the middle – and relay signaling data with modifications
    - A.K.A "spoofing"
- Reality:
  - Utilize TCP over SSL/TLS
  - Authenticate your Server (and client)
    - Lesson: Trusted Web Sites
    - Authenticate your data

Signaling Tampering:3

- Description:
  - Process inappropriate data messages
    - Too Many Packets arriving
      - A.K.A. "Flooding"
  - Process out-of-state or unauthenticated messages
    - Process "register, "invite," or "bye" messages from strangers
- Reality:
  - Rate-Filter your Data (Robustness)
  - Utilize TCP over SSL/TLS
  - Authenticate the Data Source
    - Lesson: Trusted Web Servers with Client Authentication

Directory Tampering

- Description:
  - Registration manipulation can erase, add or hijack a phone's registration
  - Calls can be redirected to another phone without the caller's knowledge
- Reality:
  - Ditto Earlier Lessons:
    - TCP over SSL/TLS to Authenticate Clients and Servers
    - Any Database should be Read-Only unless you are an administrator
      - VOIP or otherwise

Feature and Function Tampering

- Description:
  - Features that can be enabled and disabled without authorization from the administrator
  - Incoming and outgoing calls can be blocked by the setting arranged in the call server
  - Applications in the call server can be blocked or enabled improperly

- Reality:
  - Poor Product Design and Implementation – Don't Buy
    - Don't allow administrative functions to be performed by non-administrators
  - TCP over SSL/TLS to Authenticate Clients and Servers

SPIT

- Description:
  - SPam over Internet Telephony
  - "Robs the network of bandwidth, interfere with QoS and overload voicemail systems"
  - "It also takes longer to eliminate SPIT from a voicemail box when the caller is unknown and the listener must hear the call to determine whether it is legitimate"

- Reality:
  - Bandwidth Theft?
  - Call Blocking: It is not just a good idea…
    - Actually Made Easier with VoIP Products
    - Note earlier recommendation on Trusting your Clients (TLS/SSL)
  - Don't Listen to your entire voicemail
    - [OPPORTUNITY Here]

RTP Attacks

- Description:
  - RTP attacks can inject sounds into a phone conversation
  - The speaker does not know of the injected sounds and the listener thinks the sounds are coming from the speaker, not a third device injecting other sounds
    - What if someone is on a conference call or calls home to say he is working late, but the listener hears restaurant or bar sounds instead?
- Realty:
  - In theory, this might make a good special effect for a movie
  - In practice, implement SRTP (readily available)
    - SRTP: Secure Real Time Protocol
    - authenticates RTP packets
    - tamperproof

Check-sync messages

- Description:
  - These can be sent to the endpoints, causing repeated reboots that do not allow the phones to work properly
  - Cisco SIP Phone: NOTIFY:check-sync messages inform phone to upgrade firmware (and config files)

- Reality:
  - TCP over SSL/TLS to Authenticate Clients (UA) and Servers
  - "Don't execute administrative commands from people you don't trust."

Caller-ID Spoofing

- Description:
  - Caller ID is now carried in a data packet that can be generated falsely
  - This can have an adverse effect because attackers can pretend to be valid executive or special phones, IVR or call centers
  - The caller ID simulation cannot be detected by an unknowing caller or called party

- Reality:
  - Carry-over from PSTN (Legitimate)
  - Authenticate your callers
  - TCP over SSL/TLS to Authenticate Clients (UA) and Servers
    - User-based and Authority-based Certificates

Eavesdropping

- Description:
  a) This is easier to perform with IP-based calls than TDM-based calls. Any protocol analyzer can pick and record the calls without being observed by the callers. There are software packages for PCs that will convert digitized voice from standard CODECs into WAV files
  b) The speakerphone function can be turned on remotely, with the caller on mute so that there is no sound coming from the phone. This has happened with some IP phones in executives' offices. Their offices can be listened to without their knowledge
  c) PCs and laptops that have microphones attached or integrated into them can be enabled as listening devices without the user's knowledge. There is a rootkit available for this purpose

Eavesdropping

- Reality:
  a) False:
    - Wires are easier to use than PCs
    - Encrypted RTP is commonplace and it is not just a good idea
      - Thwarts protocol analysis

  b) Feature of phone which can be disabled (auto answer)
    a) Existed in PSTN world
    b) Disable it

  c) Related to VOIP or function of OS?
    a) If your PC is infected with root-kit, GAME OVER (VoIP or not)

- System Robustness / Product Maturity -

- Description:
  - VoIP Components still utilizing more software components and network services than necessary
    - Inherited from Underlying OS or Co-resident applications
    - E.g. Unnecessary Open Ports
  - VoIP components are not implementing or enabling secure protocols
    - Supported Security Features which are not used
  - VoIP message processing is not designed for cloudy-day scenarios

- Reality:
  - Most Enterprise product vulnerabilities are a result of product immaturity
  - Vulnerabilities will decline over time as products mature

Trends

- VoIP and IP Telephony will Continue
  - Driver: Business Integration / Collaboration
  - Driver: Convenience (other stuff on IP)
  - Driver: Global Communications
  - VoIP Communities

- Identity and Authentication:
  - User-based Certificates (x509)
    - Phones, Tokens, etc.
    - Basis for secure identity, privacy, and commerce
  - SSL/TLS as the Security Protocol
    - IPSec/IPv6 may compete
  - [OPPORTUNITY: A "new kind" of phone book]

Trends

- Robustness
  - Product Maturity
    - Design as if somebody's life depended on it
- Scam Artists / Charlatans / "Experts"
  - Continue to sell fear, uncertainty, snake oil, and "their advice"
  - We gave them the opportunity
- VoIP Security Concerns will be addressed and dissipate through improved product maturity and robustness

Actions

Steps you can pursue TODAY:

- Defense in Depth
- Understand solution component interaction
  - (who talks to who)
- Compartmentalize: Utilize ACL's, FWs, & VLANS to restrict communications to only the ports/protocols that are required
  - Use a separate VLAN for Administration
- Understand your vendor's security integration
- Understand your vendor's vulnerability classification, response and remediation policy
- Keep software components current
- Sign-up to be notified of any security vulnerabilities of your products
  - Stay engaged with your vendor's security group – "know" them
- Keep up to date on the topic at hand

Pearls

- Know the difference between *design/feature flaws* and *development bugs* which raise security issues
- Most Vulnerabilities Never Get Exploited
- Most worms and viruses attack old vulnerabilities
- Fear sells Security. Use knowledge and understanding to alleviate your fears and make your actions count.

Questions?

Thank you!