

Atacando VoIP.... Un paraíso

Giovanni Cruz Forero



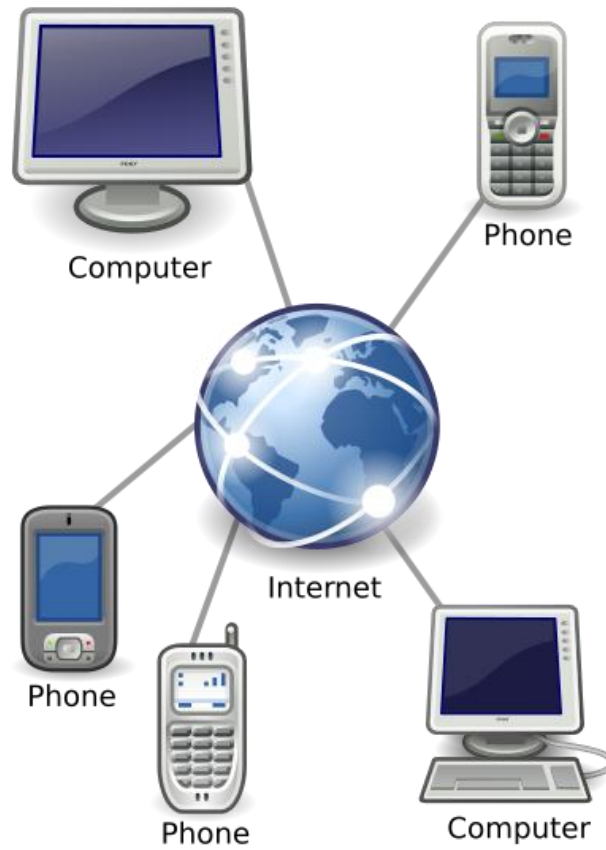
Agenda

- Intro
- Protocolos
- Ataques Recientes
- Herramientas
- Demo # 1
- Demo # 2
- Demo # 3



Intro

VoIP



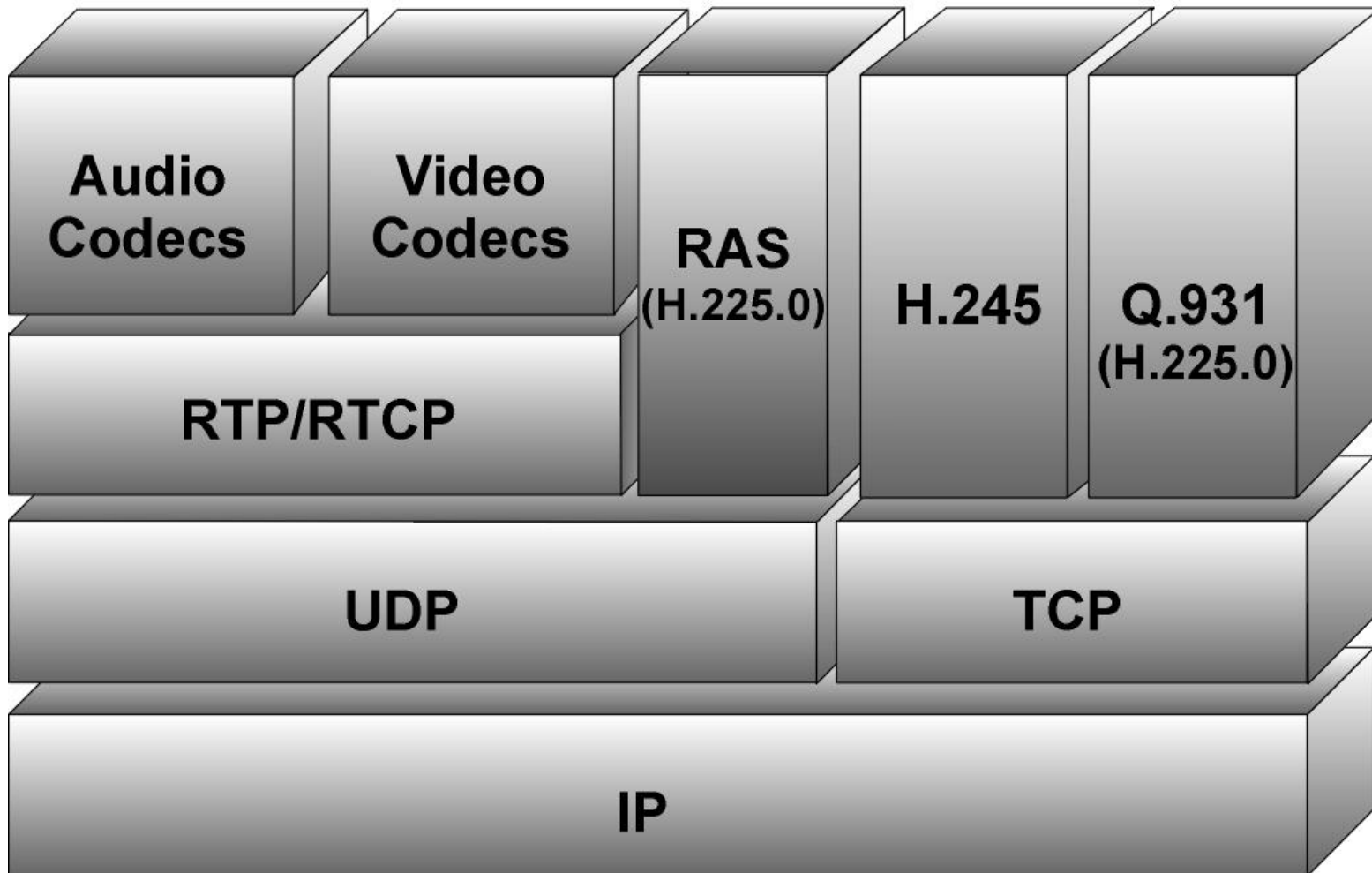
Componentes

- Endpoints (Softphones, Hardphones)
- IP PBX
- Base de Datos
- Servidores Web
- Sistemas Operativos
- H.323 Gatekeeper
- SBC
- PSTN
- B2BUA
 - UAS
 - UAC
- SIP Proxy
- SIP Registrar
- Softswitch
- Media Gateways
- Location Server
- Directorio

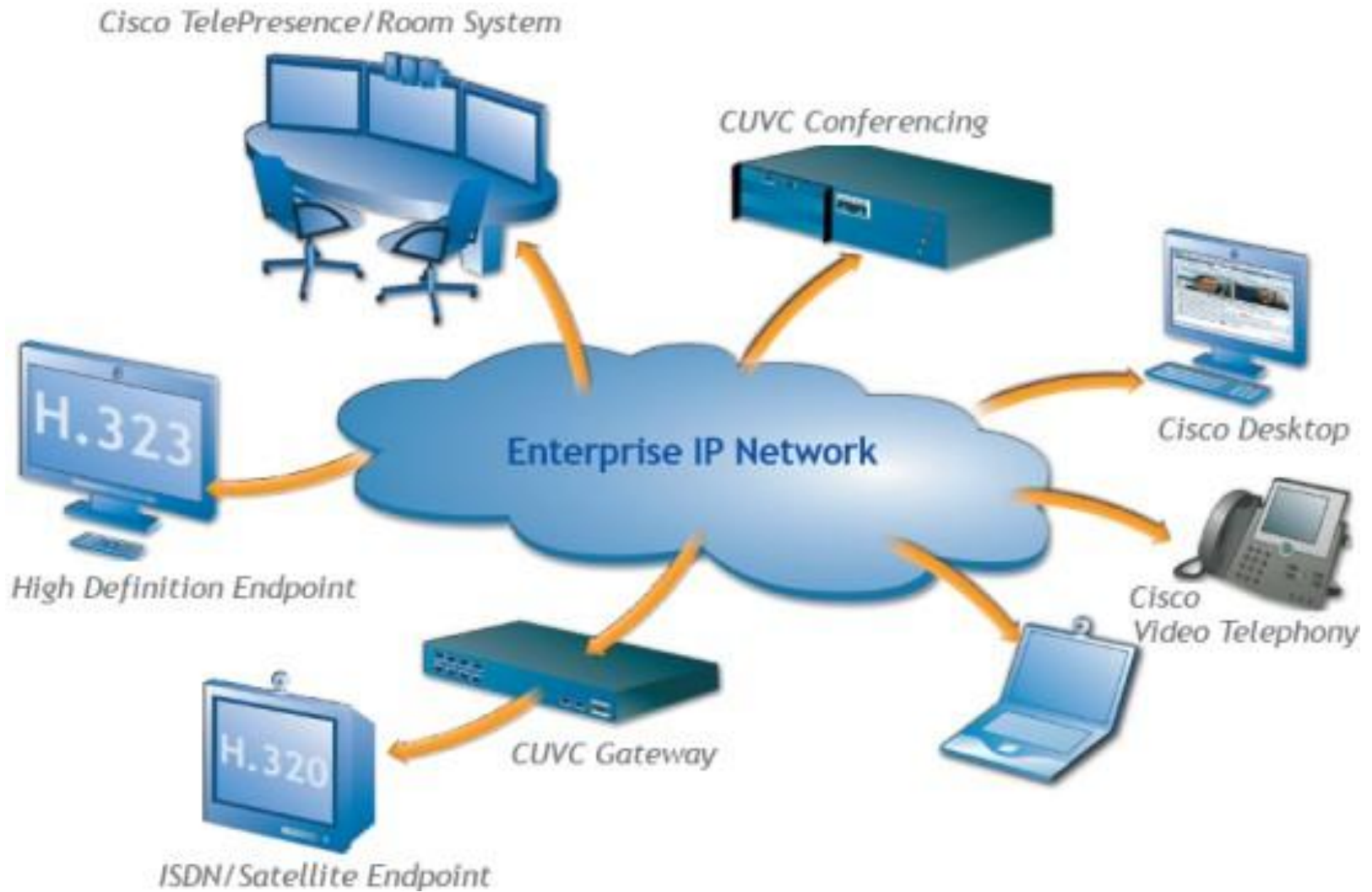
Protocolos

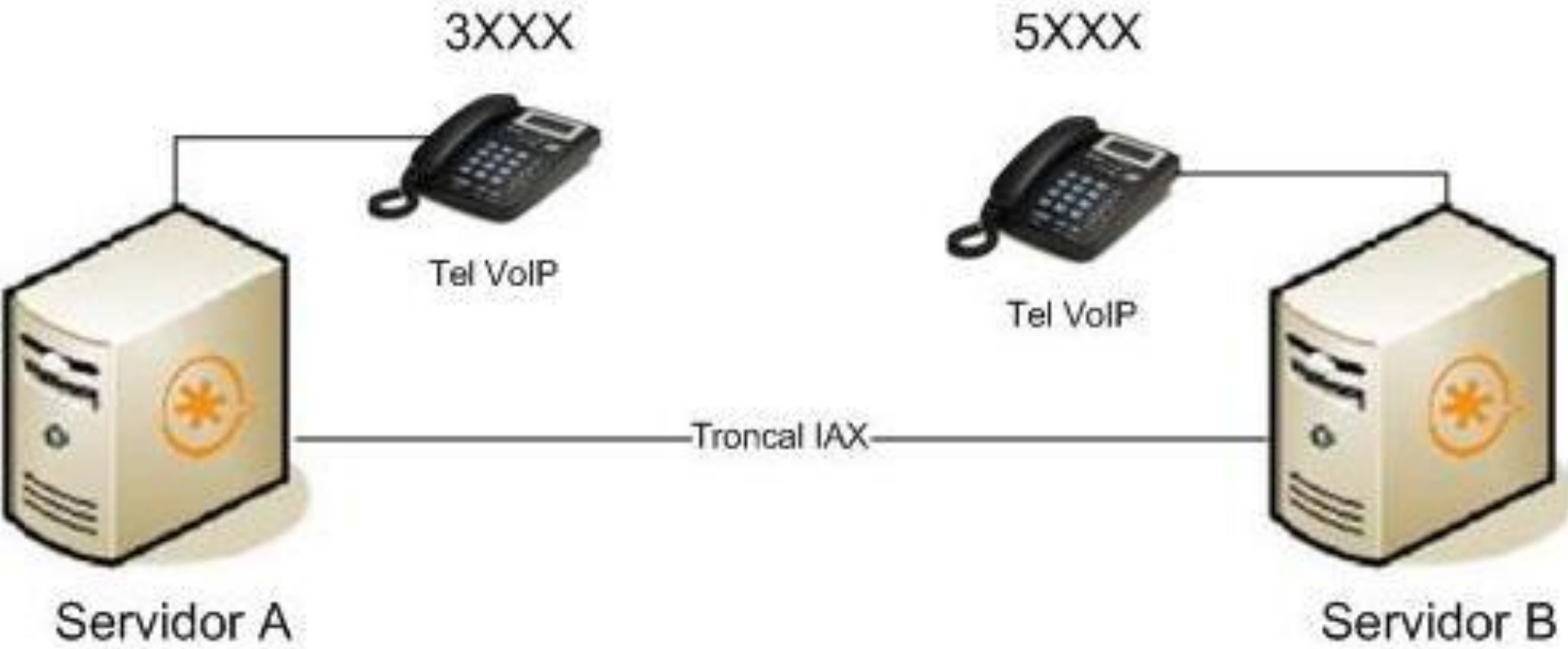
H.323

Protocol Stack



SCCP





IAX

SIP

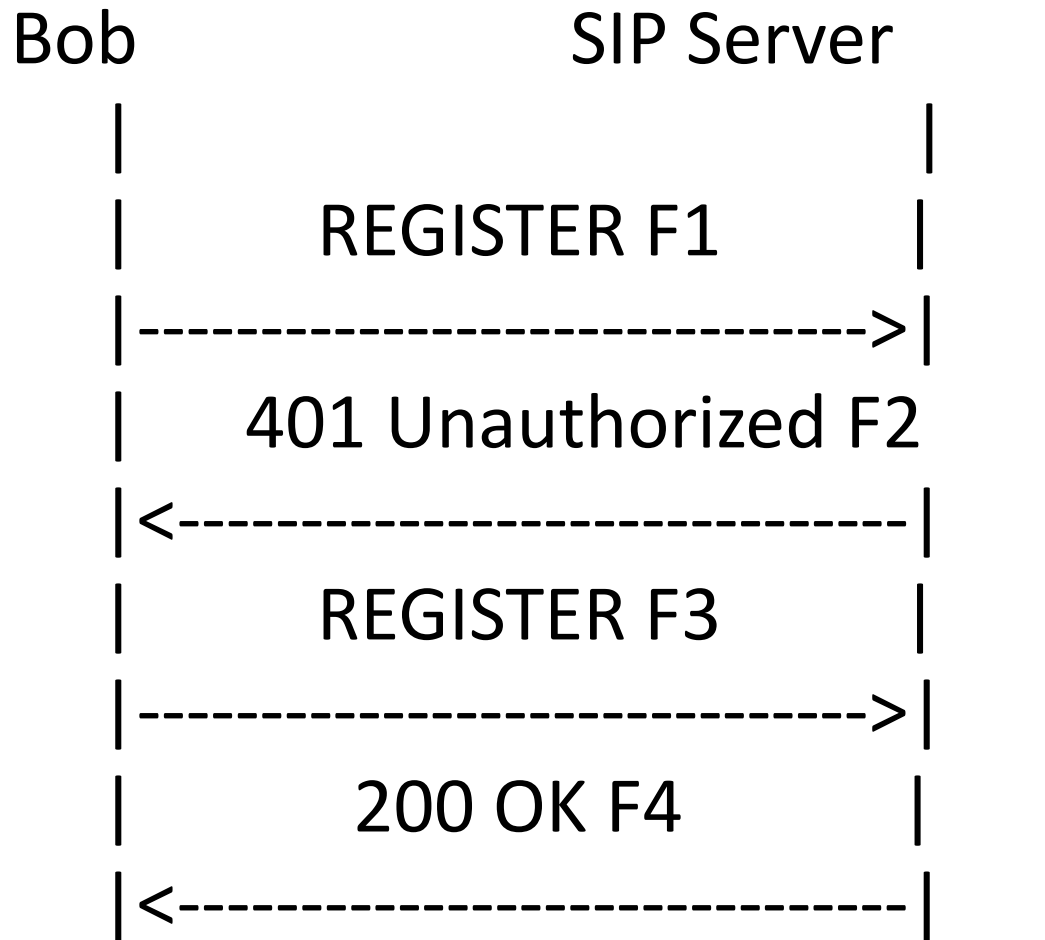
PETICIONES

- INVITE
- ACK
- BYE
- CANCEL
- REGISTER
- OPTIONS

RESPUESTAS

- 1XX – Provisionales
- 2XX – Exitosa
- 3XX – Redirección
- 4XX – Error de cliente
- 5XX – Fallas del Servidor
- 6XX – Fallas Globales

Registro



F1 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0

Via: SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bK
nashds7

Max-Forwards: 70

From: Bob

<sips:bob@biloxi.example.com>;tag=a73kszlfl

To: Bob <sips:bob@biloxi.example.com>

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 1 REGISTER

Contact: <sips:bob@client.biloxi.example.com>

Content-Length: 0

F2 401 Unauthorized SIP Server -> Bob

SIP/2.0 401 Unauthorized

Via: SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bKnashds7
;received=192.0.2.201

From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl

To: Bob <sips:bob@biloxi.example.com>;tag=1410948204

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 1 REGISTER

WWW-Authenticate: Digest realm="atlanta.example.com",
qop="auth",

nonce="ea9c8e88df84f1cec4341ae6cbe5a359",

opaque="", stale=FALSE, algorithm=MD5

Content-Length: 0

F3 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0

Via: SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bKnashd92

Max-Forwards: 70

From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlfIH

To: Bob <sips:bob@biloxi.example.com>

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact: <sips:bob@client.biloxi.example.com>

Authorization: Digest username="bob",

realm="atlanta.example.com"

nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",

uri="sips:ss2.biloxi.example.com",

response="dfe56131d1958046689d83306477ecc"

Content-Length: 0

F4 200 OK SIP Server -> Bob

SIP/2.0 200 OK

Via: SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bKnashd
92

;received=192.0.2.201

From: Bob

<sips:bob@biloxi.example.com>;tag=ja743ks76zlfIH

To: Bob

<sips:bob@biloxi.example.com>;tag=37GkEhwI6

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact:

<sips:bob@client.biloxi.example.com>;expires=3600

Content-Length: 0

SDP





BEWARE!

INSECURITY Ahead

Ataques

JUL 14

New Denial of Service Vulnerability on Cisco Unified Communications Manager

Posted by valeri

Cisco Unified Communications Manager Denial of Service Vulnerability the Level of the attack is moderately critical. It is between 3 and 5. The attacker could launch the attack remotely. This Vulnerability concerns CUCM version 5.

1. Some vulnerabilities have been reported in **Cisco Unified Communications Manager**. An attacker could start Denial of Service (DoS) attacks to the Cisco CUCM version 5.

An error in the handling of SIP INVITE messages can be used to complete a review and disrupt voice services.

2. An error in the interpretation of network connections can be exploited to prevent further connections to system services, which are furnished by the creation of a large number of TCP connections with an affected system.

3. Two errors in the processing of SIP and SCCP packets can be exploited to the SIP port in the vicinity (5060/TCP and 5061/TCP) and SCCP port (2000/TCP and 2443/TCP) in the Flood affected system with a TCP packet.

Up to the date of this article, **Cisco Systems** does not have released a patch to circumvent this issue.

Note: **Cisco** Unified Communications Manager is an enterprise-class IP telephony call-processing system that provides traditional telephony features

Cisco®
CCIE
There are only 20,000 in the world. Join Them!
ipexpert
IPexpert.com Ads by Google

The DDOS Specialist
Identify and block DDOS attacks automatically and in real time.
www.riorey.com

Learn To Make Money Online For Free!



Get Over \$4,000 Worth of FREE Personalized tutorials to teach you how to make money online. **This Is Free!**

2 Bonuses Valued At \$97 Are Also Included!

This Offer Is Limited To Next 237 Subscribers!

Hurry, Sign Up Below...

Name:

Email:

[We respect your email privacy](#)

Would You Like To Earn

While Sitting On Your

Phone Scam

The image is a screenshot of a web browser displaying the FBI website. The browser's address bar shows the URL www.fbi.gov/page2/june10/phone_062110.html. The page features the FBI logo and the text "FEDERAL BUREAU OF INVESTIGATION". A search bar is visible on the right side of the header. The main content area is titled "Headline Archives" and features a news article with the headline "THE LATEST PHONE SCAM Targets Your Bank Account" dated "06/21/10". The article includes a photograph of a telephone handset and a coiled cord. The text of the article describes a "telephone denial-of-service attack" where criminals use automated dialing programs to overwhelm phone lines and raid victims' bank accounts. A sidebar on the left contains navigation links such as "Contact Us", "Learn About Us", "Get Our News", "Be Crime Smart", "Use Our Resources", and "Visit Our Kids' Page".

FBI — Phone Scam - Press ... x

www.fbi.gov/page2/june10/phone_062110.html

Links The Binary Auditor™ ... bxi:blog Hackers Center Secur... Aprendizaje de securi... TacVoIP: Hardcore Vo... Noticias Ubuntu WPA CRACKER Category: .NET Packe... Otros marcadores

Home | Site Map | FAQs

FEDERAL BUREAU OF INVESTIGATION

SEARCH

Contact Us

- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us

- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News

- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart

- Wanted by the FBI
- More Protections

Use Our Resources

- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Headline Archives

THE LATEST PHONE SCAM Targets Your Bank Account

06/21/10



Imagine getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

It's annoying, no doubt. But it could be more than that—it could be a sign that you're being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could be the precursor to a crime targeting your bank accounts.

Denial-of-service attacks, by themselves, are nothing new—computer hackers use them to take down websites by flooding them with large amounts of traffic.

In a recent twist, criminals have transferred this activity to telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens.

Why are they doing it? Turns out the calls are simply a diversionary tactic: while the lines are tied up, the criminals—masquerading as the victims themselves—are raiding the victims' bank accounts and online trading or other money management accounts.

SHARE

Here, in a nutshell, is how the whole thing works:

- Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that this person's bank or financial institution would have—like account numbers and passwords. Perhaps the victim responded to a bogus e-mail, clicking for information, inadvertently gave out sensitive

Amazon EC2

The screenshot shows a web browser window with the address bar displaying www.mgrav.es.org/2010/04/amazon-responds-about-sip-attacks-from-ec2/. The browser's tab is titled "Graves on SOHO Techno...". The page content includes a header for "Graves on SOHO Technology" with the tagline "End User Perspective On SOHO Technology" and an RSS icon. Below the header is a navigation menu with links for HOME, ABOUT, GUIDES & HOW-TO'S, PRODUCT REVIEWS, BEST OF..., and RAVES. The main article is titled "Amazon Responds About SIP Attacks From EC2" and is dated April 23, 2010. The article text states that on April 18th, Amazon finally responded publicly to SIP attacks originating from EC2 instances. To the right of the text is a logo for "SIP DOS Attacks powered by amazon web services™". A search bar is located above the "Recent Comments" section, which lists several comments from users like mgrav.es and Oliver on topics such as "A Talk In The Clouds: Asterisk on EC2" and "HDVoice In Support of Radio: Tieline At TAB 2010".

Graves on SOHO Technology
End User Perspective On SOHO Technology

HOME ABOUT GUIDES & HOW-TO'S PRODUCT REVIEWS BEST OF... RAVES

Amazon Responds About SIP Attacks From EC2

mgrav.es | April 23, 2010

On April 18th **Amazon** finally responded publicly with respect to the **SIP** attacks recently suffered from hosts within their EC2 service. Their response comes in the form of an informational security bulletin posted to their **AWS Security Center**.

SIP DOS Attacks
powered by
amazon
web services™

There have been some recent discussions about SIP brute force attacks originating from Amazon EC2. We can confirm that several users reported SIP brute force attacks originating from a small number of Amazon EC2 instances about a week ago. It appears these attacks were designed to exploit security vulnerabilities in the SIP protocol. There is nothing specific about this attack that requires Amazon EC2. It was a brute force attack that could be launched from any computer on any network.

Recent Comments

mgrav.es on A Talk In The Clouds: Asterisk on EC2

Oliver on A Talk In The Clouds: Asterisk on EC2

George Jones on HDVoice In Support of Radio: Tieline At TAB 2010

mgrav.es on The Mythical POTS Advantage: Line Powered Phones

George Pajari on The Mythical POTS Advantage: Line Powered Phones

Making Use Of HDVoice Right Now!

Contraseñas por defecto....

The British Tabloid Phone-H... x

www.nytimes.com/2010/09/05/magazine/05hacking-t.html?_r=2

Links The Binary Auditor™... bxipli:blog Hackers Center Secur... Aprendizaje de securi... TacVoIP: Hardcore Vo... Noticias Ubuntu WPA CRACKER Category: .NET Packe... Otros marcadores

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS Try Times Reader today Log In Register Now TimesPeople

The New York Times Magazine Search All NYTimes.com Go **ING DIRECT**

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

IT'S NOT JUST A CARD. IT'S YOUR CANVAS. **TAKE CHARGE®** REPLAY
CREATE YOURS AT ZYNCCARD.COM

Tabloid Hack Attack on Royals, and Beyond




Lewis Vihyd/Getty Images

Members of the royal household had their voice mail messages hacked into by News of the World employees.


By **DON VAN NATTA Jr.**, **JO BECKER** and **GRAHAM BOWLEY**
Published: September 1, 2010

Log in to see what your friends are sharing on nytimes.com. **Log In With Facebook**
Privacy Policy | What's This?

What's Popular Now

In Iraq, Clearer Image of U.S. Support  Who's the Con Man? 

Travel Deals E-mail newsletter
Sign up for travel deals and discounts on airfare, hotels, transportation and more!
 Sign Up
[See Sample](#) | [Privacy Policy](#)

 **MONEY DOES**

Fraude Telefónico

Tony's Blog » VoIP Attack Rings Up \$120,000 Phone Bill

VoIP Attack Rings Up \$120,000 Phone Bill

An Australian company received quite a shock when they got their phone bill and found that it was **\$120,000 higher than they expected**. Investigators determined that attackers were able to access the companies phone system and place over 11,000 unauthorized international calls within a window of about 2 days.

The reports so far seem a little light on details. It does seem though that the attackers compromised **both** traditional PBX and VoIP systems. **Toll fraud of this type** has been around long before VoIP came into existence. In some cases, attackers are able to use social engineering tactics to trick a receptionist or employee into **redirecting their call to an outside line**. However insufficient or inadequate security controls can also be exploited by attackers to allow their unauthorized devices to place calls through the system. Or, in some cases attackers may just directly attack the VoIP server and gain access which would allow them to change configuration settings and authorize any devices they choose.

Again- toll fraud and some other attacks common to VoIP security have been around since Alexander Graham Bell invented the phone. The threats and the attacks themselves are not new to VoIP. However, the convergence of VoIP onto the same IP network shared by the rest of the network and the public Internet means that the voice systems are much more accessible and that it is easier to automate attacks and execute them more quickly.

Companies employing VoIP solutions should begin by realizing that their VoIP hardware and software need to be protected at least the same as other servers and applications on their data network. In addition, VoIP communications should be encrypted to prevent eavesdropping or call interception. Attackers might be able to gather information from unencrypted VoIP data packets that will allow them to compromise the VoIP system. One of the best defenses against this simple attack though is diligent monitoring. Call logs should be reviewed on a regular basis, or better yet some sort of **VoIP IPS or anomaly detection system** to automatically monitor activity and notify administrators and/or block suspicious activity when anomalies are detected.

Posted Jan 25 2009, 07:27 AM by Tony Bradley

Filed under: VoIP, VoIP security, encryption, social engineering, monitor call logs, toll fraud

Comments

Tony's Blog

[Home](#)

[About](#)

[Contact](#)

Syndication

[RSS for Posts](#)

[Atom](#)

[RSS for Comments](#)

[Email Notifications](#)

Recent Posts

[Protecting Mobile Devices](#)

[Who Is Responsible for VoIP Security?](#)

[SIP Over TLS](#)

[Predictions for 2009](#)

[VoIP Security Threats: Call Redirection](#)

+ Fraude

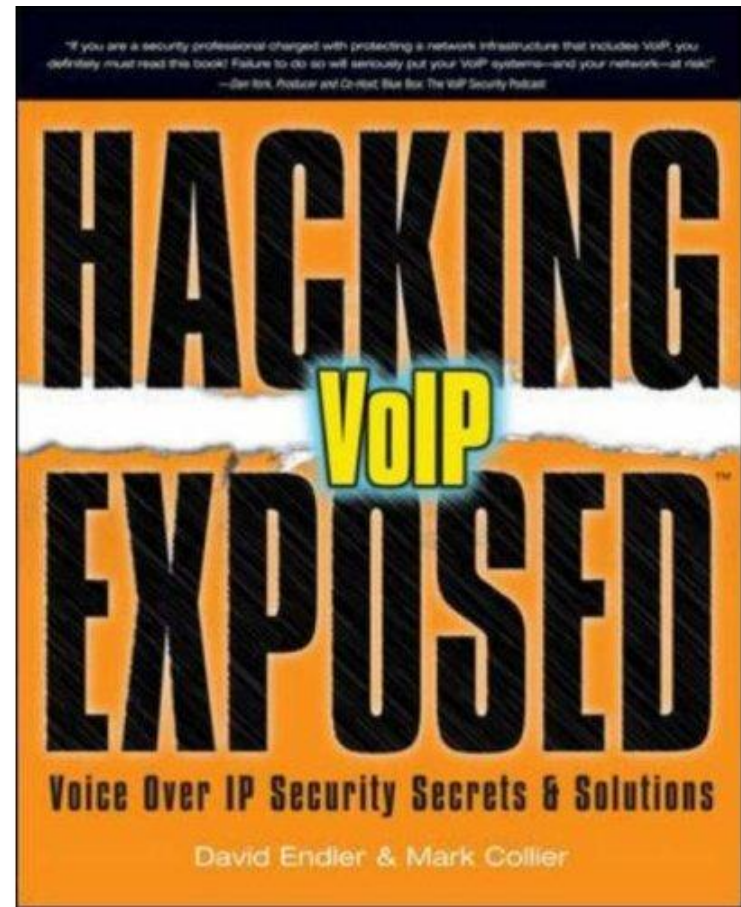
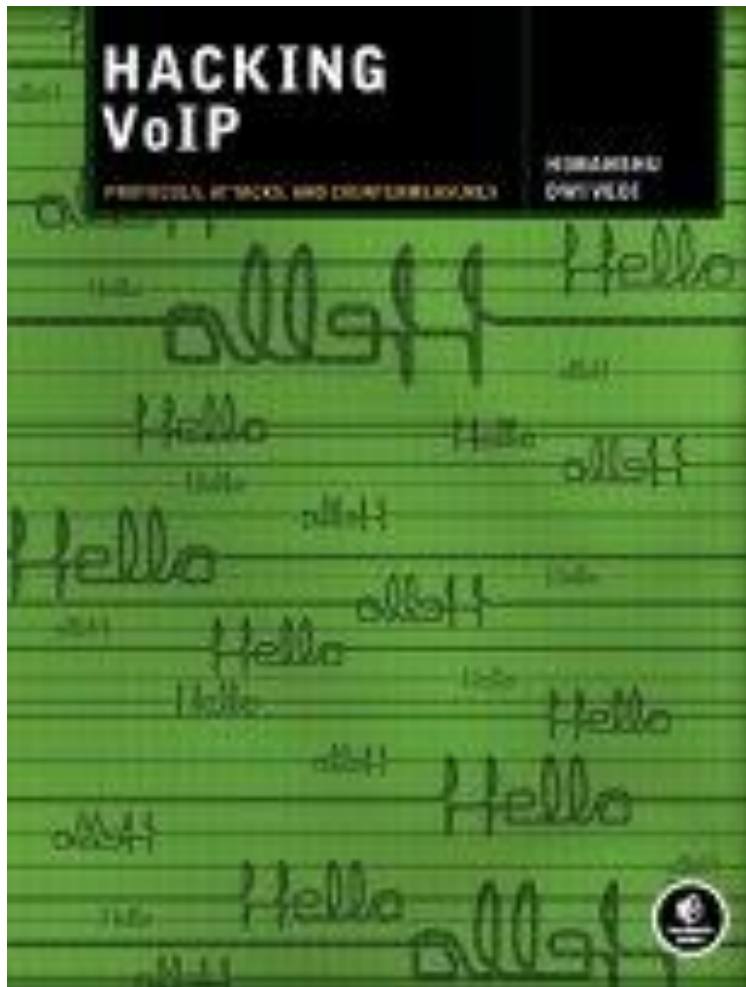
The screenshot shows the Fox News website interface. At the top left is the Fox News logo with the tagline "Fair & Balanced". A search bar and a "Search" button are located at the top center. Below the search bar, there are navigation links for "What's Hot", "New Section! Leisure", "Who Deserves the Oscar?", and "First 100 Days". A horizontal menu contains categories: HOME, U.S., WORLD, BUSINESS, POLITICS, ENTERTAINMENT, LEISURE, HEALTH, SCITECH, OPINION, SPORTS, and ON AIR.

A large banner advertisement for Samsung Blast and T-Mobile is displayed, with the text "The Coolest Way" and a "Get It Now" button. Below the banner, the "SciTech" section is highlighted.

The main article is titled "Hacker Sticks Company With \$43,000 Phone Bill" and is dated Tuesday, December 23, 2008. The article text reads: "It's a long way from Manitoba to Bulgaria — and phone calls from one to the other can get really expensive. That's what one hapless Canadian small-business owner discovered after a hacker broke into his company's voice-mail system and placed hundreds of calls to the Balkan nation, landing him with a \$43,000 phone bill. 'If I have to pay that whole bill out of my own pocket, I'm looking at having to lay off one of my employees,' Alan Davison, owner of HUB Computer Solutions in Winnipeg, told the Winnipeg Free Press. 'It's quite obvious something was right out of whack. There were hundreds of phone'".

On the right side, there is a "FOX NEWS VIDEOS" section with "TOP VIDEOS" including "Cloud Commuting", "Next Stop: HAL?", and "Animal Hou Blues". Below this is a "SCITECH" section with a list of items: "Salvage firm locates legendary warship" and "Scientists anxiously monitor Mt. Redoubt".

Herramientas



DEMO # 1

DEMO # 2

DEMO # 3