

Ameaças a Tecnologia VoIP

Frederico Madeira

LPIC-1, CCNA

fred@madeira.eng.br

www.madeira.eng.br

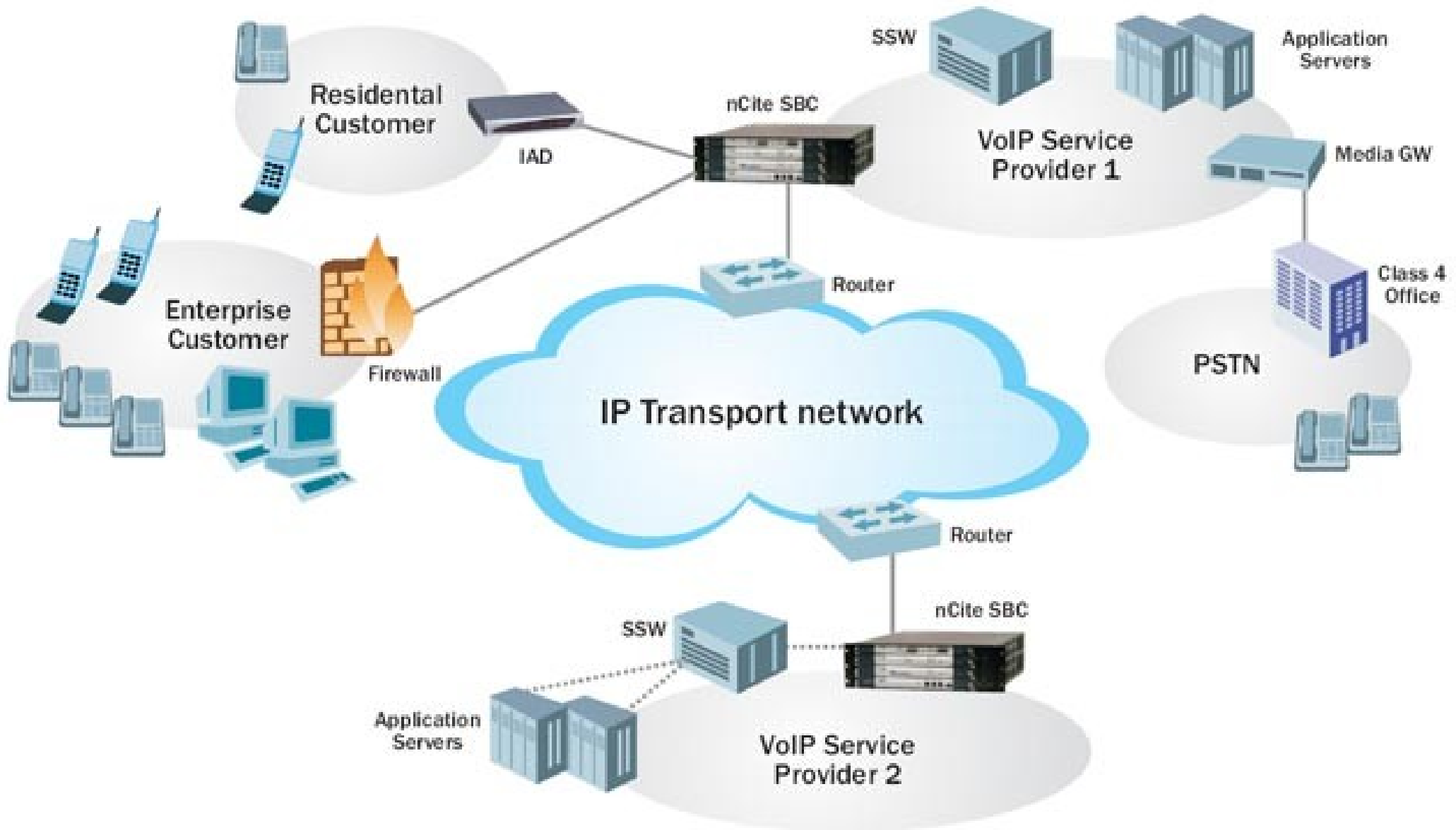
Agenda

- x Introdução
- x Infra-Estrutura VoIP
- x Cenário Atual
- x Protocolos
- x SIP (Session Initiation Protocol)
- x Ameaças: Modelo em Camadas
- x Ameaças Emergentes

Introdução

- VoIP é um conjunto de tecnologias que permite que chamadas de voz sejam feitas através da internet (ou ainda através de outras redes desenhadas para carregar dados), através do IP (Internet Protocol)
- Possibilita realização de chamadas de baixo custo, ou até mesmo gratuitas.
- Redução de custos com infra-estrutura.
- Acrescenta novas funcionalidades ao serviço telefônico
- Significa uma MUDANÇA nas Telecomunicações

Infra-Estrutura



Infra-Estrutura

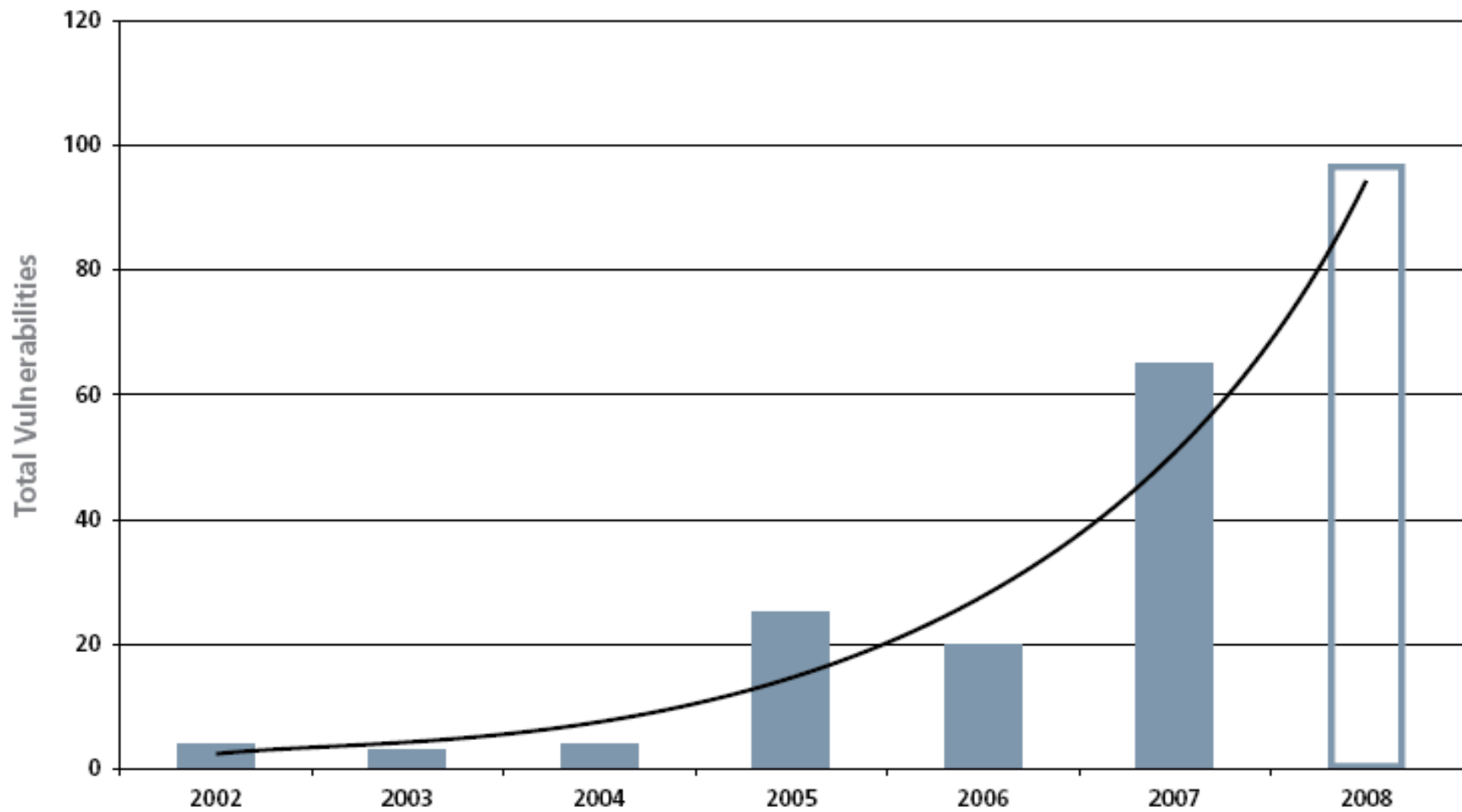


Cenário Atual

- Pesquisas apontam o crescente avanço da adoção da tecnologia VoIP em empresas e residências;
- Projetos de software livre incentivam o uso de VoIP
- **Pesquisas prevêem grande aumento em ataques a redes VoIP**
- Falta de documentação técnica detalhando/descrevendo as ameaças
- Ausência de profissionais qualificados na área

Cenário Atual

VoIP Vulnerabilities



Source: National Vulnerability Database

Protocolos

Protocolos de Sinalização

Responsáveis por inicial, monitorar, modificar e terminar chamadas VoIP.

- SIP (Session Intitation Protocol) - RFC 3261
- SDP (Session Description Protocol) - RFC 4566
- MGCP (Media Gateway Control Protocol) - RFC 3435
- Megaco / H.248 - RFC 3525

Protocolos

Protocolos de Mídia

Responsáveis por transportar o fluxo de mídia (Voz ou Imagens)

- RTP (Real Time Protocol) – RFC 3550
- RTCP (Real Time Control Protocol) – RFC 3605
- SRTP / ZRTP

Protocolos

Codecs

Realizam a compressão do fluxo de mídia de forma que possa ser otimizada a banda.

- G.711 (64 kbit/s)
- GSM (12.2 kbit/s)
- G.729 (8 kbit/s)
- G.723 (6.3 kbit/s)

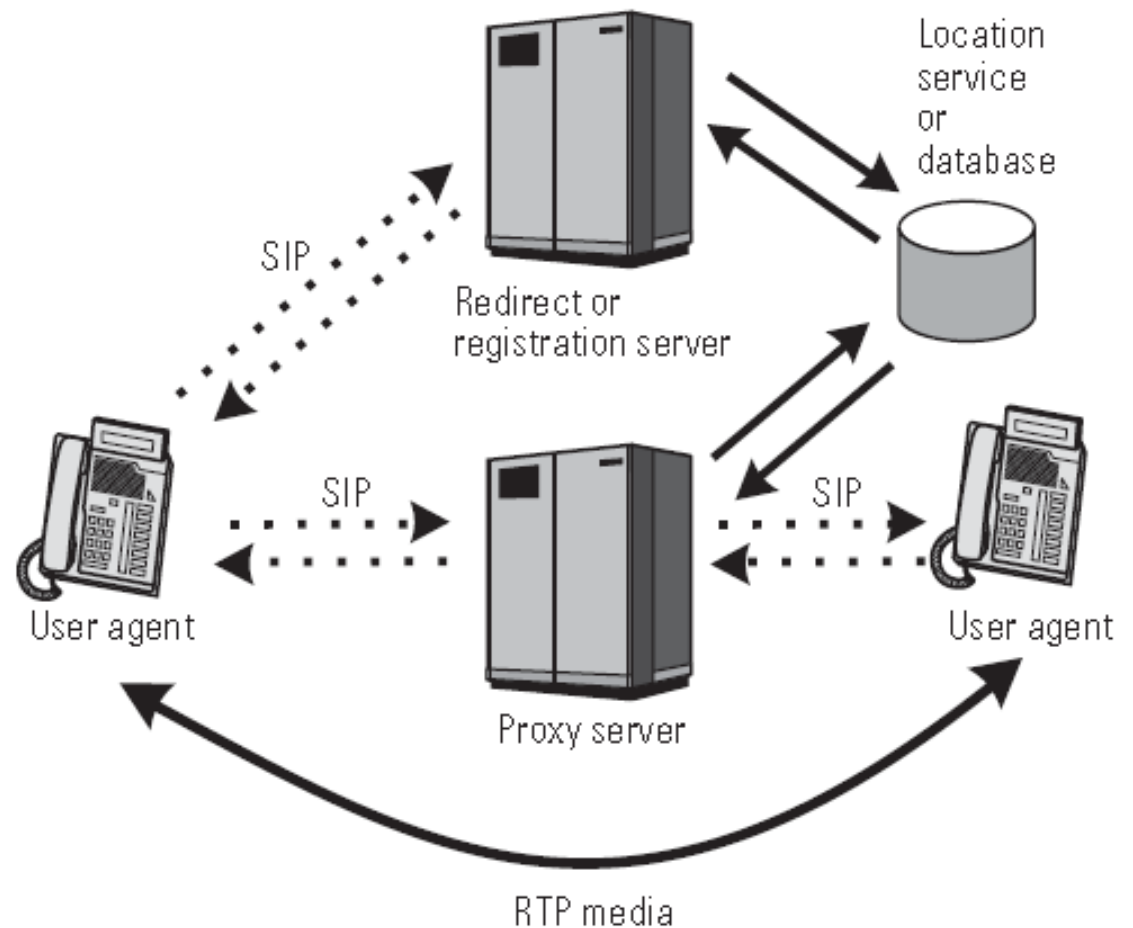
SIP (Session Intitation Protocol)

- Protocolo de sessão mais utilizado dentro da tecnologia VoIP
- Arquitetura baseada no modelo de cliente-servidor onde os clientes iniciam uma chamada e o servidor responde às chamadas.
- Protocolo baseado em texto e se assemelha com o HTTP
- mensagens SIP são compostas de requisições e respostas específicas

SIP (Session Intitation Protocol)

Elementos da Arquitetura

- *User agents (UA)*
- *Proxy Server*
- *Registrar Server*
- *Redirect Server*
- *Location Server*



SIP (Session Intitation Protocol)

Requisições

Método	Funcionalidades
INVITE	Mensagem usada para iniciar uma chamada
ACK	Mensagem de Confirmação Final
BYE	Libera uma chamada
CANCEL	Cancela uma requisição pendente. Não possui efeito em uma chamada já estabelecida
OPTIONS	Consulta as funcionalidades suportadas
REGISTER	Mensagem usada para registrar um usuário em um servidor sip

SIP (Session Intitation Protocol)

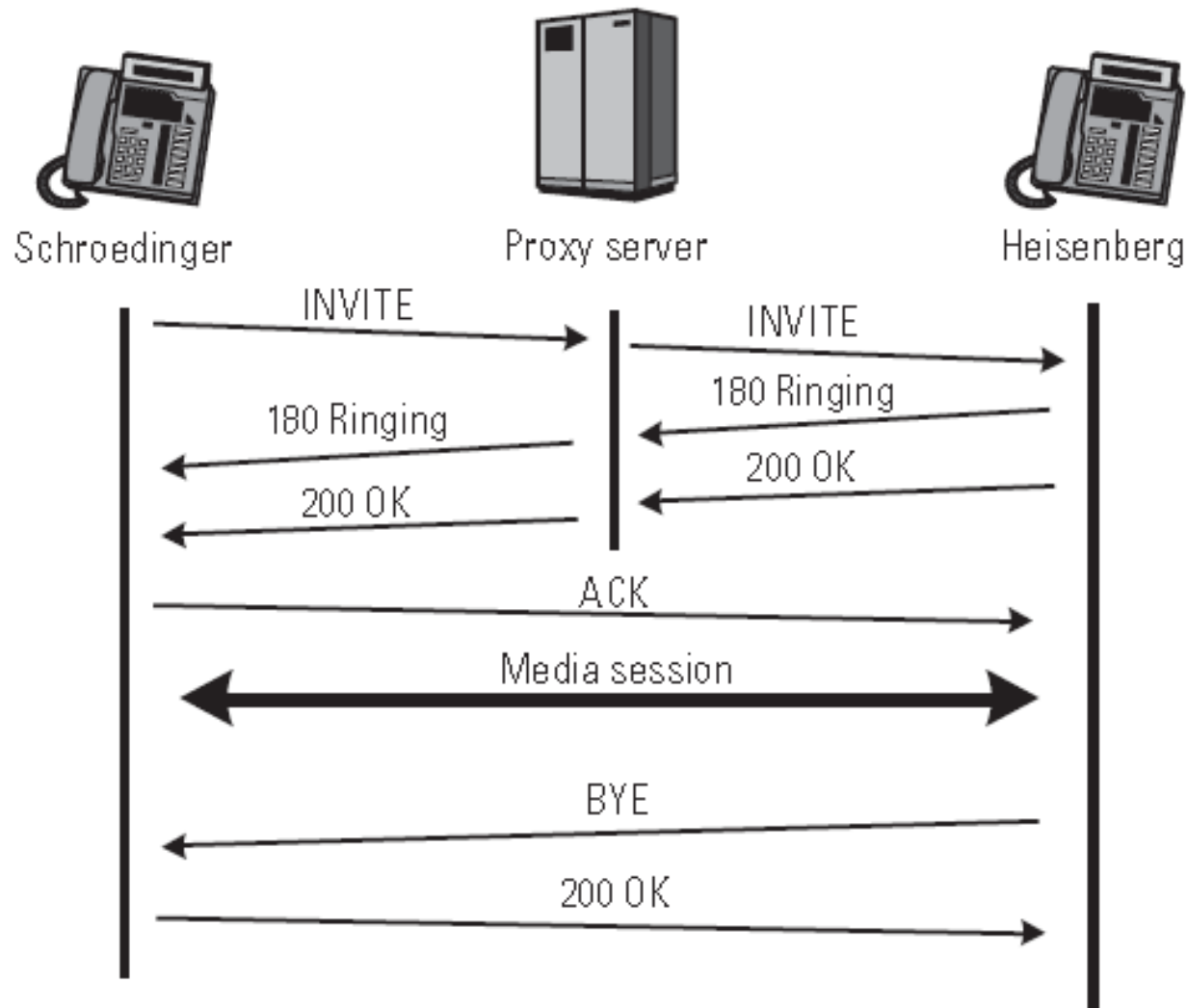
Respostas

Cód	Respostas	Principais Mensagens
1xx	Informativas	100 Trying 180 Ringing 181 Call forwarded 182 Queued 183 Session Progress (Early Media)
2xx	Sucesso	200 OK 202 Accepted

Cód	Respostas	Principais Mensagens
3xx	Redirecionamento	300 Multiple Choices 301 Moved Perm 302 Moved Temp 380 Alternative Serv
4xx	Falhas de requisições	400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found 405 Bad Method 415 Unsupp Content 420 Bad Extensions 486 Busy Here
5xx	Falhas no Servidor	504 Timeout 503 Unavailable 501 Not Implemented 500 Server Error
6xx	Falhas Globais	600 Busy Everywhere 603 Decline 604 Doesn't Exist 606 Not Acceptable

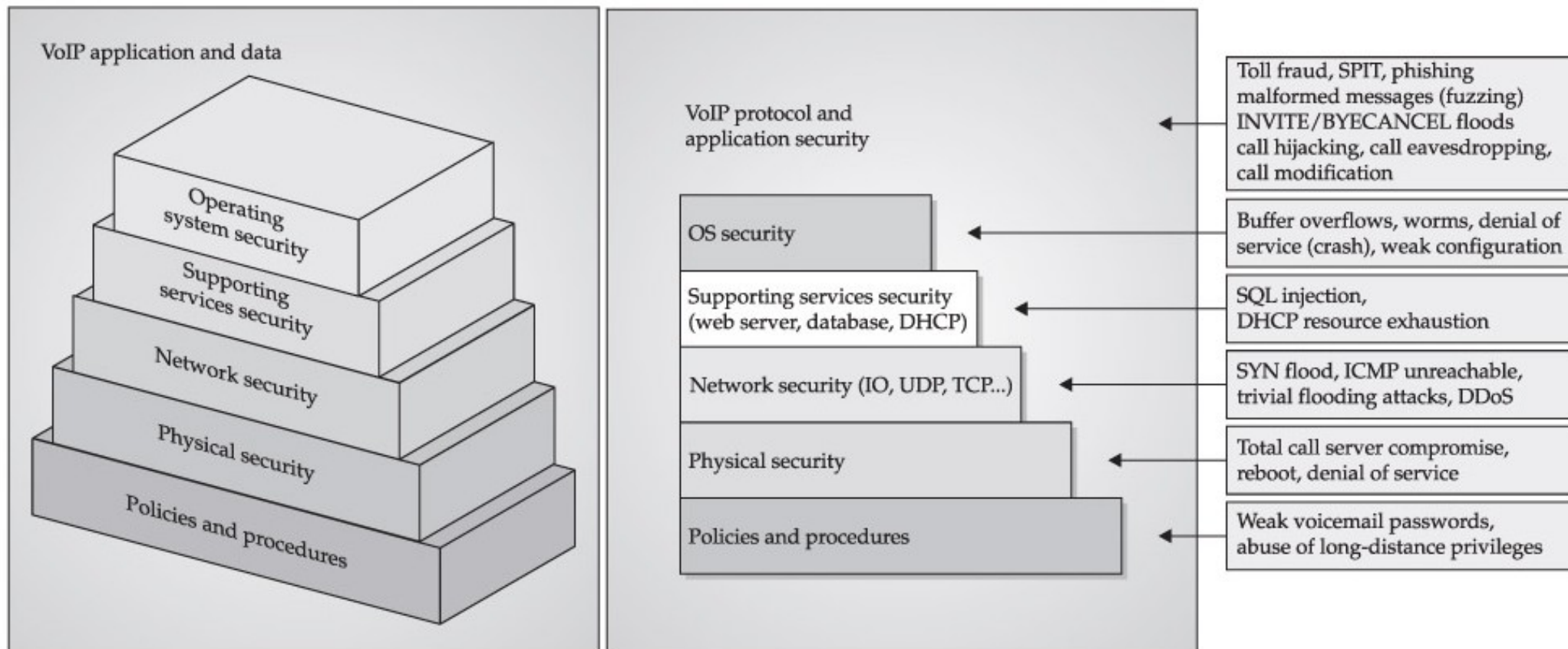
SIP (Session Intitation Protocol)

Call Flow



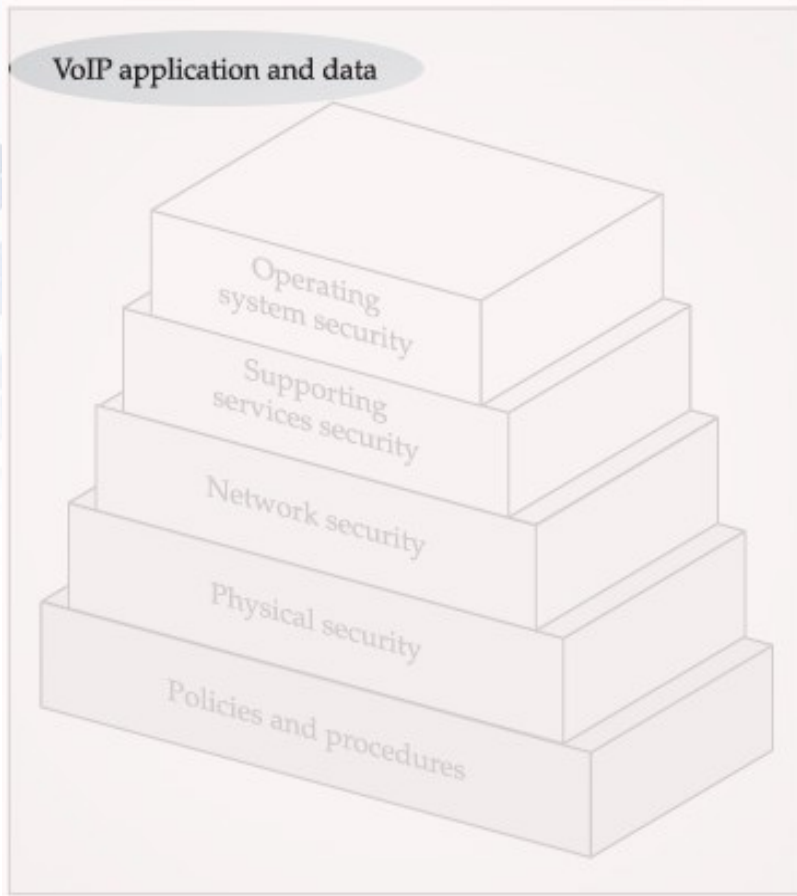
Ameaças: Modelo em Camada

Proposto por David Endler e Mark Collier em seu livro:
Hacker Exposed: VoIP



Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP



Ameaças

- Invite Flood
- Registration Hijacking
- Escuta Telefônica
- Fuzzing
- SPIT

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: INVITE FLOOD

- INVITE = Mensagem usada para iniciar uma chamada
- Consiste em enviar milhares de mensagens invite com algumas modificações na mensagem (From, To, invalid IP, invalid Domain, etc...)
- Como o SIP utiliza (na maioria dos casos) o UDP é fácil gerar pacotes com origem spoofed.

INVITE sip:UserB@biloxi.com SIP/2.0

Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9

Max-Forwards: 70

From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl

To: LittleGuy <sip:UserB@biloxi.com>

Call-ID: 3848276298220188511@atlanta.com

CSeq: 1 INVITE

Contact: <sip:UserA@client.atlanta.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 143

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: INVITE FLOOD - Ferramentas

- * IAXFlooder
- * INVITE Flooder
- * RTP Flooder
- * SIPsak -
SIP swiss army knife.



Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

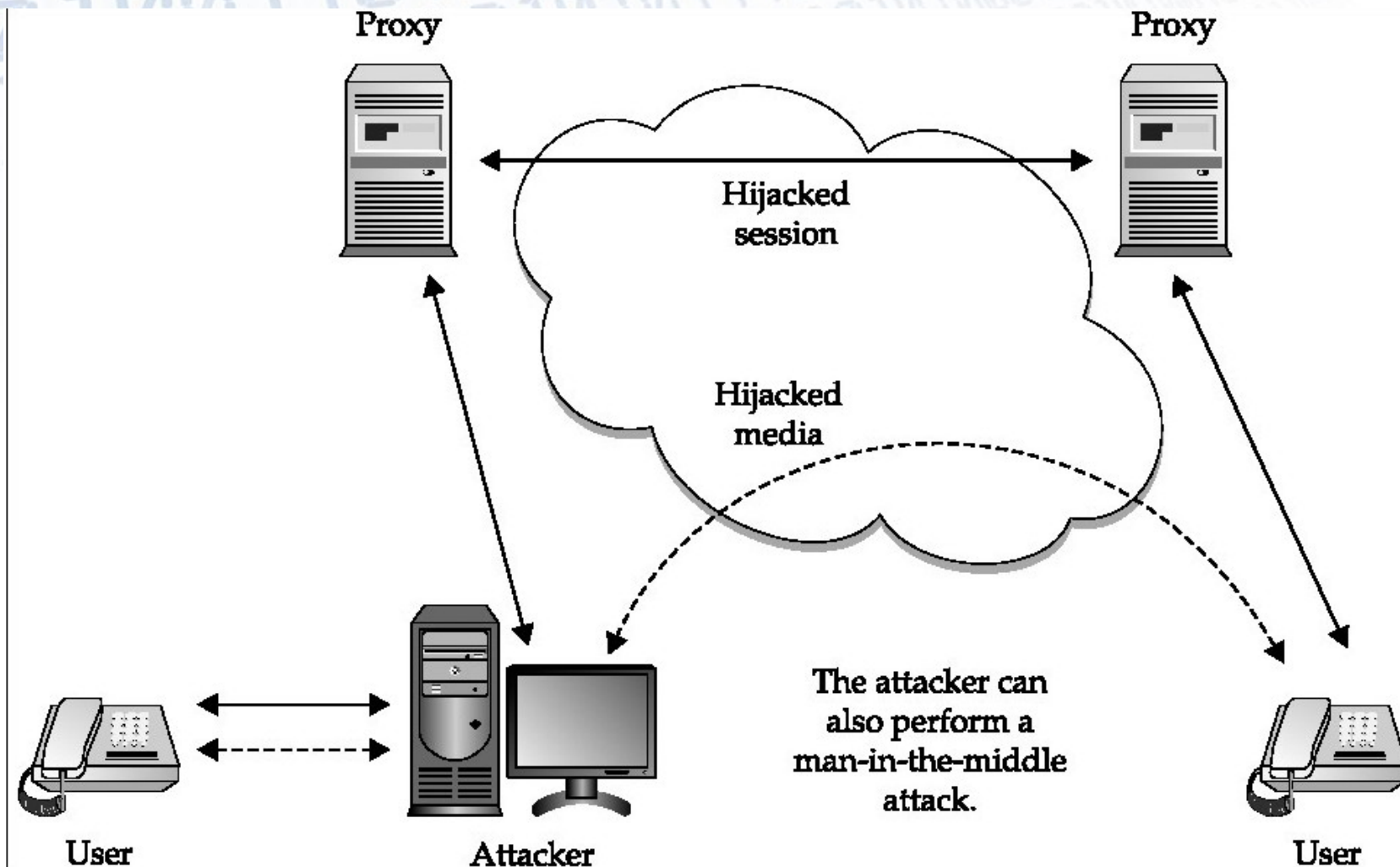
Ameaças: Registration Hijacking

- REGISTER = Mensagem usada para registrar um usuário em um servidor sip
- UA se registram a cada 1800 ou 3600s nos Proxy Servers
- Consiste em:
 - substituir o registro de um usuário legítimo por um falso
 - remover o registro de um usuário válido
- Usado como base para ataques de MITM.

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Registration Hijacking



Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Registration Hijacking

```
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.56:5060
From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6
To: <sip:0987654321@sip.my_proxy.com>
Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA
CSeq: 500646445 REGISTER
Contact: <sip:654321@192.168.1.56:5060>
Expires: 1800
User-Agent: VEGA400/10.02.07.2xS009
Content-Length: 0
```

REGISTRO
VÁLIDA

```
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.56:5060
From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6
To: <sip:0987654321@sip.my_proxy.com>
Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA
CSeq: 500646445 REGISTER
Contact: *
Expires: 0
User-Agent: VEGA400/10.02.07.2xS009
Content-Length: 0
```

REMOÇÃO DE
UM REGISTRO

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Registration Hijacking

```
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.56:5060
From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6
To: <sip:0987654321@sip.my_proxy.com>
Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA
CSeq: 500646445 REGISTER
Contact: <sip:654321@192.168.1.56:5060>
Expires: 1800
User-Agent: VEGA400/10.02.07.2xS009
Content-Length: 0
```

REGISTRO
VÁLIDA

```
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.56:5060
From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6
To: <sip:0987654321@sip.my_proxy.com>
Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA
CSeq: 500646445 REGISTER
Contact: <sip:654321@192.168.1.101:5060>
Expires: 1800
User-Agent: VEGA400/10.02.07.2xS009
Content-Length: 0
```

SEQUESTRO DE
UM REGISTRO

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Registration Hijacking

Ferramentas:

- Registration Adder
- Registration Eraser
- Registration Hijacker
- reghijacker

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Call Eavesdropping (Escuta Telefônica)

- é o método pelo qual um atacante é capaz de **monitorar toda a sinalização e fluxo de dados** entre dois ou mais endpoints

- Fornece ao atacante:

- Para quem e de quem se recebe chamadas
- O que se fala em uma chamada
- O que se digita no telefone durante uma chamada

- É necessário que o atacante possua um certo **nível de acesso a pontos chaves da rede.**

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Call Eavesdropping (Escuta Telefônica)

- Como se realiza:

- **Step 1: técnicas**

- Man-in-the-middle (Arp Poisoning): Ettercap, Cain e Abel

- Port Mirroring no switch

- **Step 2: ferramentas para filtrar os pacotes**

- Wireshark

- Cain e Abel

- Vomit

- Voipong

- Oreka

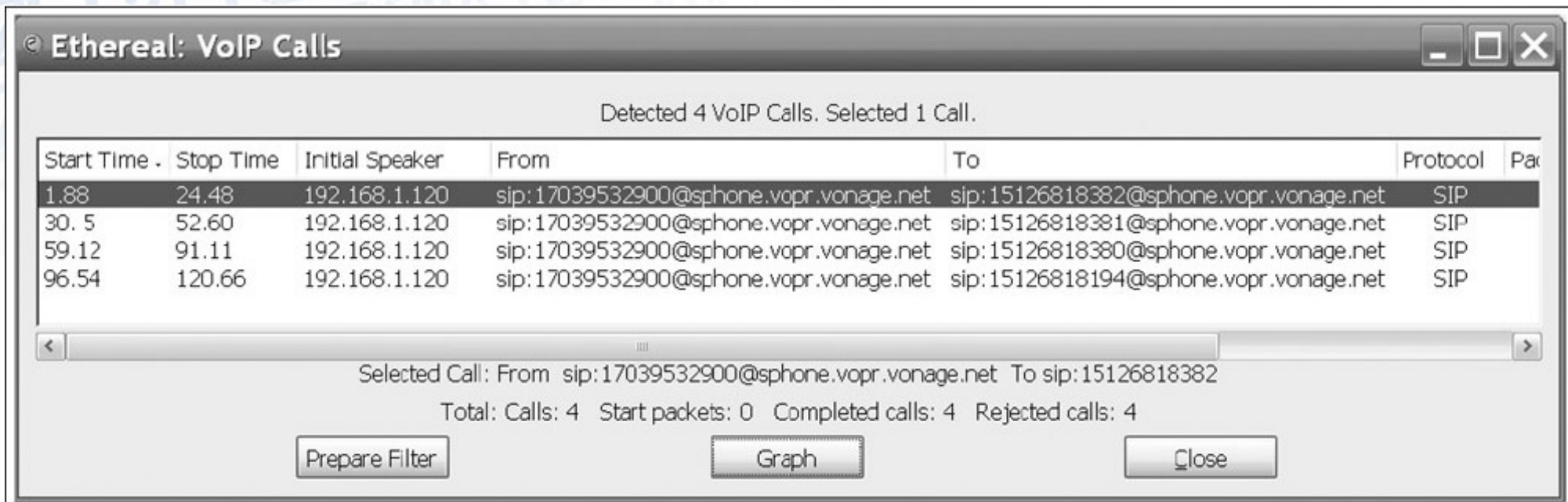
- DTMF Decoder

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Call Eavesdropping (Escuta Telefônica)

Padrão de chamadas



e **Ethereal: VoIP Calls**

Detected 4 VoIP Calls. Selected 1 Call.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packet
1.88	24.48	192.168.1.120	sip:17039532900@sphone.vopr.vonage.net	sip:15126818382@sphone.vopr.vonage.net	SIP	
30.5	52.60	192.168.1.120	sip:17039532900@sphone.vopr.vonage.net	sip:15126818381@sphone.vopr.vonage.net	SIP	
59.12	91.11	192.168.1.120	sip:17039532900@sphone.vopr.vonage.net	sip:15126818380@sphone.vopr.vonage.net	SIP	
96.54	120.66	192.168.1.120	sip:17039532900@sphone.vopr.vonage.net	sip:15126818194@sphone.vopr.vonage.net	SIP	

Selected Call: From sip:17039532900@sphone.vopr.vonage.net To sip:15126818382

Total: Calls: 4 Start packets: 0 Completed calls: 4 Rejected calls: 4

Prepare Filter Graph Close

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Call Eavesdropping (Escuta Telefônica)

Salvando conversações

Etherreal: RTP Streams

Detected 5 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
192.168.1.120	8000	69.59.241.162	12534	1470379210	ITU-T G.711	6	(0.0%)	20.71	0.15	0.44	
69.59.241.162	12534	192.168.1.120	8000	128316882	ITU-T G.711	208	(0.0%)	21.96	0.60	0.30	
192.168.1.120	8000	69.59.241.159	12264	2580194303	ITU-T G.711	6	(0.0%)	20.84	0.15	0.46	
69.59.241.159	12264	192.168.1.120	8000	521271002	ITU-T G.711	8780	(0.0%)	31.02	1.47	0.26	
192.168.1.120	8000	69.59.241.156	12264	9551111111	ITU-T G.711	6	(0.0%)	20.83	1.34	3.64	

Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

Etherreal: RTP Stream Analysis

Forward Direction Reversed Direction

Analysing stream from 69.59.241.159 port 12264 to 192.168.1.120 port 8000

Packet	Sequence	Delta (ms)	Jitter (ms)	BW (kb)	Marker	Status
327	895	0.00	0.00	1.60		[Ok]
331	896	20.03	0.00	3.20		[Ok]
333	897	19.90	0.01	4.80		[Ok]
334	898	20.10	0.01	6.40		[Ok]
336	899	20.08	0.02	8.00		[Ok]
337	900	19.92	0.02	9.60		[Ok]
338	901	19.97	0.02	11.20		[Ok]
339	902	20.01	0.02	12.80		[Ok]
340	903	20.41	0.05	14.40		[Ok]

Max delta = 0.031025 sec at packet no. 2022
Total RTP packets = 8780 (expected 8780) Lost RTP packets = 0 (0.00%) Sequence errors = 0

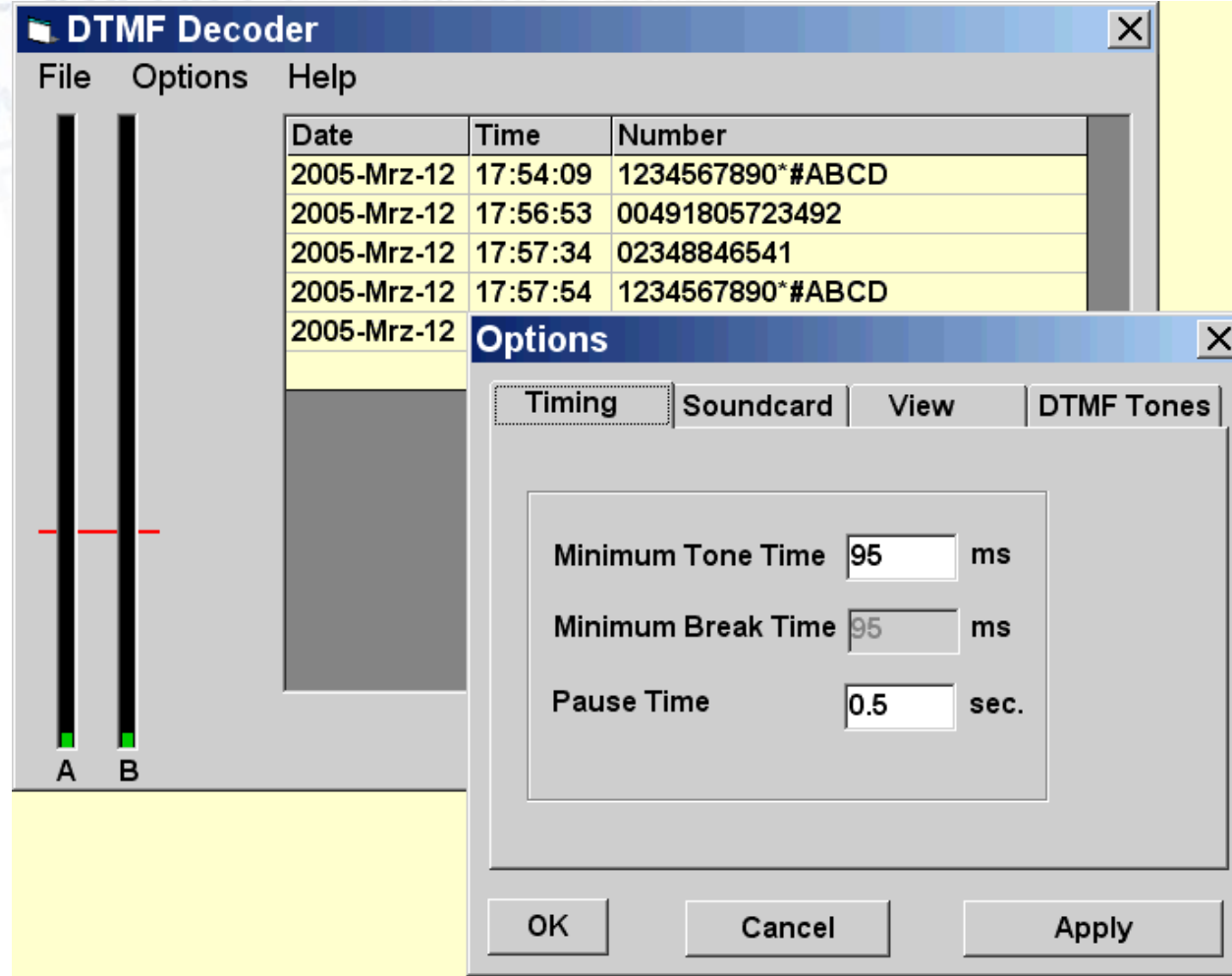
Save payload... Save as CSV... Refresh Jump to Graph Next non-Ok Close

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Call Eavesdropping (Escuta Telefônica)

Detectando dígitos



The screenshot displays a software application titled "DTMF Decoder". The main window has a menu bar with "File", "Options", and "Help". On the left, there are two vertical bars labeled "A" and "B" with a red horizontal line across them. The main area contains a table with the following data:

Date	Time	Number
2005-Mrz-12	17:54:09	1234567890*#ABCD
2005-Mrz-12	17:56:53	00491805723492
2005-Mrz-12	17:57:34	02348846541
2005-Mrz-12	17:57:54	1234567890*#ABCD
2005-Mrz-12		

An "Options" dialog box is open in the foreground, showing the "Timing" tab. It contains the following settings:

- Minimum Tone Time: 95 ms
- Minimum Break Time: 95 ms
- Pause Time: 0.5 sec.

At the bottom of the dialog are "OK", "Cancel", and "Apply" buttons.

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Fuzzing

É um método para **encontrar erros e vulnerabilidades**, através da **criação de diferentes tipos de pacotes** direcionados para o protocolo que se deseja testar, levando as especificações do protocolo ao seu ponto de quebra.

Resultados obtidos:

- Buffer Overflows
- Format String Vulnerability
- Integer Overflow
- Endless Loops and Logic Errors

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: Fuzzing

Ferramentas:

- * *Asteroid*
- * *Fuzzy Packet*
- * *Interstate Fuzzer*
- * *ohrwurm*
- * *PROTOS H.323 Fuzzer*
- * *PROTOS SIP Fuzzer*
- * *SIP Forum Test Framework (SFTF)*
- * *Sip-Proxy*

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

Ameaças: SPIT (SPAM over Internet Telephony)

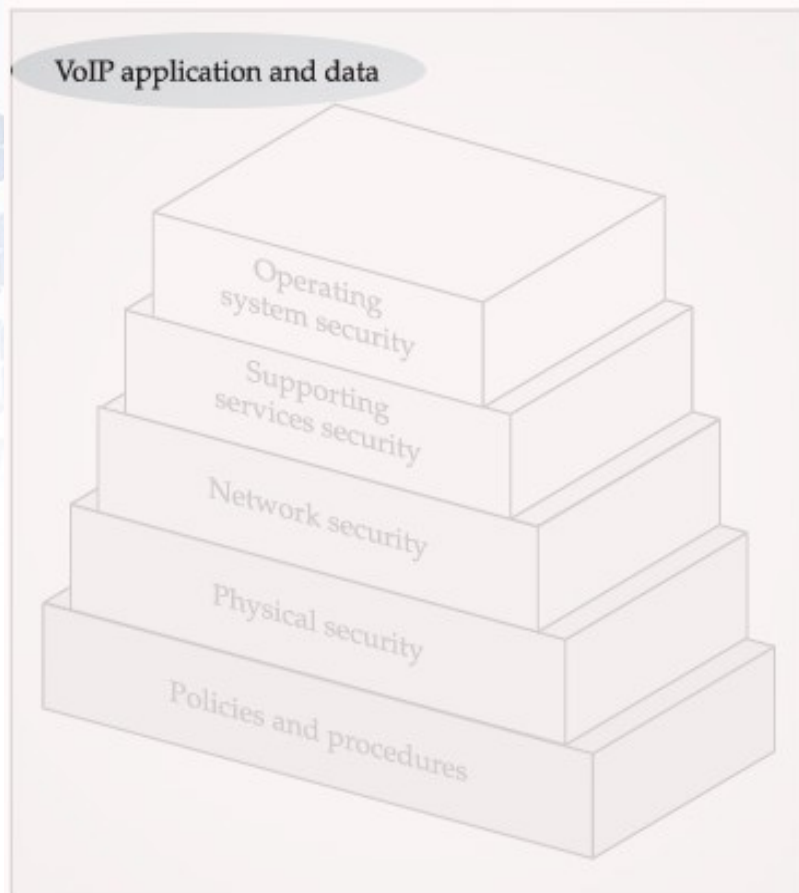
- Geração, automatizada, de chamadas não solicitadas
- Não é possível deletar a chamada (como fazemos com SPAM)

Ferramentas:

- Spitter
- TeleYapper

Ameaças: Modelo em Camada

Camada 6 - Aplicações e Dados VoIP

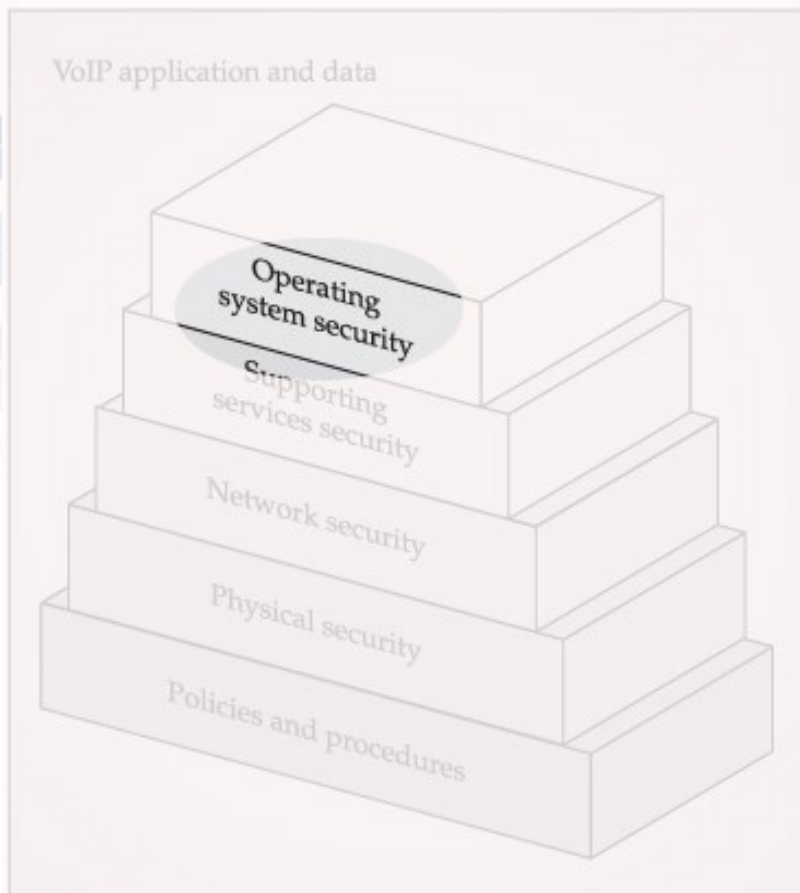


Contra-medidas

- Utilização de TCP/TLS
- Segmentação com VLAN
- Utilização de Autenticação em SIP
- Encriptação de Mídia (ZRTP/SRTP)
- Diminuição do tempo de registro
- Gerenciamento de Identidades (RFC4474)

Ameaças: Modelo em Camada

Camada 5 - Segurança no Sistema Operacional



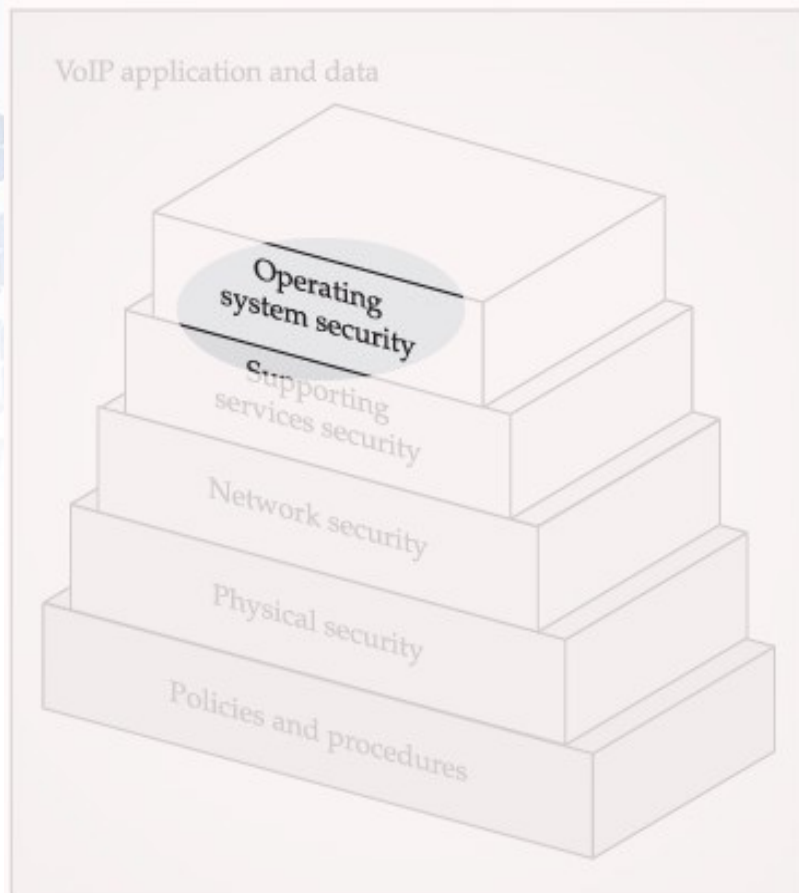
Ameaças

- Vulnerabilidades do S.O.
- Buffer Overflow;
- Virus/Worms
- Erros de configuração
- Fragmentação de Pacotes
- Exaustão de recursos

Ameaças: Modelo em Camada

Camada 5 - Segurança no Sistema Operacional

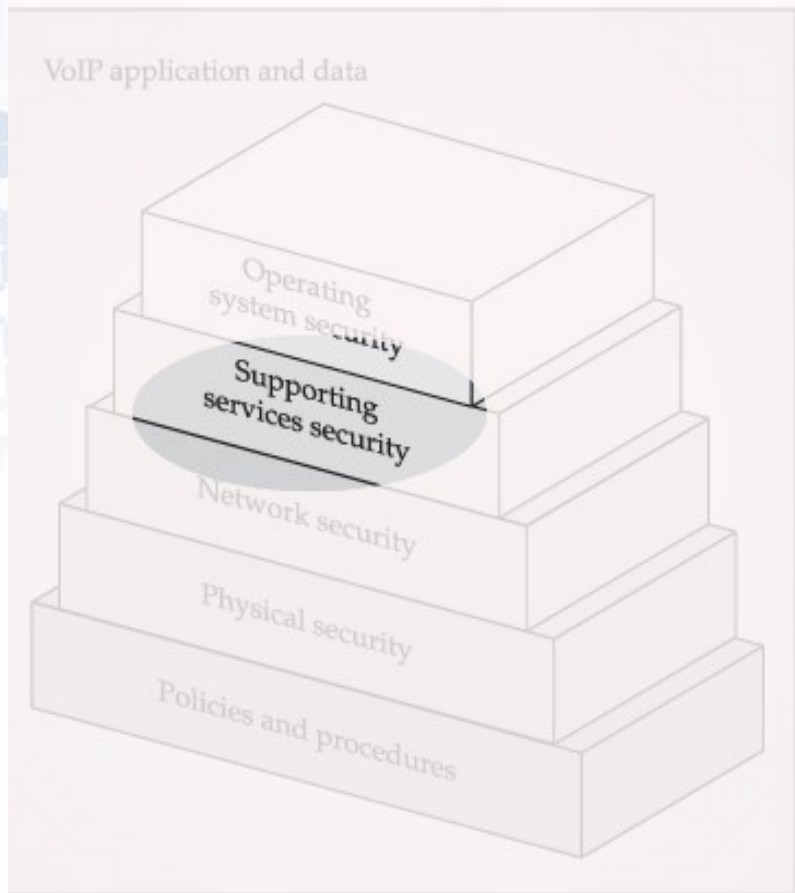
Contra-medidas



- Atualizações Contante(patches)
- Processos de hardening
- Segmentação com VLAN
- Desabilitação de serviços desnecessários;
- Utilização de equipamentos de rede capazes de minimizar ataques DoS e ter procedimentos definidos para esse ataque.

Ameaças: Modelo em Camada

Camada 4 - Segurança dos Serviços de Suporte

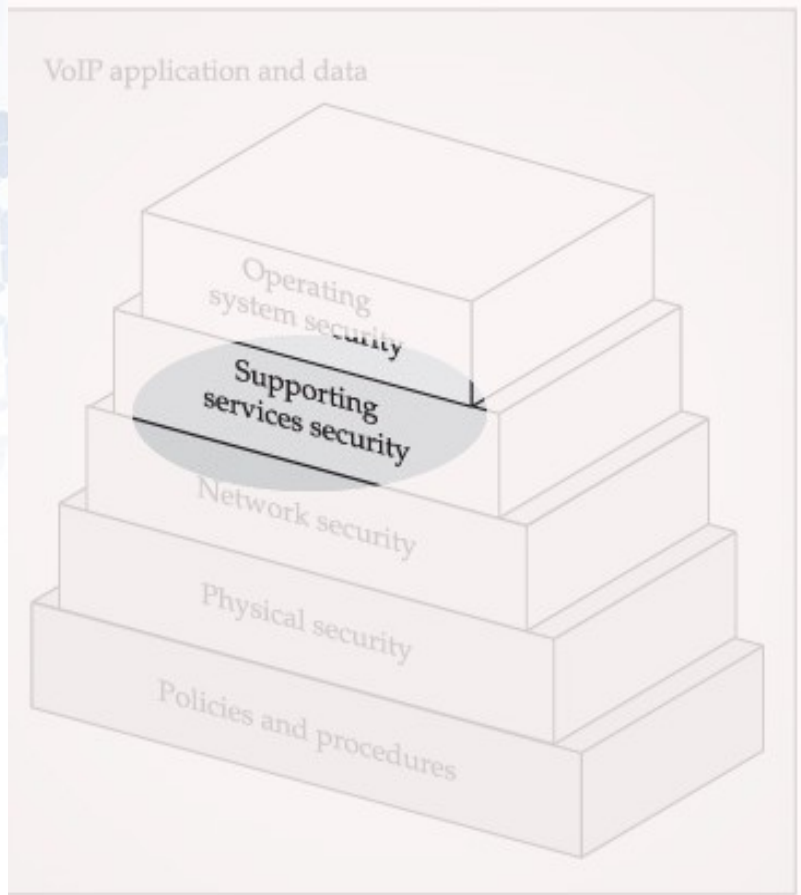


Ameaças

- Exaustão de DHCP
- Envenenamento de DNS
- DNS Flood
- MITM
- Captura de Arquivos TFTP
- Sniffing

Ameaças: Modelo em Camada

Camada 4 - Segurança dos Serviços de Suporte

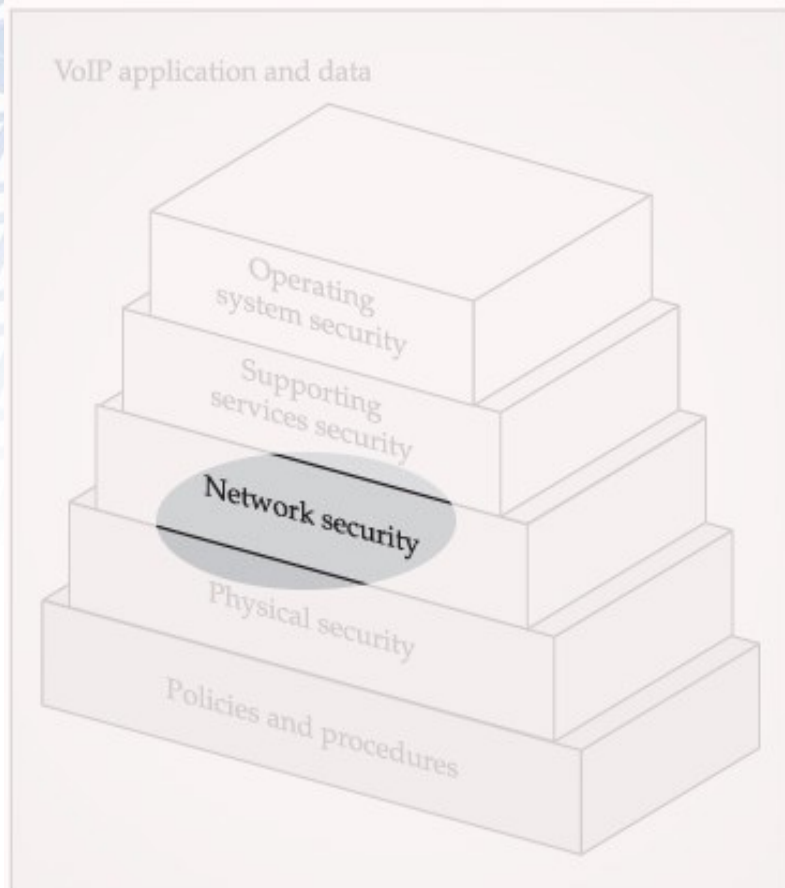


Contra-medidas

- Segmentação com VLAN
- Utilizar Https ao invés de TFTP
- Utilização de VPN

Ameaças: Modelo em Camada

Camada 3 - Segurança da Rede

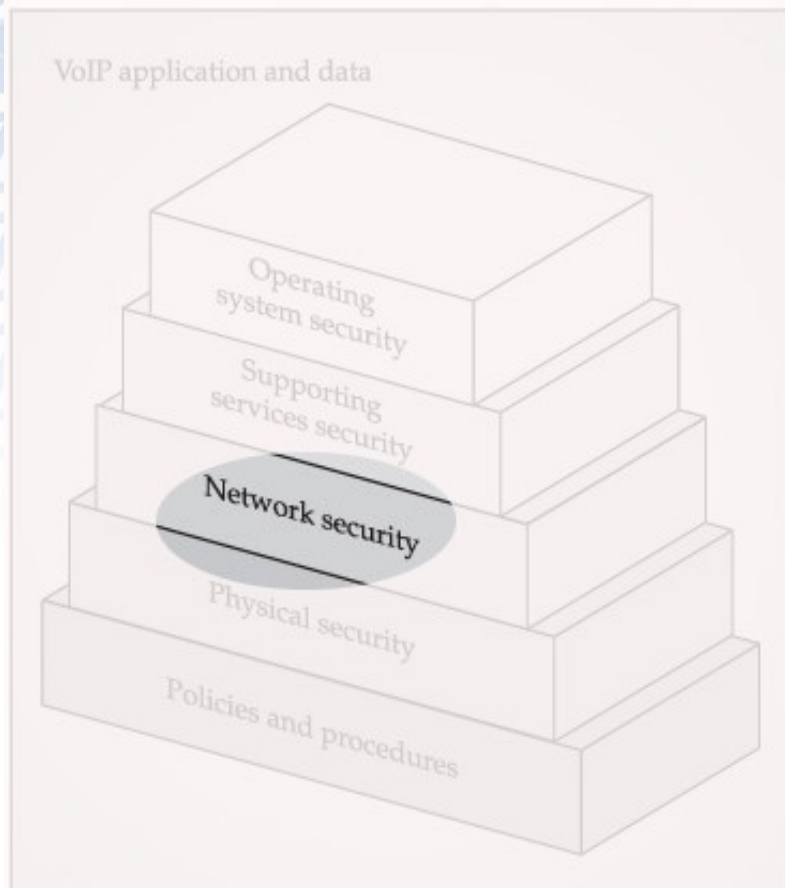


Ameaças

- Ataques de Flood: UDP Flooding, TCP SYN Flood, ICMP, Smurf Flooding.
- Modificação de QOS
- Sniffing

Ameaças: Modelo em Camada

Camada 3 - Segurança da Rede

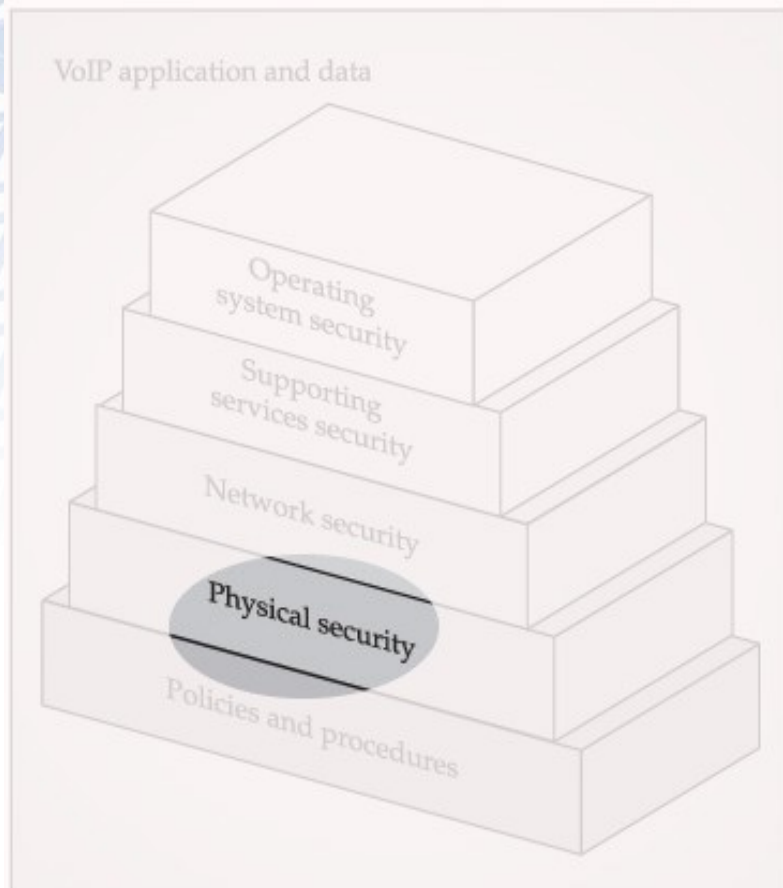


Contra-medidas

- Segmentação com VLAN
- Desabilitar envio de Broadcast roteadores de borda
- Utilização de TCP/TLS
- Utilização de VPN
- Fortificação Perímetro de rede
- Definição de procedimentos

Ameaças: Modelo em Camada

Camada 2 - Segurança Física

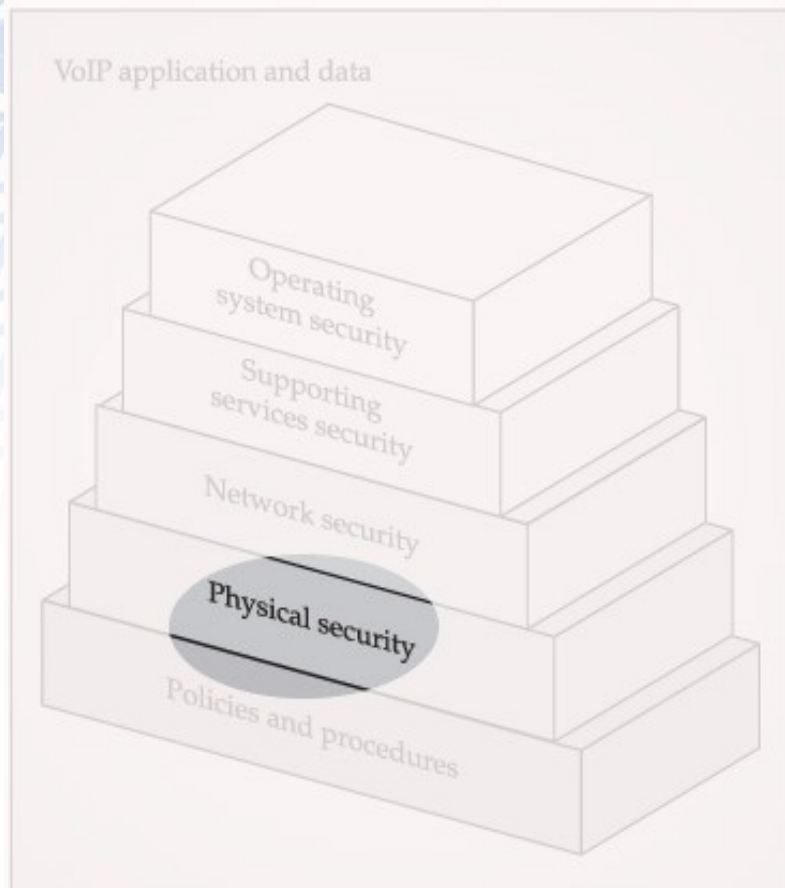


Ameaças

- Desligar / Reiniciar servidores, gateway, roteadores, switches, etc.
- Alteração de cabeamento, configuração
- Instalação de host malicioso para captura de tráfego ou exaustão de recursos

Ameaças: Modelo em Camada

Camada 2 - Segurança Física

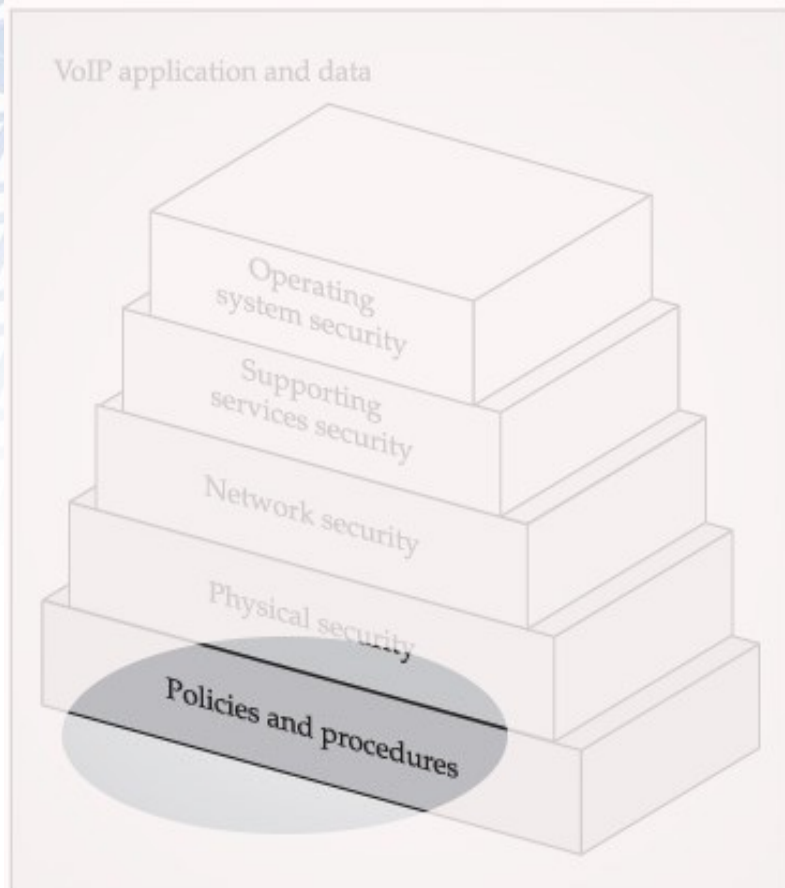


Contra-medidas

- Utilização de controles de acessos a ambientes;
- Monitoração de ambientes

Ameaças: Modelo em Camada

Camada 1 - Políticas e Procedimentos

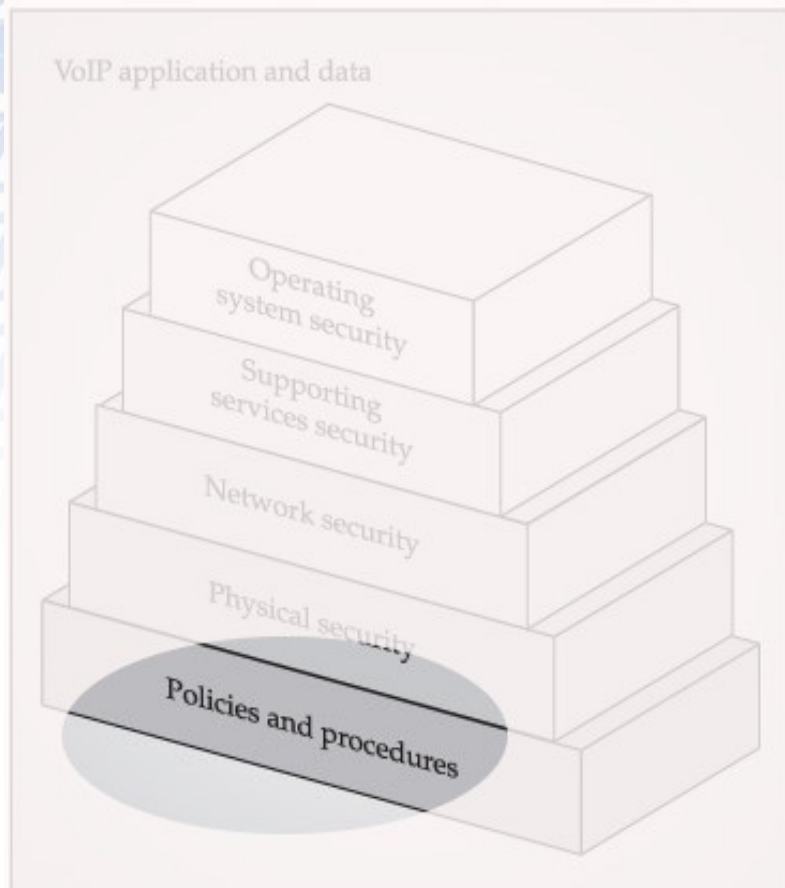


Ameaças

- Acesso a senhas de voicemail e registro de linhas SIP
- Obtenção de privilégios de discagem
- Senhas fracas (Acesso Web)

Ameaças: Modelo em Camada

Camada 1 - Políticas e Procedimentos



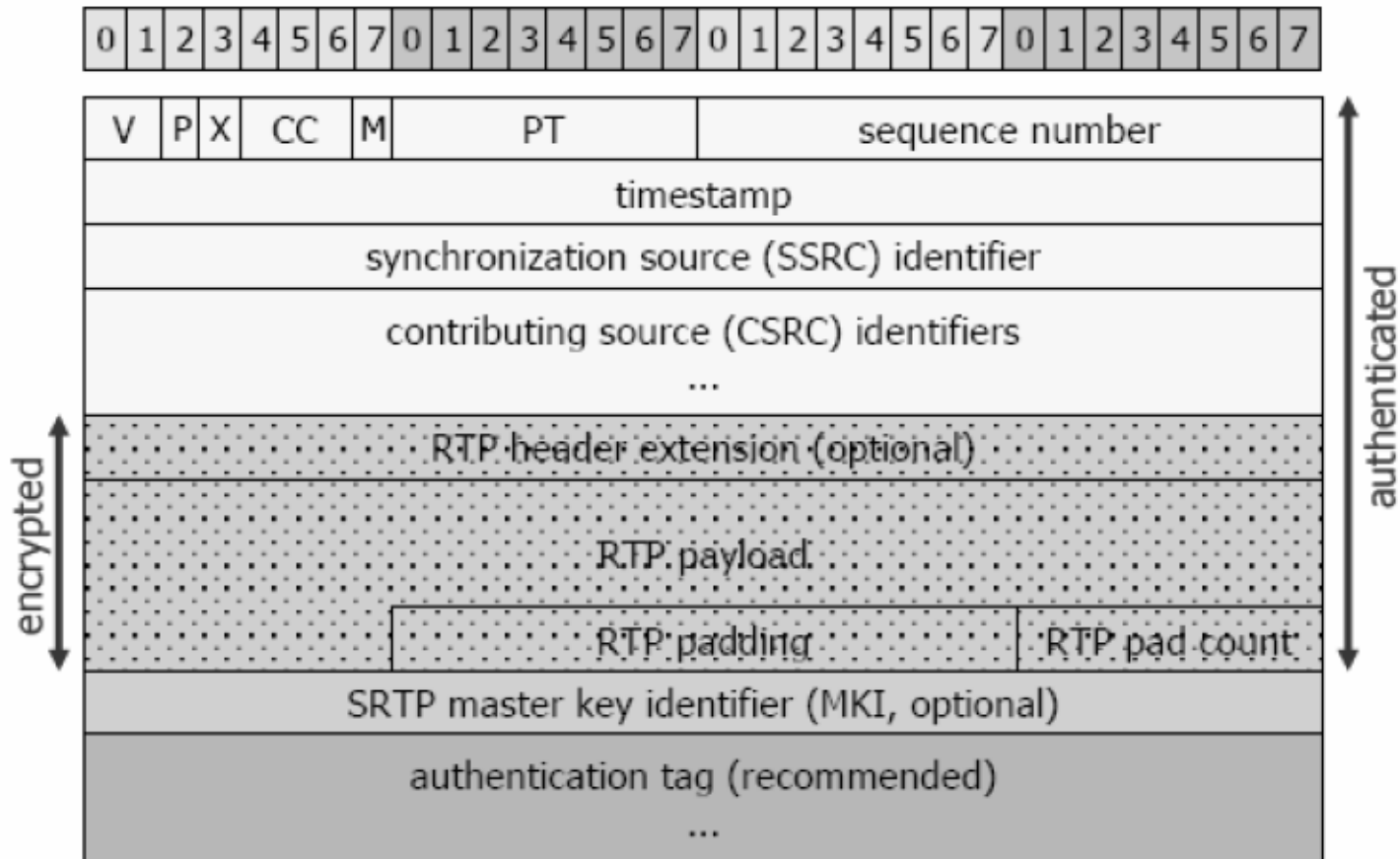
Contra-medidas

- Políticas de utilização de senha (tamanho, geração randômica/automática, encriptadas no banco)
- Disponibilização do recurso de discagem apenas para quem for necessário

Ameaças Emergentes

Esteganografia em Fluxos RTP

“Esteganografia é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra”



RTP Header

Ameaças Emergentes

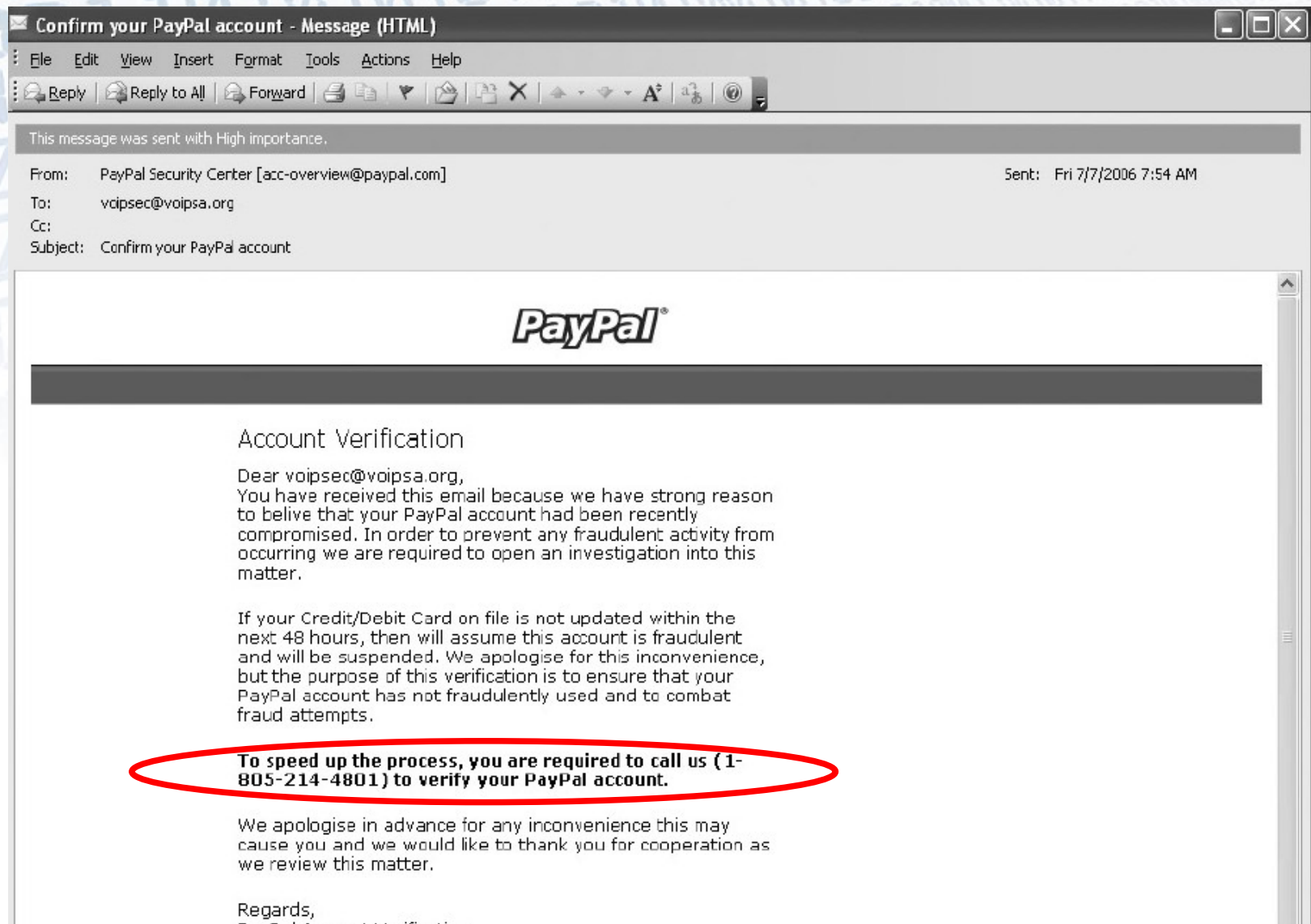
Vishing (VoIP Phishing)

“É a prática criminal de uso de Engenharia Social e VoIP para obter informações privadas, pessoais e financeiras do público com o objetivo de recompensa financeira”

- Primeiro ataque registrado: 23 de junho de 2006

Ameaças Emergentes

Vishing (VoIP Phishing)



The image shows a screenshot of a web browser window displaying a phishing email. The browser's address bar shows the title "Confirm your PayPal account - Message (HTML)". The email header includes the following information:

From: PayPal Security Center [acc-overview@paypal.com] Sent: Fri 7/7/2006 7:54 AM
To: voipsec@voipsa.org
Cc:
Subject: Confirm your PayPal account

The email body features the PayPal logo at the top. Below the logo, the text reads:

Account Verification

Dear voipsec@voipsa.org,
You have received this email because we have strong reason to believe that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then we will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently been used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,

Ameaças Emergentes

Vishing (VoIP Phishing)

Requisitos:

- x Micro convencional com o Asterisk e com IVR
- x Contratação de um número 800 de um provedor VoIP;
- x Lista de email;
- x Programa para envio do e-mail em massa.

DÚVIDAS ???



Ameaças a Tecnologia VoIP

OBRIGADO.

Frederico Madeira <fred@madeira.eng.br>

www.madeira.eng.br