

v o i p s e c

Pablo Catalina <pcatalina@s21sec.com>



Pablo Catalina

Auditor Seguridad Telemática

Grupo S21sec Gestión, S.A.

pcatalina@s21sec.com

VOIP: Características

- Un único medio independiente para todo:
 - datos: p2p, http, ftp, smtp, ...
 - voz: streams, voip, ...
 - vídeo: streams, voip, ...
- Control del tráfico
- Negociación por parte del cliente
- Deslocalización
- Varios canales duplex
- Estados y presencia

VOIP: Desventajas

- Seguridad:
 - Un único medio: Sniff, MiTM, DoS, DDoS
- Costes:
 - Es necesario tener acceso a una red de datos
- Calidad del servicio garantizada
 - QoS, RSVP, 802.11q, ...

VOIP: ¿Cómo funciona?

- Arquitectura de red
- Protocolos de Señalización
 - Inicio, fin y cambios de sesión
 - Negociación de la sesión
 - Localización
 - Aceptar, rechazar, añadir, desviar llamadas
- Transporte de datos
 - Codificación de voz
 - Codificación de vídeo
 - Envío de texto y datos

VOIP: Arquitectura

- Terminales:
 - Clientes por software o hardware
- Gatekeeper:
 - PBX por software
- Gateway:
 - Pasarelas entre tecnologías (A/D)

VOIP: Señalización

- Protocolos:
 - H.323, SIP, IAX, IAX2
- Parámetros:
 - Clientes: Origen, destino
 - Control:
 - Registro
 - Control de estado
 - Llamada: aceptar, espera, rechazar, agregar, transferir
 - Detección y corrección de errores
 - Tipo de datos y codecs
 - Localización

VOIP: Codificación

- Audio:
 - G711 ulaw, alaw
 - GSM
 - G729
 - Speex
 - adpcm
- Vídeo:
 - H.261
- Datos:
 - Texto: Jabber, XML
 - S/MIME



VOIP: Hackin' it

- Arquitectura de red:
 - Capas 1, 2 y 3 del modelo OSI:
 - MiTM
 - Sniffing
 - MAC e IP Spoofing
 - DoS y DdoS
 - TCP-Reset
 - Exploits
 - 802.11q
 - STP Root
 - MAC Flooding
 - ICMP Err y TCP/RST
 - ...

VOIP: Hackin' it

- Arquitectura de red VoIP:
 - Spoofing Identities:
 - Call Hijacking
 - Modificación de parámetros de señalización
 - Rechazo de llamadas
 - Integridad y autorización
 - DoS y DDoS:
 - Consumo de CPU
 - Consumo de Memoria
 - Consumo de almacenamiento
 - Modificaciones de Terminal:
 - Firmware y actualizaciones modificables
 - Backdoors, troyans.

VOIP: Hackin' it

- Trasmisión de datos
 - Escucha de conversaciones
 - Call Spoofing

Escenografía

- PBX IP:
 - Asterisk: <http://www.asterisk.org/>
- Voip Tests:
 - PROTOS: <http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/>
 - SIP Forum Test Framework: <http://www.sipfoundry.org/sftf/>
- CALL Detection:
 - VOIPONG: <http://www.enderunix.org/voipong/>
- Información:
 - SIP: <http://www.packetizer.com/voip/sip>
 - H.323: <http://www.packetizer.com/voip/h323>
 - <http://www.voipsa.org/Resources/>
 - <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt>

Agradecimientos

Pablo Catalina <pcatalina@s21sec.com>



- Grupo S21SEC
Gestión, S.A.

<http://www.s21sec.com>

- SysnetWorks

<http://www.sysnetworks.net/>