^безопасность VOIP

“I just called to say I pwn you
I just called to say how much I care
I just called to say I own you
And I mean it from the bottom of my heart”

POSITIVE TECHNOLOGIES

ggritsai@ptsecurity.ru

План

О VOIP

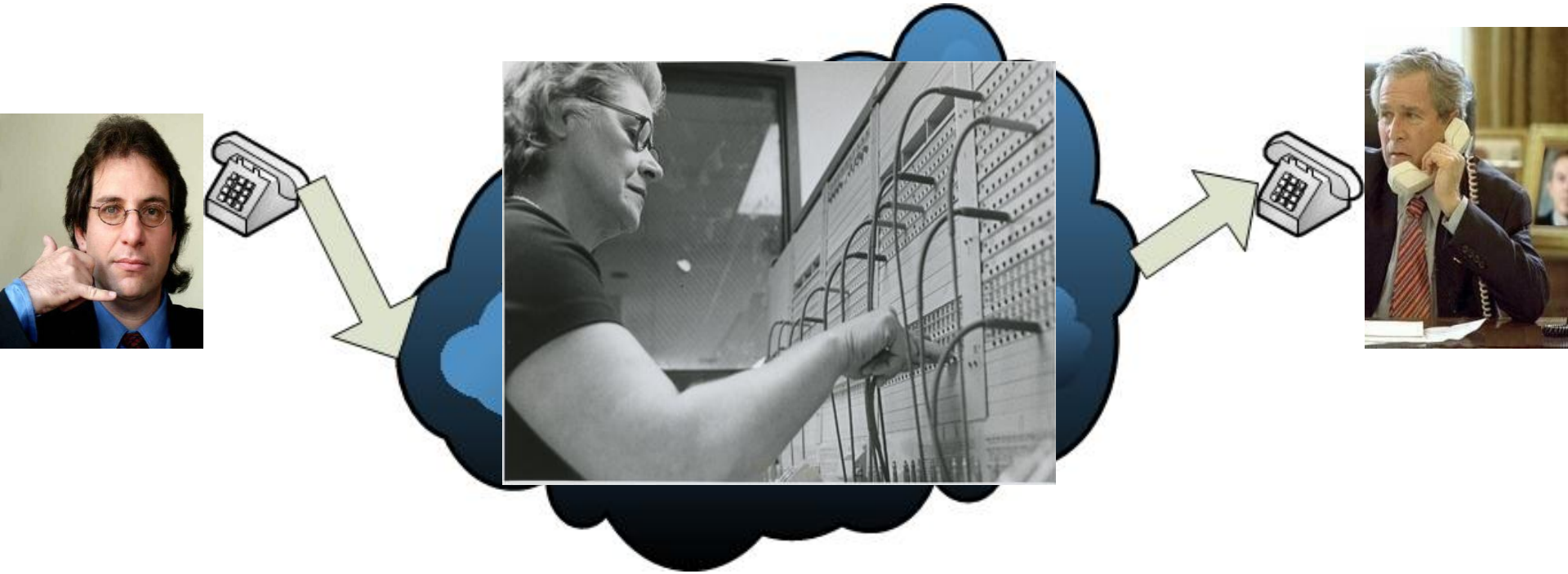
- **PSTN & VOIP**
- **PSTN vs. VOIP**
- **Безопасность VOIP**

Атаки на VOIP

- **Обнаружение / recon**
- **RTP**
- **SIP**

PSTN / Public switched telephone network

PSTN - Телефонная сеть общего пользования



VOIP / Voice over Internet Protocol

VOIP

PSTN vs. VOIP

Среда передачи данных

- **PSTN – Закрытая сеть**
- **VOIP – Открытая сеть – Интернет**

Конечные устройства

- **PSTN – Простые устройства – Ограниченный функционал**
- **VOIP – Сложные устройства**

Идентификация (Аутентификация)

- **PSTN – Отсутствие мобильности – Идентификация осуществляется по физическому каналу**
- **VOIP – Мобильность**

Проблемы безопасности VOIP

Конфиденциальность

- **перехват/запись звонков**

Доступность

- **DoS**

Аутентичность

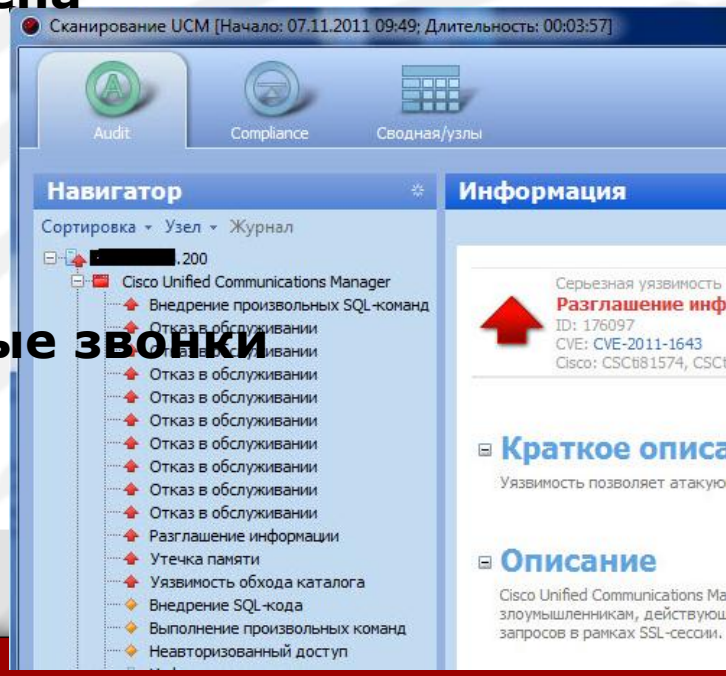
- **перехват регистрации, подмена Caller ID**

Хищения

- **toll fraud**

SPIT (SPAM over IP Telephony)

- **voice phishing, нежелательные звонки**



POSITIVE TECHNOLOGIES

Проблемы безопасности VOIP
Обсуждаем сегодня

Поиск VOIP устройств

- **поиск в открытых источниках**
- **использование порт сканеров**

Протокол RTP

- **перехват/запись звонков**
- **внедрение потока в звонок**
- **DoS**

Протокол SIP

- **ищем телефонные номера**
- **SIP digest**
- **подмена Caller id + DoS**

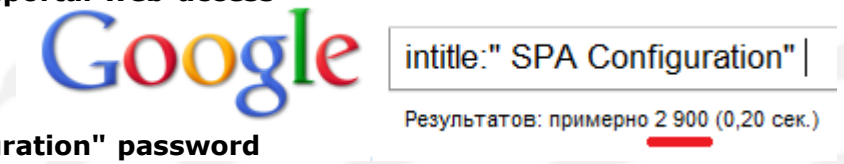
Поиск VOIP устройств
Google hacking

Google hacking

- GHDB
- User manual -> запрос Google
  - inurl:
  - intitle:
  - site:<Customer> !

Примеры:

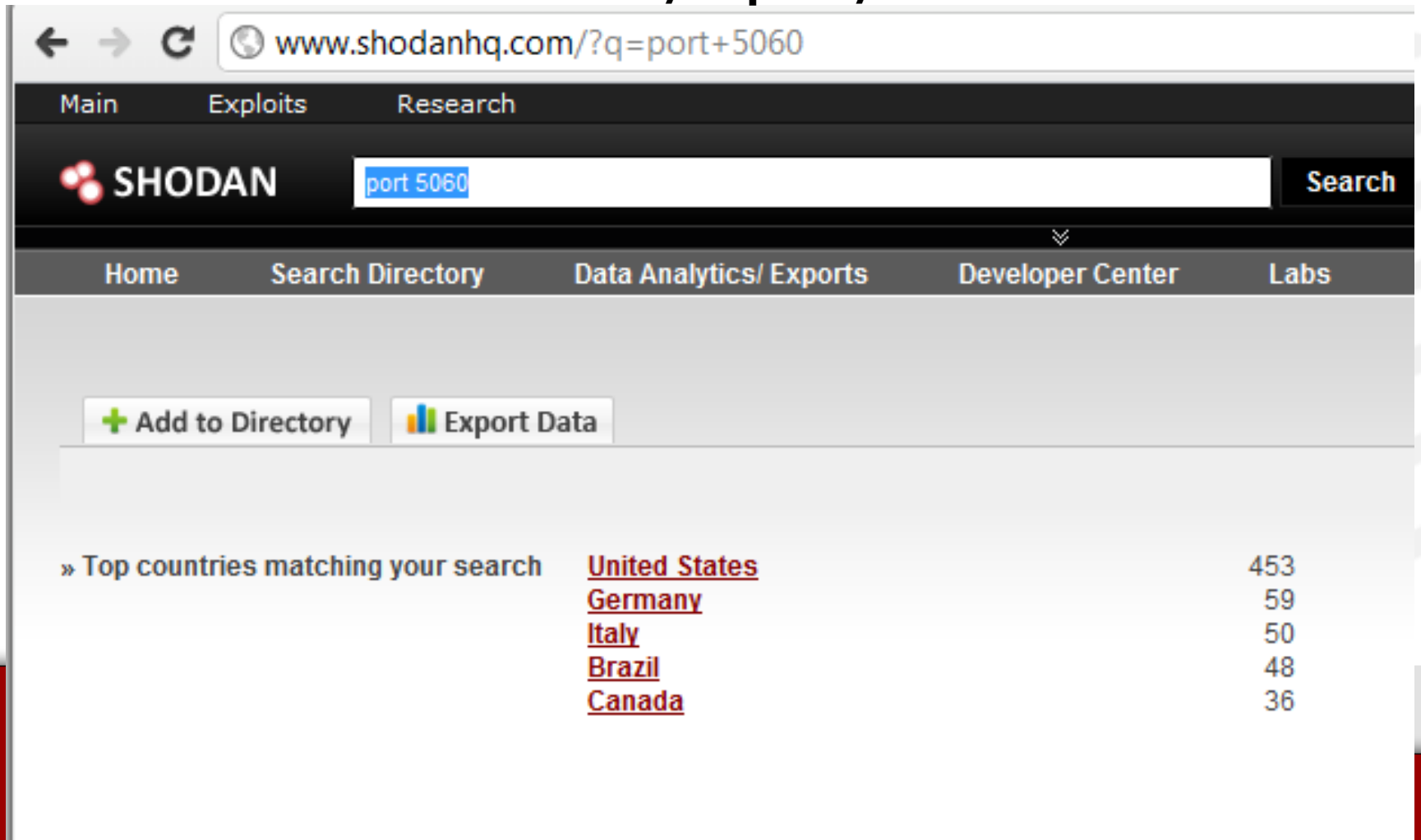
Asterisk Management Portal: intitle:asterisk.management.portal web-access
Cisco Phones: inurl:"NetworkConfiguration" cisco
Cisco CallManager: inurl:"ccmuser/logon.asp"
D-Link Phones: intitle:"D-Link DPH" "web login setting"
Grandstream Phones: intitle:"Grandstream Device Configuration" password
Linksys (Sipura) Phones: intitle:" SPA Configuration"
Polycom Soundpoint Phones: intitle:"SoundPoint IP Configuration"



Поиск VOIP устройств
Shodan [1/2]

www.shodanhq.com

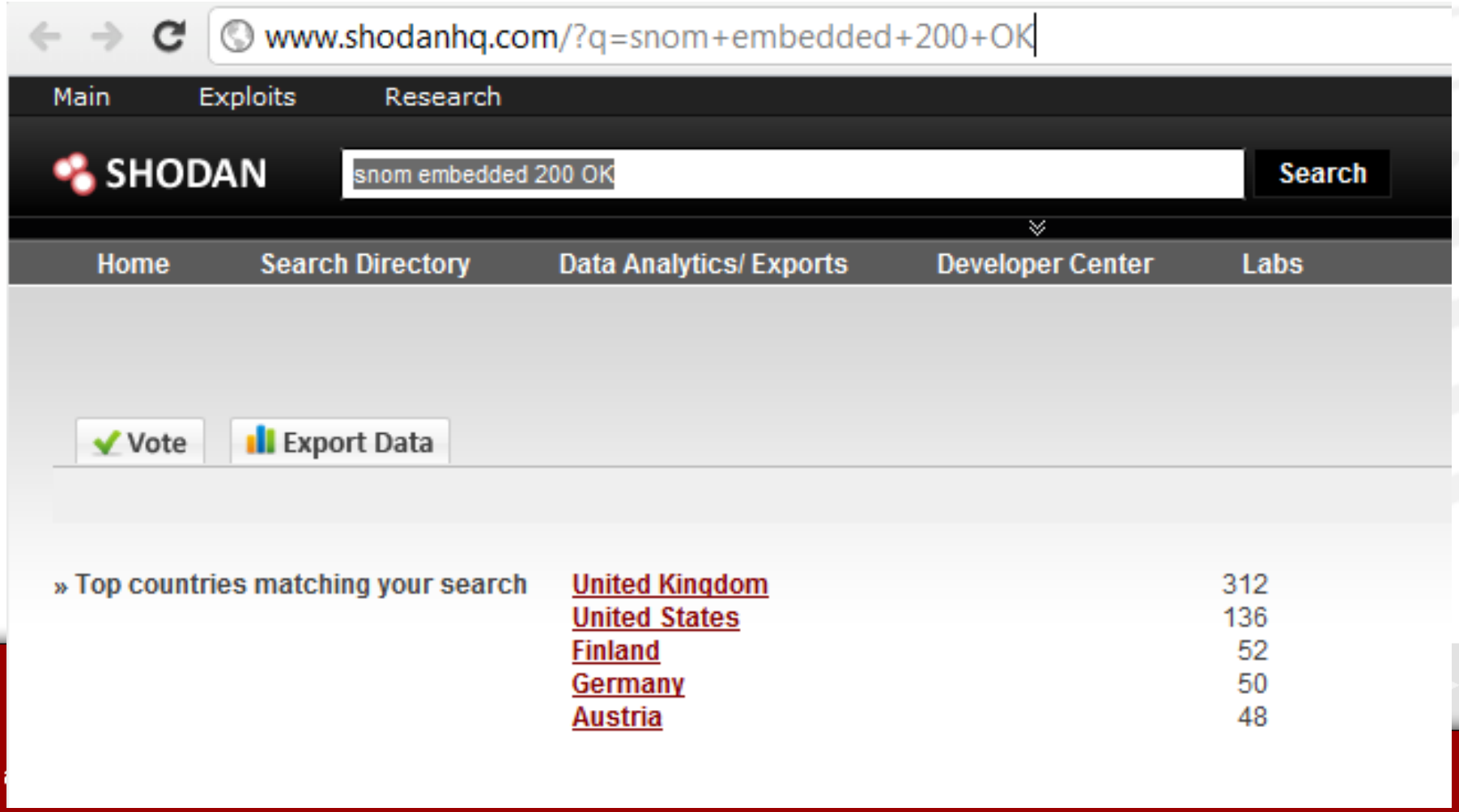
- **поиск по хостам/портам/etc в сети**



Поиск VOIP устройств
Shodan [2/2]

shodanhq индексирует баннеры сервисов

- **поиск телефонов Snom без паролей**



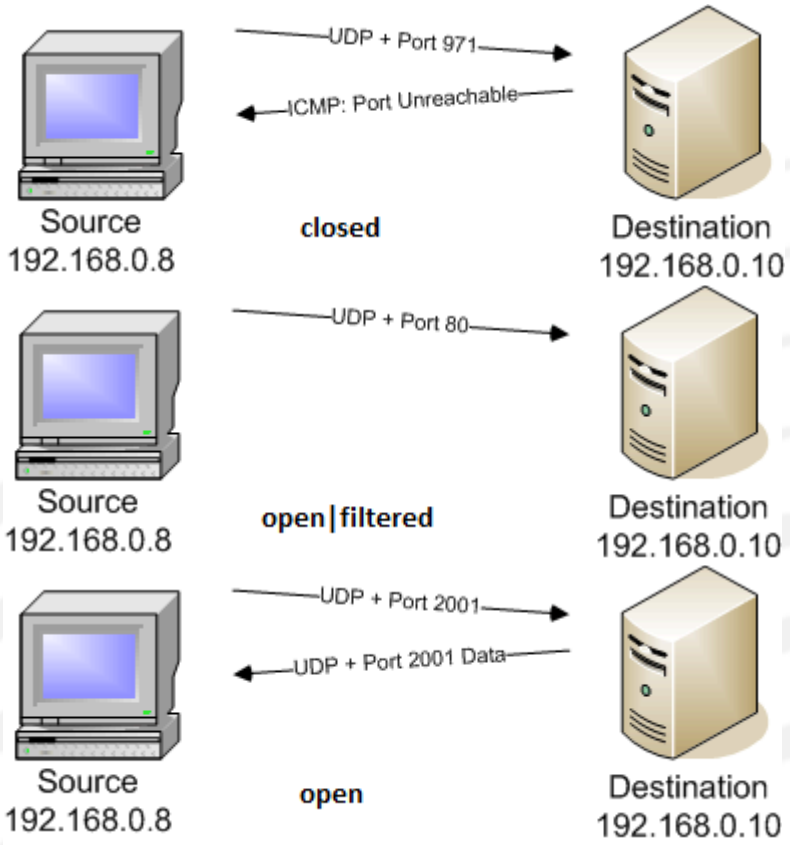
Поиск VOIP устройств
nmap

Специализированные VOIP сканеры

- **smap**
- **svmap (sipvicious)**

Fyodor's nmap

- **-sU**
  - **Проблемы сканирования UDP**



Поиск VOIP устройств
Распространенные порты

VOIP протоколы

- **5060-5070, 1718-1720, 2517, ….**
- **RTP порты выделяются динамически**

Протоколы управления (вектор вне контекста)

- **TCP 21-23, 80, 443, 8088, …**
- **UDP 161, 162, 69, …**

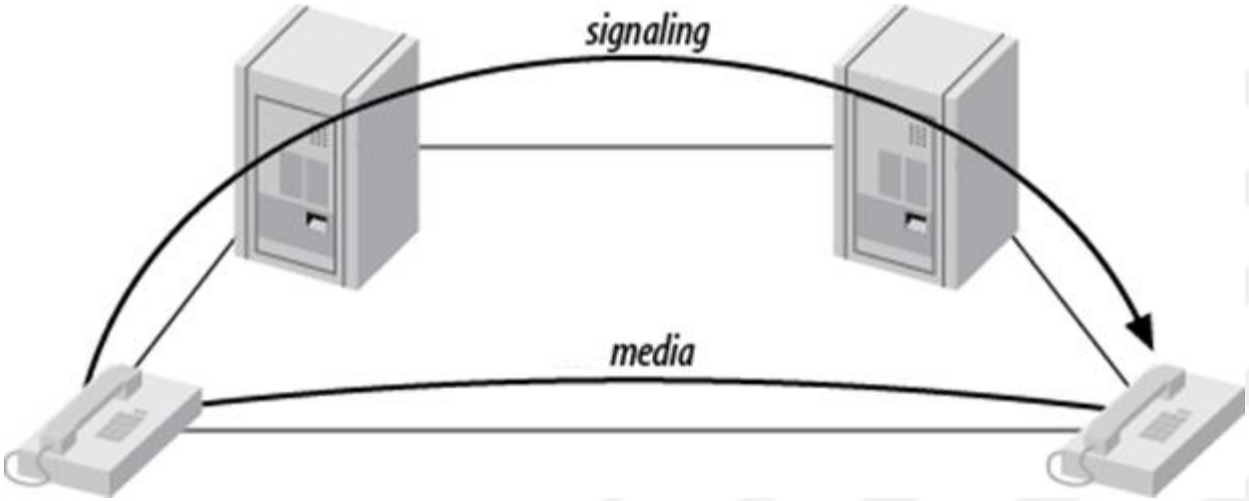
IANA

- **Internet Assigned Numbers Authority**
- **grep <vendor> www.iana.org/assignments/port-numbers**

SIP/RTP signaling/media

Signaling **Сигнальные протоколы**

Media **Потоковые протоколы**



Установка соединения и передача потоковых данных происходит по разным маршрутам

RTP

Real-time Transport Protocol

- RFC 1889 (1996) заменен на RFC 3550 (2003)
- Передача мультимедийных потоков через IP/UDP
- Переупорядочивание пакетов
- Пересылка времени отправителя получателю
- Используется с сигнальными протоколами (SIP, H.323, MGCP)

RTCP (Real-time Transport Control Protocol)

- RTP (обычно) использует четный порт, RTCP использует RTP port + 1

RTP Атаки

Перехват сессии

- **Атакуем уровни < UDP**
- **Декодируем перехваченную информацию**

Внедрение трафика

- **Ищем RTP порт**
- **Внедряем медиа поток**

Отказ в обслуживании

- **Флудим RTP**

RTP Атаки
Перехват сессии

ARP spoofing

- **Cain & abel**
- **ettercap**
- **arpspoof (dsniff)**

Wireshark

- **Telephony**
- **VOIP calls**

RTP Атаки
Внедрение трафика

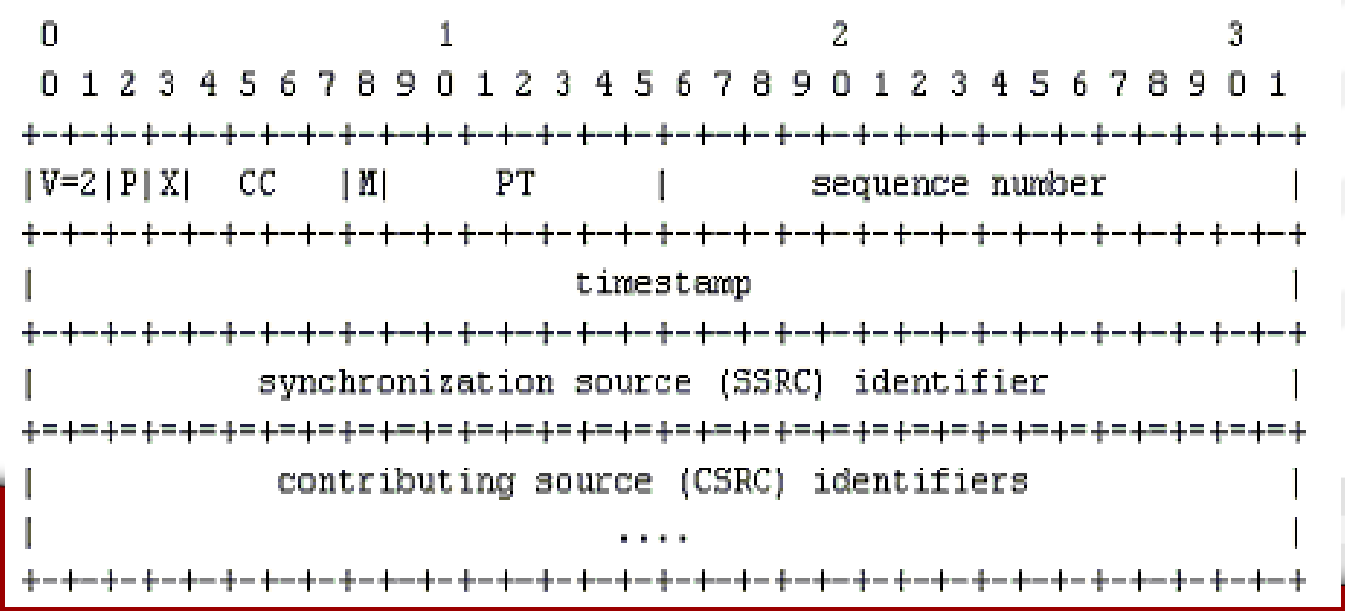
Отсутствие шифрования

- **сложность настройки (отладки)**
- **нагрузка на канал – качество потока**
- **ключи plain text**

UDP – нет установки соединения

RTP Атаки
Внедрение трафика: Синхронизация

sequence number	**позиция в медиа потоке**	**+=1**
timestamp	**воспроизведение потока (сэпмлинг)**	**+=1**
SSRC	**идентификация отправителя (32 битное случайное число)**	**const**
payload type	**используемый кодек**	



RTP Атаки
Внедрение трафика

Мониторинг/что нужно перехватить

- **SSRC – константа**
- **timestamp, sequence number – монотонно возрастающие**
- **timestamp, sequence number можно фаззить**

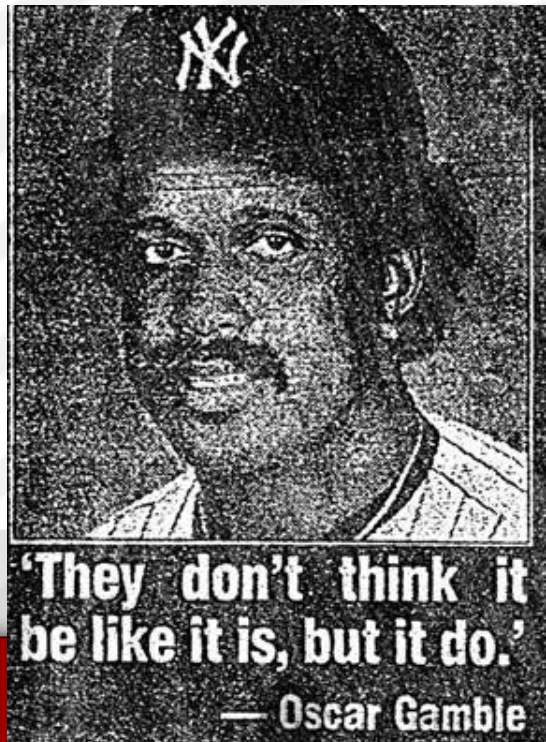
Поиск RTP порта

- **Перехватываем SDP**
- **Сканируем порты**

Внедряем данные

- **Срабатывание != 100%**
- **Готовим данные для внедрения**
  - **Частота**
  - **Кодек**

video



RTP Атаки
Отказ в обслуживании

Флуд

- **Низкие требования к нагрузке канала**
- **Медиа поток - вычислительные мощности**
- **UDP - нет установки соединения**

SIP

Session Initiation Protocol

Application layer (TCP/UDP)

ASCII сообщения

Заголовок SIP ~= Заголовок e-mail

Сообщение

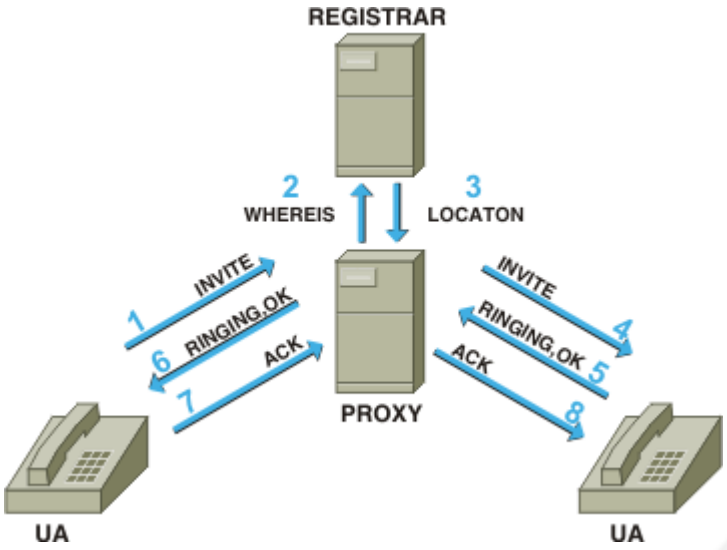
- **URI**

```
Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-154271288;rport
Content-Length: 0
From: "6070"<sip:6070@192.168.131.141>; tag=3630373001343231303631333632 39
Accept: application/sdp
User-Agent: friendly-scanner
To: "6070"<sip:6070@192.168.131.141>
Contact: sip:6070@192.168.131.141
CSeq: 1 INVITE
Call-ID: 3459752419
Max-Forwards: 70
```

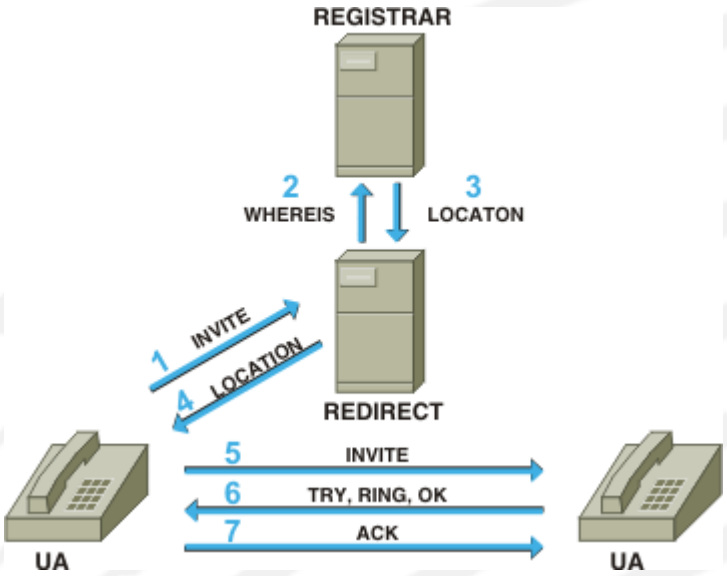
SIP Компоненты

UA (User agent), Proxy, Registrar, Redirect

Звонок через Proxy



Звонок через Redirect

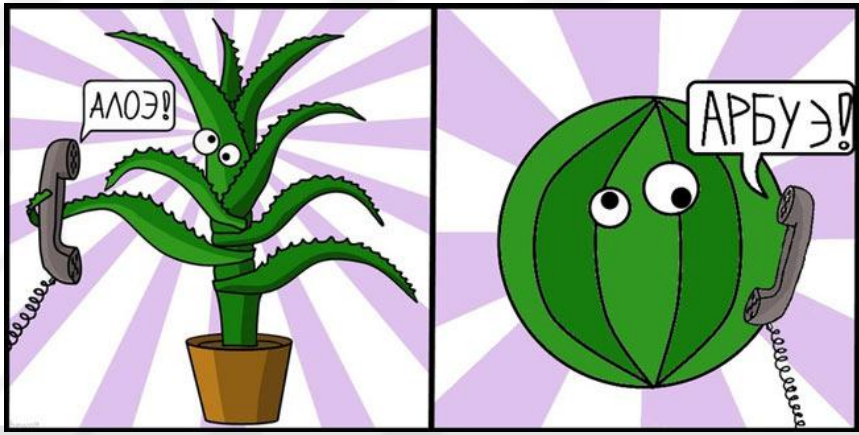


SIP Атаки

Звоним через PBX по соседству

Ломаем SIP digest

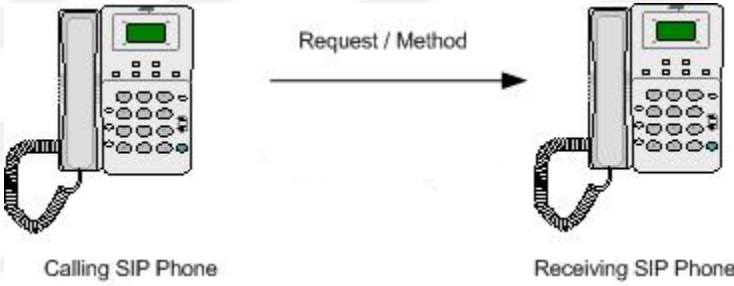
Подмена Caller id + Отказ в обслуживании



SIP Запросы

INVITE	**инициализация звонка**
BYE	**завершение соединения**
OPTIONS	**типы SIP сообщений и кодеки**
REGISTER	**регистрация пользователя**
ACK	**подтверждение INVITE-а**
CANCEL	**завершение неустановленных соединений**

другие



SIP Ответы

1xx Informational (100 Trying, 180 Ringing)

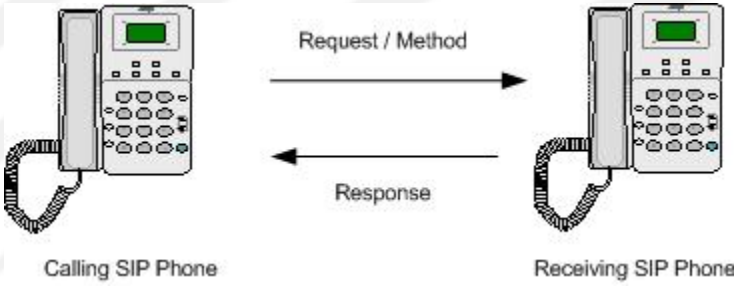
2xx Successful (200 OK, 202 Accepted)

3xx Redirection (302 Moved Temporarily)

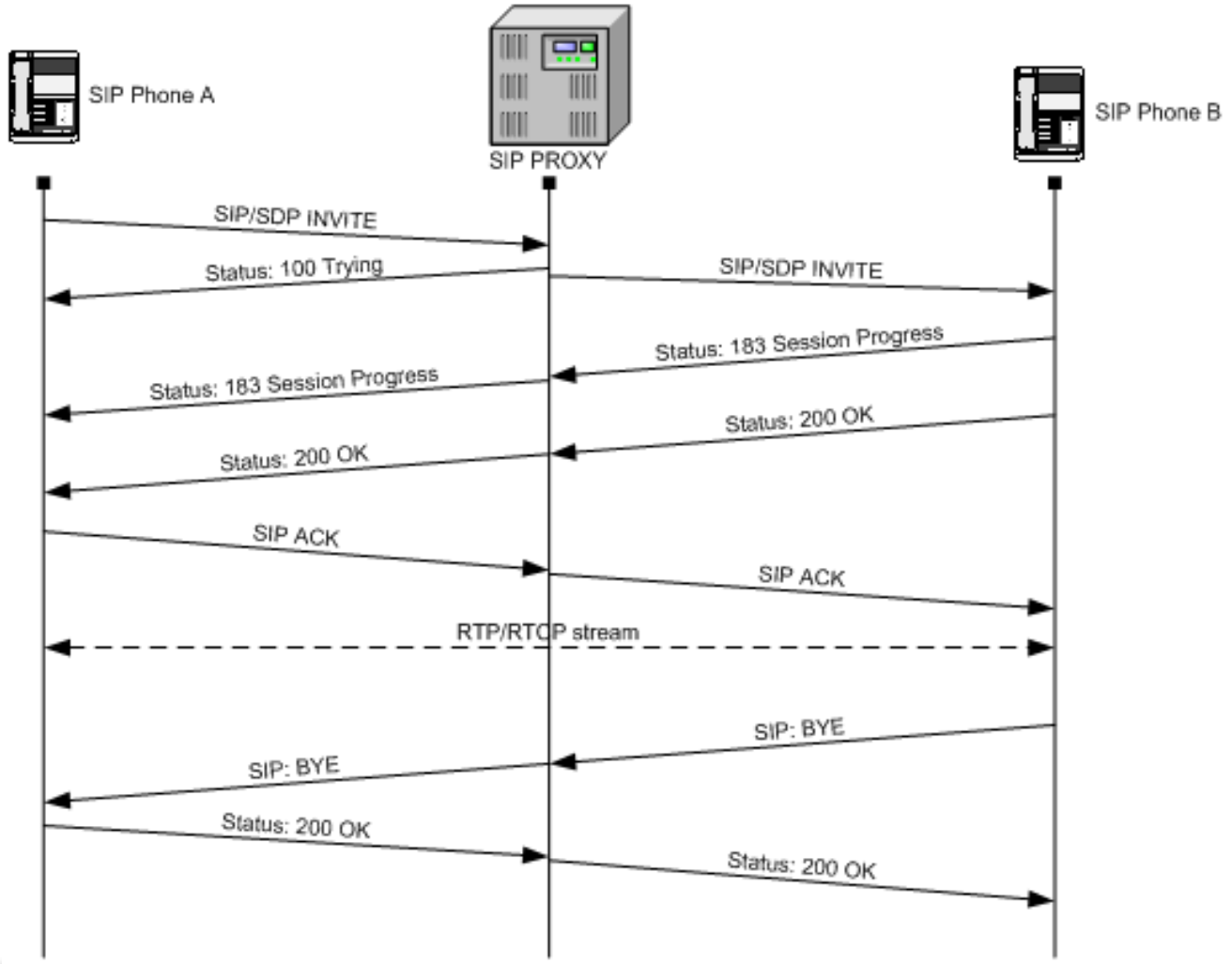
4xx Request Failure (404 Not Found, 482 Loop Detected)

5xx Server Failure (501 Not Implemented)

6xx Global Failure (603 Decline)



SIP соединение



Звоним через PBX по соседству

- Ищем extension-ы
- Брутим пароли
- Совершаем звонок

video

SIP Атаки
SIP digest

SIP digest authentication (= HTTP digest)

- **Сервер генерирует digest challenge**
- **Клиент отвечает digest response-ом**

Digest leak

- **INVITE -> phone**
- **phone: pick up + hang up**
- **BYE <- phone**
- **407 + challenge -> phone**
- **phone отвечает response-ом**
- **offline взлом**

video

SIP Атаки
Подмена Caller id + Отказ в обслуживании

Подмена Caller id

- **Поле From в заголовке INVITE запроса**

Отказ в обслуживании

- **Без аутентификации**
  - **-> INVITE**
  - **<- TRYING … <- Busy here**
- **HTTP digest**
  - **-> INVITE**
  - **Генерация и хранение nonce**

video

Материалы для дальнейшего изучения

- **Подготовить лабораторию**
  - **http://enablesecurity.com/resources/how-to-set-up-a-voip-lab-on-a-shoe-string/**
- **Читать книгу и экспериментировать**
  - **Hacking Exposed VoIP—Voice Over IP Security Secrets & Solutions**
- **Разбираться с более сложными и современными атаками**
  - **“Having fun with RTP” by kapejod**
  - **“SIP home gateways under fire” by Anhängte Dateien**
- **Fuzzing**
  - **Awesome asterisk on PROTOS**

QA