VoIP Security

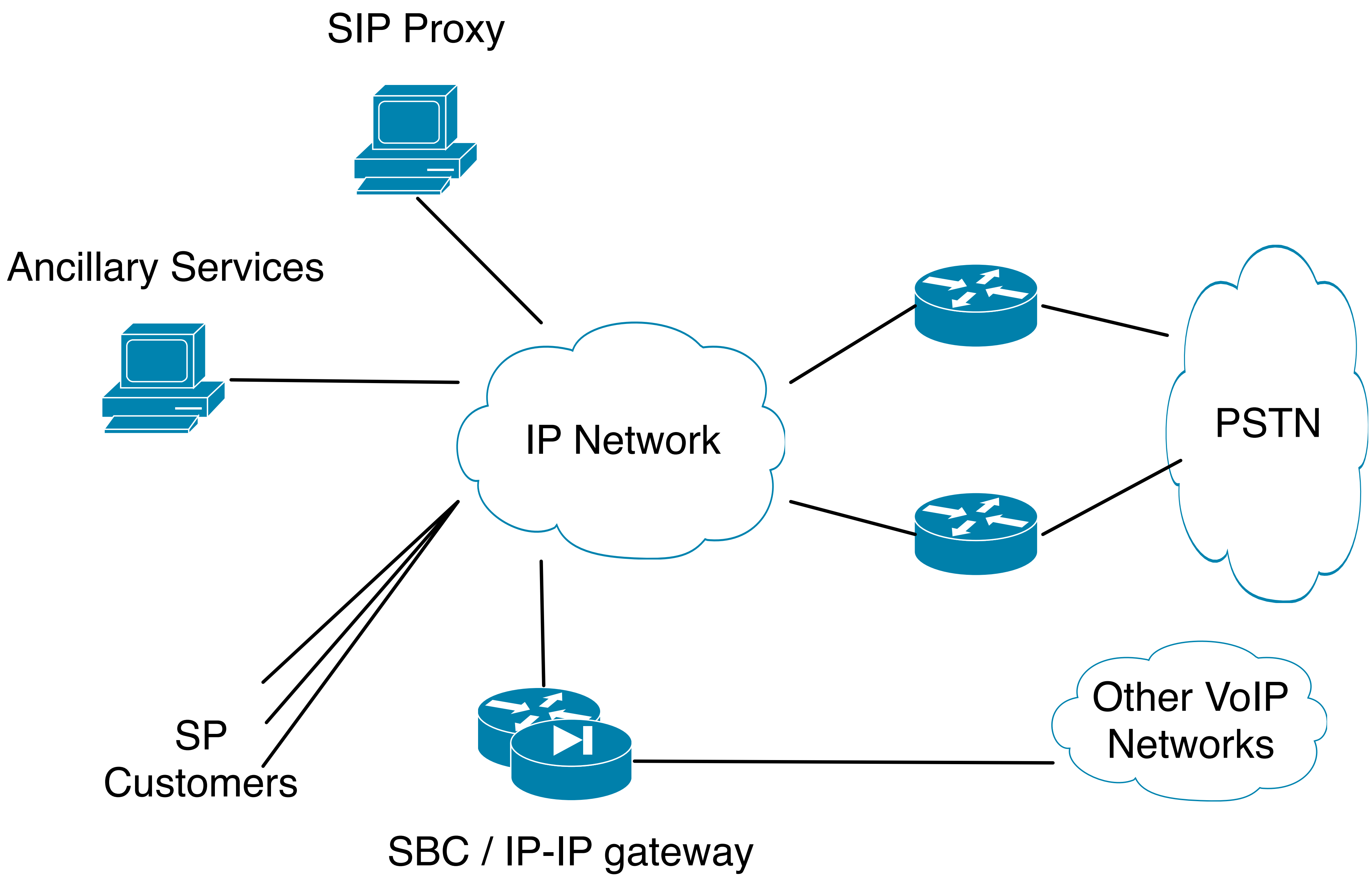
APRICOT 2009
Manila, February 2009

Jonny Martin - jonny@jonnynet.net

VoIP Security

- A specialised security field
- We’ll look at just one particular issue
- It has cost many operators and users a lot of money
  - Including me :(
- We’re going to look at war-dialing and rogue VoIP calls out gateways
  - Calls we don’t expect or know about that are accepted
- And how to secure things

Example SP VoIP Network



Network roles

- Gateways - provide access from VoIP domain to other networks, either PSTN or VoIP
  - TDM interfaces to get to PSTN
  - Session Border Controller (SBC) / IP-IP Gateway to get to other IP networks
- Central SIP Proxy - provides call control for entire network
- Ancillary Services Server - voicemail, etc.

VoIP Attacks

- Motivation --> $$$ for hax0r
- If you are running a VoIP network on the public internet, attackers will probe it
- If you have high-value routes available via your network, attackers will eventually find them. And use them.
    - Cuba, Pacific Islands, Mobile phones in many countries, 1-900, Iridium
    - Easily $1 - $2 per minute (pick your currency)
- These routes are likely to be via one of your upstreams. And cost you a lot.

Attack Business Model

1. Attacker uses you directly as an outbound gateway for their business

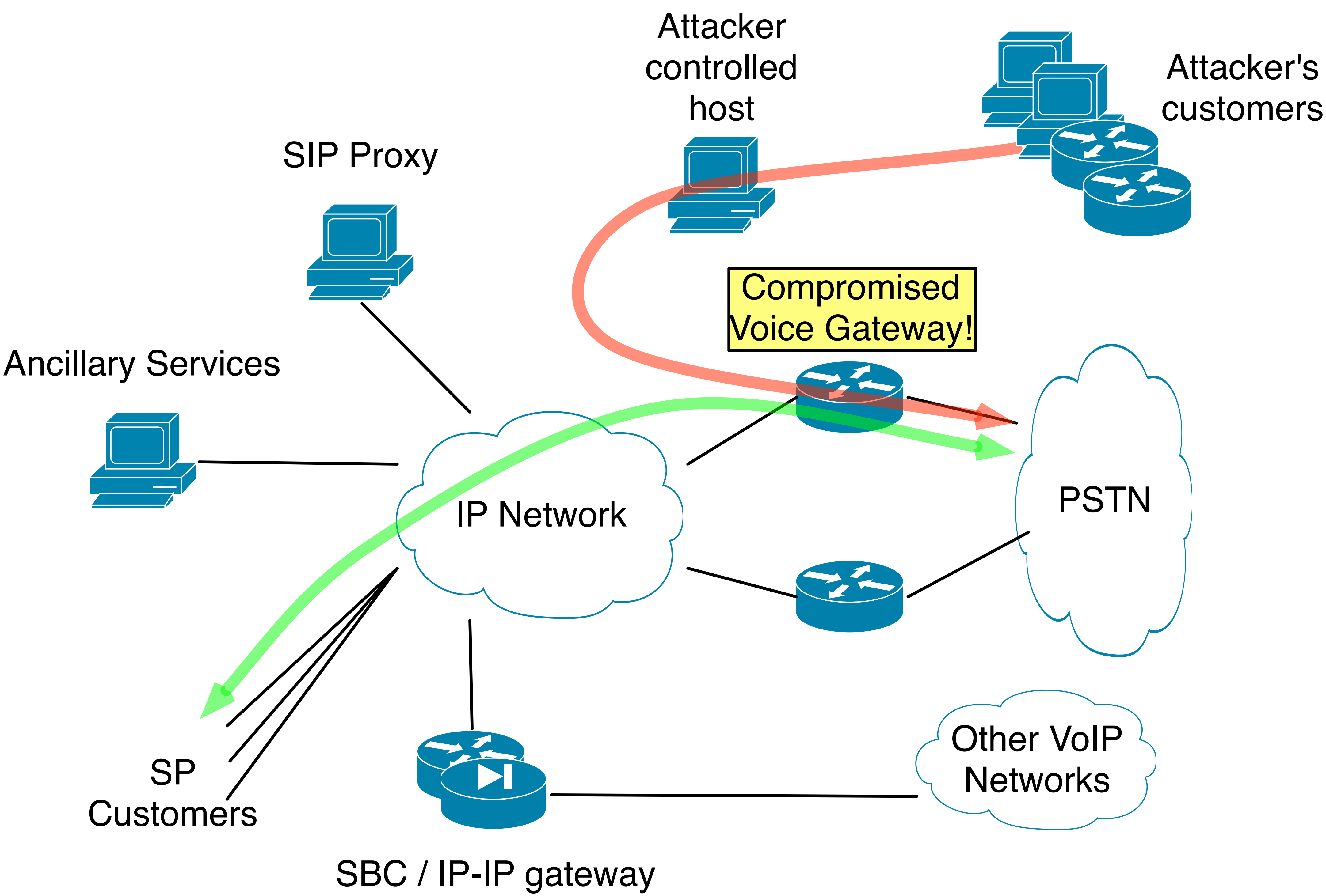
    - Somewhat risky, as presumably the attacker has a (legitimate?) business to protect

2. Attacker sells (your) minutes to another provider

    - Other provider unaware of how their minutes are terminated

    - Attacker sets up a media proxy (Asterisk or similar) on a compromised host, and routes calls via it

Successful Attack in Use



How Does the Attacker Do It?

- Port scan for open SIP (5060) and H.323 (1760) ports
  - Both UDP and TCP 5060 for SIP!
- Once an open port is found, SIP INVITES are sent until a call completes
  - May need to war-dial many incantations of dial-string:
    15105551212
    0015105551212
    001005105551212
    915105551212
- All this can be easily scripted with Asterisk, including notification of success
- No compromising of usernames or passwords required

So What Was Configured Wrong?

- Default configuration on a Cisco router with voice enabled IOS has SIP and H323 enabled!
    - Cisco routers route voice in a similar manner to IP. If the destination pattern matches are there, it will sit and route calls
- Asterisk boxes often have their contexts mis-configured
    - Contexts provide the mechanism to determine which SIP/H.323 peers have access to what extension matches (i.e. trunks)
    - Misconfigured contexts and SIP configuration can result in unauthenticated devices having access to your outbound trunks
- Two stage dialing is inherent to both and creates security holes too.

Cisco IOS Voice Gateways

- Cisco routers use dial-peers to direct voice traffic.
  - You only need one pots dial-peer configured pointing to a TDM interface and you are at risk
- Even when configured properly, unauthenticated SIP and H.323 calls will be accepted
- Even if you don't have any TDM interfaces, you may still be at risk!
  - IP-IP SBC functionality - you may be allowing attackers to send calls to a secure gateway elsewhere via your IP-IP gateway

Default Cisco IOS voice config

```
c2800#show run | inc voice
voice-card 0
c2800#show run | inc sip
c2800#show run | inc 323
```

Asterisk Configuration

sip.conf

```
allowguest=yes  ; allows anonymous inbound calls
                ; calls land in default context
                ; needed for inbound ENUM calls
```

extensions.conf

```
[default]
exten => _1X.,1,Dial(SIP/${EXTEN:1}@sip-gateway)
exten => _2X.,1,Dial(ZAP/g1/${EXTEN:1})

exten => 3001,1,Dial(SIP/${EXTEN}@custA-phone)
exten => 4001,1,Dial(SIP/${EXTEN}@custB-phone)
```

<u>Don’t ever use the default context for your trunks!</u>

So, How to Fix Things?

- Filter / ACL / Firewall off traffic to trusted sources only
    - This may not be possible for customer facing SIP proxies/registrar servers
- Use a SBC on your network edge, particularly facing other providers where possible
    - If not, Filter / ACL / Firewall off traffic to trusted sources only
- Shutdown services that are not required
- Never allow inbound contexts in Asterisk to have access to outbound routes
- Monitor your logs!

So, How to Fix Things?... ctd

- Talk to your PSTN provider about their fraud prevention methods
  - Some carriers will toll bar you within an hour of detecting fraudulent looking activity
  - Other carriers don't and will happily bill you for those calls
- Turn on toll barring at the PSTN provider if a gateway is only to be used for incoming calls
- Consider matching outbound trunk patterns with a 4-digit code in front
  - Security through obscurity. Harder for an attacker to discover appropriate dial-codes for outbound calls - provides additional time to detect.
- Use SIP TLS and SRTP if possible

Filtering

- Allow gateway access to:
- UDP/5060 from your SIP proxy only
  - Or from your customer subnets if they talk to the gateway directly, however you should really use a SIP proxy
- UDP+TCP/1720 from your gatekeeper and trusted endpoints only for H.323
- UDP/RTP-ports from your SIP proxy if terminating media, or customer endpoints if media is peer to peer
- Standard filtering practice - filter as specifically as possible on all devices

Shutting Down SIP/H.323 on Cisco Routers

- If you don't need voice features on a router, use a non-voice IOS
- Disabling the SIP listener

```
router(config)#sip-ua
router(config-sip-ua)#no transport tcp
router(config-sip-ua)#no transport udp
```

- On many IOS images H.323 can't be disabled, you need to filter traffic

```
router(config)#access-list 100 deny tcp any any eq 1720
router(config)#access-list 100 deny udp any any eq 1720
router(config)#interface X
router(config-if)#ip access-group 100 in
```

Asterisk Configuration

sip.conf

```
allowguest=yes  ; allows anonymous inbound calls
```

extensions.conf

```
[default]
exten => _30XX,1,Goto(phones,${EXTEN},1)
exten => _40XX,1,Goto(phones,${EXTEN},1)

[phones]
exten => 3001,1,Dial(SIP/${EXTEN}@custA-phone)
exten => 4001,1,Dial(SIP/${EXTEN}@custB-phone)
exten => _001NXXNXXXXXX,1,Goto(trunks,${EXTEN:1},1)

[trunks]
exten => _1NXXNXXXXXX,1,Dial(Zap/g1/${EXTEN})
```

Attack CDRs

Initial Probing:

"","asterisk","**590690868843**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/2-1","Dial","Zap/g1/h","2008-08-17
12:30:12",,"2008-08-17 12:30:22",10,0,"CHANUNAVAIL","DOCUMENTATION"

"","asterisk","**00590690868843**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/2-1","Dial","Zap/g1/h","2008-08-17
12:34:27",,"2008-08-17 12:34:41",14,0,"NO ANSWER","DOCUMENTATION"
"","asterisk","**0021277154725**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/2-1","Hangup","","2008-08-17 12:41:10",,"2008-08-17
12:41:23",13,0,"NO ANSWER","DOCUMENTATION"
"","asterisk","**00359881540770**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/2-1","Hangup","","2008-08-17 12:44:25",,"2008-08-17
12:44:27",2,0,"NO ANSWER","DOCUMENTATION"
"","asterisk","**00956**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/-1","Hangup","","2008-08-17 12:54:04",,"2008-08-17
12:54:05",1,0,"NO
ANSWER","DOCUMENTATION","","asterisk","0041764288077","default","""asterisk""
<asterisk>","SIP/72.46.136.4-0813cbb8","Zap/2-1","Dial","Zap/g1/h","2008-08-17
13:02:16",,"2008-08-17 13:02:31",15,0,"NO ANSWER","DOCUMENTATION"
"","asterisk","**0041762759680**","default","""asterisk"" <asterisk>","SIP/
72.46.136.4-0813cbb8","Zap/2-1","Dial","Zap/g1/h","2008-08-17
13:04:51",,"2008-08-17 13:05:05",14,0,"NO ANSWER","DOCUMENTATION"

These Attacks are Very Real...

- VoIP attacks of this nature have increased substantially in the past six months
- Can easily terminate 3000 calls per hour through an ISDN primary rate
    - Average 2min holdtime, sold by attacker at $1/min...
    - Attacker income $6000 per hour
    - Attacker cost $0
- People really need to get on with deploying secure VoIP protocols
- But securing what they have now is a good start