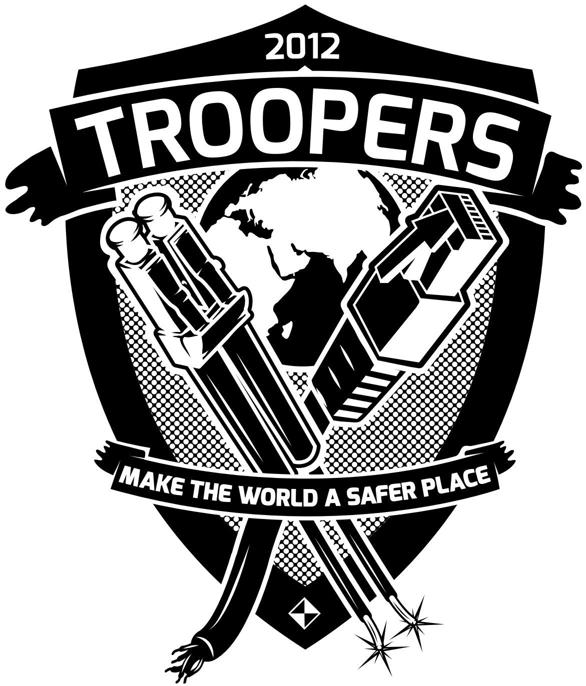
ERNW
providing security.

Don't Pay Money for Someone Else's Calls

A Practical Analysis of VoIP-based Toll Fraud Cases

Who am I

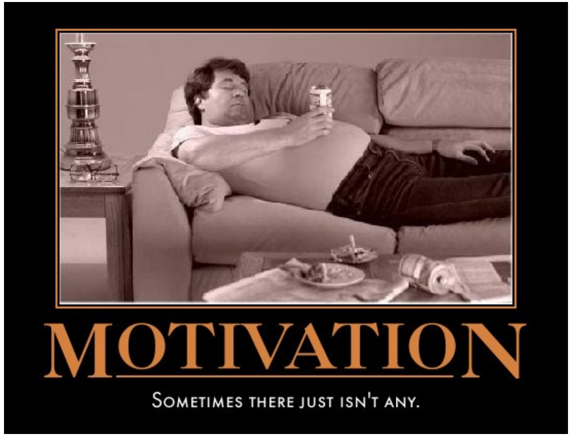


- Network geek, working as security researcher for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: www.insinuator.net
- Conference: www.troopers.de

Agenda

- Motivation
- ERNW's *Seven Sisters of Infrastructure Security*
- Typical Components in a VoIP environment
- Case Study 1
- Case Study 2
- Case Study 3
- Final Wisdom

Motivation



- VoIP is just another application which gets transported over an IP network
- So, the general rules for securing the environment apply (see next slide)
- VoIP has one “special” property
  - Failing in properly securing the environment will directly result in a financial loss.

Seven Sisters

Access Control

Isolation (Segmentation)

Restriction (Filtering)

Encryption

Entity Protection

Secure Management

Visibility

7 Sisters

- D ic
  Q

- Can we limit who’s taking part in some network, protocol, technology, communication act?
- Any need to isolate stuff due to different protection need, different (threat) exposure or different trust(worthiness)?
- What can be done, filtering-wise, on intersection points?
- Where to apply encryption, in an operationally reasonable way?

Generic Questions (2)

- What about the security of the overall system's main elements?
- How to manage the infrastructure elements in a secure way?
- How to provide visibility as for security-related stuff, with reasonable effort?

Typical Components in a VoIP environment

VoIP Terminals

- Device which is able to initiate and receive phone calls
- This can be a hard phone or a softphone which is running on the PC (or Smartphone) of the user

Call Manager

- Call processing entity
- Typically VoIP Phones are registered to one Call Manager
- Handles call routing, number translations etc.

Voice Gateway

- Typically a layer 3 device (router) with an ISDN card to interconnect the VoIP world to the PSTN

Additional Components

- Typically, valued added services are provided for the VoIP environment
  - Voice Mail systems
  - Music on Hold
  - Yadda, yadda, yadda

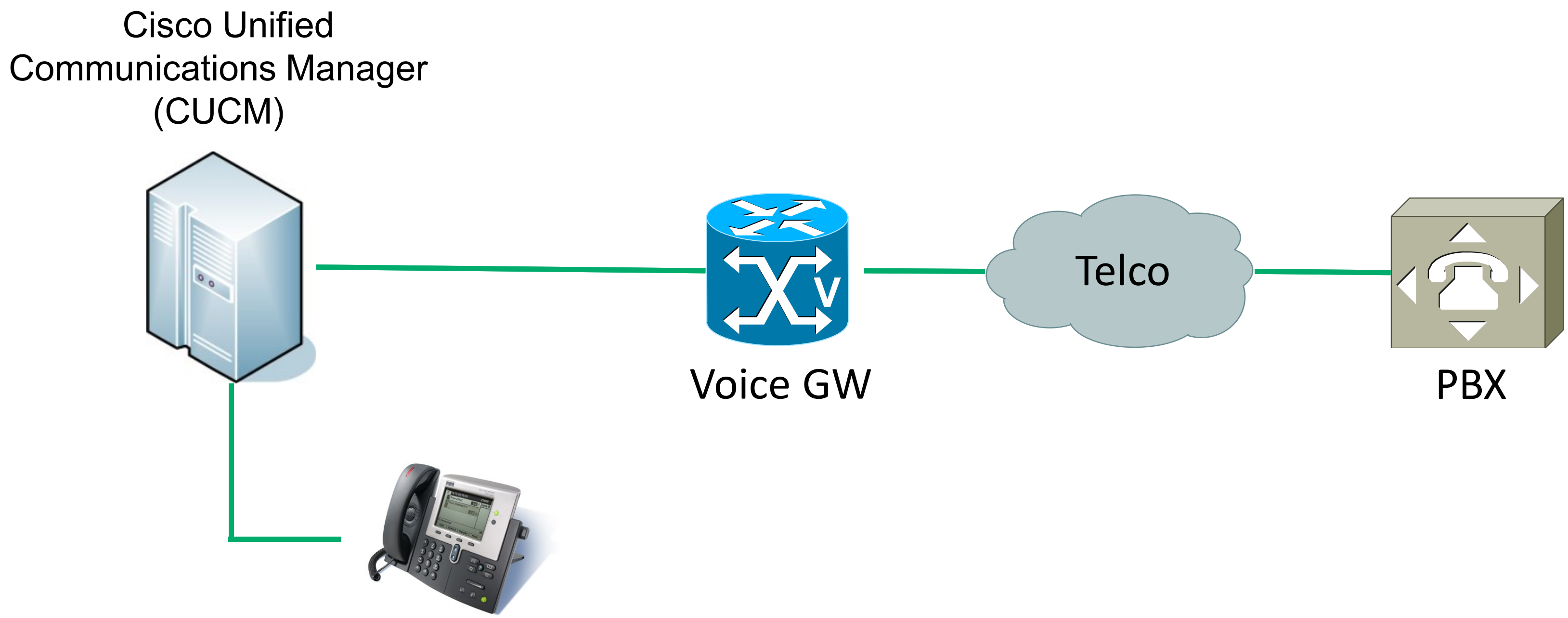
Case Study #1

Manufacturing Company

How it all began

- It all started on a Monday morning at 7am
- Received a call from Enno
  - Actually receiving a call from him at this time is never a “good” sign ;)
- The targeted company called and told him they had a toll fraud incident over the weekend which cost them nearly 75.000 €.

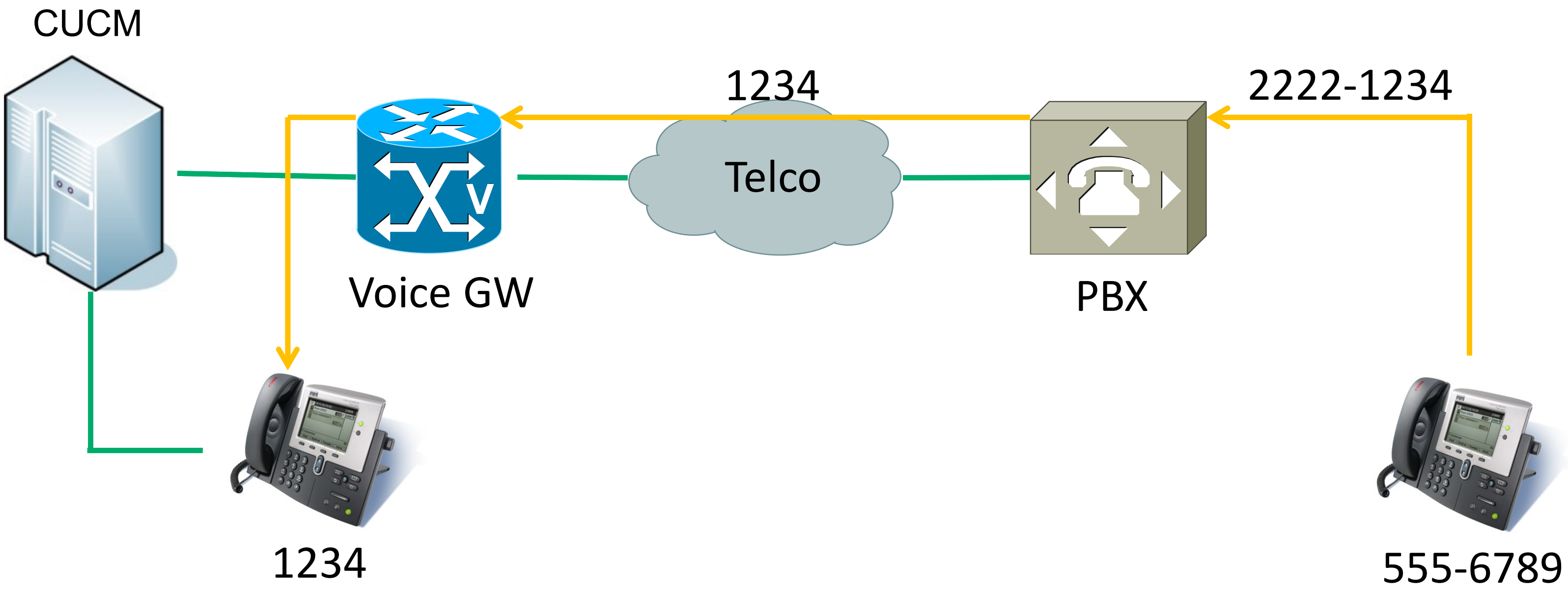
Introduction to the VoIP environment



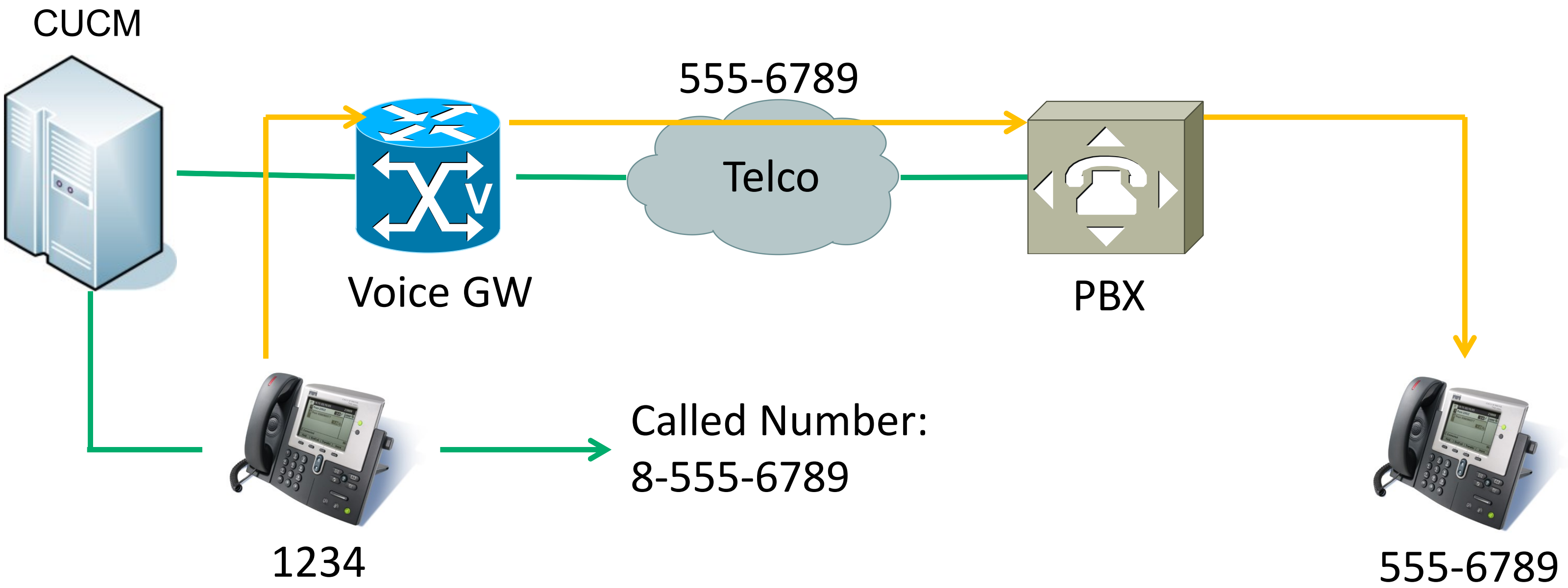
Customer Setup

- Customer was using Direct Inward Dial (DID)
- Basically means that you have a head number (in network terms a prefix) together with some phone extension.
- Also, for outgoing calls the digit “8” must be prepended to a called number in order to receive a dial-ton
  - Remember that ;)

Directed Inward Dial (DID) – Incoming Calls



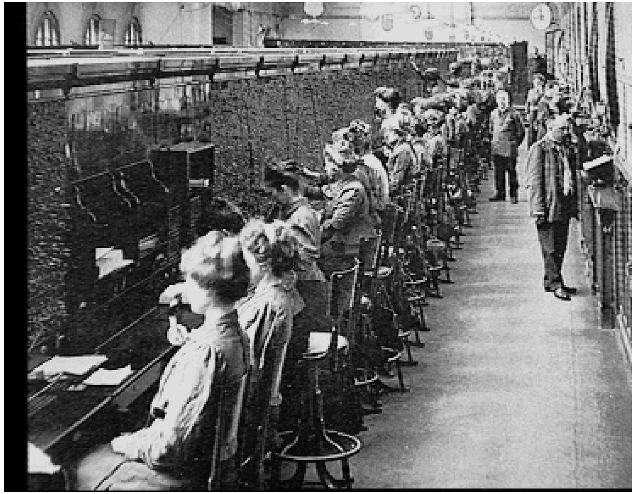
Outgoing Call Flow – Prepending the 8



Time to start digging

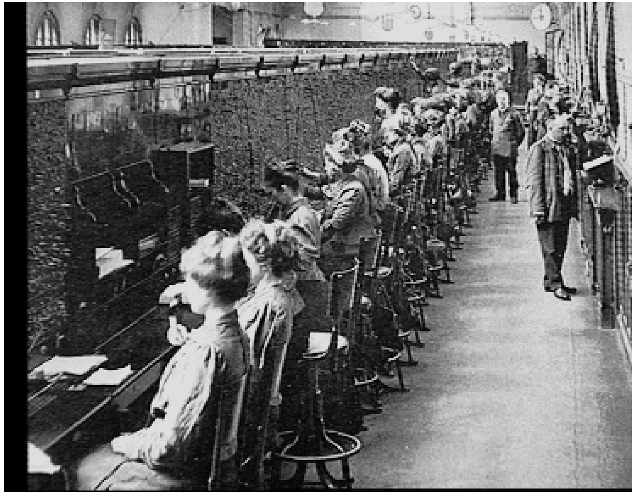
- After having a good overview of the overall design, it was time to start digging in the configuration and log files of the components.
  - Luckily the company *literally* logged everything ,)
- Some hours later, I was able to identify why the incident happened
  - Before going into detail, a short introduction on how call routing is implemented in the Cisco world might be useful….

Call Routing on Cisco IOS



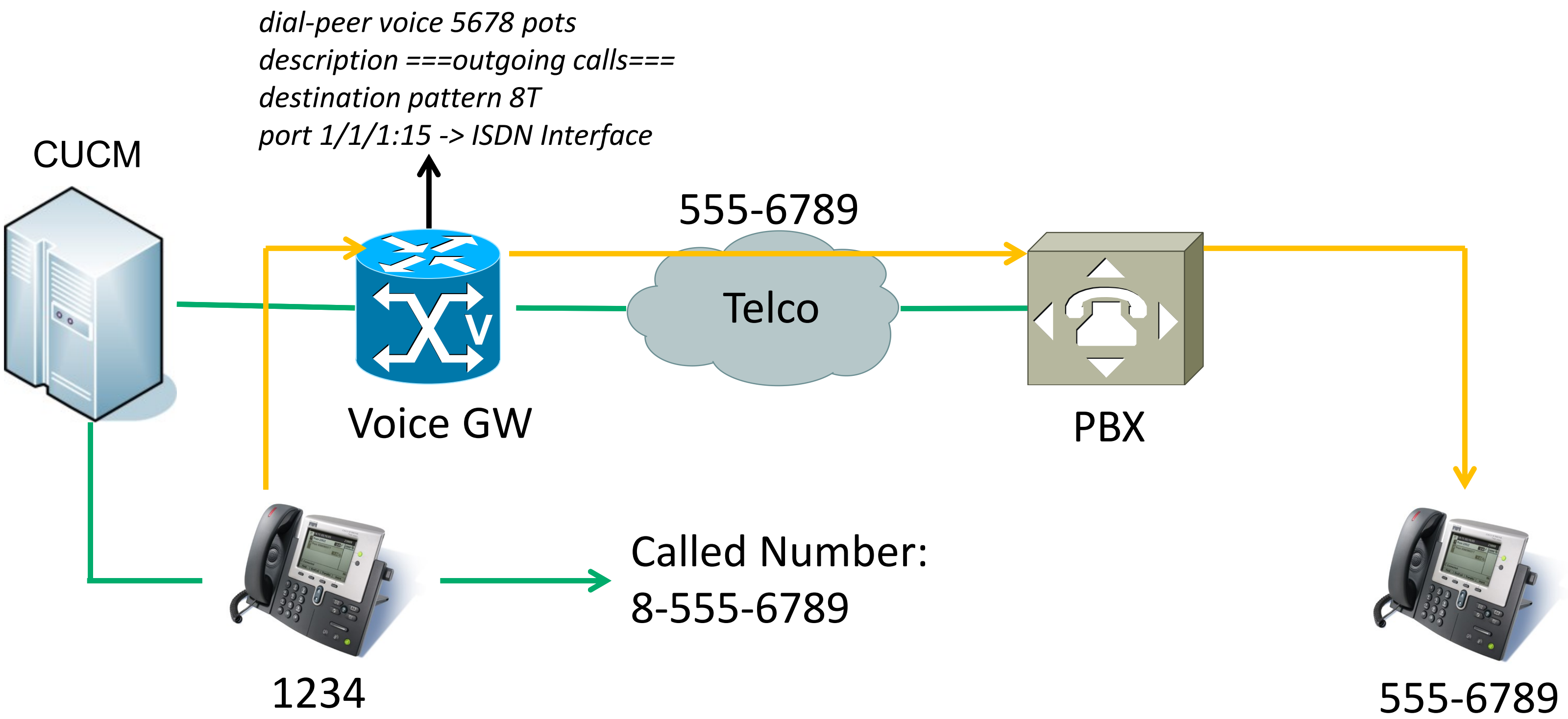
- In order to determine how a call gets forwarded so called “dial peers” are used in the Cisco world.
- These dial peers specify to which interface a call to a specific destination number gets forwarded

Quick Example

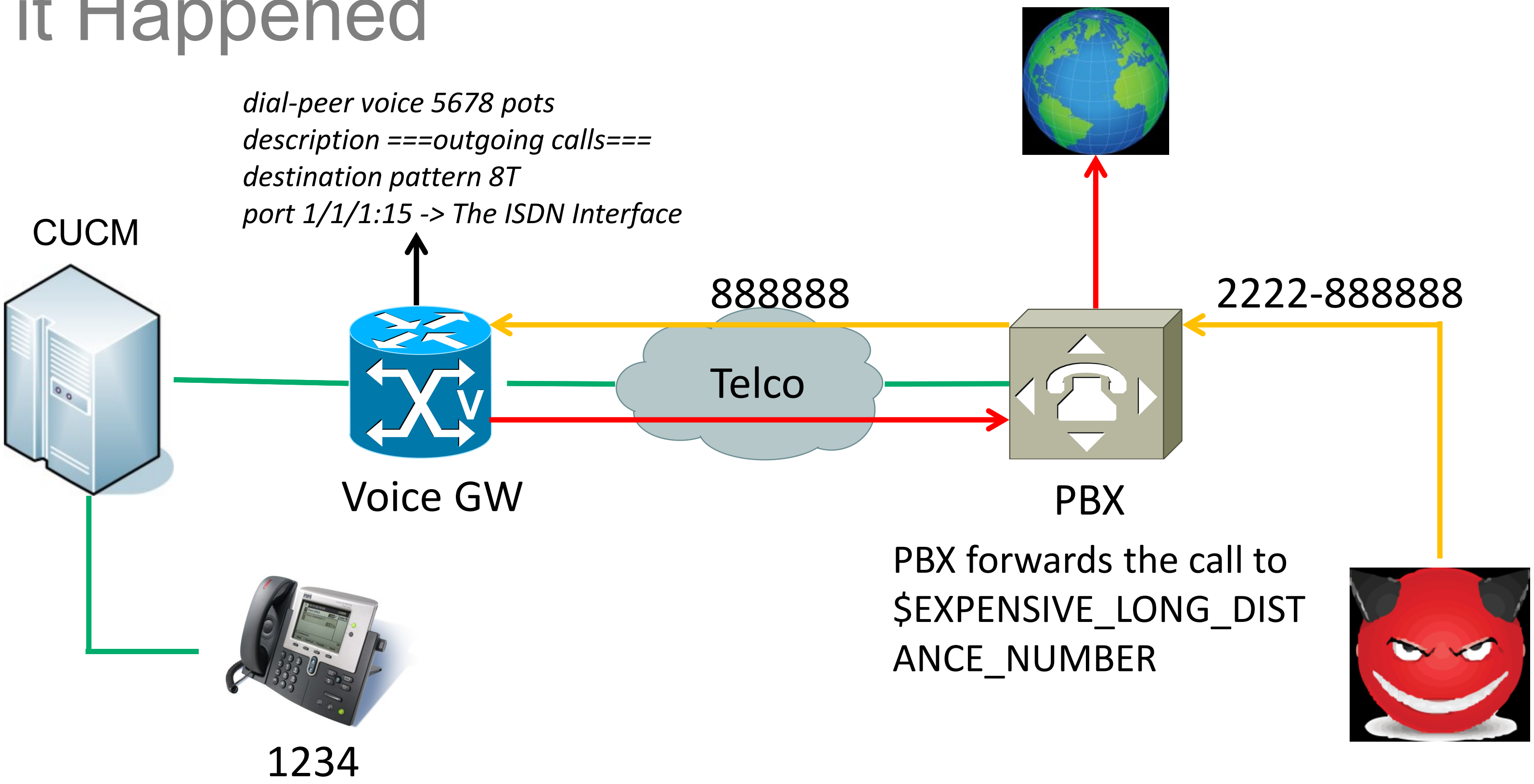


- Generic Example:
  - ```
    dial-peer voice 1234 pots
    description ===incoming_calls===
    incoming called number ^[2-7]..$
    port 0/3/0
    ```
- The company actually configured the following dial-peer for outgoing calls:
  - ```
    dial-peer voice 5678 pots
    description ===outgoing calls===
    destination pattern 8T
    port 1/1/1:15 -> The ISDN Interface
    ```

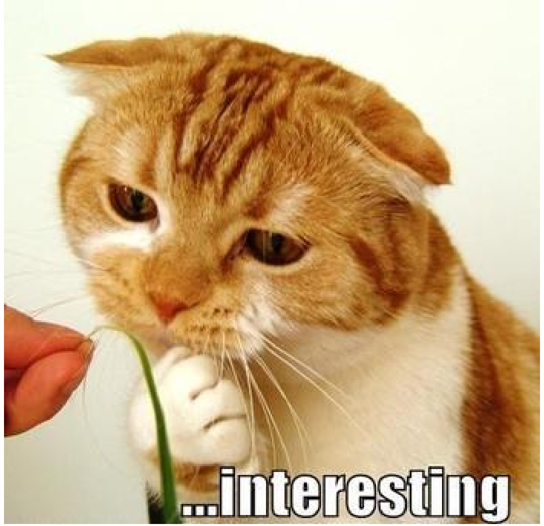
Dial Peer Configuration – Graphical View



How it Happened



An interesting side note



- The initial deployment was done by an external company
- The Telco told me that our customer was the 8th victim in one week.
- Interestingly, there is only one company in this small country right next to germany which offers deployment and configuration of VoIP systems
  - Maybe they all hired the same company….

Lessons learned?

- Be careful when you are planning your dial-patterns
  - As errors in this space can cost you quite a lot of money
- Verify the implementation of your implementer
  - As they might not have security in mind
  - Or the necessary know-how

Case Study #1, Summary

	No Major Weaknesses	Major Weaknesses Identified	Relevant Business Risk
Entity Protection		X	X
Visibility		X	**X**

Case Study #2

Typical Enterprise Environment

Groundhog Day

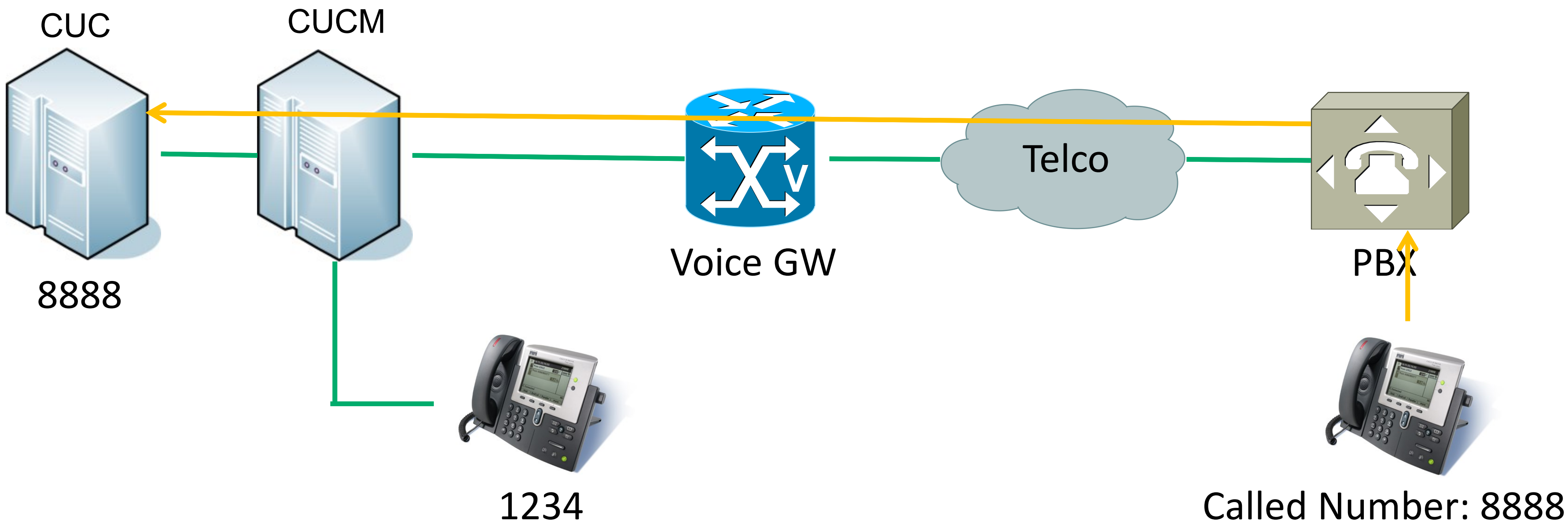
- It all started like the last incident just one week later
- Again at 7am on an Monday morning I received yet another call
- The targeted company had also a toll fraud incident over the weekend which cost them nearly 150.000 €.

Introduction to the VoIP environment

Customer Setup

- In this case the environment was configured to be able to call the voicemail system from external
  - So that road warriors can listen to their messages
- After calling this number, one has to specify the internal extension followed by a 4 digit PIN for authentication purposes
- After successful authentication one is presented with a Telephone UI
  - Where you can configure your greeting message, listen to your voice mails and also configure a call transfer to an **arbitrary** number.

Cisco Unity Connection



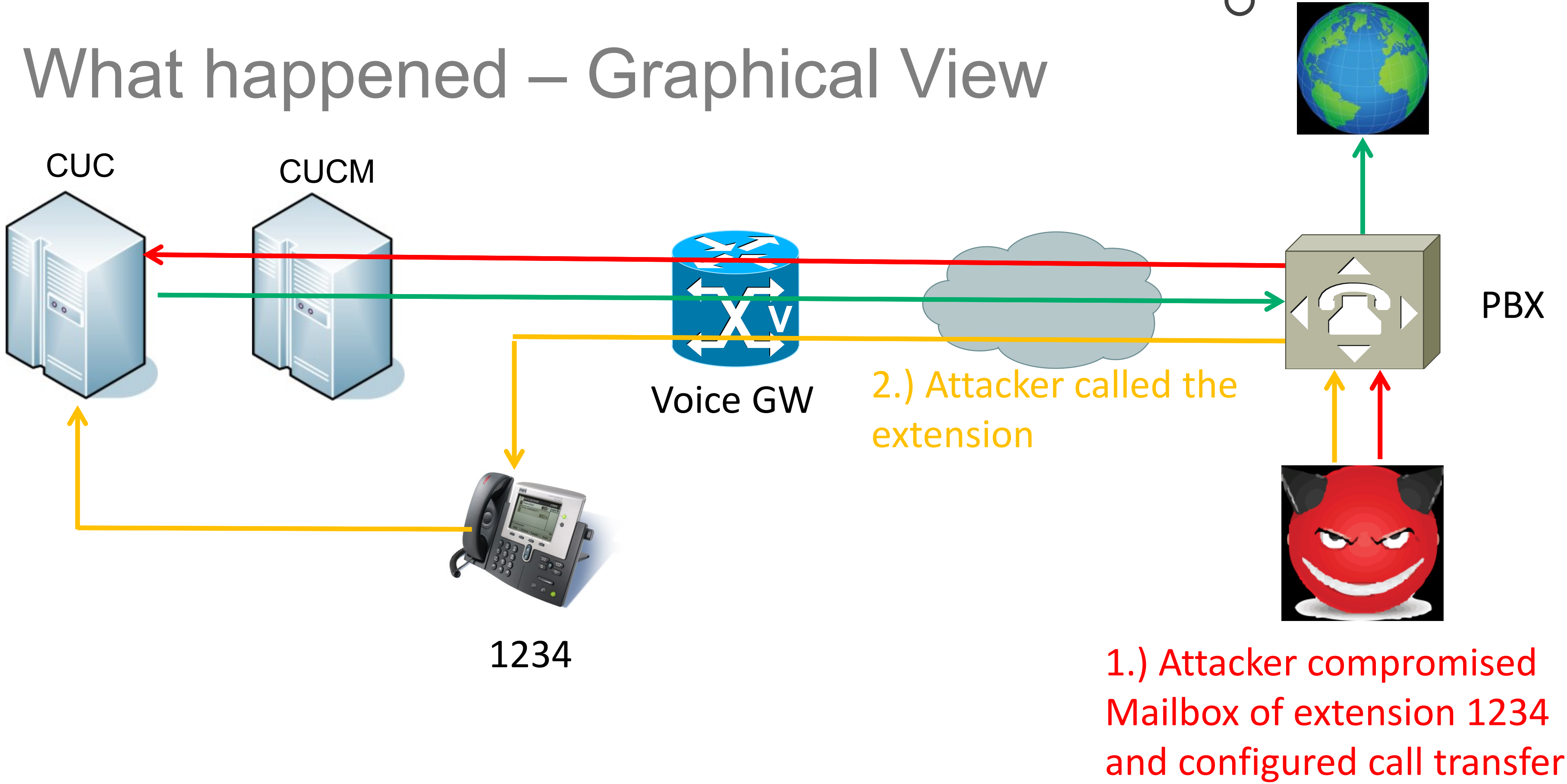
Time to start digging again ;)

- After having a good overview of the overall design, it was time to start digging in the log files of the components.
  - This customer also logged literally everything ,)
- Due to size of the environment, it took me about 1 ½ days until I was finally able to reconstruct what happened

Here’s what happened

- 1.) The PIN of a mailbox was compromised
  - On Thursday evening
- 2.) The attackers waited until Friday evening
  - Because nobody was in the office anymore, and the user who owns the mailbox forwarded all calls to his number to the mailbox before leaving.
- 3.) The attacker configured a call transfer via the Telephone UI to $EXPENSIVE_LONG_DISTANCE_NUMBER
- 4.) and finally called the extension of the affected user, who had the forwarding to the mailbox configured.

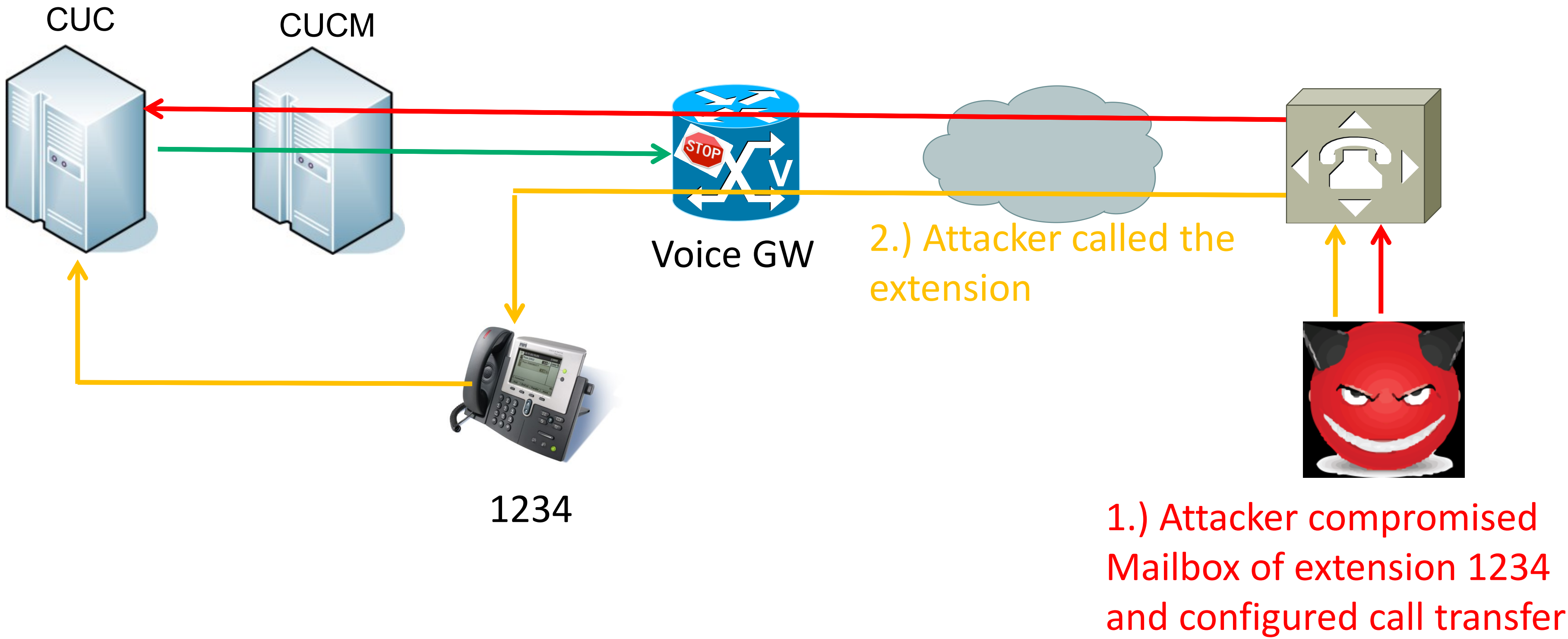
What happened – Graphical View



But….

- They noticed relatively quickly that the call transfer was not working as desired
  - Because the Voice Gateway was configured to reject calls to “suspicious” numbers.

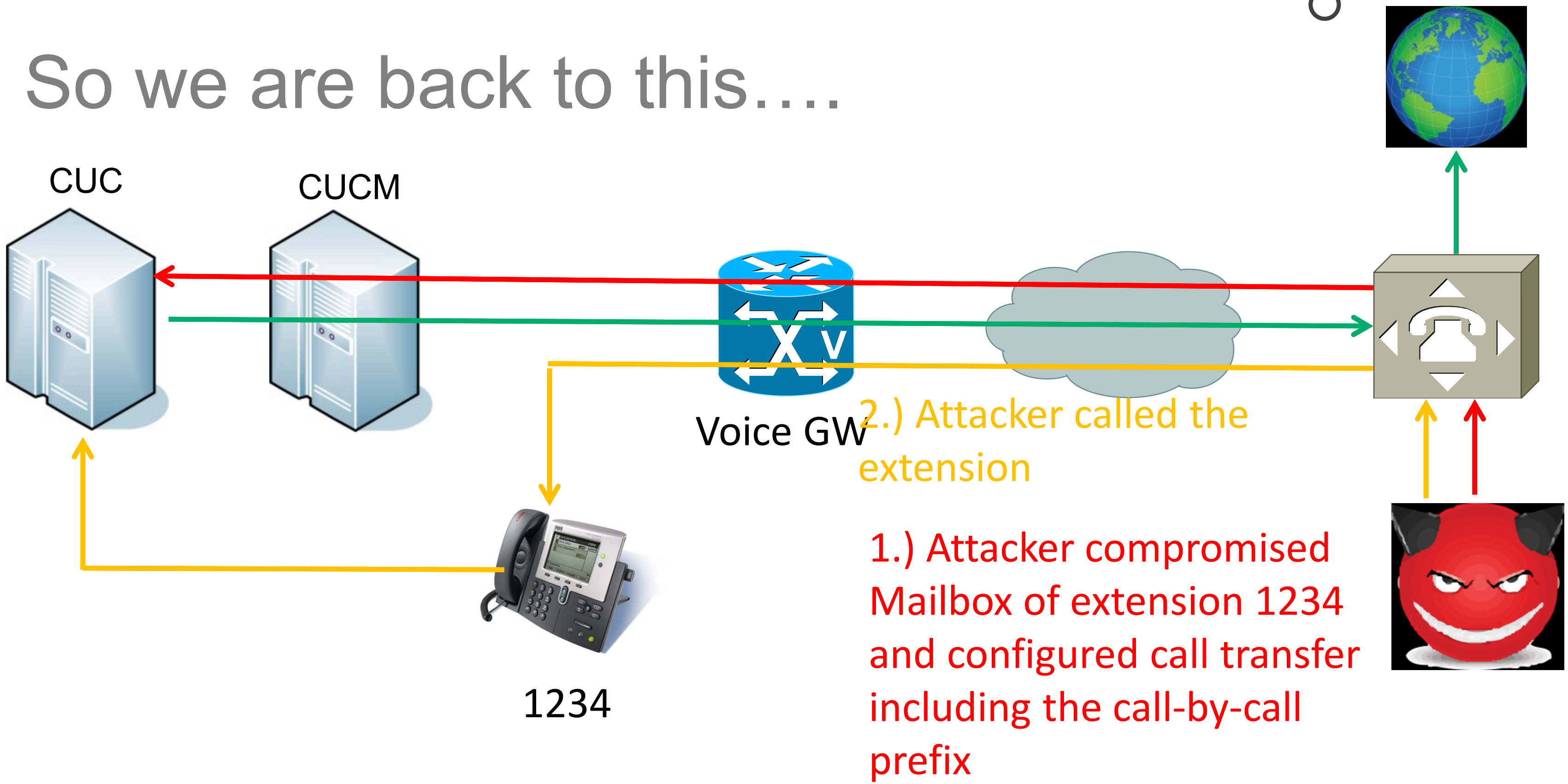
What happened – Graphical View



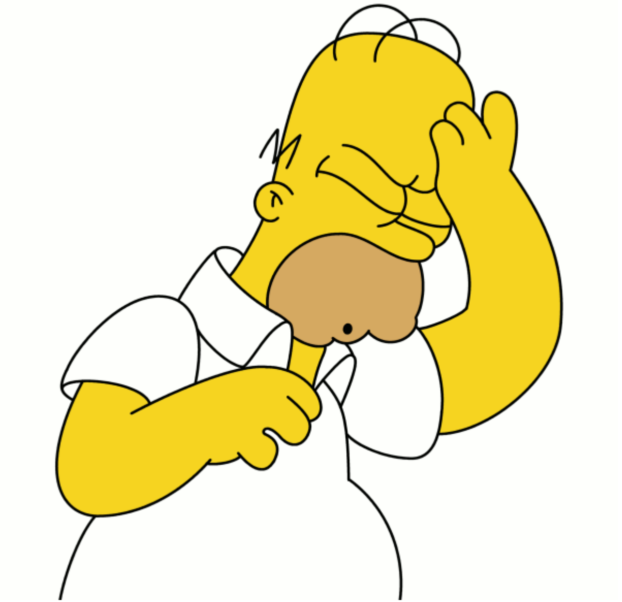
How could they circumvent the restriction?

- They found a clever way to circumvent the restriction
- In Germany one can use a so called “Call-by-Call” Provider
  - Basically if you want to use such a provider you must prepend a provider specific prefix to the number
  - E.g. 01049 + $EXPENSIVE_NUMBER
- They configured the call transfer and prepended a call-by-call provider prefix, and were able to circumvent the restriction

So we are back to this….



So how could all of this happen in the first place?



- 1.) Unity Connection was able initiate outbound calls
  - Well, that's debatable whether it should be able to, but business requirements demanded for it.
- 2.) The PIN was only 4 digit long
- 3.) Trivial PINs were allowed
  - E.g. "0000" or "1111"
- 4.) No proper restriction to which numbers a call transfer can be configured.

Lesson learned

- These properties are a little unfortunate as Unity Connection gives you all the tools you need to address the issues mentioned above.
- So this case could basically be broken down to configuration weaknesses which favored the attacker to exploit the issue.
- Like in the last incident, the initial deployment and configuration was done by an external company ;)

Case Study #2, Summary

	No Major Weaknesses	Major Weaknesses Identified	Relevant Business Risk
Entity Protection		X	X
Visibility		X	**X**

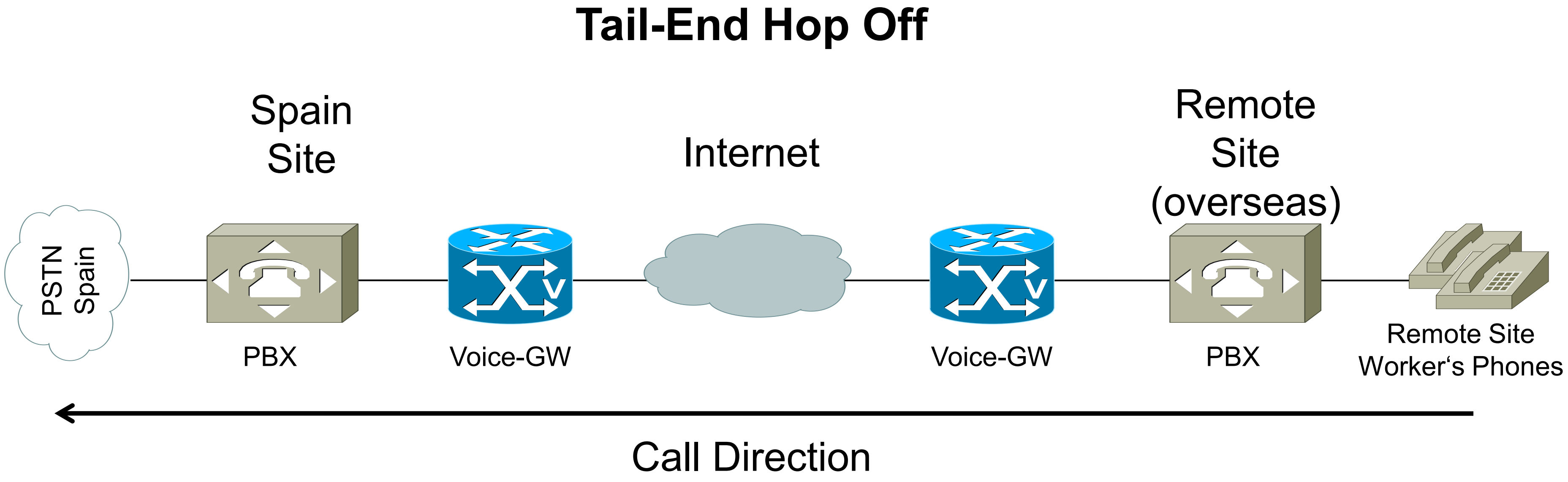
Case Study #3

Call Center

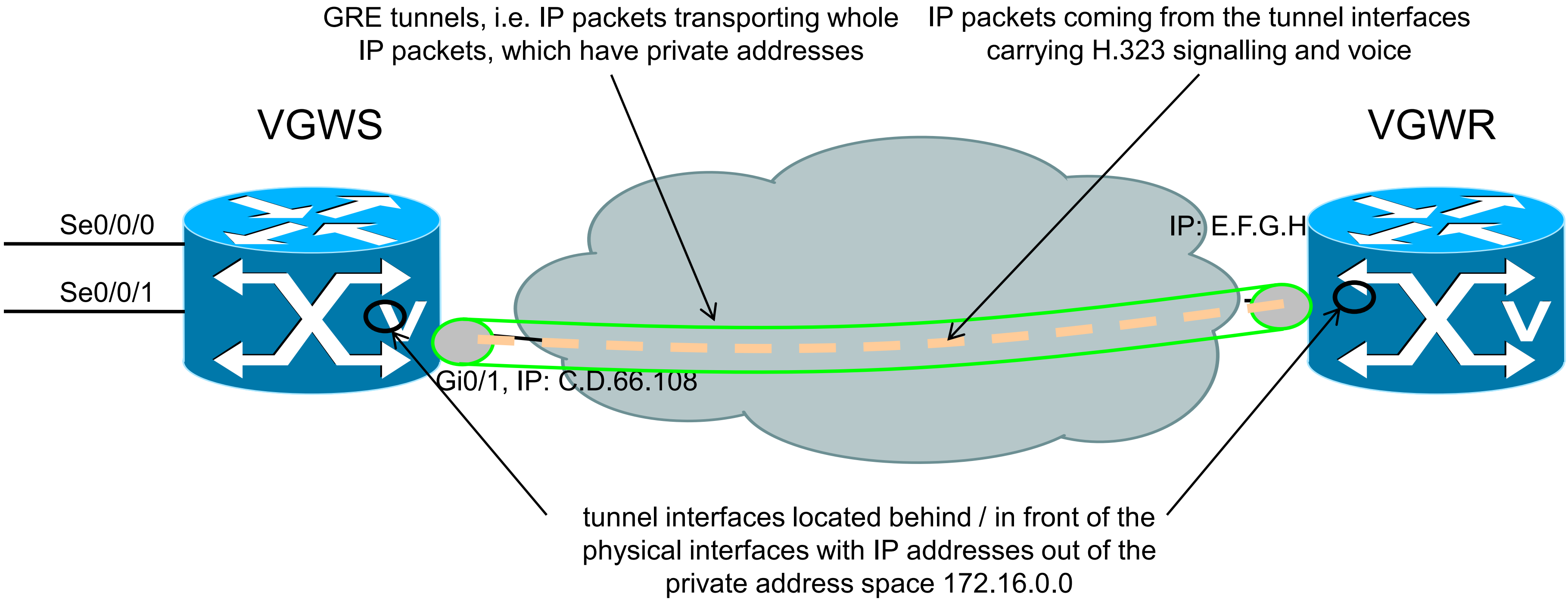
The Scenario

- A company headquartered in Spain has a callcenter in Argentinia.
- Between the two sites a H.323 Trunk is established.
- Requirement: The calls from the Call Center are going over the spanish hq into the normal PSTN. Nobody else has access to the voice trunk between the two sites.
- Problem which arised: On the Spanish site 800 000 minutes of calls to Africa and the Caribic were generated (according to Telefonica) and nobody knows how this happened.
  - Router configuration was implemented by a external company
  - No logs available, no accounting information available

The Scenario (graphical version)



GRE-Tunnels


GRE tunnels, i.e. IP packets transporting whole IP packets, which have private addresses
IP packets coming from the tunnel interfaces carrying H.323 signalling and voice
VGWS
VGWR
Se0/0/0
Se0/0/1
IP: E.F.G.H
Gi0/1, IP: C.D.66.108
tunnel interfaces located behind / in front of the physical interfaces with IP addresses out of the private address space 172.16.0.0

Call Routing -- Which calls goes where?

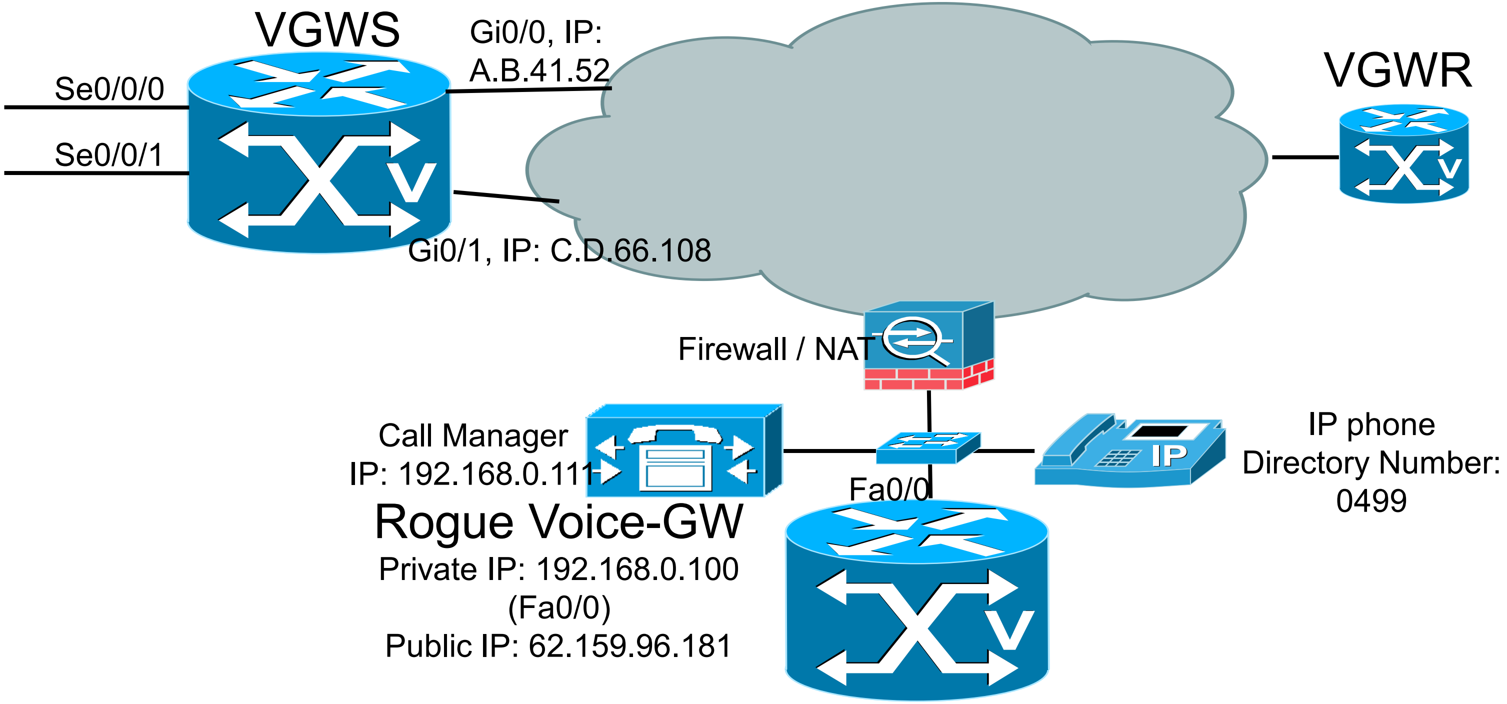
```
dial-peer voice 15 pots
 destination-pattern 89........  <<<<< call destination
 direct-inward-dial
 port 0/0/0:15  <<<<< outgoing interface (ISDN conn. to PBX)
 forward-digits 9
!
dial-peer voice 20 pots
 destination-pattern 86........  <<<<< call destination
 direct-inward-dial
 port 0/0/0:15  <<<<< outgoing interface (ISDN conn. to PBX)
 forward-digits 9
!
dial-peer voice 25 pots
 destination-pattern 8T  <<<<< "route any calls with '8…'…
 direct-inward-dial
 port 0/0/0:15  <<<<< … and send them to the PBX"
```

Short Analysis

1. The Call Routing configuration passes calls to all numbers to the PBX
2. No Access Control in place (ACL or Authentication).
3. The first 2 Points are a security vulnerability, which attackers can exploit to do unauthorised calls.
4. But it depends on the configuration of the pbx what happens to the calls, whether they are forwarded to the PSTN or discarded*

   *After the incident was known to the company, the pbx was reconfigured to discard all calls from the Voice-GW

Proof of Concept – Attack scenario



The Results (1)

H.323-Subsystem receives a request (setup):

```
VGWS#
Dec 10 17:06:19: //-1/xxxxxxxxxxxx/H323/cch323_h225_receiver:
   Received msg of type SETUPIND_CHOSEN
Dec 10 17:06:19: //-1/xxxxxxxxxxxx/H323/setup_ind: Entry
Dec 10 17:06:19: //961121/50A7036680E6/H323/setup_ind:
   callingNumber[0499] calledNumber[8005322694234]
```

H.323-Subsystem answers the request:

```
Dec 10 17:06:19:
   //961121/50A7036680E6/H323/cch323_h225_receiver:
   SETUPIND_CHOSEN: src address = C.D.66.108; dest address =
   62.159.96.181
```

The Results (2)

Fitting Dial-Peers were found:

```
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=8005322694234, Peer Info
   Type=DIALPEER_INFO_SPEECH
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=8005322694234
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Result=Success(0) after DP_MATCH_DEST
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersMoreArg:
   Result=SUCCESS(0)
   List of Matched Outgoing Dial-peer(s):
     1: Dial-peer Tag=25
       2: Dial-peer Tag=26
```

The Results (3)

ISDN-Subsystem tries to forward the call to the PBX...

```
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0, Calling num 0499
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0, Called num 005322694234
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: TX -> SETUP pd = 8  callref = 0x5704
        Bearer Capability i = 0x8090A3
                Standard = CCITT
                Transfer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA1839F
                Preferred, Channel 31
        Progress Ind i = 0x8183 - Origination address is non-ISDN
        Calling Party Number i = 0x0081, '0499'
                Plan:Unknown, Type:Unknown
        Called Party Number i = 0x80, '005322694234'
                Plan:Unknown, Type:Unknown
Dec 10 17:06:19: //961121/50A7036680E6/H323/run_h225_sm: Received event H225_EV_CALLPROC while at state H225_SETUP
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_set_new_state: Changing from H225_SETUP state to
    H225_CALLPROC state
Dec 10 17:06:19: //961121/50A7036680E6/H323/generic_send_callproc: ====== PI = 0
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: RX <- SETUP_ACK pd = 8  callref = 0xD704
        Channel ID i = 0xA9839F
                Exclusive, Channel 31
```

The results (4)

…but the call is rejected: No route to destination

```
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: RX <- DISCONNECT pd = 8  callref = 
   0xD704
        Cause i = 0x8283 - No route to destination
        Progress Ind i = 0x8288 - In-band info or appropriate now 
   available
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: call_disc: PI received in 
   disconnect; Postpone sending RELEASE for callid 0xD607
```

The H.323-Subsystem informs our Voice-GW:

```
Dec 10 17:06:19: //961121/50A7036680E6/H323/run_h225_sm: Received event 
   H225_EV_RELEASE_PI while at state H225_CALLPROC
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_send_release: 
   Cause = 3; Location = 0
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_send_release: 
   h225TerminateRequest: src address = -721405989; dest address = 
   62.159.96.181
```

Lesson learned

- Like in case #1 one should be careful about the configured dial plan.
- Missing access control on the voice gateway side
  - Which invited the whole Internet to configure a H.323 trunk and routing calls over this link billed to someone else.

Case Study #3, Summary

	No Major Weaknesses	Major Weaknesses Identified	Relevant Business Risk
Access Control		X	X
Entity Protection		X	X
Visibility		X	

Final Wisdom

- VoIP is complex technology
- Failure in securing your VoIP environment can and will cost you quite a lot of money
- Verify the (secure) configuration of your environment if an external company initially deployed it.
  - As all three incidents had in common that an external company had done the deployment.

Final Wisdom

- But it is not rocket science to secure it either...
- As VoIP is just another application over IP, the basic rules apply:
  - Access Control
  - Isolation
  - Restriction
  - Encryption
  - Entity Protection(!)
  - Secure Management
  - Visibility

There's never enough time…

THANK YOU…

...for yours!