Black Hat

IVR Security:- Internal Attacks Via

Who am I ?

- Rahul Sasi
- Security Researcher @ iSIGHT Partners .
- Member Garage4Hackers.

Garage 4 Hackers

Information Security professionals from Fortune 500, Security research and Consulting firms from all across the world.

- Security Firms
- Consulting Firms
- Research Firms
- Law Enforcements

http://www.Garage4Hackers.com

IVR Application

Phone Banking

Telephone Assistant | Operator

Hospital | Medical Enquiry

What Made Me Interested: IVR Application

- My Phone Banking.
- How it works.
- It used 16 digit Account No followed by 4 digit ATM pin for authentication using a voice call to IVR.

How it could be Hacked: In Theory

- Probability Theory

Probability that event A occurs

$$P(A) = n(A) / n(S).$$

where,

n(A) - number of event occurs in A

n(S) - number of possible outcomes

n(A) = n no of customers (huge)

n(S) = no of pin combination (9000)

More Theory

- So if we make a program that dials into IVR and tries to authenticates into users account

  Starting form account no 1000 to 2000 for password 6666.
- The chances of 1000 users having ‘6666’ as pin for there accounts is very high :D .

  The lowest possibility lets say ‘10’ accounts.

Enough Theories

- Individual Users after 3 invalid attempts, there account gets blocked.
- And every night at 12 clock your account would be automatically activated ;)
- So if I start my brute force program at night 10 O’clock , I could try 5 different pins for 1000 accounts with out blocking any accounts :D

Now what

- With the above logic any one would be able to crack least 50 ATM pins in 4 hours time :O

Enough Theories

AT Commands Basic

- Sending DTMF tones using phone modem.
  - AT [Attention]
  - ATD
  - ATZ + vts
  - ATH

How to Automate

- Serial Port Communication
- Talk to your phone modem.

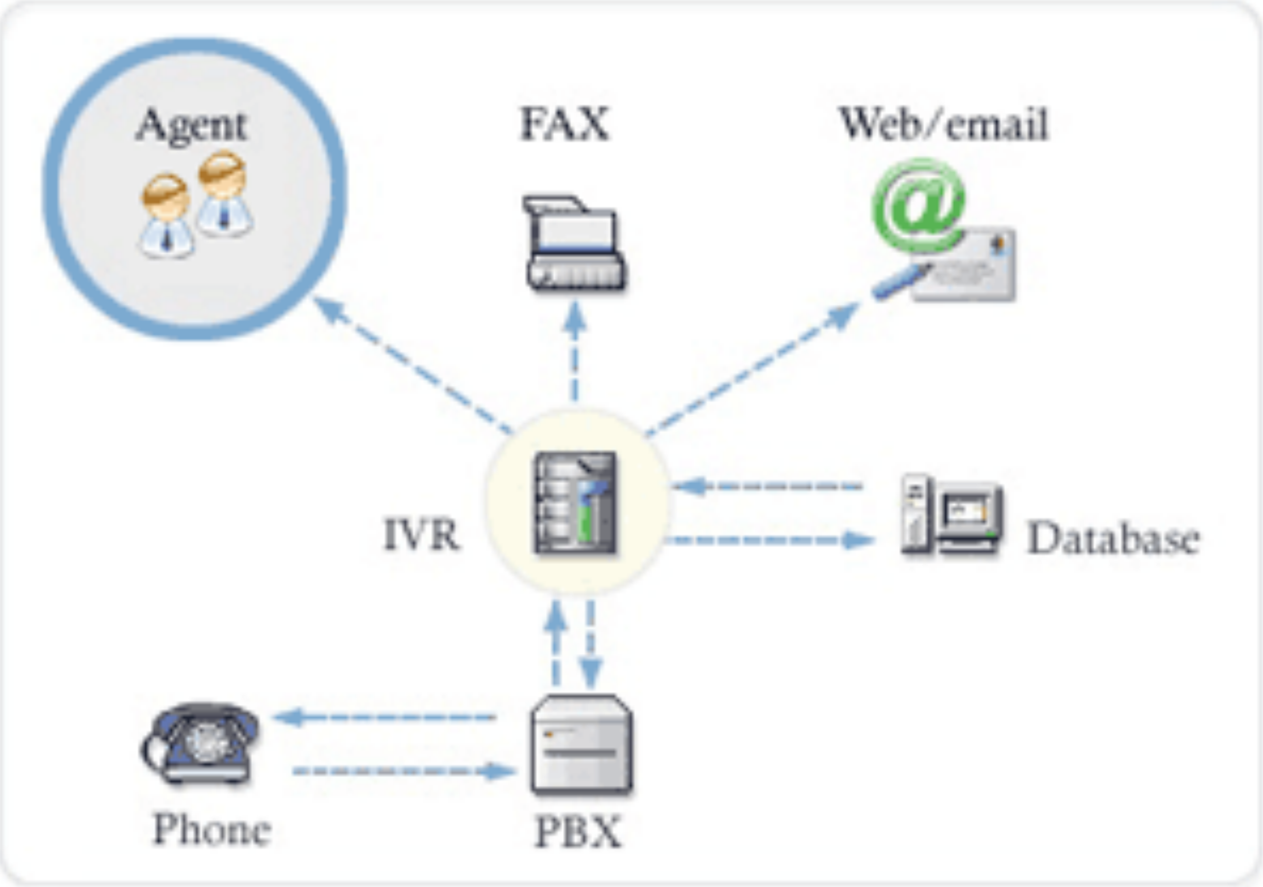
Demo #1

IVR Brute.mp4

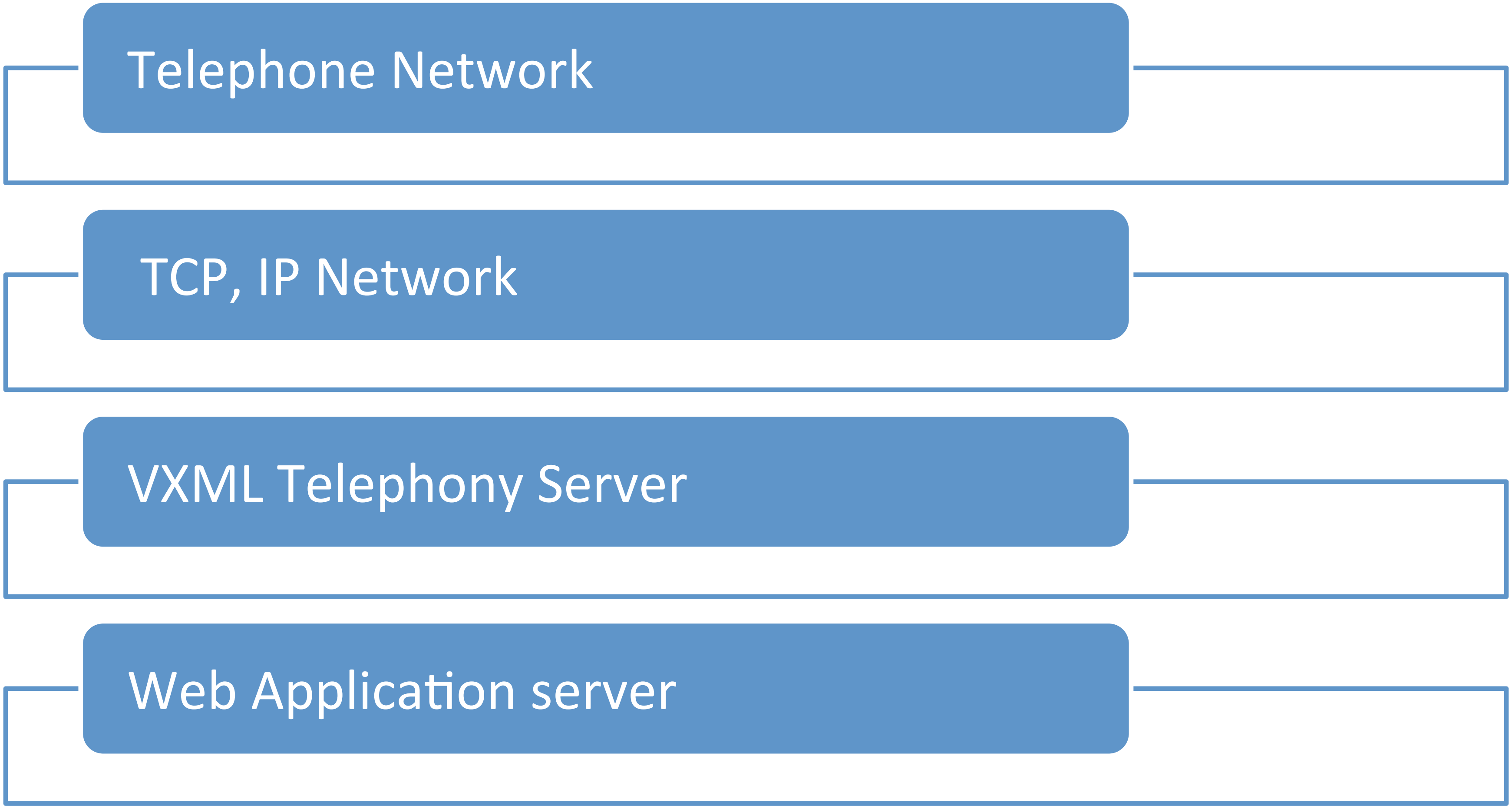
IVR: Introduction

- Interactive Voice Recognition systems, use Touch-tone or Speech Recognition to make callers interact with the system.
- Touch Tones: DTMF inputs.
- Speech Recognition: Could send in voice commands, and TTS(Text to Speech) Engine Could detect it.

IVR Architecture



Layers of IVR



Telephone Network

TCP, IP Network

VXML Telephony Server

Web Application server

Modules: How it works

- Client (Telephone Phone)
- Telephone Network
  - PBX (Private Branch Exchange)
- VXML Telephony Server
  - VXML
  - CXML

- Web Application Servers
- Databases

Finger Printing Internal Servers:

- Triggering Errors:
  - If we could trigger error messages on Internal servers , the text to voice (tts) machine would read out the error.
- There are many ways to trigger error, Fuzz for the grammar files, or best way is source code auditing .
- Automated Fuzzing for Errors.(tools)

Vulnerable Programs

- Sample Vulnerable Program:

  error_vul.xml

Demo #2

Finger Printing Internal Servers

[Demo Video]

ivr_error_video.mp4

Input Validation Attacks:

- Using Grammar files [Nonsense Grammar format]

- Using prebuilt grammar files .

Chances of SQL Injection Attack

Vulnerable Program

Demo #3

Fuzzing for Grammar files

SQL Payloads Via DTMF

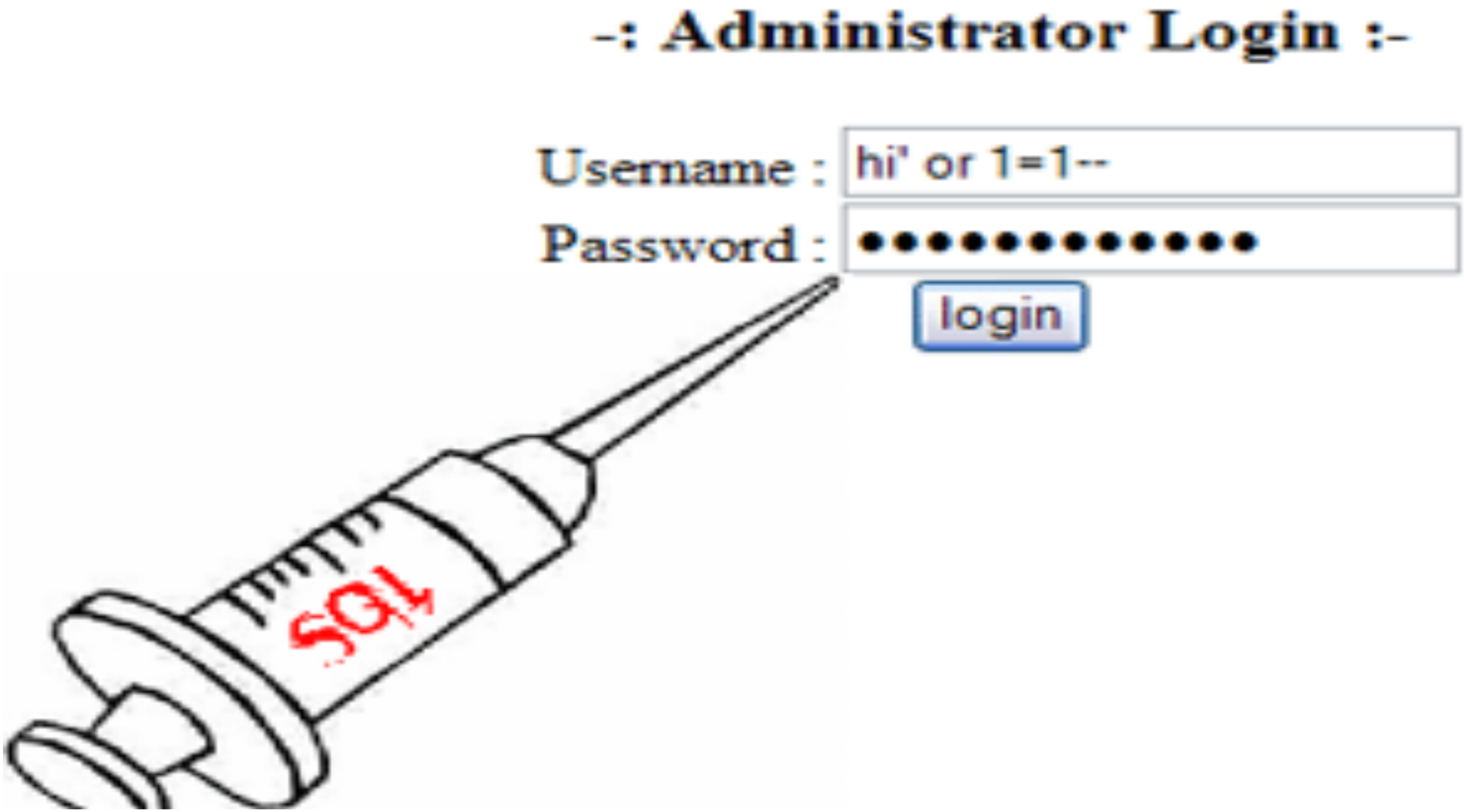
- DTMF Limitations , we could only send

[0-9] * # A B C D

Advance SQL injection Based on [False Injection]

- Basic Injection:

select * from users where id='$id' and password='$password’ ‘or 1=1



-: Administrator Login :-

Username : hi' or 1=1--

Password : ••••••••••••••

- select * from users where id='$id' and password='$password’ '=0#

Input: '=0# [and It Works]

Other inputs that will work:

- Addition

  ‘+0#

- Multiplication

  '*9#

  1*0*0*1 [True]

  1*0*0*1 [False]

http://www.exploit-db.com/papers/18263/

IVR: Enter User ID

User: 1337

IVR: Wrong User ID, Please try again

IVR: Enter User ID

User: 31337

IVR: Welcome Rahul Sasi

IVR: Enter User ID

User: 31337*1*1*1*1

IVR: Welcome Rahul Sasi

IVR: Enter User ID

User: 31337*1*1*1*0

IVR: Invalid User [or] “No Response “

SQL Injection Check using DTMF

Demo Video

Long strings, chances of Buffer Overflow .

- Improper Input validation on input to CGI applications form VXML server.
- Voice and DTMF Fuzzing could Reveal Bugs.
- Our tool will be having voice fuzzing Support.

Limitations.

- Payloads cannot have “/” and other special characters.
  - Sending payload using “Upper Case Alpha Numeric Shell code.
- The payload has to be converted to DTMF (0-9) and Alphabets (A-Z)

Vulnerable Program

- Demo Video

The making of Voice Payload.

Upper Case Alpha Numeric Payload

Demo #4

IVR: Attacking Internal Server using Voice Payload.