Call Fraud in Calling (VoIP, SIP)

Non-legit/ DDos attacks

Shambhu Kumar

Table of Contents

What is Fraud ?

To understand it better, let's try to see what Fraud in Calling is.

1. A janitor using the Desk phone after the staffs have left the office in the evening. Will it be considered as fraud?
2. Your friend using your phone while you are in the rest room. Will it be considered as fraud?
3. Your Co-Worked using your desk phone when you are away. Will it be considered as fraud?
4. A machine originates Calls on behalf of an actual uses. Will it be considered as fraud?

The answers to all the above question are **YES**. Any Calls placed from your phone which wasn't made by you can (**MUST**) be considered as a fraud. You don't know whether these calls were made for ransom calls or to premium services. But since those calls originated from the account registered on your name you can be considered responsible (legally) for any consequences.
There has also been a dilemma on whether we need to consider Phones as private as our credit card. You will never hand over your credit card to anyone then how can you be okay with anyone using your Phone. You can keep the Credit card in your wallet, but can you keep your phone in there ☺
The problem with Service providers or Phone manufactures are, they can create phone with Lock/key but cant help in securing the line which connects to these phones. Anyone with Physical access to the location can swap the Hardware device and can use your Tel line to make calls. Most of the DoS attacks works this way.

As per Wikipedia, According to a 2011 survey by CFCA, an industry group created to reduce fraud against carriers, the five top fraud loss categories reported by operators were:[1]

US$4.96 billion – compromised PBX/voicemail systems
$4.32 billion – subscription/identity theft
$3.84 billion – International Revenue Share Fraud
$2.88 billion – by-pass fraud
$2.40 billion – cash fraud

Now if we look at the revenue lost in these frauds, these are equivalent to revenue of some of the Giant companies in the world.

Can these frauds be averted?
Simple answer to this is, **No** every time you detect a fraud a next type of fraud will peep in.
So what do we need?

The need of the Hour

Since now we all understand what a fraud is. Let's categorize it, there are two types of frauds with calling.

Someone (or some machine) uses your device/account to make calls, for which Cost to be paid by the owner of the account.

Someone steals your identity or your financial data to use it impersonate you and put up some financial losses to you.

As we don't have a singular problem, the solution can't be singular. Our need is to get a solution which can protect Us as well as Our devices. It needs to protect us from the incoming calls which are made to us. It also needs to protect our phone to not allow such kind of Outgoing calls.

Solution for both the problem are alike (not name)

Monitor the pattern
Improve the pattern
Learn from Pattern
Allow Pattern design by All Consumer (Service provider till the actual user)

Let's try to understand what a Pattern in calling is:
A Pattern is a usual way of flow for the consumer, it can be daily or weekly or monthly pattern. Let's talk about an example

Alice is based in Dallas.

- Her Monthly calling pattern resembles –
  National calls - Max Number to Chicago & NY
  National Calls- Never to LA
  International Calls- Max Calls to UK
  International Calls – Never to Japan
  Active hours – 9 AM to 3 PM
  Non-Active hrs – 11 PM to 3 AM
  Registration – Most through IP network with series 192.12.xxx.xxx
  Registration – Never (or only on Sunday) through Mobile network
  Length – Max length of her call is 30 Min to NY, Avg National Call length= 12 Min, Avg International= 7 Min

Now in this example a pattern for Allice is defined, any deviation from it can be Fraud. The chances for deviation are very rare but yes it might be possible as we can't predict human. If we see a call at 11:30 PM on Monday, then it would be wise if Alice must confirm that its her who is making calling before allowing instead of what happens today.

Now if this call is Legit and is being made by Alice then the solution needs to Learn and improve itself (consider it as exception on Monday)

We also need to allow Alice to improve this pattern when she wants to, Alice now stays late at work till 11:30 PM so she needs to change the pattern to learn pattern till 11:30 PM every day.

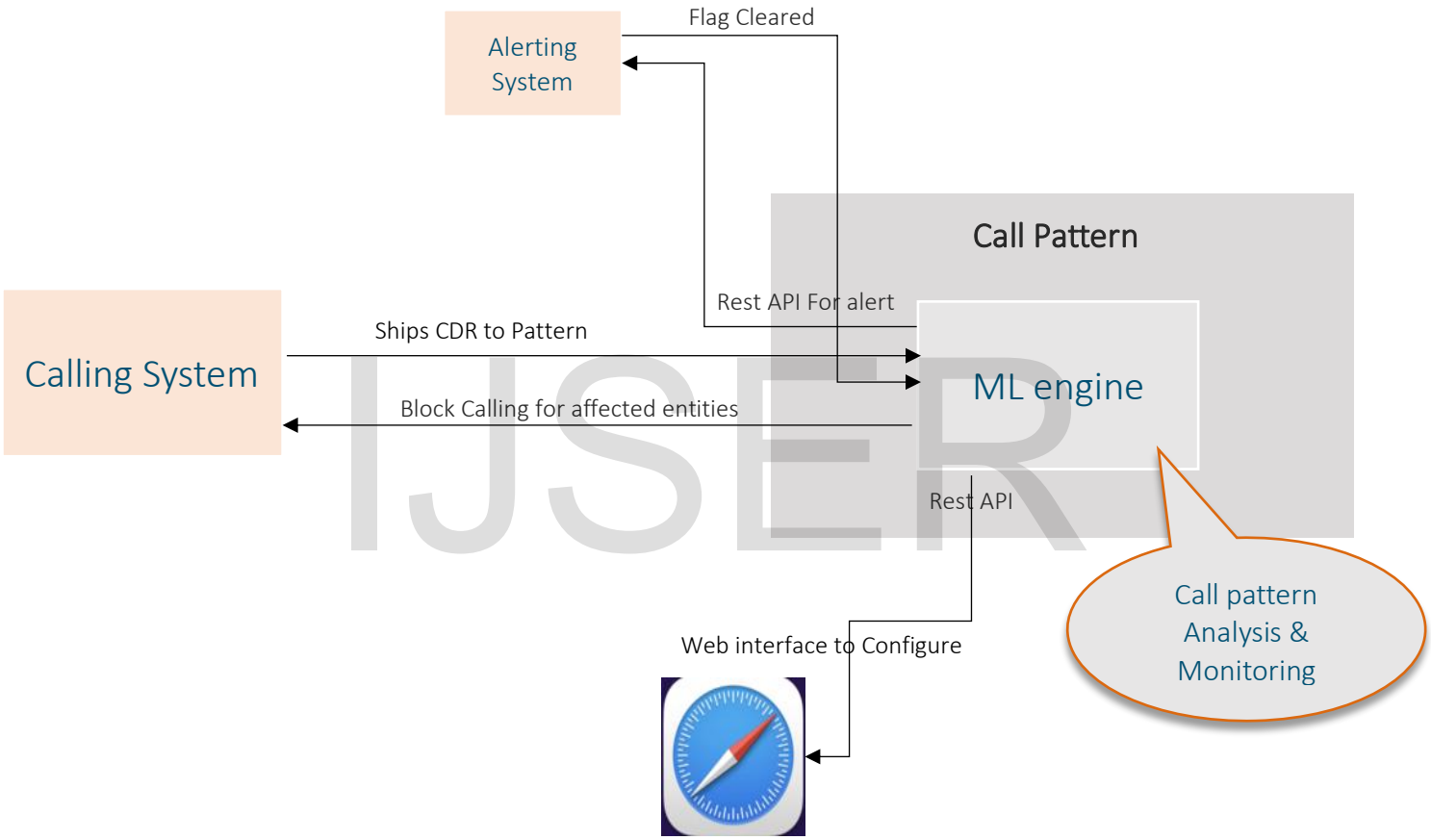
Benefits of Pattern

Pattern based on Usage are real data which can predict the ***trend***. It can also classify the Calls on their ***legitimacy***.

Pattern based detection also honors the ***Privacy*** of consumer by not recording any PII. Even the called number will be categorized and stored, instead of storing the number

Patterns can self-evolve based on usage. Its tamper proof from unauthorized usage.

Design



Details on Design

The entire Design of Call Pattern system is based on 3 components

CDR receiver

The stack which will receive the CDR from the Calling system. Its sole purpose is to Read the CDR > Anonymize it > Store Non PII Data like Called location type, Time of call, Caller's Device information.

Rest API interface

- This stack allows Call Pattern monitor to Allow Configuration by Service provider/Administrator and by the Consumer itself
- It also allows connectivity to other alerting system to flag any fraudulent activity and accept the flag clearance by Service provider/Administrator and by the Consumer itself

ML Engine

ML engine is the core of the solution, It is used to derive the call pattern by consuming the data from CDR receiver and Configured pattern through Rest API. This engine learns from the Flag and Pattern hence can detect any anomaly.

Flow Scenario

- A global UCaaS/ CaaS (Calling as a Service) service provider configures a Calling pattern for its Reseller as
  - ~ 100000 Concurrent calls per hour
  - ~ Calls to Afghanistan is considered as rare (max 5 calls in a week)
  - ~ Calls to Premium Service limited to 10$ per hour
- Service Provider "MyPhoneService" gets onboarded to the UCaaS. Service provider sets this config for calling pattern for its user & Enterprises and Location
  - *~ 1000 Concurrent calls per Enterprise per Hour*
  - *~ 100 Concurrent calls per Location per Hour*
  - *~ 50 calls per user per Hour*
  - *~ Calls to Tunisia and Cuba are considered as Rare (max 5 calls in a week) per enterprise*
  - *~ Calls to Premium Services limited to 3$ per hour for each enterprise*
  - *~ Calls to Premium Services limited to 2$ per hour for each Location*
  - *~ Calls to Premium Services limited to .5$ per hour for each User*
- Service Provider "MyPhoneService" sells an Enterprise Calling service to "MyEnterprise". MyEnterprise configures following pattern for calling –
  - *~ 50 Concurrent calls per Location per Hour*
  - *~ 30 calls per user per Hour*
  - *~ Calls to Brazil and India are considered as Rare (max 5 calls in a week) per enterprise*
  - *~ Calls to Premium Services limited to 2$ per hour for each Location*
  - *~ Calls to Premium Services limited to 1$ per hour for each User*
- MyEnterprise onboards its two location: New York & London. In New York, Alice gets onboarded.
- Alice doesn't like to make lots of calls and would want to make sure that her phone doesn't get misused. Alice configures her pattern
  - ~ Block all International Calls
  - ~ Block all Premium calls on Monday & Tuesday
  - ~ Max calls allowed in a day 10
  - ~ Working hours defined as 9 AM till 7 PM
- Machine learnt/Adapted

~ Alice never makes calls to Premium Number after 2 PM
~ Alice never makes calls to California
~ Alice never makes calls to international numbers after 11 AM.
~ Alice never talks for more than 10 mins on a single call

Fraud Scenario 1

- After Alice leaves office at 6:30 PM on Monday. The Janitor uses Alice's Phone and dials a Premium number
  - Since Core engine has learnt that Alice doesn't make call at 6:30. Hence an alert get sent to Alice and MyEnterprise , MyPhoneService and Global UCaaS admin.
  - Alice clears the flag since Janitor already updated her. ML learns for this exception case, hence no action done on the active call
- At Midnight, some Machine initiates Multiple automated calls from Alice's account.
  - ML engine detects this Fraud as its against pattern of Alice. Hence an alert get sent to Alice and MyEnterprise , MyPhoneService and Global UCaaS admin.
  - Alice confirms it as a Fraud. ML initiates a terminate thread to get the call terminated by Calling System. It marks it as fraud and blocks further calls
- Alice's Phone registers to the calling system from an IP originating from Israel.
  - ML engine detects this Fraud as its against registration pattern of Alice. Hence an alert get sent to Alice and MyEnterprise , MyPhoneService and Global UCaaS admin.
  - MyEnterprise confirms it as a Fraud. ML initiates a terminate thread to get the call terminated by Calling System. It marks it as fraud and blocks further calls from Alice's phone until Alice confirms.

Conclusion

The Fraud system proposed here is capable of

- Handling fraud which originates by Automated dialing machines
- Handling Fraud due to unauthorized access of Device.
- Initiating a regional lockout of User or Location or Enterprise or Entire system

Benefits

- Saves Billions of $ which gets lost in Fraud.
- Enhance customer's trust on the organization.
- Portable, Cloud native, Can be attached to any UCaaS service.