Threat Detection Risk Identification Model in Telecom Operators

Winter Online Doctoral Workshop 2018

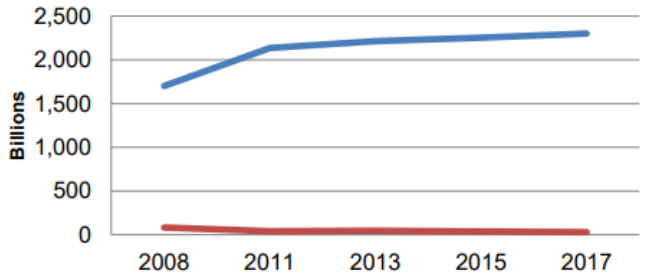
Pedro Fidalgo

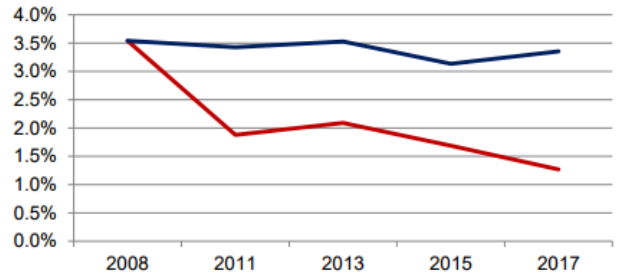
Topics

- Telecom Fraud Numbers
- Evolution to IP Networks
- Fraud Classification
- Fraud Detection
- Complex Adaptive System

Fraud Numbers

	2008	2011*	2013	2015	2017	% Var
Estimated Global Revenues	$1.7 Trillion (USD)	$2.1 Trillion (USD)	$2.2 Trillion (USD)	$2.25 Trillion (USD)	$2.30 Trillion (USD)	+2.2%
Estimated Global Fraud Loss	$60.1 Billion (USD)	$40.1 Billion (USD)	$46.3 Billion (USD)	$38.1 Billion (USD)	$29.2 Billion (USD)	-23.3%
% Loss*	3.54%	1.88%	2.09%	1.69%	1.27%	-0.4%





- 2017 - 29.2 B per year , 1.27% of their revenues
- 2008 – 60.1 B per year, 3.54% of their revenues

Change to all IP Networks

CHANGE

- Shifting from TDM (Time-Division Multiplexing) to IP
- Not only phones …IoT..3.5 IP addresses per capita in 2021 (2.3 today)

IMPACT

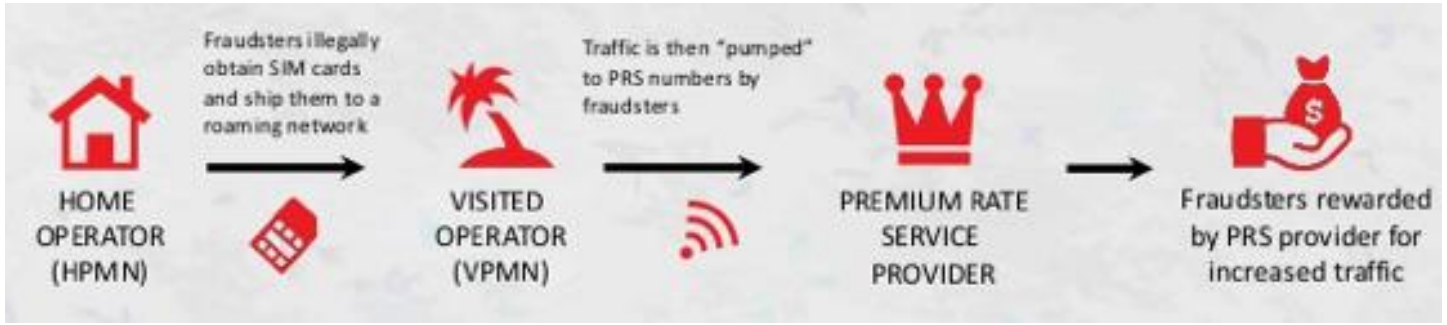
- Increase of the attack Surface and Vectors
- Higher volumes of data, more time to detect…more revenue loss
- New Risks and Unknown threats

Unknow Threats

While Fraud types tend to be the same, the enablers and methods to commit it are mutating and evolving constantly, year after year. The patterns that trigger the fraud alarms today can be totally new tomorrow, or, changed for combination and mutation of existing methods, that's what makes fraud hard to detect, sometimes with a large amount of false positives.

Fraud Classification

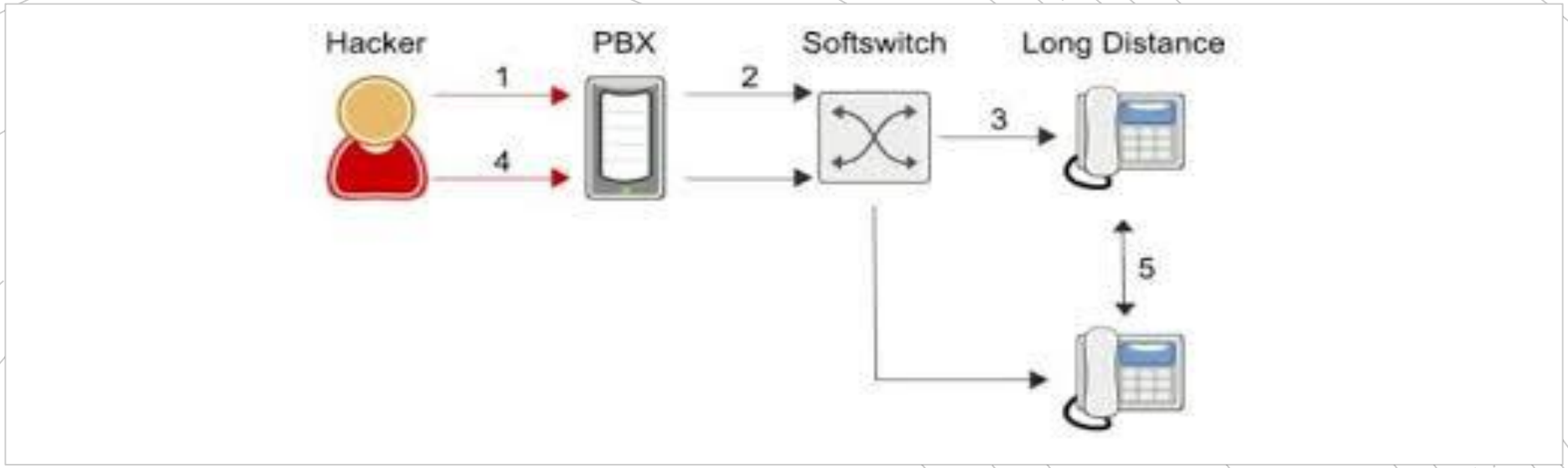
- 2 Dimensional Fraud Classification Model (CFCA & TM Forum)
  - Fraud Enabler or Method
  - Fraud Type (Monetize)



Method - Subscription Fraud

One Fraud Type …. Multiple Fraud Methods

Fraud Type - International Revenue Fraud



Method – PBX Hacking

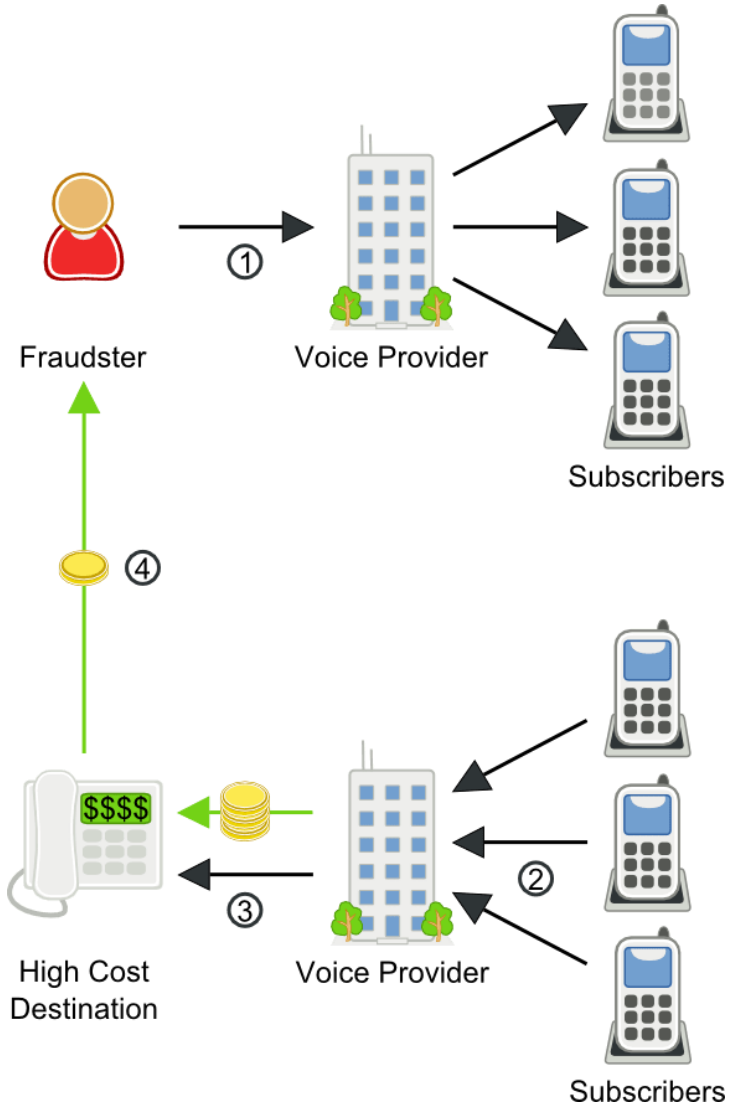
One Fraud Type …. Multiple Fraud Methods

Fraud Type - International Revenue Fraud

Method – Wangiri

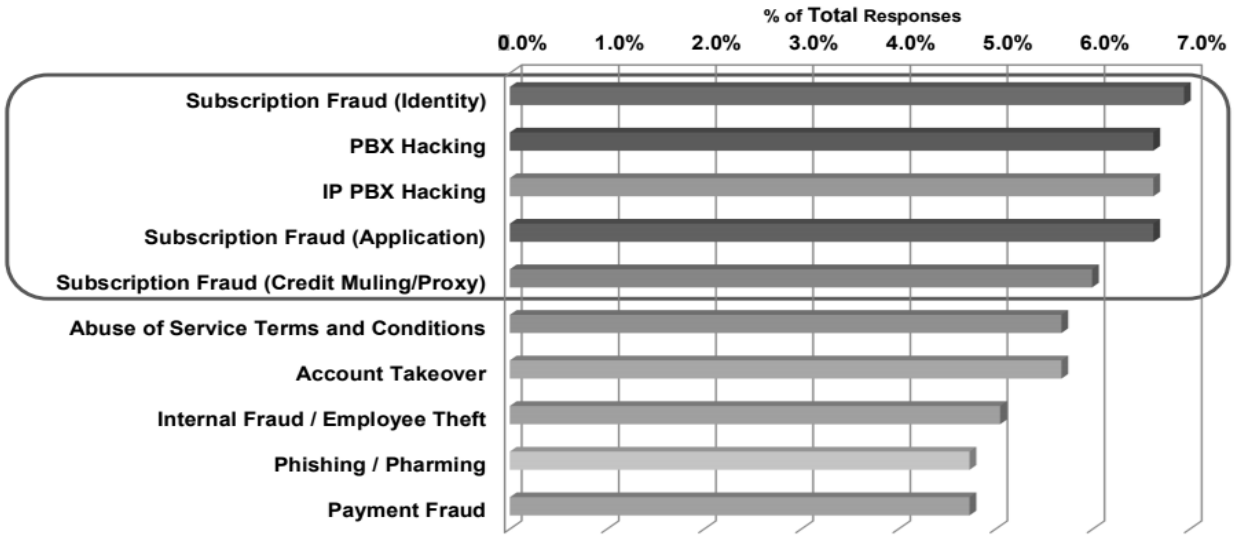
One Fraud Type …. Multiple Fraud Methods

Fraud Type - International Revenue Fraud

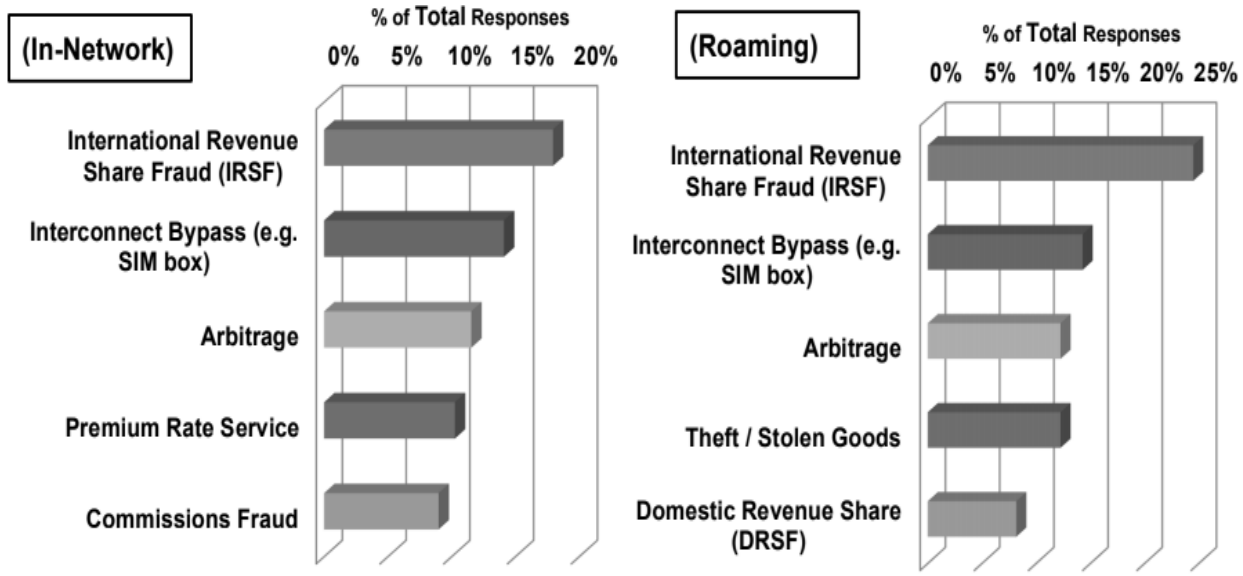


Location Changes the goals and methods

- Top 5 Fraud Methods



- Top 5 Fraud Types



Risk Identification Aproaches (State of the Art)

- Model Based Engineering - > UML Sec, TREsPASS, CRID
- Threat Modelling - > STRIDE, PASTA …
- Structural Analysis –> Frame analysis
- Business Processes - > BPM oriented to risk
- Data Mining -> Clustering and Classification (patterns)
- Methods and Standarts -> ISO 9001, NIST
- Survey and Brainstorming -> think like a fraudster, audit quality
- Probalistic Analisys -> Neural Networks, past behavior vs current

Fraud Detection Methods (focus on Know)

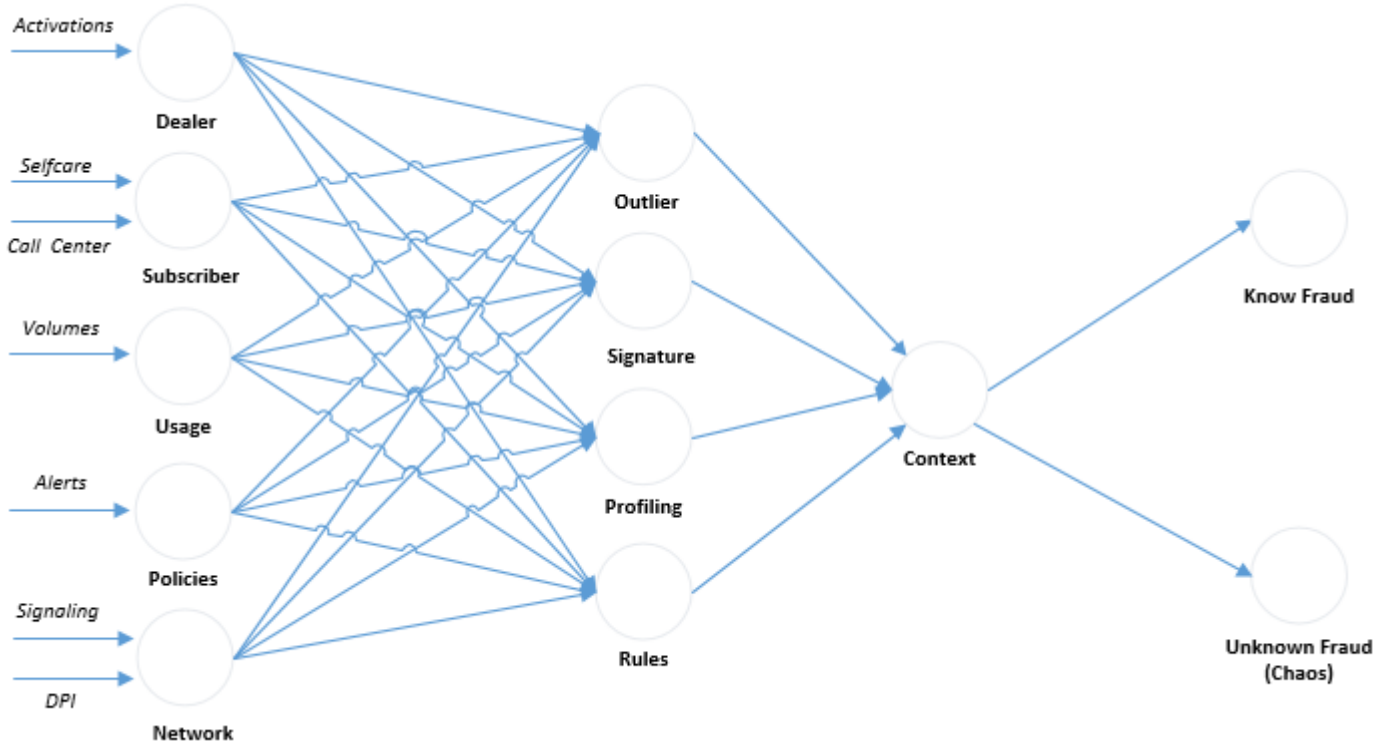
- ***Misused Detections***, where previous fraud behaviors under the form of patterns or signatures are compared with current activity
- ***Anomaly or Behavior Detection (Profiling)***, compares current activity with normal past behavior looking for significant deviations
- ***Specification Based Detection***, the system behavior is defined and any behavior outside the defined boundaries is labelled as attack
- ***Outlier Detection***, a non-standard observation with a high level of deviation from other observations

Fraud(Key) Chalenges

- ***Reduce detection time***
- ***Increase Accuracy Rate***
- ***Predictive Pattern Generation***
- ***Adaptive Pattern Recognition***
- ***Context Aware***

Complex Adaptive System

(Emergent Behavior)



The study of complex systems requires a system approach. Such an approach "focuses on the arrangement of and relations among the parts, which connect them into a whole (von Bertalanffy, 1968).

Directions

- "Chaos provides an understanding of the appearance of **unpredictable behavior by constructing models which reveal order**."[Kellert, 2014]
- ***Pattern Prediction on Complex Phenomena***