Fraude dans la Telephonie

Aurélien Francillon

Merve Sahin

With Monaco Telecom

Also with cooperations:
NYU Abu Dhabi
Georgia Tech
Telecom Paris Tech (Marc Relieu)

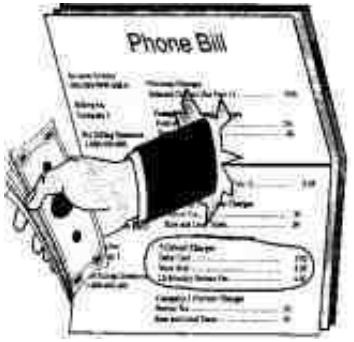
Telephony Fraud

- A long-standing problem (1870s → 2010s)
  - Early fraud mechanisms: aiming to make free calls

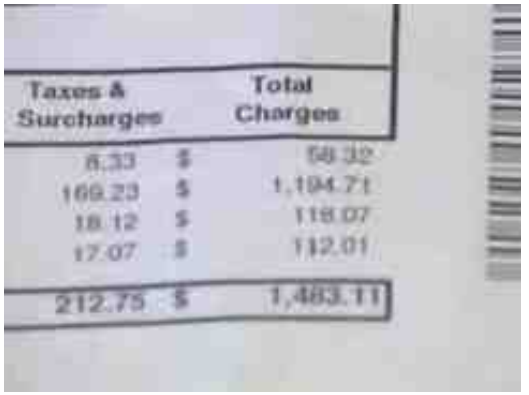
  - Today:
    - Convergence of multiple technologies
    - Multiple actors involved
      - Operators, VoIP providers, 3rd party services, enterprises…
    - Touching over 7 billion people
    - Massive volume of traffic

Telephony fraud: Some examples

- Small charges on your phone bill



- Stolen phone or SIM card



- Unknown international caller IDs

- Unwanted calls and voicemails

Consequences of Telephony Fraud

In 2015, estimated **financial loss for operators** was $38.1 billion*

[*] CFCA Global Fraud Loss Survey, 2015

- In the US, 400K+ **spam call complaints** (monthly)
- In France, 574K complaints last year

Attacks on **critical infrastructure** (e.g., TDoS* on emergency lines)

[*] Guri et al., “9-1-1 DDoS: Attacks, Analysis and Mitigation”, EuroS&P'17

Effects on **online security**

- Technical support scams
- Telemarketing calls recording sensitive information

[*] D. Cameron, “Major leak exposes 400K recorded telemarketing calls, thousands of credit card numbers”, 2017.

Problems with Telephony Fraud

- Multi-dimensional problem
  - Technologies, regulations, law, historical background
- Multiple fraudulent actors
- Various skills and motivations
- Confusing terminology
  - Different terms for the same problem
  - Same term for different problems
- Limited public documentation, not comprehensive

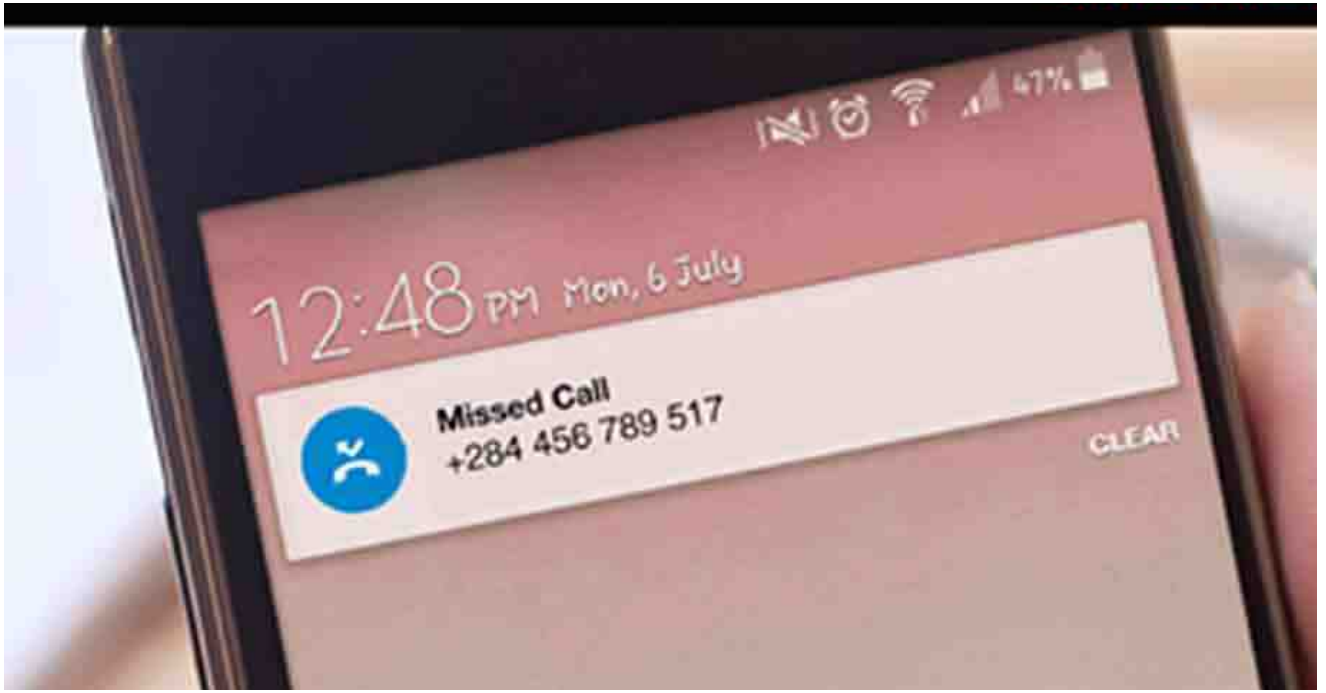
Telephony fraud and vulnerabilities are not well understood

Without a good understanding, we cannot effectively fight fraud!

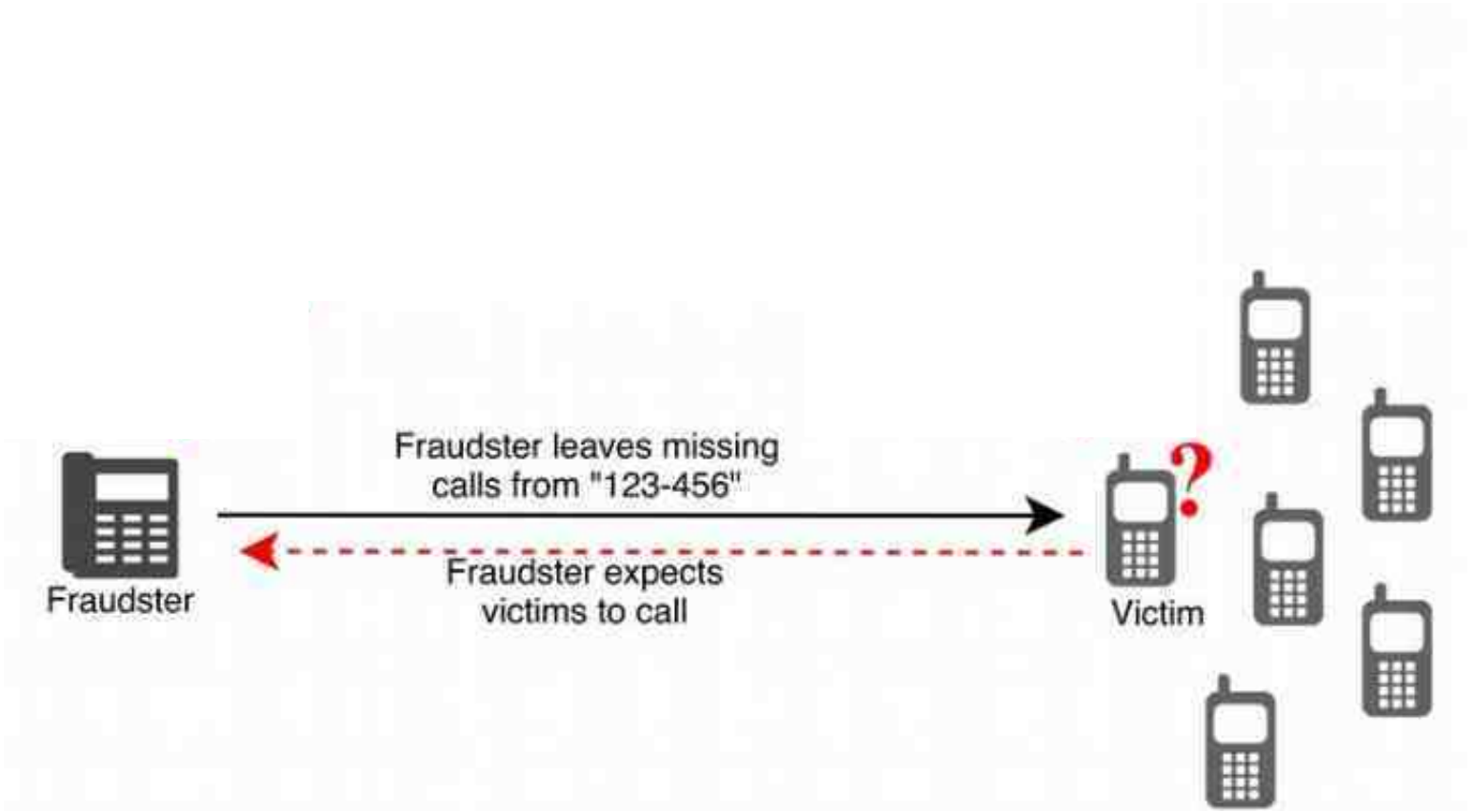
Some of your work, so far

- A taxonomy for telephony fraud [IEEE EuroS&P'17]
  - Holistic view, clear terminology, a publicly available guide
- Detailed study of 3 fraud schemes
  - Over-The-Top (OTT) bypass fraud [ACM CCS'16]
    - Position it in the taxonomy
    - Evaluate existing solutions
    - Measure its effects with a case study
  - International Revenue Share Fraud (coming soon...)
    - Understand why it is difficult to address
    - Understand the drawbacks of existing solutions
    - Propose a way to improve detection
  - Voice spam [Usenix SOUPS'17]
    - Analyze a new defense approach

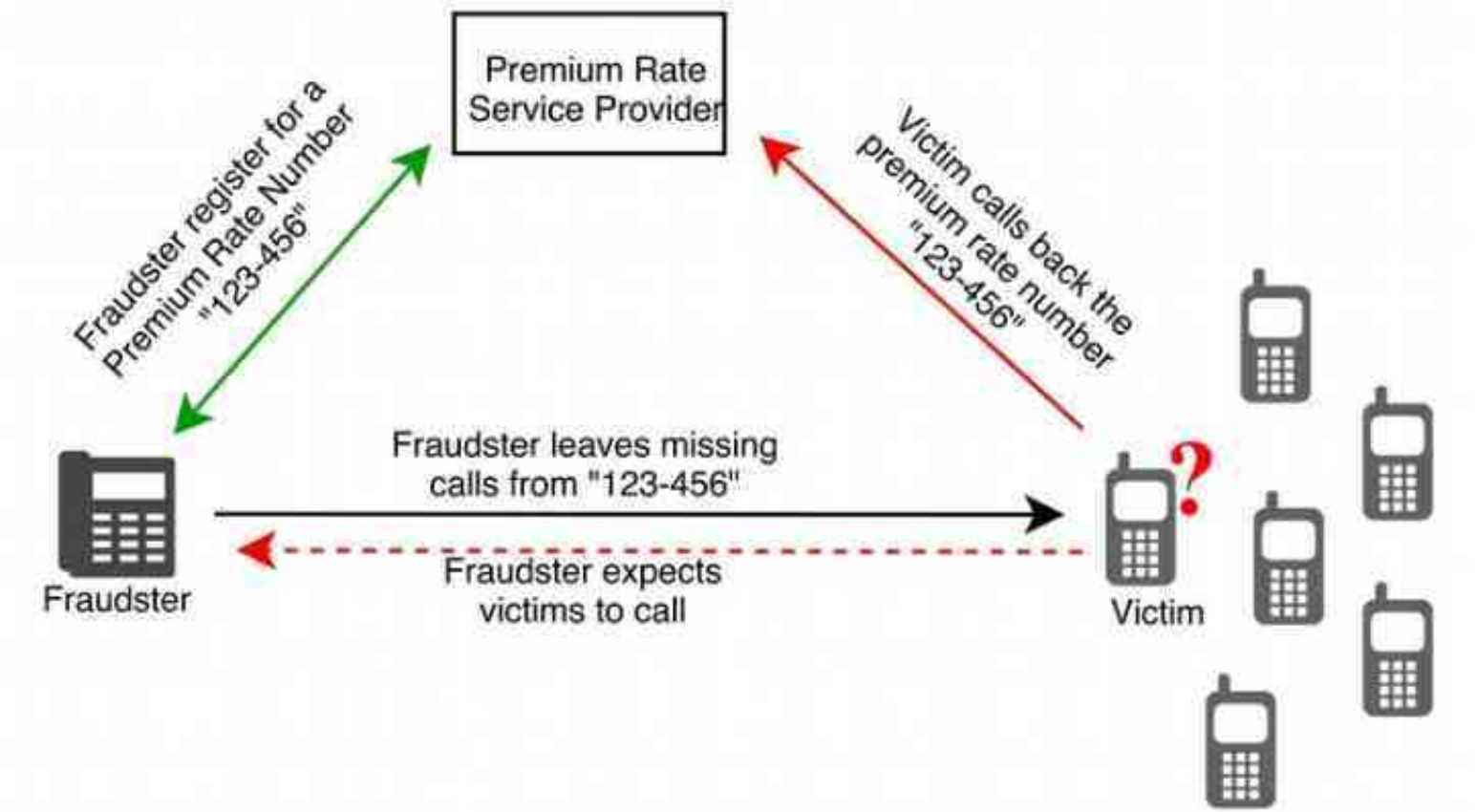
Example: Callback Scam



Example: Callback Scam



Example: Callback Scam

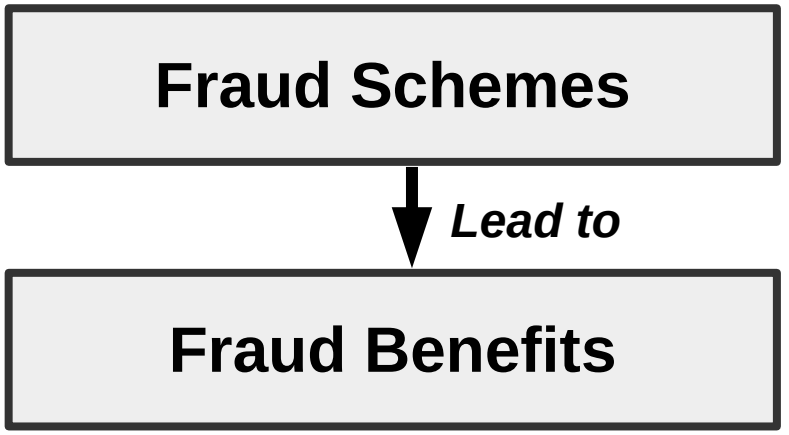


Example: Callback Scam

Fraud Schemes

Callback scam

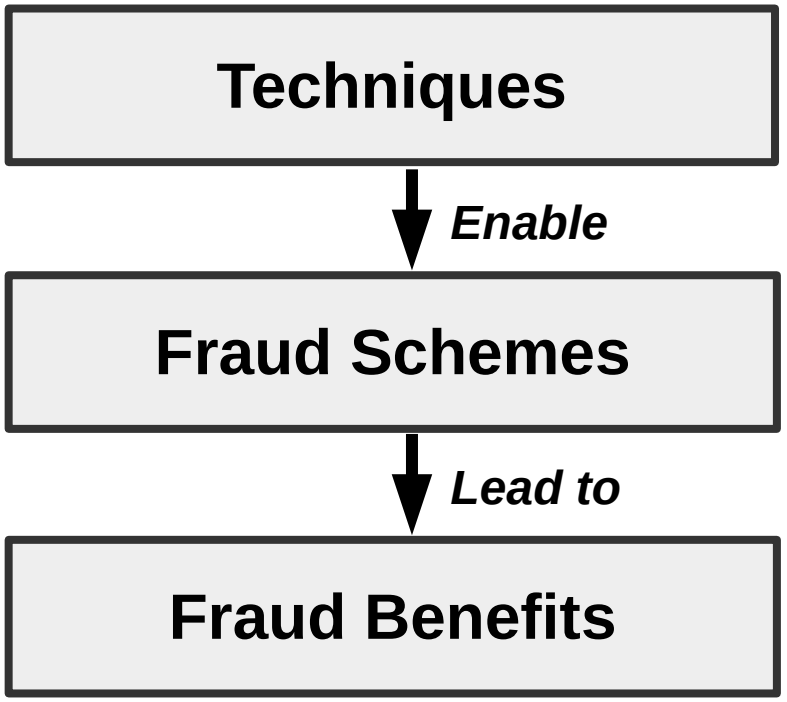
Example: Callback Scam



Callback scam

Get a share from call revenue

Example: Callback Scam

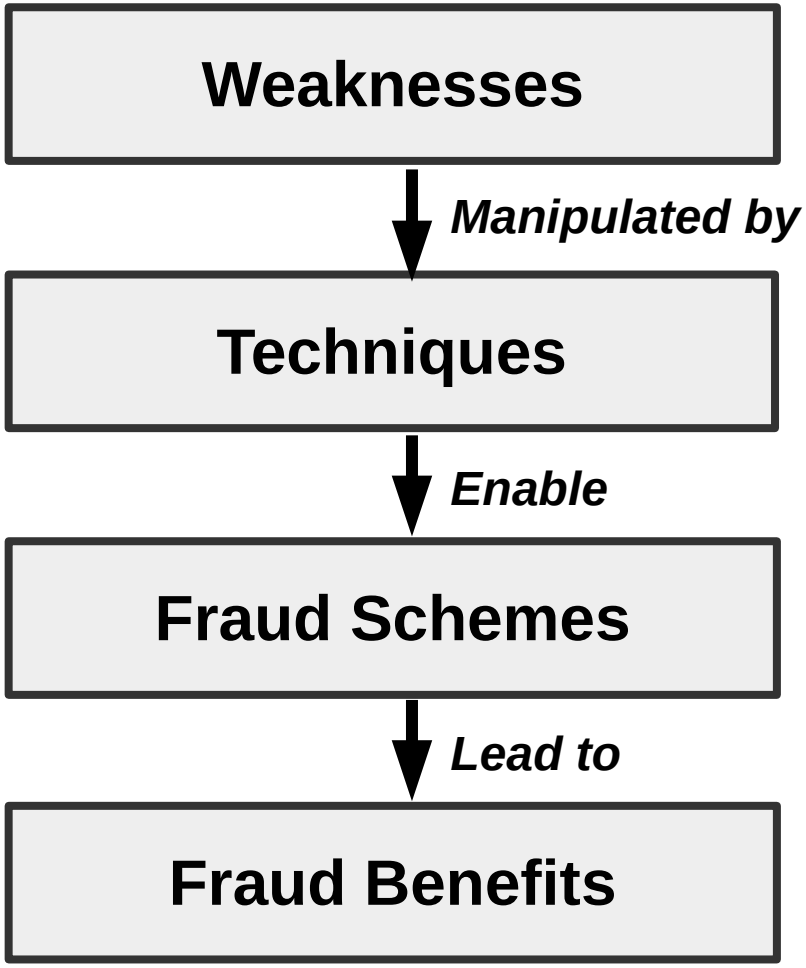


Caller ID spoofing, Auto-dialers, Social engineering

Callback scam

Get a share from call revenue

Example: Callback Scam



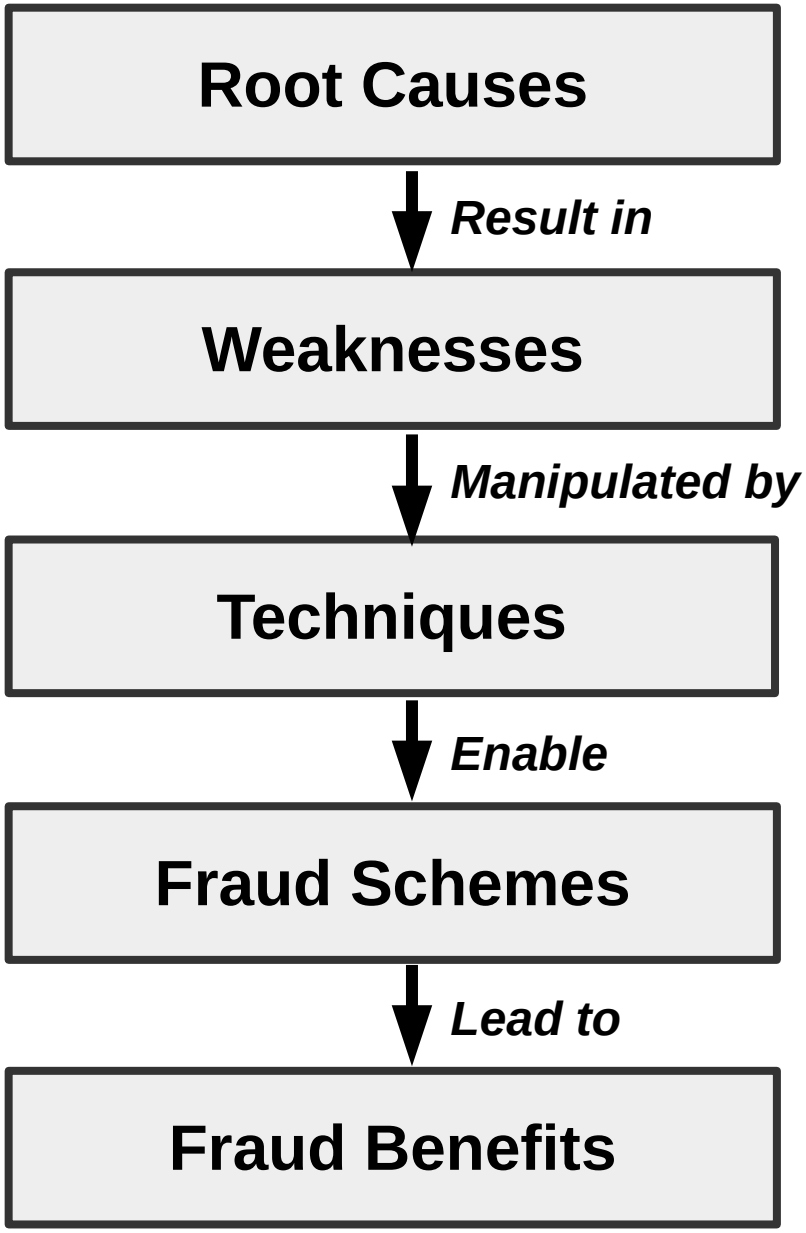
Lack of Caller ID authentication,
Lack of security & fraud awareness

Caller ID spoofing, Auto-dialers,
Social engineering

Callback scam

Get a share from call revenue

Example: Callback Scam



Legacy/Insecure protocols,
Interconnection of poorly understood technologies

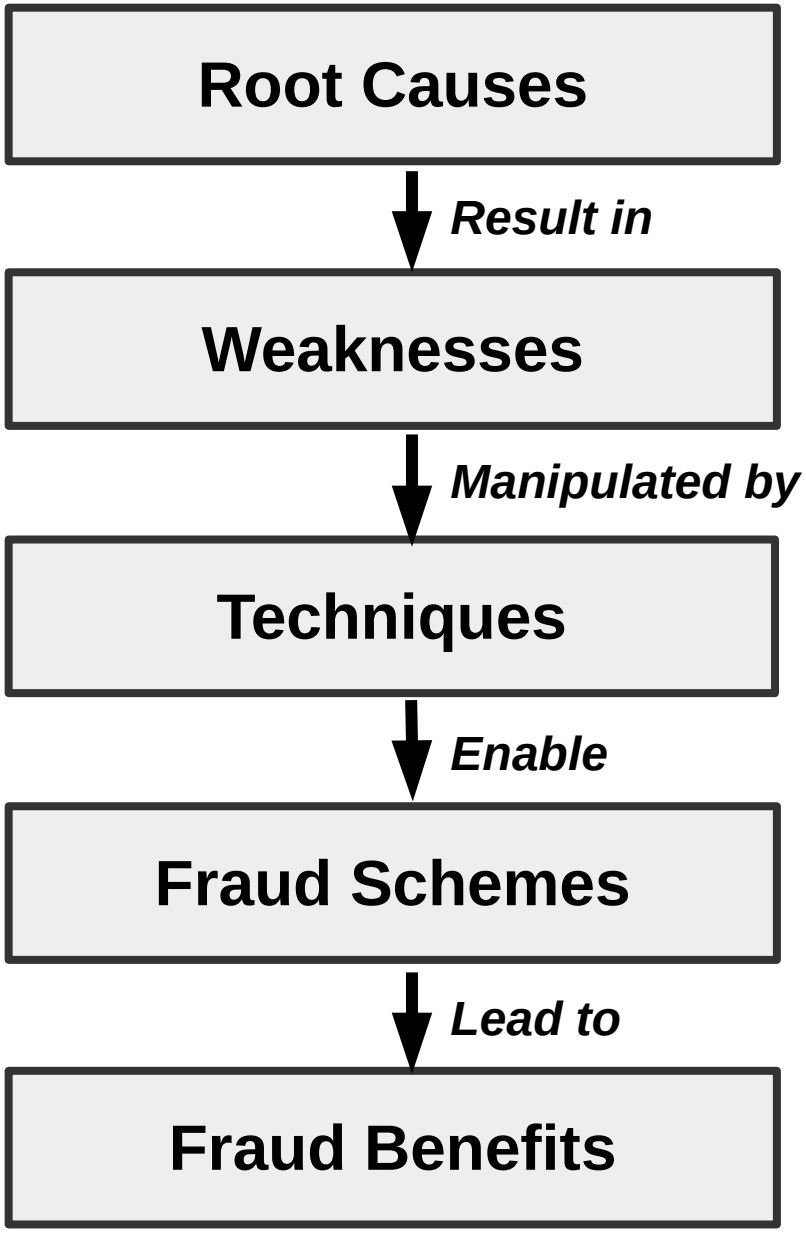
Lack of Caller ID authentication,
Lack of security & fraud awareness

Caller ID spoofing, Auto-dialers,
Social engineering

Callback scam

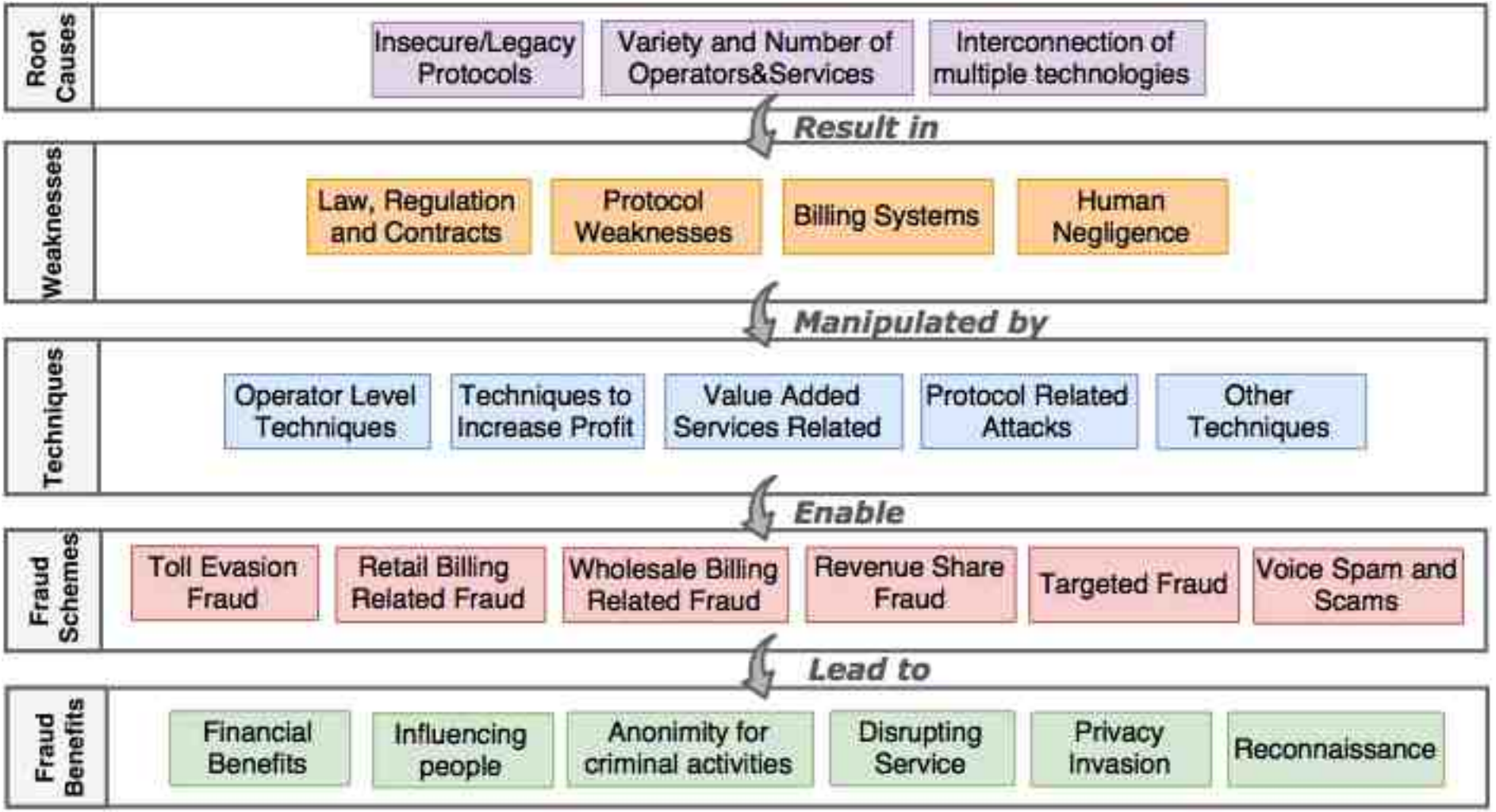
Get a share from call revenue

A definition

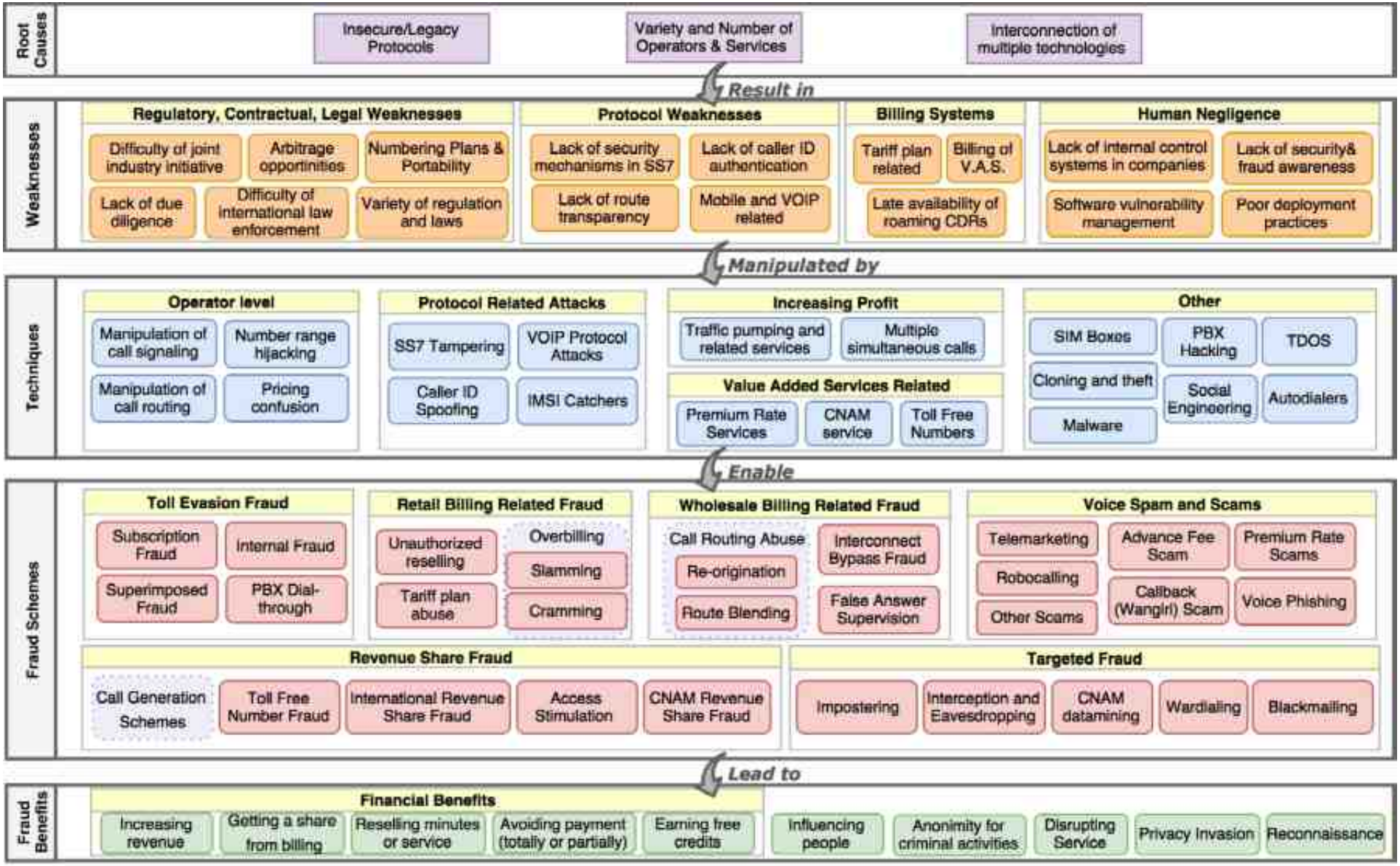


- A **fraud scheme** is a way to obtain an **illegitimate benefit** using a **technique**. Such techniques are possible because of **weaknesses** in the system, which are themselves due to **root causes**.

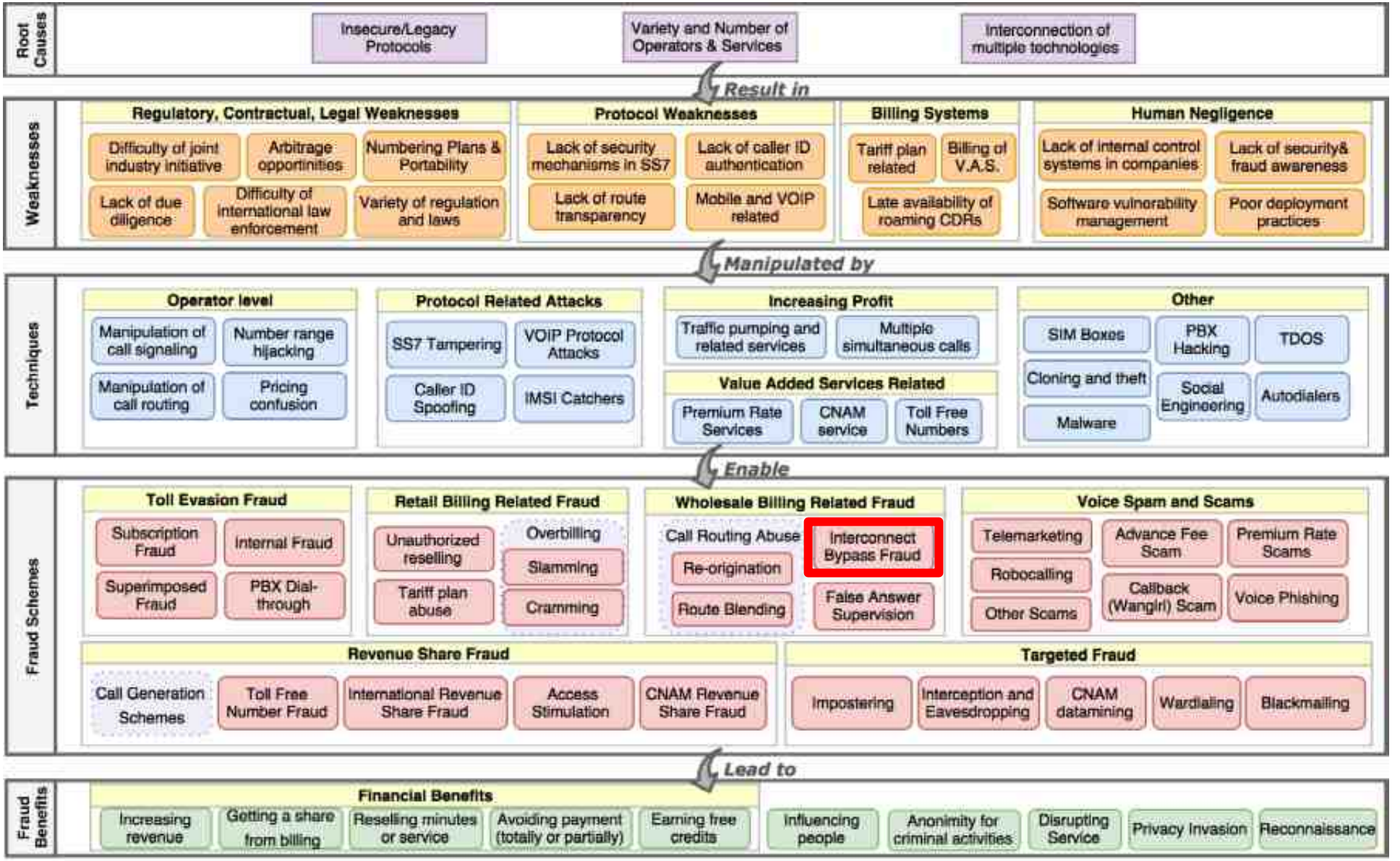
Our taxonomy



Our taxonomy



Interconnect Bypass Fraud



Interconnect Bypass Frauds

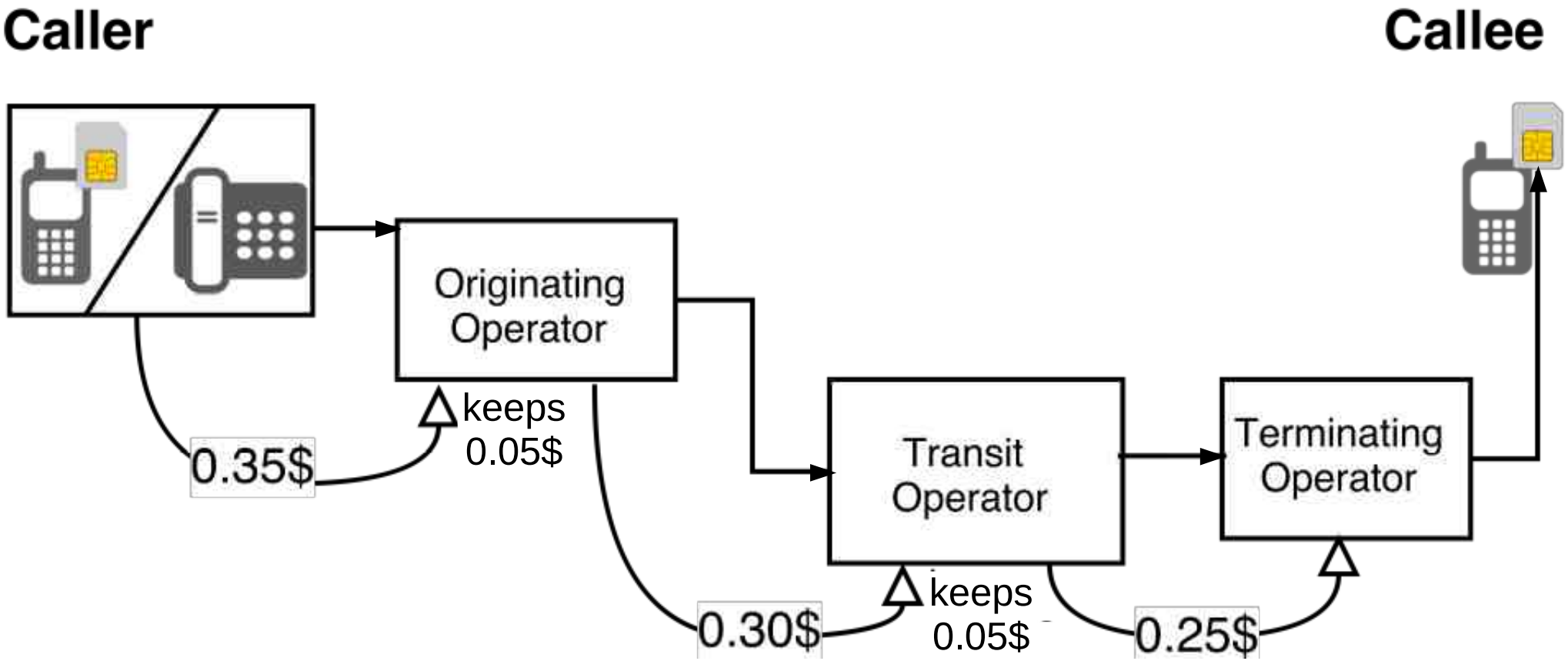
- Bypassing International call termination fees
  - Not going through normal routes
  - Calls routed on “VoIP”
- Multiple well known schemes:
  - SIM Boxes (VOIP-GSM gateways) used with stolen sim cards
  - Compromised (IP-)PBX
- OTT-Bypass:
  - More recent, uses Smartphones voice chat applications*
  - “Cooperation” with transit operators

SIM Box with many sim cards (sim card server)

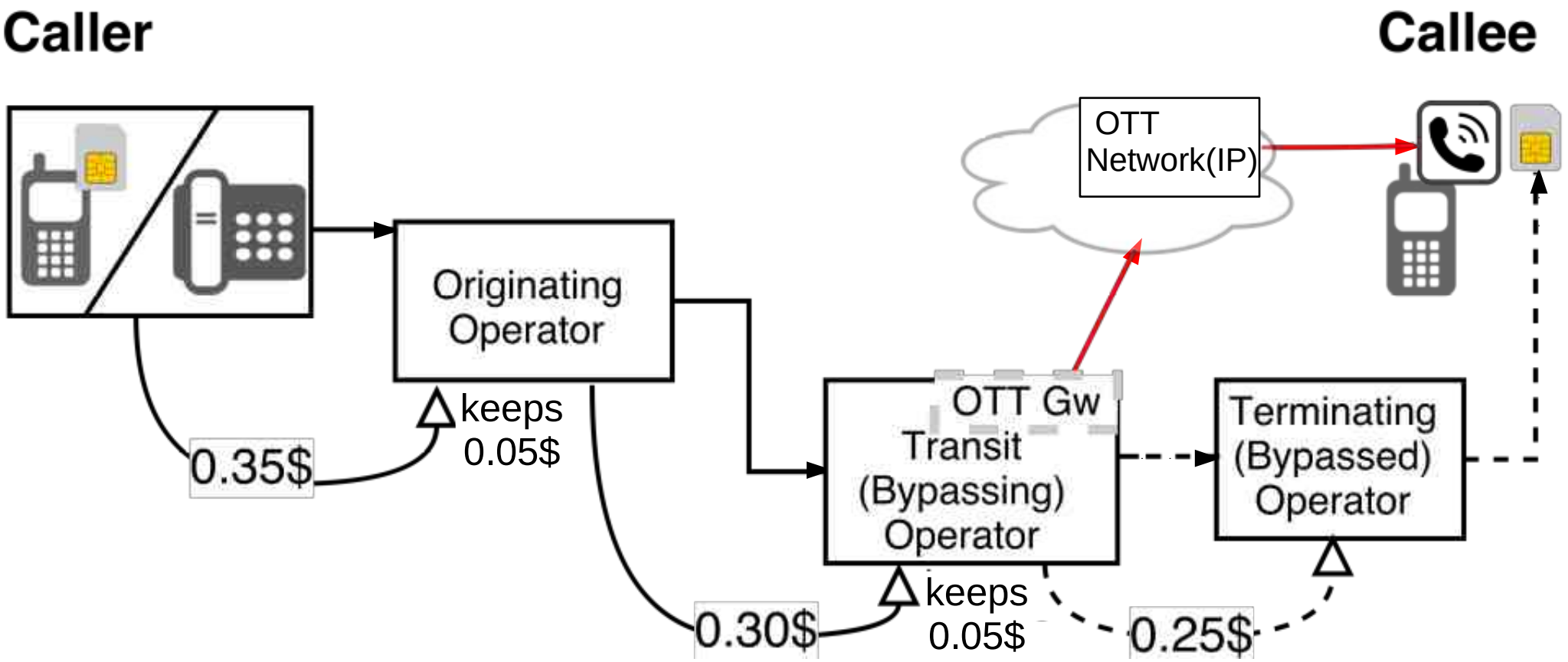
IP-PBX, voice communication server over IP

* Sorry ! Our lawyer does not want us to disclose which app

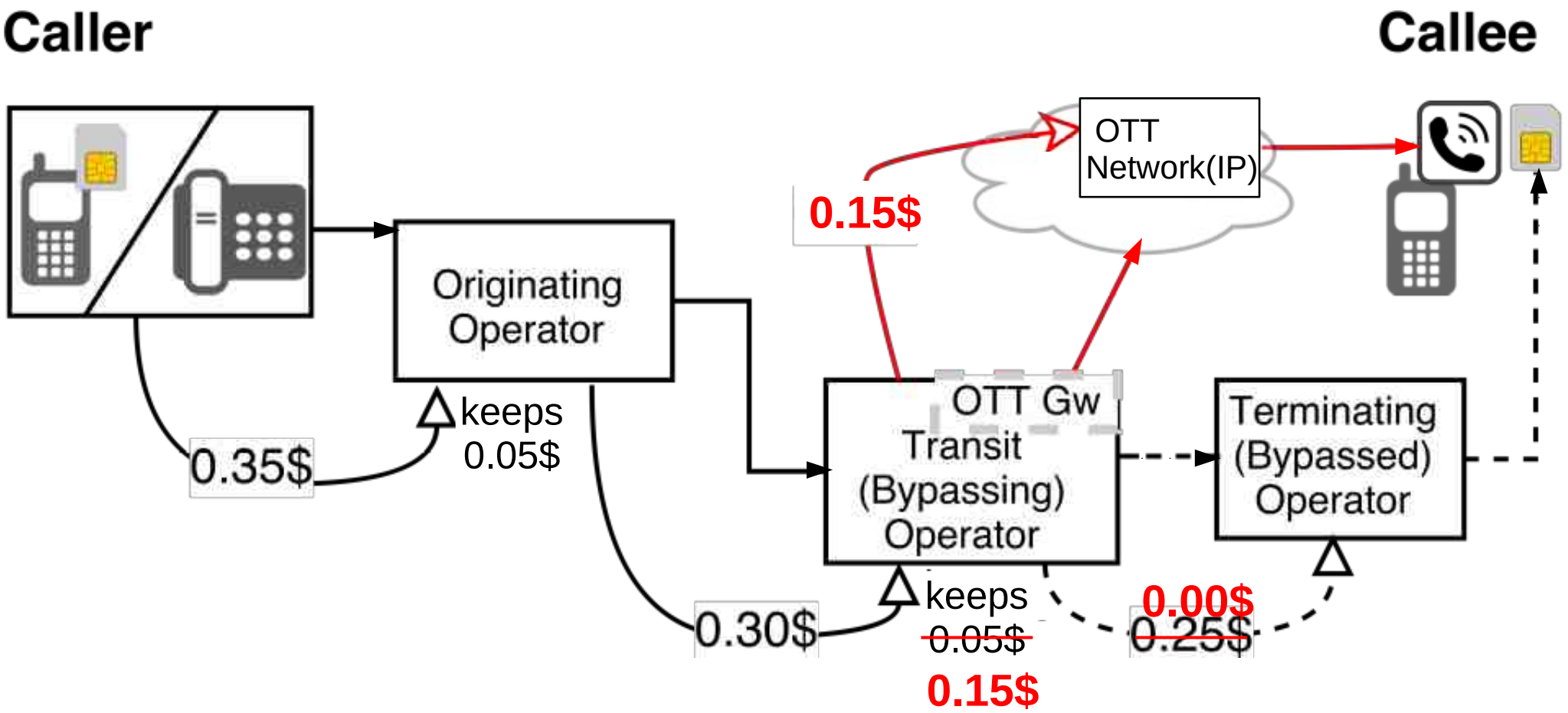
Regular International Call



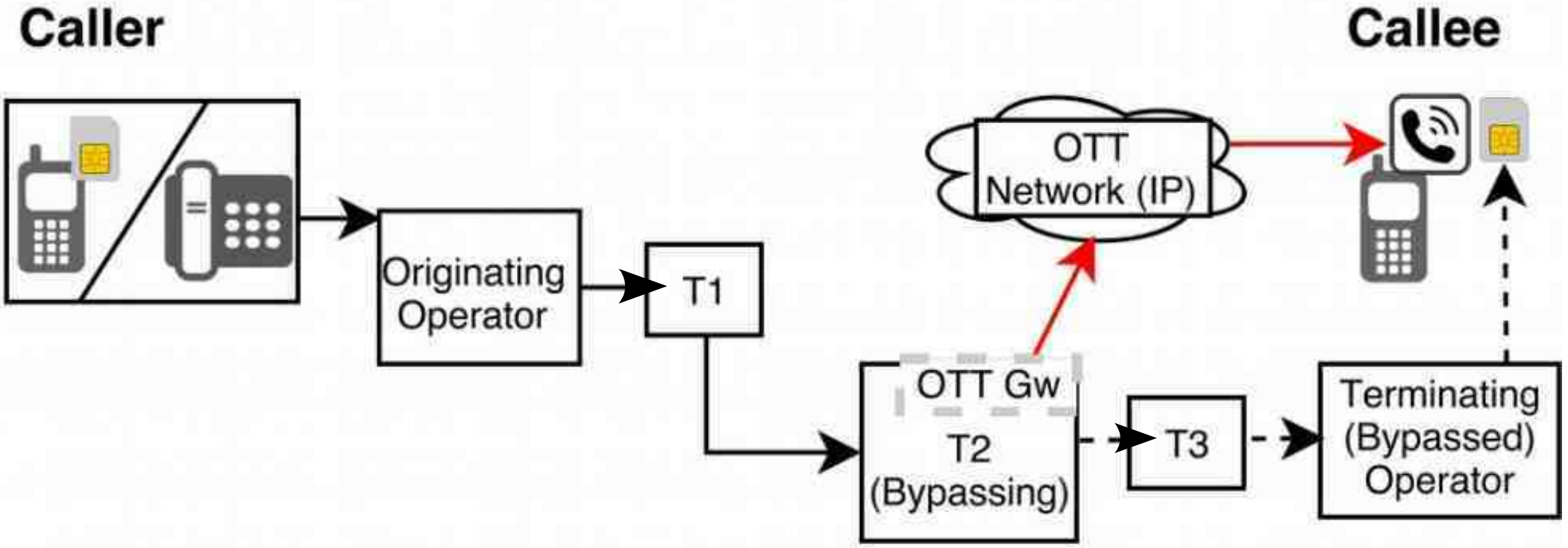
OTT Bypass Call



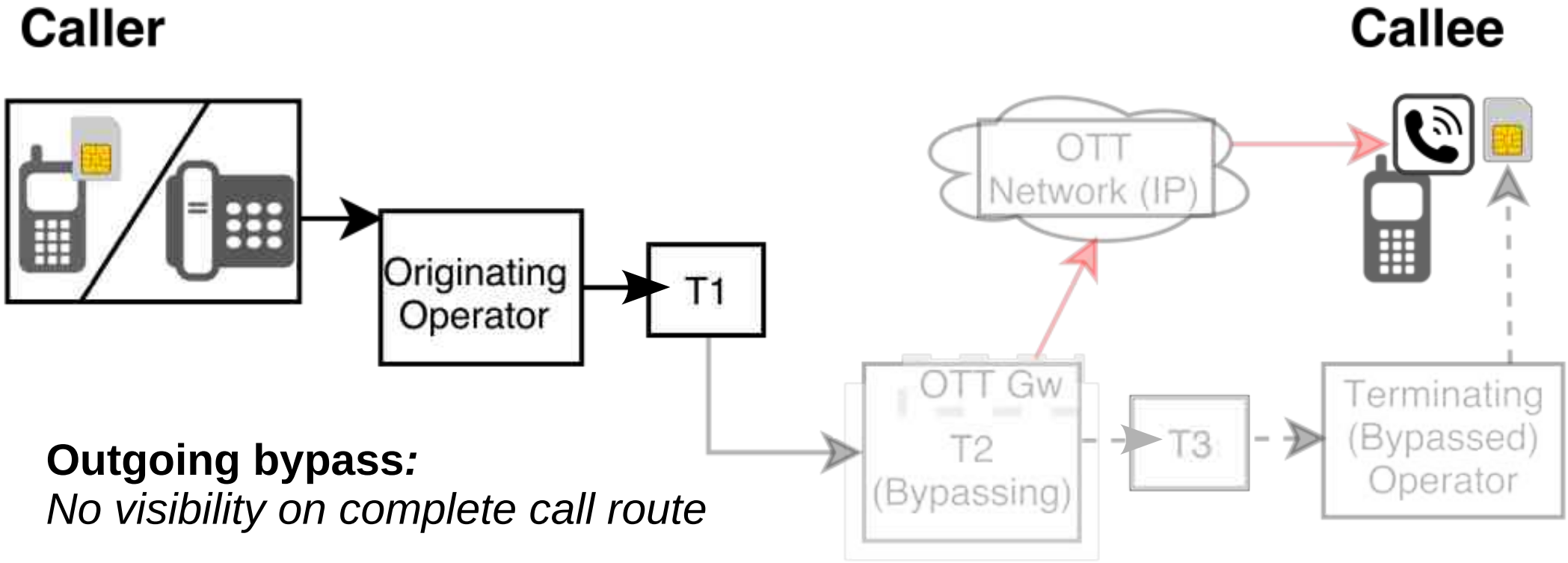
OTT Bypass Call



Detecting and Measuring OTT Bypass: Challenges

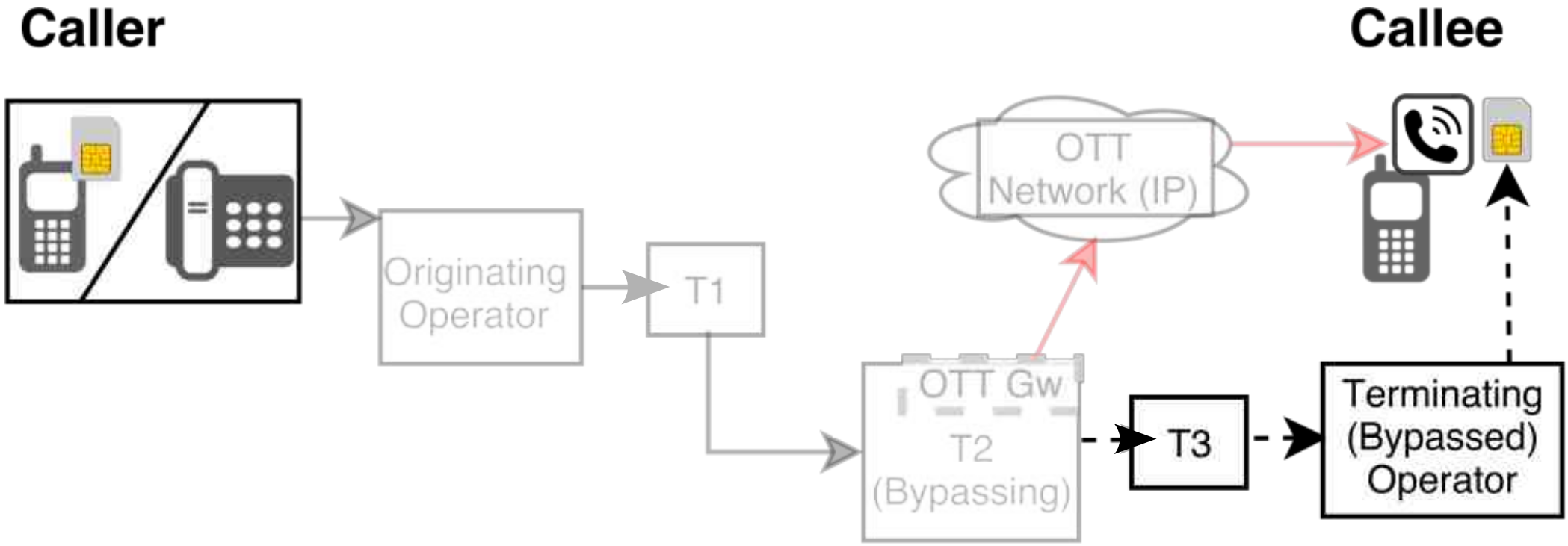


Detecting and Measuring OTT Bypass: Challenges



Outgoing bypass*:*
No visibility on complete call route

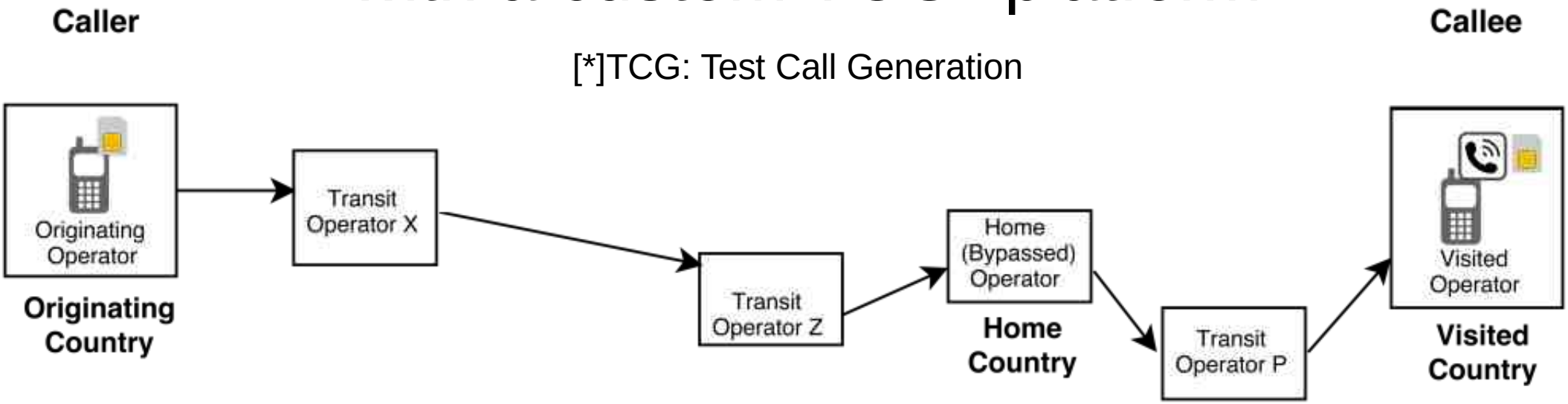
Detecting and Measuring OTT Bypass: Challenges



Incoming bypass*:*
No visibility on bypassed call logs

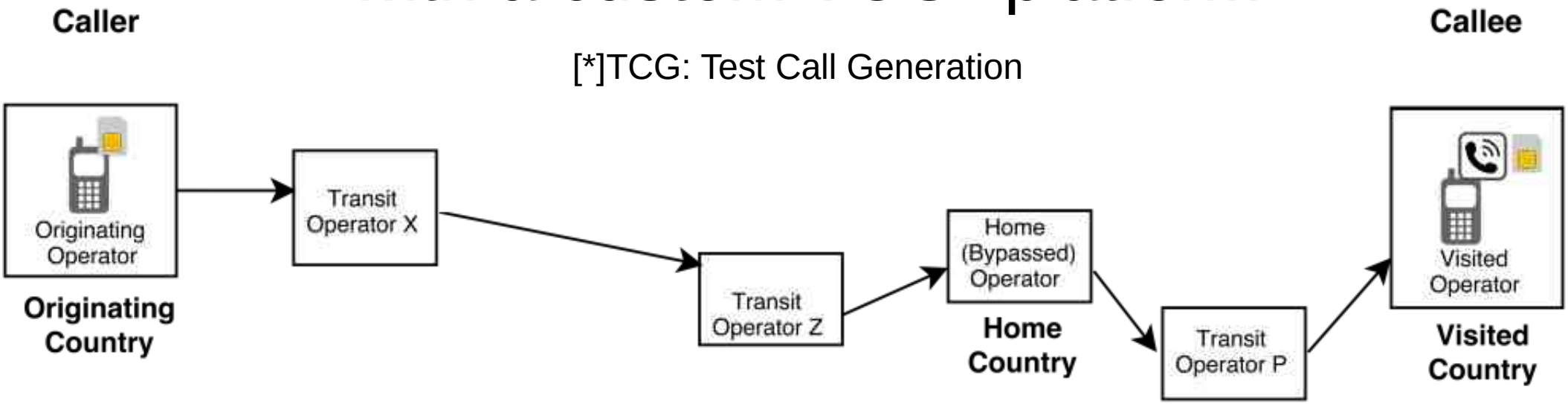
Case Study: Measuring OTT bypass
- on a Small European Country
- with a custom TCG* platform

[*]TCG: Test Call Generation



Case Study: Measuring OTT bypass - on a Small European Country - with a custom TCG* platform

[*]TCG: Test Call Generation



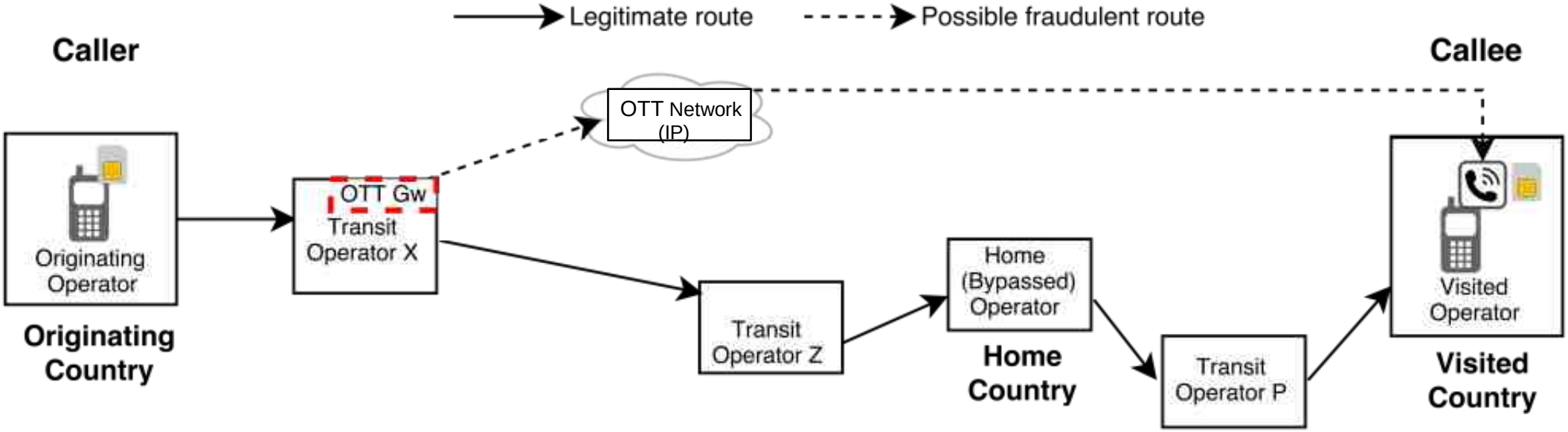
- *Spain*
- *Turkey*
- *United Kingdom*
- *Italy*
- *Netherlands*
- *Germany*
- *Austria*
- *Switzerland*

Experiment Setup

- Customized Android phones
- 4 SIM cards from victim operator
- Recipient phones roaming in France
- Calls originating from 8 countries (1 operator per country)
- Centralized collection of call logs
- 15000+ test calls over 4 months

- *France*

Overall bypass

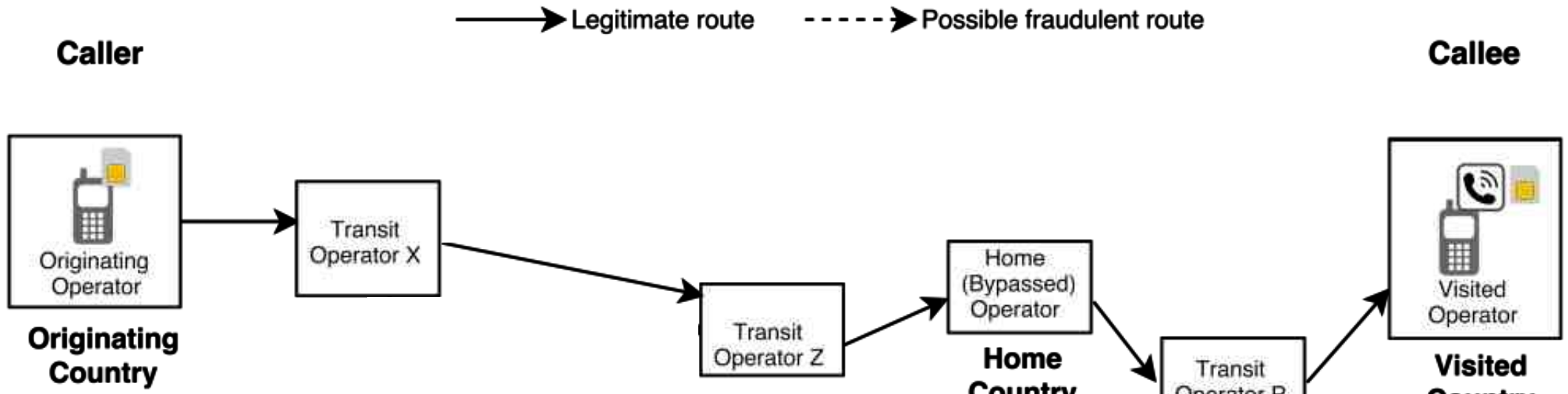


- ***Spain – 83%***
- ***Turkey – 72%***
- ***United Kingdom – 61%***
- ***Italy – 56%***
- ***Netherlands – 53%***
- ***Germany – 42%***
- *Austria*
- *Switzerland*
- *France*

Results

- Up to 83% of calls were subjected to bypass in 6 of 8 countries
- OTT bypass leads to quality problems in call establishment
- Multiple fraud schemes may collide

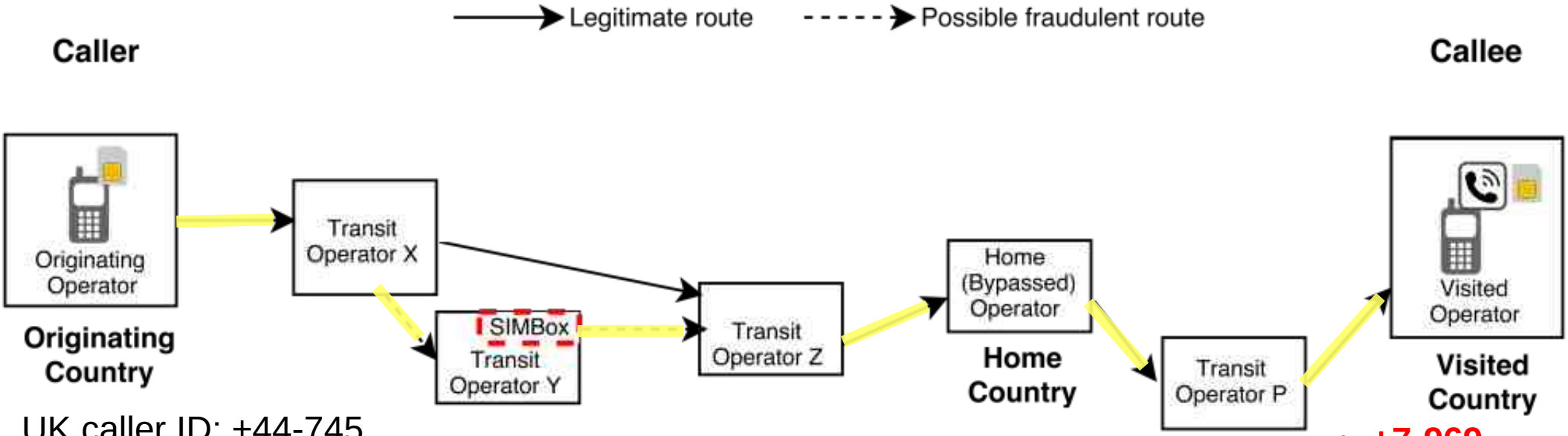
Example: Simbox and OTT Bypass



UK caller ID: +44-745...

- +44-745...
- Mobile termination

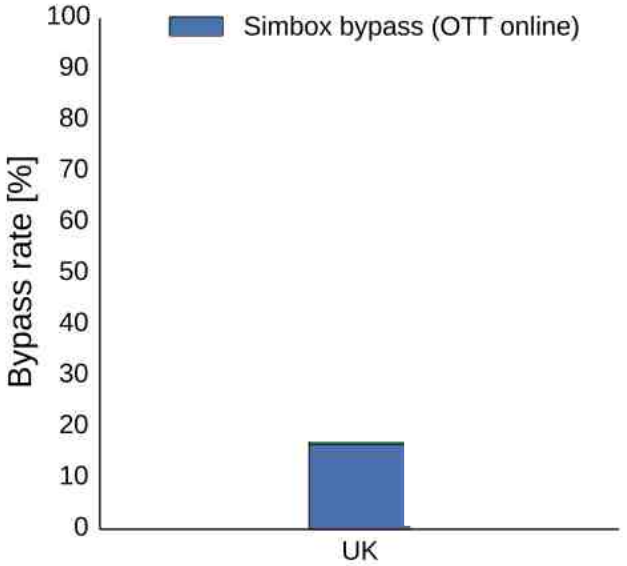
Example: Simbox and OTT Bypass



UK caller ID: +44-745...

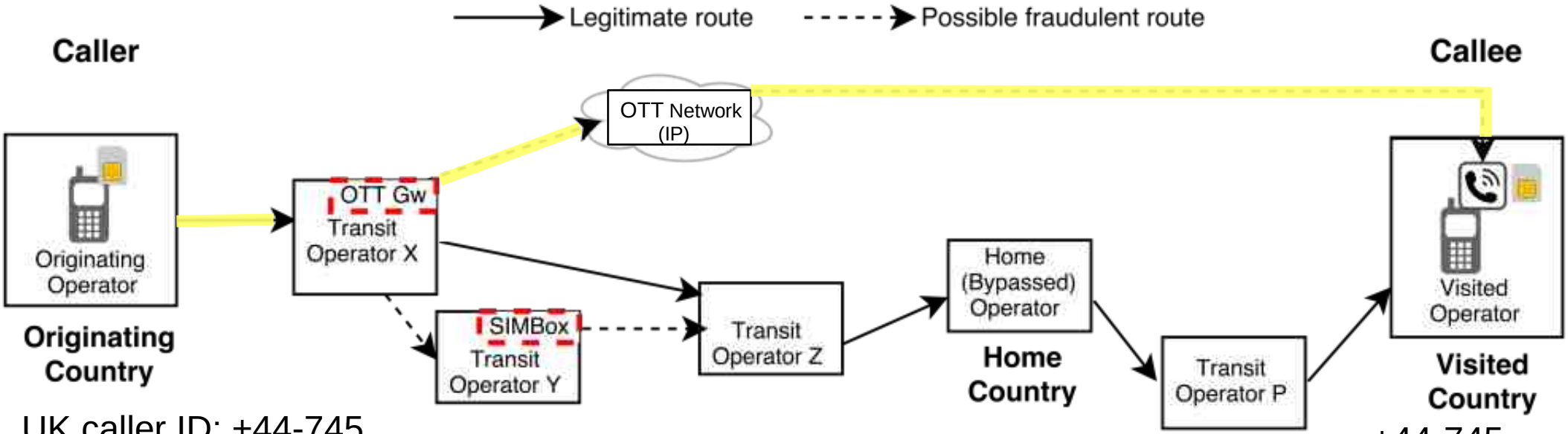
- **+7-969...**
- Mobile termination

- 16% Simbox bypass (over Russian mobile numbers)



Recipient phone is online on OTT

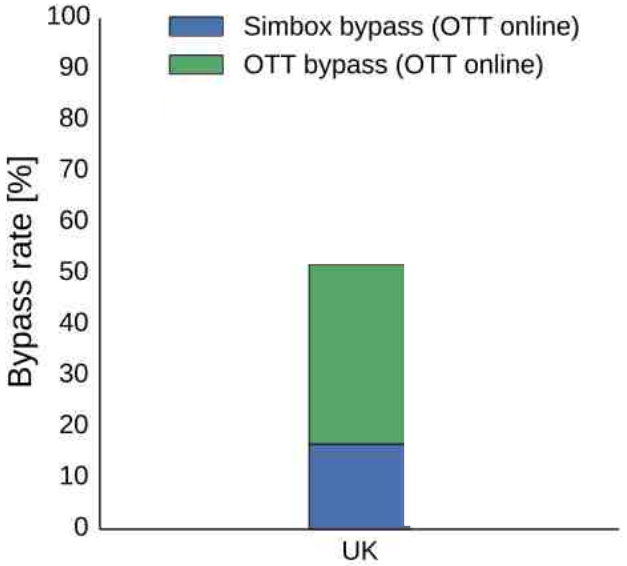
Example: Simbox and OTT Bypass



UK caller ID: +44-745...

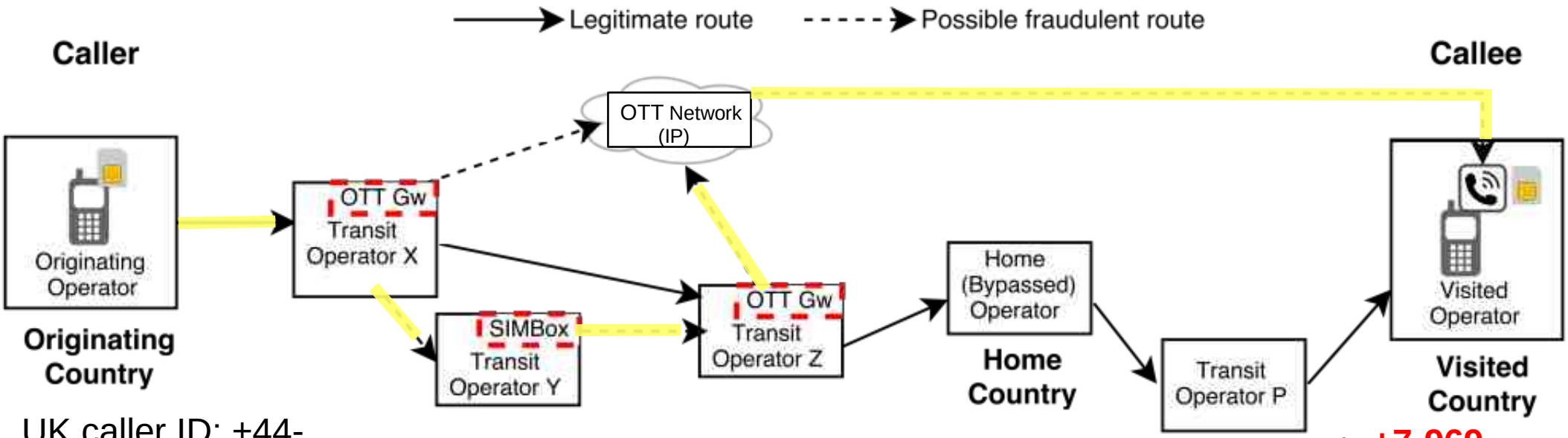
- +44-745...
- **OTT termination**

- 16% Simbox bypass (over Russian mobile numbers)
- 36% OTT bypass



Recipient phone is online on OTT

Example: Simbox and OTT Bypass

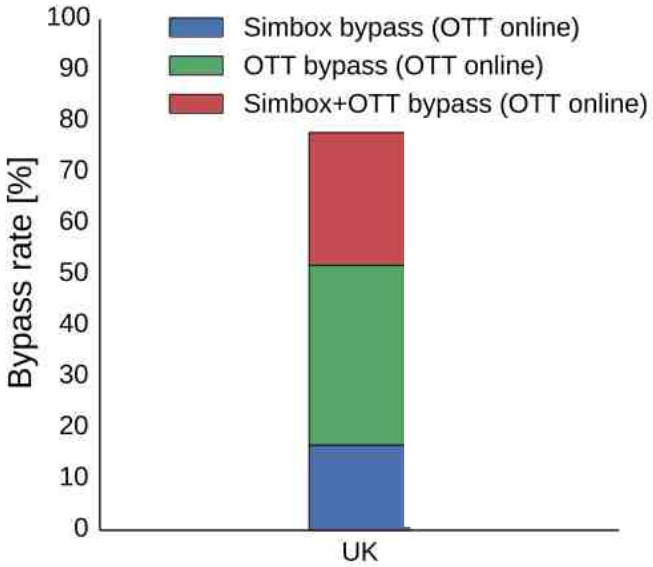


UK caller ID: +44-...

- +7-969...
- OTT termination

- 16% Simbox bypass (over Russian mobile numbers)
- 36% OTT bypass
- 25% Simbox + OTT bypass

~80% fraudulent call termination



Recipient phone is online on OTT

Conclusions

Telephony fraud is likely to remain as a significant problem

- Several weaknesses (in protocols, regulations…) that are difficult to fix
- New technologies will bring new vulnerabilities
- Fraudsters are smart and have strong incentives
- Fighting fraud is costly (fraud loss $\overset{?}{>}$ cost of detection/prevention)

We need industry cooperation... and data !

References

- Merve Sahin, Aurélien Francillon, Payas Gupta, Mustaque Ahamad, “SoK: Fraud in Telephony Networks” IEEE European Symposium on Security and Privacy (EuroS&P'17), 2017, Paris, France
- Merve Sahin, Aurélien Francillon, “Over-The-Top Bypass: Study of a Recent Telephony Fraud” ACM conference on Computer and communications security (CCS), 2016, Vienna, Austria
- Merve Sahin, Marc Relieu, Aurélien Francillon “Using chatbots against voice spam: Analyzing Lenny's effectiveness” Usenix Symposium on Usable Privacy and Security (SOUPS), 2017
- eMarketer. Digital content and advertising key revenue generators for messaging apps. emarketer, November 2015.
- New threat to mobile network operator revenues. Revector Company Blog, February 2016.
- B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor. Boxed out: Blocking cellular interconnect bypass fraud at the network edge. In USENIX Security, 2015.
- Vijay A. Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael T. Hunter, and Patrick Traynor. 2010. PinDr0p: using single-ended audio features to determine call provenance. ACM CCS.
- Miramirkhani et al., “Dial One for Scam: A Large-Scale Analysis of Technical Support Scams”, NDSS'17.
- Guri et al., “9-1-1 DDoS: Attacks, Analysis and Mitigation”, EuroS&P'17.
- D. Cameron, “Major leak exposes 400K recorded telemarketing calls, thousands of credit card numbers”, 2017. Available at www.dailydot.com.
- L. Notenboom, “I got a call from Microsoft and allowed them access to my computer. What do I do now?”, 2014. Available at http://askleo.com.