SoK: Fraud in Telephony Networks

Merve Sahin, Aurélien Francillon

Partially in cooperation with:
Payas Gupta, Pindrop
Mustaque Ahamad, Georgia Tech
Telephony Fraud

• 1870s: Closed telephone network, trusted operators → 2010s: Multiple parties involved, various technologies & services, IP convergence

• Performing fraud is easy and low risk
  – Easily monetized services
  – Massive volume of traffic
  – Remote attacks with little technical knowledge
Cost of Telephony Fraud

- Fraud loss estimated by operators was $38.1 billion in 2015\textsuperscript{1}
  - 1.69% of total revenue

\textsuperscript{1} CFCA Global Fraud Loss Survey, 2015
Cost of Telephony Fraud

- What about cost to society (financial, social, psychological)?

  • US Federal Trade Commission (FTC) receives an average of 400,000 complaints per month\(^1\)

  • In France, 574,000 voice spam complaints received in 2016\(^2\)

Cost of Telephony Fraud

- Critical infrastructure that millions of users rely on
  - (e.g., Telephony DoS on emergency services*)

Cost of Telephony Fraud

• Telephony vulnerabilities also affect online security: e.g.,
  – Online account hijacks by social engineering telcos' customer representatives
  – Technical support scammers installing remote administration tool / malware *
  – Leakage of recorded telemarketing calls that include sensitive information (addresses, credit card numbers..)
Motivation

- Telephony is considered as a trusted medium, but it is not always!
- We need a better understanding of fraud to effectively fight it.
Exploring the fraud ecosystem: Challenges

- Telephony fraud is a multi-dimensional problem
  - technology, environment, victim, techniques, impact...
- Fraudsters have various skills and motivations
  - Every actor has a different fraud experience
- Current fraud terminology can be confusing and misleading
  - Different terms for the same problem
  - Same term for different problems
- Public documentation is limited (e.g., restrictions from industry associations), sometimes incomplete (e.g., whitepapers)
Analyzing fraud in multiple layers

- 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.
Example: Wangiri (Callback) Scam
Example: Wangiri (Callback) Scam

- Japanese word for “One (ring) and cut”
Example: Wangiri (Callback) Scam

- **Root Causes**
  - Legacy/Insecure protocols,
  - Interconnection of poorly understood technologies

- **Weaknesses**
  - Lack of Caller ID authentication,
  - Lack of security & fraud awareness

- **Techniques**
  - Caller ID spoofing, Auto-dialers,
  - Social engineering

- **Fraud Schemes**
  - Callback (Wangiri) scam

- **Fraud Benefits**
  - Get a share from call revenue
Our taxonomy
Our taxonomy
Example: International Revenue Share Fraud

<table>
<thead>
<tr>
<th>Root Causes</th>
<th>Insecure/Legacy Protocols</th>
<th>Variety and Number of Operators &amp; Services</th>
<th>Interconnection of multiple technologies</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Weaknesses</th>
<th>Regulatory, Contractual, Legal Weaknesses</th>
<th>Protocol Weaknesses</th>
<th>Billing Systems</th>
<th>Human Negligence</th>
</tr>
</thead>
</table>

- Difficulty of joint industry initiative
- Arbitrage opportunities
- Numbering Plans & Portability
- Lack of security mechanisms in SS7
- Lack of caller ID authentication
- Lack of route transparency
- Mobile and VOIP related
- Tariff plan related
- Billing of V.A.S.
- Late availability of roaming CDRs
- Lack of internal control systems in companies
- Software vulnerability management
- Lack of security & fraud awareness
- Poor deployment practices

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Operator level</th>
<th>Protocol Related Attacks</th>
<th>Increasing Profit</th>
<th>Other</th>
</tr>
</thead>
</table>

- Manipulation of call signaling
- Number range hijacking
- Pricing confusion
- SS7 Tampering
- VOIP Protocol Attacks
- Caller ID Spoofing
- IMSI Catchers
- Traffic pumping and related services
- Multiple simultaneous calls
- Premium Rate Services
- CNAM service
- Toll Free Numbers
- SIM Boxes
- PBX Hacking
- TDOS
- Cloning and theft
- Social Engineering
- Autodialers

<table>
<thead>
<tr>
<th>Fraud Schemes</th>
<th>Toll Evasion Fraud</th>
<th>Retail Billing Related Fraud</th>
<th>Wholesale Billing Related Fraud</th>
<th>Voice Spam and Scams</th>
</tr>
</thead>
</table>

- Subscription Fraud
- Internal Fraud
- Superimposed Fraud
- PBX Dial-through
- Unauthorized reselling
- Slaming
- Tariff plan abuse
- Cramming
- Call Routing Abuse: Re-origination
- Interconnect Bypass Fraud
- False Answer Supervision
- Telemarketing
- Advance Fee Scam
- Callback (Wangirl) Scam
- Voice Phishing

<table>
<thead>
<tr>
<th>Revenue Share Fraud</th>
<th>Targeted Fraud</th>
</tr>
</thead>
</table>

- Toll Free Number Fraud
- International Revenue Share Fraud
- Access Stimulation
- CNAM Revenue Share Fraud
- Impostering
- Interception and Eavesdropping
- CNAM datamining
- Ward dialing
- Blackmailing

<table>
<thead>
<tr>
<th>Fraud Benefits</th>
<th>Financial Benefits</th>
</tr>
</thead>
</table>

- Increasing revenue
- Getting a share from billing
- Reselling minutes or service
- Avoiding payment (totally or partially)
- Earning free credits
- Influencing people
- Anonymity for criminal activities
- Disrupting Service
- Privacy Invasion
- Reconnaissance
Regular International Call

Op-A

Caller

Op-B

Callee
Regular International Call

Op-A

Caller

pays $1

Op-B

Callee

$1
Regular International Call

- **Caller** pays $1 and keeps 20 cents.
- **Op-A** receives $0.80 and operator fee.
- **Op-B** is connected to the **Callee**.
Regular International Call

- Caller pays $1.
- Op-A keeps 20c and forwards $0.8 to T3.
- T3 forwards $0.6 to T4.
- T4 keeps 20c.
- Op-B and Callee are unspecified in the diagram.
Regular International Call

- Caller pays $1
- Op-A keeps 20c, pays $0.80 to T3
- T3 receives $0.60
- T4 keeps 20c, receives $0.40
- Op-B keeps 40c
- Callee
International Revenue Share Fraud

Op-A

Victim

Fraudster
generating calls

Op-B

Callee

Legitimate
Fraudulent

0.8$
keeps 20c

0.6$

0.4$
keeps 40c

0.6$
keeps 20c

(PBX hacking Stolen SIM cards Mobile malware...)
International Revenue Share Fraud

Op-A ➔ T1
Op-B ➔ T4
T3 ➔ 0.6$
T4 ➔ 0.4$
Op-A keeps 30c (instead of 20c)
Op-B keeps 40c

Fraudster generating calls

Victim pays $1

(PBX hacking, Stolen SIM cards, Mobile malware...)

Legitimate
Fraudulent
International Revenue Share Fraud

Op-A
- keeps 30c (instead of 20c)
- keeps 20c
- pays 1$

Victim
- pays 1$

Fraudster
generating calls

Op-B
- keeps 40c

Callee

T1
- keeps 20c
- 0.7$

T2
- keeps 20c
- 0.5$

T3
- keeps 20c
- 0.6$

T4
- keeps 20c
- 0.4$

(PBX hacking
Stolen SIM cards
Mobile malware...)
International Revenue Share Fraud

- **Legitimate**
- **Fraudulent**

- **Op-A**
  - keeps 30c (instead of 20c)
  - 1$ pays 1$

- **Victim**
  - (PBX hacking, Stolen SIM cards, Mobile malware...)

- **Fraudster**
  - generating calls

- **T1**
  - keeps 20c
  - 0.7$

- **T2**
  - keeps 20c
  - 0.5$

- **T3**
  - keeps 20c
  - 0.6$

- **T4**
  - keeps 20c
  - 0.4$

- **Op-B**
  - keeps 40c
International Revenue Share Fraud

**Victim**: Unreachable and unaware callee (PBX hacking, Stolen SIM cards, Mobile malware...)

**Premium Rate Service Provider**

**Fraudster generating calls**

[Diagram showing the flow of revenue with various percentages and labels indicating the parties involved.]
International Revenue Share Fraud

- **Op-A**: Victim pays $1, which is kept by the Premium Rate Service Provider ($1 - $0.1 = $0.9, keeps $0.5, leaves $0.4 for the caller).
- **T1**: keeps $0.2, leaves $0.5 for the next step.
- **T2**: keeps $0.3, leaves $0.2 for the caller.
- **Op-B**: keeps $0.4, leaves $0.1 for the caller.
- **Unreachable and unaware callee**: keeps $0.1, leaves $0.2 for the caller.

**Fraudster generating calls**: earns $0.1

**Legitimate vs. Fraudulent**

- **Op-A**: keeps $0.8, leaves $0.6 for the caller.
- **T1**: keeps $0.6, leaves $0.4 for the caller.
- **T2**: keeps $0.4, leaves $0.2 for the caller.
- **Op-B**: keeps $0.2, leaves $0.0 for the caller.

**Premium Rate Service Provider**

- **Op-A** to **Victim**: $1 paid by the victim, $0.1 kept by the Premium Rate Service Provider, $0.9 for the caller.
- **Victim** to **Op-A** (in instead of $0.2): keeps $0.3, leaves $0.2 for the caller.

**Stolen SIM cards, Mobile malware...**
IRSF in fraud taxonomy

**Weaknesses**
- Regulatory, Contractual, Legal Weaknesses
  - Arbitrage opportunities
  - Difficulty of international law enforcement
  - Difficulty of joint industry initiative
  - Numbering plans & portability
  - Lack of due diligence
- Billing Systems
  - Billing of V.A.S.
  - Lack of route transparency

**Techniques**
- Operator level
  - Call short-stopping
  - Number range hijacking
- Value Added Services
  - Premium Rate Services

**Fraud Schemes**
- Revenue Share Fraud
  - IRSF
- Call Generation Schemes
  - Toll Evasion Fraud
  - Scams

**Fraud Benefits**
- Financial Benefits
  - Increasing revenue
  - Getting a share from billing
**Technique: Number Range Hijacking**
- Advertising cheap rates for a number range to attract traffic
- Similar to false BGP prefix advertisements (BGP hijack)

**Weakness: Lack of due diligence & Least cost routing policy**
**Technique: Number Range Hijacking**
- Advertising cheap rates for a number range to attract traffic
- Similar to false BGP prefix advertisements (BGP hijack)

**Weakness: Lack of a global numbering plan that lists all valid & used ranges**

**Fraud Scheme: IRSF**

**Fraud Benefit: Financial**
IRSF in fraud taxonomy

- Regulatory, Contractual, Legal Weaknesses
  - Arbitrage opportunities
  - Difficulty of international law enforcement
  - Difficulty of joint industry initiative
  - Numbering plans & portability
  - Lack of due diligence

- Billing Systems
  - Billing of V.A.S.
  - Lack of route transparency

- Operator level
  - Call short-stopping
  - Number range hijacking

- Value Added Services
  - Premium Rate Services

- Revenue Share Fraud
  - IRSF

- Call Generation Schemes
  - Toll Evasion Fraud
  - Scams

- Financial Benefits
  - Increasing revenue
  - Getting a share from billing
Technique: Call short-stopping

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

Weakness: Lack of route transparency
Fraud Scheme: IRSF

Fraud Benefit: Financial

Technique: Call short-stopping

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

Weakness: Lack of end-to-end security in call signaling

![Diagram of call flow]

- Op-A to T1
- T1 to T2
- T2 to Op-B
- Premium Rate Service Provider to Unreachable customer
- Victim to Op-A

Network charges:
- 1.6$ from Op-A to T1
- 0.7$ from T1 to T2
- 0.5$ from T2 to Op-B
- 0.2$ from Premium Rate Service Provider to Unreachable customer
- 0.6$ from Op-B to Premium Rate Service Provider
- 0.4$ from Unreachable customer to T2
**Technique: Call short-stopping**

- Manipulation of call routing to terminate (short-stop) the call on a pre-recorded voice message
- Short-stopped calls do not reach the legitimate destination

**Weakness: Lack of end-to-end security in call signaling**
IRSF in fraud taxonomy

Weaknesses
- Regulatory, Contractual, Legal Weaknesses
  - Arbitrage opportunities
  - Difficulty of international law enforcement
  - Difficulty of joint industry initiative
  - Numbering plans & portability
  - Lack of due diligence

Billing Systems
- Billing of V.A.S.
- Protocol Weaknesses
  - Lack of route transparency

Techniques
- Operator level
  - Call short-stopping
  - Number range hijacking

Value Added Services
- Premium Rate Services

Fraud Schemes
- Revenue Share Fraud
  - IRSF

Call Generation Schemes
- Toll Evasion Fraud
- Scams

Fraud Benefits
- Financial Benefits
  - Increasing revenue
  - Getting a share from billing
Technique: Premium Rate Services
- Abuse of billing (cash-back) mechanism

Weakness: Complexity of billing systems
**Technique: Premium Rate Services**

- Abuse of billing (cash-back) mechanism
- Abuse of expensive destinations as pseudo “international premium rate numbers” *(Legitimate allocation: +979 range)*

**Weakness: Variety of regulation and laws**
Addressing IRSF?

- Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  - Weakness: Late availability of roaming call data records

- Solution proposed: Near Real Time Roaming Data Exchange (NRTRDE) systems
Addressing IRSF

- Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  - Weakness: Late availability of roaming call data records

- Solution proposed: Near Real Time Roaming Data Exchange (NRTRDE) systems

  ➡️ Only a countermeasure for one type of call generation
  ➡️ Real weaknesses manipulated by IRSF are not addressed
Addressing IRSF

• Initially, call generation was performed by using fraudulently obtained SIM cards in roaming
  – Weakness: Late availability of roaming call data records

• Solution proposed: Near Real Time Roaming Data Exchange (NRTRDE) systems
  – Only a countermeasure for one type of call generation
  – Real weaknesses manipulated by IRSF are not addressed

• IRSF is still an unsolved problem
  – $10.76 Billion estimated loss in 2015*

[*] CFCA Global Fraud Loss Survey, 2015
Example: Interconnect Bypass Fraud
Interconnect Bypass Fraud

- Use of illegitimate gateway exchanges to avoid the legitimate gateways and international termination fees
  - Example: SIM Boxes and VOIP gateways are frequently used to bypass international part of the calls and terminate them as domestic calls

- $5.97 Billion annual estimated loss*

- **Over-The-Top (OTT) Bypass** is a recent form of interconnect bypass fraud, performed via OTT services

[*]CFCA Global Fraud Loss Survey, 2015
Over-The-Top (OTT) Communications

- Online services that
  - run 'on top of' the operator
  - substitute/compete with traditional telecommunications services
- Global presence through smartphone application markets
- **2 billion OTT messaging users estimated by 2018**
  [eMarketer'15]
Over-The-Top (OTT) Communications

- Phone numbers often used for user identification
- **Terms of use** and default application settings
- **OTT needs revenue:**
  - Advertisement
  - Stickers, games etc.
  - **Telephony interaction**
    - e.g., Skype-in 😊
    - Skype-out 😊
  - OTT bypass 😞
Regular International Call

- **Caller**
  - **Originating Operator**: 0.35$ (keeps 0.05$)

- **Transit Operator**: 0.30$ (keeps 0.05$)

- **Terminating Operator**: 0.25$

- **Callee**
OTT Bypass Call

0.35$ keeps 0.05$

0.30$ keeps 0.05$

0.25$
OTTT Bypass Call

Caller

- 0.35$ from Caller
- OTT Gw Transit (Bypassing) Operator keeps 0.05$
- OTT Gw Transit (Bypassing) Operator keeps 0.15$
- 0.30$ from Caller

OTT Network(IP)

- 0.15$ from OTT Network(IP)

Callee

- Terminating (Bypassed) Operator keeps 0.00$
- 0.25$ from Callee
- OTT Gw Transit (Bypassing) Operator keeps 0.05$
- 0.15$ from Callee
OTT Bypass Call

- Pays for premium quality (SLA)
- Potential quality problems
OTTT Bypass Call

- Potential quality problems
- May pay for IP traffic
- Cannot use telco services (voicemail, call forwarding)
OTT Bypass Call

- Significant revenue loss
- Customer dissatisfaction

Diagram showing the flow of a call bypassing the network, with costs and revenue distribution highlighted.

- Caller
  - 0.35$ payment
  - 0.05$ kept by the originating operator

- OTT Gw (Transit, Bypassing) Operator
  - 0.15$ kept by the OTT Gw
  - 0.30$ kept by the terminating (bypassed) operator
  - 0.00$ kept by the terminating (bypassed) operator

- Callee
  - 0.15$ kept by the terminating (bypassed) operator
  - 0.25$ kept by the terminating (bypassed) operator
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
Case Study: Measuring OTT bypass - on a Small European Country - with a custom TCG platform

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

Countries: Spain, Turkey, United Kingdom, Italy, Netherlands, Germany, Austria, Switzerland, France
Summary of Results

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

 Caller

 Originating Operator

 Originating Country

 Transit Operator X

 Transit Operator Z

 Home (Bypassed) Operator

 Home Country

 Transit Operator P

 Visited Country

 Callee

 Visited Operator
Example: Simbox and OTT Bypass

Originating Operator

Transit Operator X

SIMBox
Transit Operator Y

Transit Operator Z

Home (Bypassed) Operator

Transit Operator P

Visited Operator

Visited Country

Home Country

Legitimate route

Possible fraudulent route

Caller

Callee
Example: Simbox and OTT Bypass

Recipient phone is not registered to OTT

Recipient phone is online on OTT
Example: Simbox and OTT Bypass

Recipient phone is not registered to OTT

Recipient phone is online on OTT
Example: Simbox and OTT Bypass

- **Legitimate route**
- **Possible fraudulent route**

### Diagram:
- **Caller**
  - Originating Operator
  - SIMBox
  - OTT Gw Transit Operator Y

- **OTT Network (IP)**
  - OTT Gw Transit Operator Z
  - Home (Bypassed) Operator

- **Callee**
  - Visited Operator
  - Transit Operator P

### Graphs:
1. **Recipient phone is not registered to OTT**
   - Bypass rate [%] for the UK

2. **Recipient phone is online on OTT**
   - Bypass rate [%] for the UK
   - Simbox bypass (OTT Not Registered)
   - OTT bypass (OTT online)
   - Simbox+OTT bypass (OTT online)
Post Dial Delay (PDD)
Post Dial Delay (PDD)

Connecting...

ringback signal

phone rings
Post Dial Delay (PDD)

Caller

PSTN switch

Connecting...

ringback signal

PSTN switch

Recipient

Phone rings

Ringing
Post Dial Delay (PDD)

Ring tone / Busy signal

Caller

PSTN switch

ringback signal

Recipient

PSTN switch

phone rings

Ringing
Post Dial Delay (PDD)

Caller

PSTN switch

PSTN switch

Recipient

PDD (normal)

ringback signal

Normal call

phone rings (normal)
Post Dial Delay (PDD)
Post Dial Delay (PDD)

Caller

PSTN switch

PSTN-OTT gateway

Recipient

ringback signal

PDD (normal)

phone rings (normal)

Normal call
Post Dial Delay (PDD)

* Statistics show mean & standard deviation values from 3200 calls originated from Italy.
PDD vs Ring time difference

* Statistics show mean&stdev values from 3200 calls originated from Italy.
PDD vs Ring time difference

* Statistics show mean\&stdev values from 3200 calls originated from Italy.
PDD vs Ring time difference

* Statistics show mean&stdev values from 3200 calls originated from Italy.

---

PDD (normal)

PDD (bypass)

4.7 ± 1 sec.

5.1 ± 1 sec.

ringback signal

PSTN switch

PSTN-OTT gateway

Caller

Recipient

Ring Time Difference (in seconds):

Bypassed call

Normal call

phone rings (normal)

phone rings (bypass)
Recap on OTT bypass

• OTT bypass may have severe consequences:
  – Financial losses, customer dissatisfaction for bypassed operators
  – Call establishment problems, unexpected network behavior, SLA violations
  – Poor service quality and no benefits for users

• OTT bypass is challenging to detect and measure

• Blocking OTT / OTT-bypass is a sensitive topic
  (Network neutrality, freedom of speech)

• Increasing awareness is an important step towards a solution
Conclusions

• Telephony fraud is a complex ecosystem
• A holistic view helps to effectively fight fraud
• Our taxonomy
  – Examines the problem in multiple layers (root causes, weaknesses, techniques...)
  – Helps to better understand
    • Relations and interactions between fraud components
    • Effectiveness and implications of possible countermeasures
Thanks!
References

- K. Hall, “Brit ISP TalkTalk blocks control tool TeamViewer”, 2017. Available at theregister.co.uk
- “Caller ID Revenue Share for Call Centers and Dialers”, 2016. Available at telecombrokers.com.