

Telephony Fraud and Abuse

Aurélien Fancillon

Aurelien.francillon@eurecom.fr

Background

Telephony Networks – Quick history

- 1870s: Plain Old Telephone System (POTS)
 - Enabled by transmission of voice over copper lines
 - Used **in-band signaling**: Signaling (call control & routing) information and voice/data are transmitted on the same channel
 - Switchboard operators were connecting calls (enabling social engineering attacks)
 - Operators were mostly state-owned monopolies
 - Access to the network was restricted to operators, which were 'trusted' by default



Telephony Networks – Quick history

- 1890s: Automatic telephone exchange became possible with the invention of an electromechanical stepping switch (known as Strowger Exchange/Switch)
- Early 1900s: Payphones started to be deployed in US (and they were frequently abused)
- 1950s: People started to explore the vulnerabilities of telephone network – Start of 'phone phreaking'
 - Joe Engressia (“Joybubbles”) accidentally discovered that whistling at a tone of 2600 Hz allows controlling the phone switch to make free calls
 - Phreakers developed the 'Bluebox' and other 'boxes' that can mimic certain frequencies allocated for operators' internal use (abusing in-band signaling to control call routing)
 - Some famous phreakers: John Draper (Captain Crunch), Steve Wozniak, Steve Jobs. =>book “I Woz”, Steeve Wozniak

Telephony Networks – Quick history

- 1960s: Businesses started to adopt internal telephone systems
- 1970s:
 - **Out-of-band signaling** systems: Separate channels for call control and voice/data
 - Analog cellular networks (1G)
- Early 1980s:
 - Digitization of telephone networks
 - **Integrated Services Digital Network (ISDN)**: Digital transmission of voice, video, data, fax etc. over a single line
 - **Signaling System 7 (SS7) protocol**: Out-of-band call signaling protocol
 - Premium rate services introduced

Telephony Networks – Quick history

- Early 1990s:
 - 2G cellular networks
 - The first international mobile roaming agreement
 - World Wide Web born – The first web server, browser and website
- Mid 1990s:
 - Telecommunications Act in U.S. → Deregulation and liberalization of the telecommunication industry
 - First Voice over IP system introduced
 - Pre-paid SIM cards launched

Telephony Networks – Quick history

- Late 1990s:
 - Enterprise telephony systems integrate with VOIP
 - Operators add IP capabilities to their switches
- Early 2000s: Launch of Skype and significant growth of VOIP
- Mid 2000s: 3G technology
- 2010s:
 - 4G and LTE
 - Integration of landline, cellular and VOIP networks
- 2020s:
 - 5G

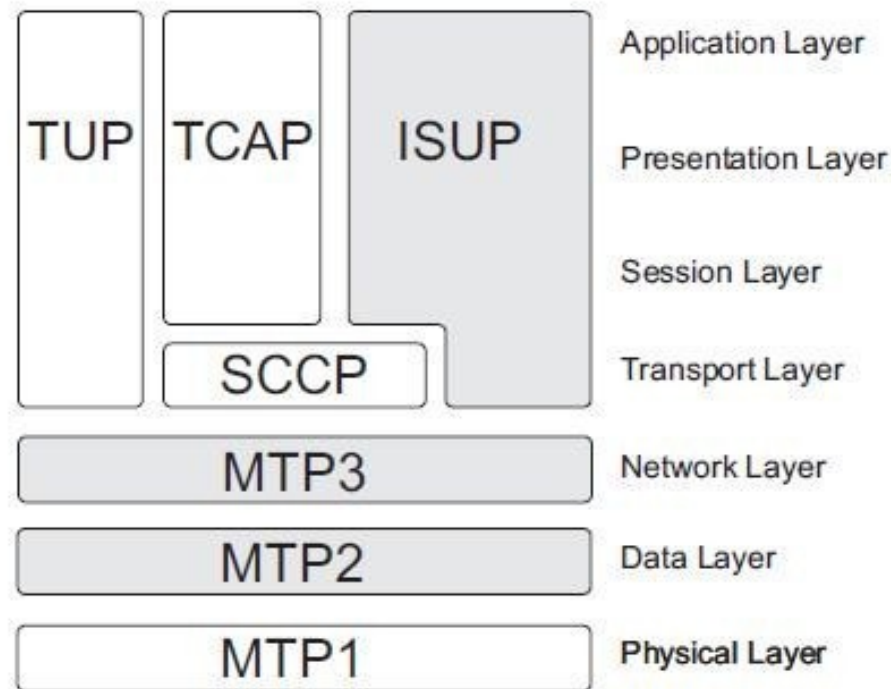
Telephony Ecosystem

- Three main networks that provide communication:
 - **Public Switched Telephone Network (PSTN)**
refers to the worldwide circuit-switched telephone network (also called POTS, fixed network, landline)
 - **Cellular (mobile) networks**
 - **IP telephony and Voice over IP (VOIP)**
- Separate channels used for call signaling and voice

Signaling System 7 (SS7)

- SS7 refers to a set of protocols used to manage call establishment in PSTN

SS7 Protocol Stack

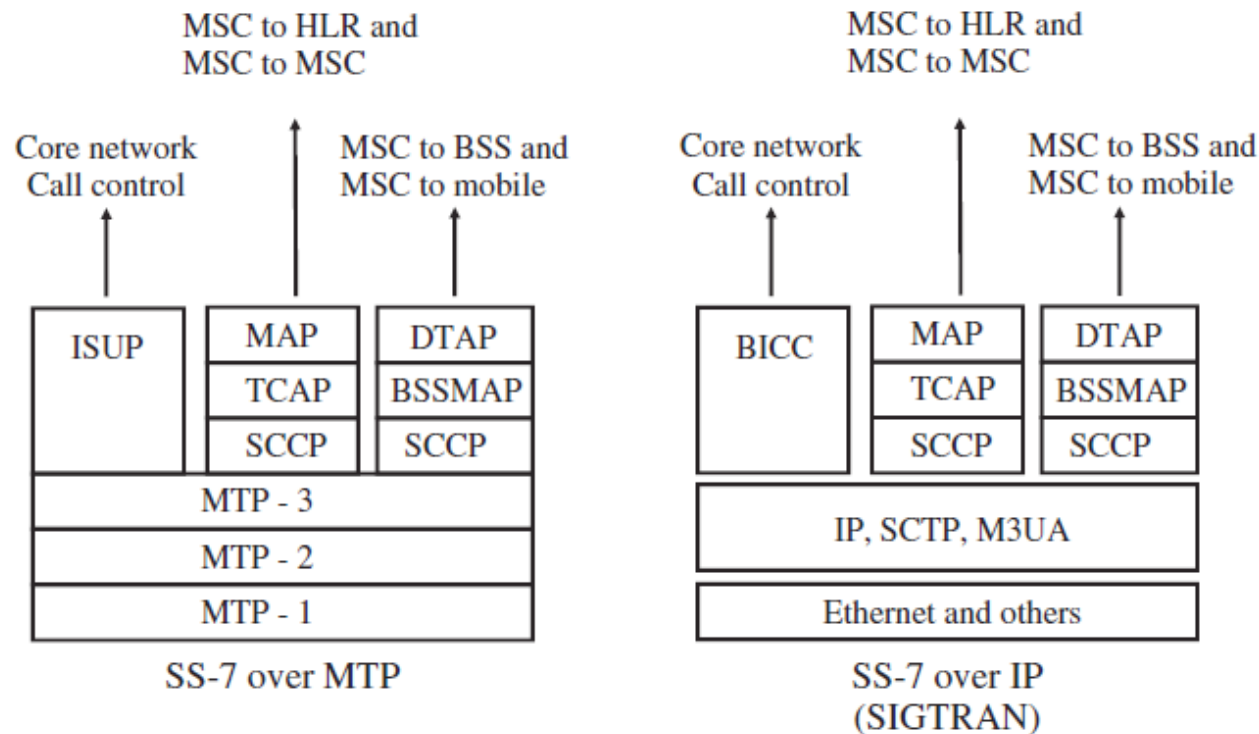


ISUP (ISDN User Part): Handles call establishment for ISDN lines.

MTP Message Transfer Part

Signaling System 7 (SS7)

- In time, SS7 is enhanced to support interconnection with cellular and IP networks



MAP (Mobile Application Part) handles communication with cellular network, location management, roaming, SMS, etc.

SIGTRAN: Replaces network layer with IP protocols, supports security mechanisms via Ipsec or TLS. However, each operator can still decrypt&tamper messages.

Cellular networks

- Global System for Mobile Communications (GSM) refers to a set of protocols describing 2G cellular networks
 - Standardized in early 1990s
 - Still commonly used (although some operators started to discontinue)
- 3G and 4G technology are very widespread too

Voice Over IP (VoIP)

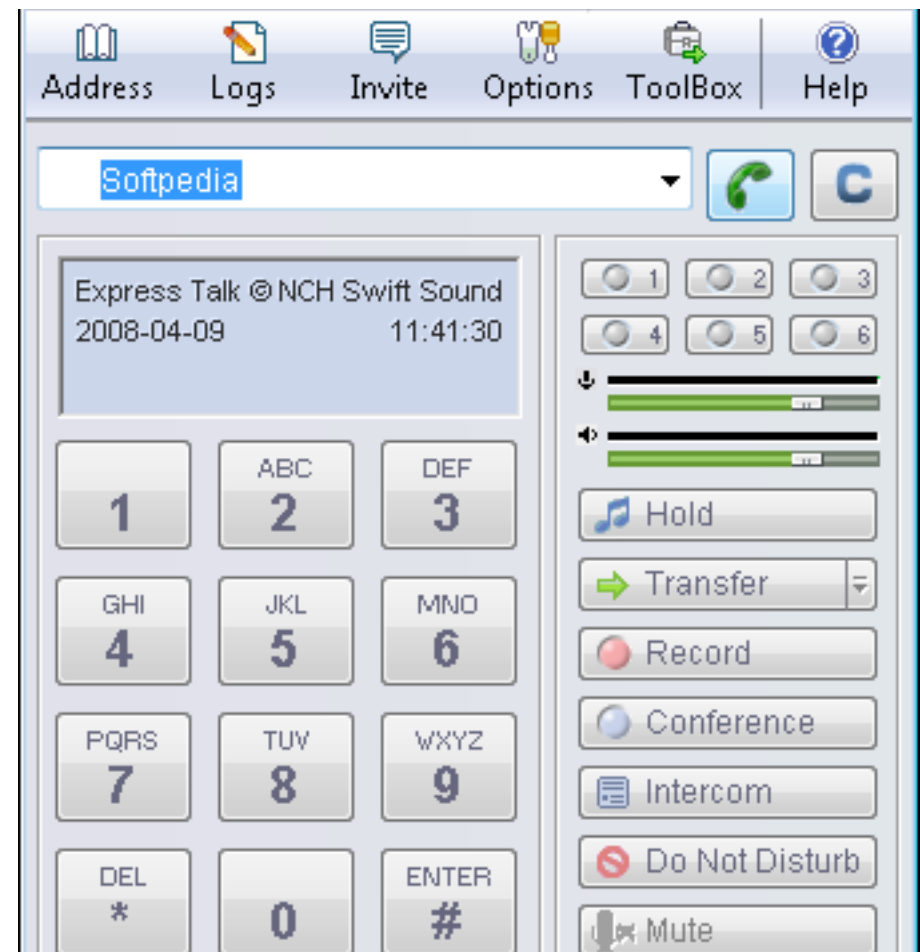
- VoIP usually refers to the transmission of voice over the public IP network
- Most common VoIP signaling protocols:
 - Session Initiation Protocol (SIP) - IETF standard
 - Usually uses UDP port 5060
 - SIP URI is the addressing scheme that identifies a communication point
sip:user:password@host:port;uri-parameters?headers
 - H.323 – ITU standard, much more complex than SIP, but commercialized before
- Many other non-standard, proprietary protocols developed by companies (e.g., Skype)

Voice Over IP (VoIP)

- IP phone



- Soft phone

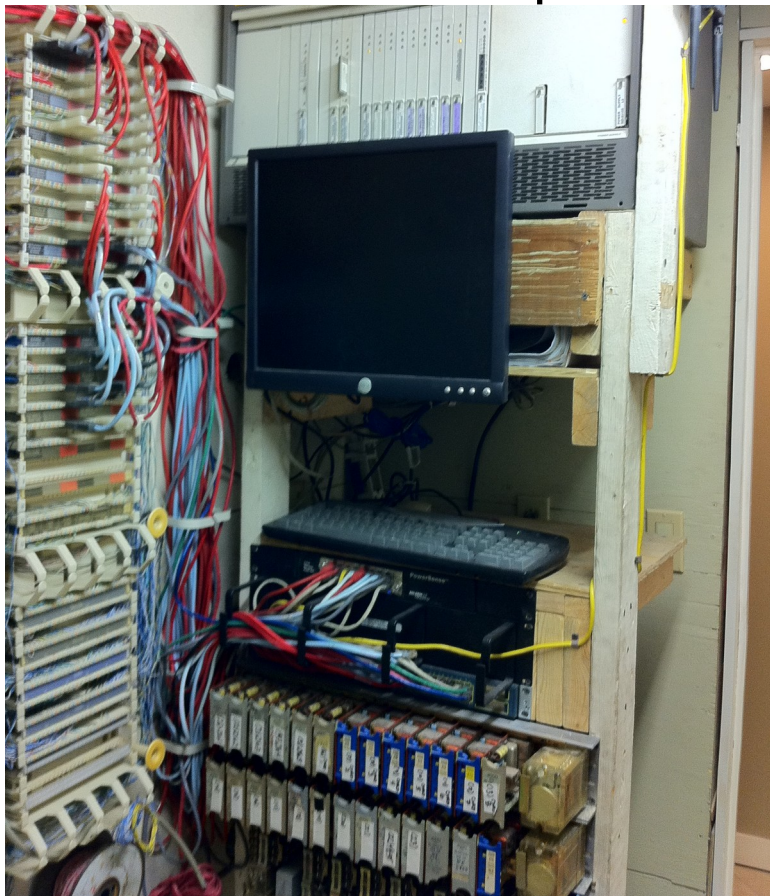


Private Branch Exchanges (PBX)

- Manages internal and external communications of enterprises
 - Enables internal routing of local calls (each phone has an 'extension' number that can be directly use within the company)
 - Provides external connectivity via a limited number of external phone lines (called 'trunks')
 - Less expensive than having an external line for every employee
 - Enables centralized support, voice mail, Interactive Voice Response (IVR) etc.
- *IVR: A set of pre-recorded voice prompts that interact with caller through pressing digits. (E.g., customer support service)

Private Branch Exchanges (PBX)

- Traditional PBX
 - ISDN trunks
 - Lots of wires, expensive



- IP-PBX
 - SIP, ISDN (with additional hardware) trunks
 - Easier to manage, cheaper



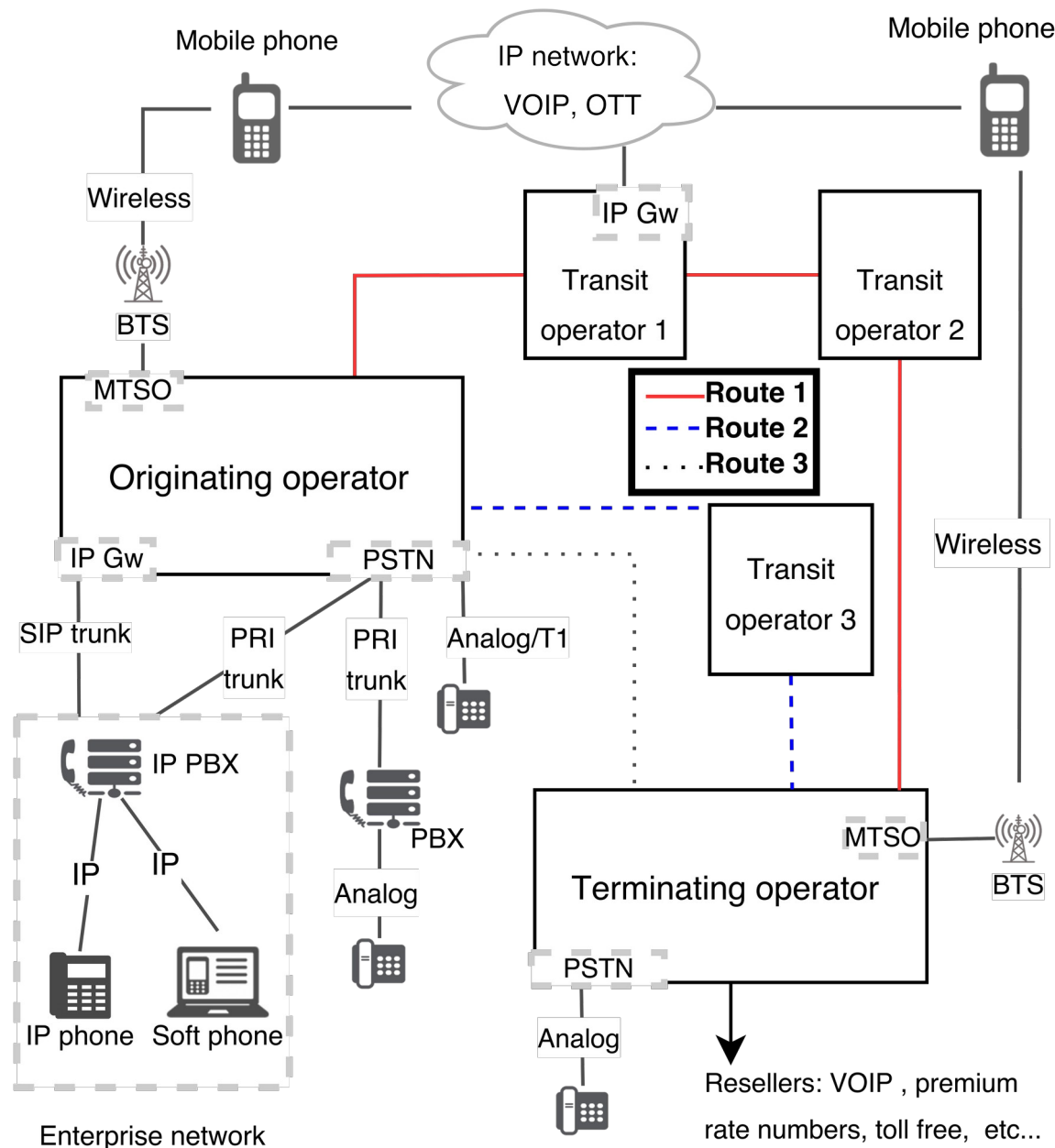
Telephony Actors

- Operators (service providers)
 - Some of them invest in or own the network infrastructure and equipment
 - Some of them only resell the service they buy from other operators (e.g., Mobile Virtual Network Operators, MVNOs).
 - Retail operators: Provide services to end-users
Wholesale operators: Provide interconnection services to other operators
- End-users
 - Individuals, enterprises

Telephony Actors

- Third Parties
 - **Value added services** deliver content to end-users via phone calls, messaging or data network (e.g., gaming, chat lines or news) and charge the content through billing of the telecommunication service
 - **VOIP resellers** buy communication services from carriers, and resell through VOIP gateways
e.g., Cloud based communication services like Twilio provide programmable voice/SMS and originating phone numbers from many countries
 - Let's have a look at examples:
<https://twilio.com> - <https://www.twilio.com/docs> ,
<https://www.bandwidth.com/> , <https://tollfreeforwarding.com/>

Telephony Ecosystem- Summary



Billing systems

- Understanding the billing processes is important to understand fraud!
- Operators use Call Detail Records (CDR) for billing:
 - A CDR is created for each call routed (originated, terminated or transited) over operator's network switches
 - CDRs include details of each transaction, such as source and destination phone numbers, date, call duration, call type, completion status
- All CDRs generated at different switches are collected and processed in a central location, then sent to the billing system to be charged

Billing systems

- Two main types of billing:
 - **Retail Billing** deals with the billing of end customers for multiple services (international or domestic landline, mobile, or data services)
Mobile billing can be
 - Post-paid (requires proper customer identification)
 - Pre-paid (requires real time billing, customer identification is also important)

Billing systems

- **Wholesale billing** relates to the operators billing each other: i.e., the billing of
 - interconnect partners (for providing interconnection to make calls to another operator's customers)
 - resellers
 - roaming partners (for providing services to their customers when they roamed in another operator's coverage area)

Billing systems

- More on roaming:
 - Roaming enables to access mobile communication services even when the subscriber is outside the coverage of his 'home' network
 - To provide roaming facility, operators should have 'roaming agreements' with the 'visited' networks
 - CDRs generated by roaming subscribers are not immediately available to the home operator!
 - Near Real Time Roaming Data Exchange (NRTRDE) systems mandate maximum 4 hours to exchange CDRs

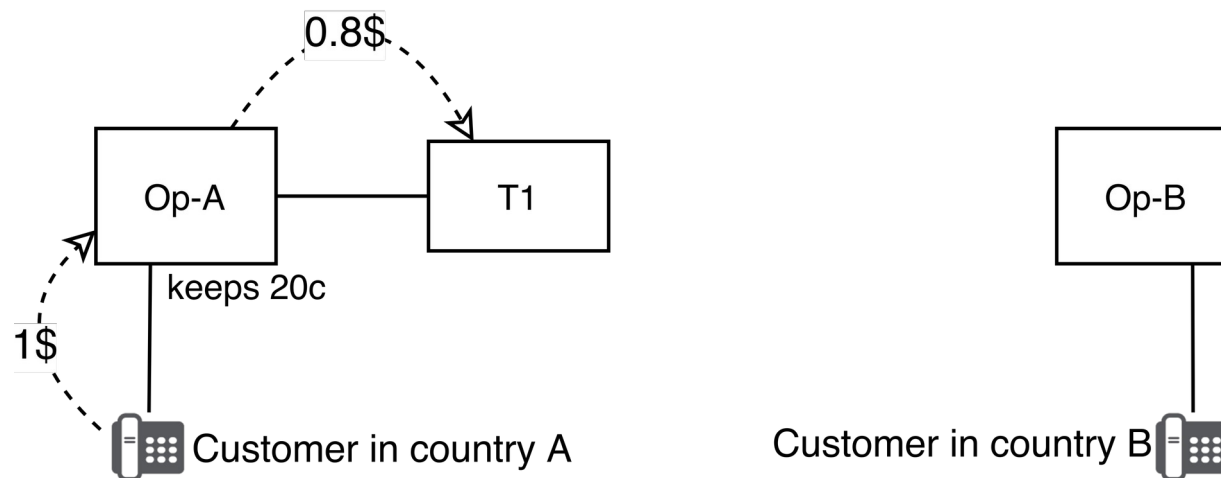
International call routing and money flow

- Collection charge, termination and transit fees
- Lack of route transparency
 - Visibility of the call route is limited for each operator
 - No “traceroute” mechanism as in computer networks



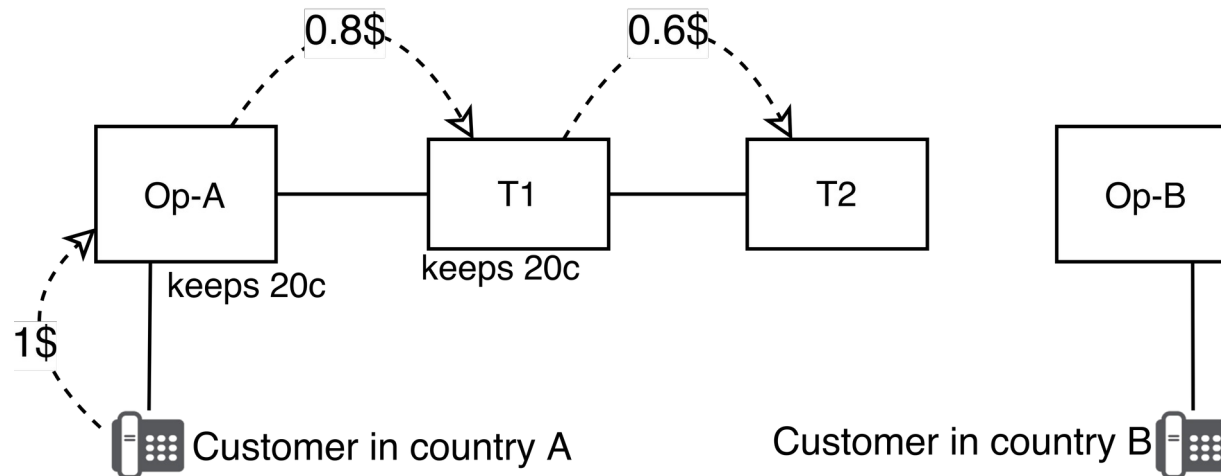
International call routing and money flow

- Collection charge, termination and transit fees
- Lack of route transparency
 - Visibility of the call route is limited for each operator
 - No “traceroute” mechanism as in computer networks



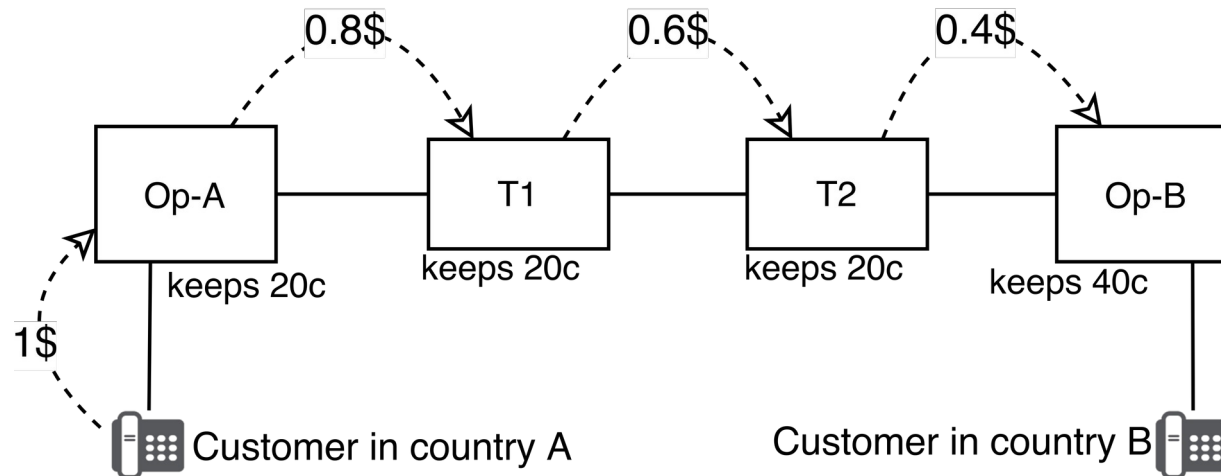
International call routing and money flow

- Collection charge, termination and transit fees
- Lack of route transparency
 - Visibility of the call route is limited for each operator
 - No “traceroute” mechanism as in computer networks



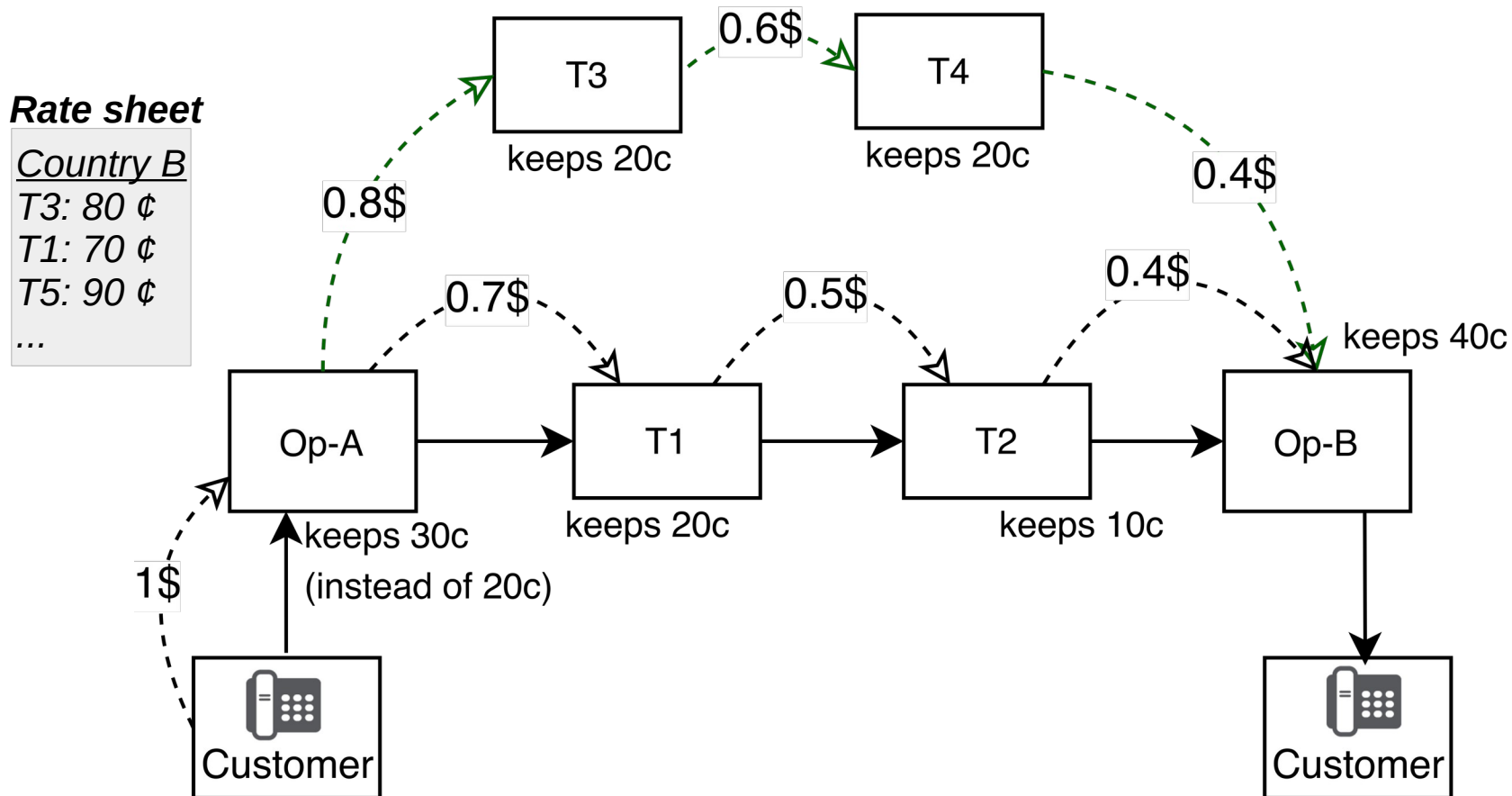
International call routing and money flow

- Collection charge, termination and transit fees
- Lack of route transparency
 - Visibility of the call route is limited for each operator
 - No “traceroute” mechanism as in computer networks



International call routing and money flow

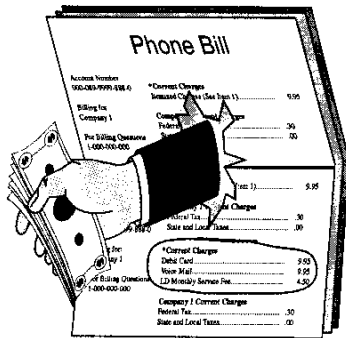
- Least Cost Routing mechanism



Telephony Fraud

Telephony fraud: Some examples

- Small charges on your phone bill



- Stolen phone or SIM card

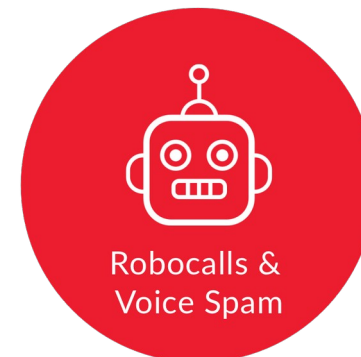
A photograph of a phone bill. The bill shows a large total charge of \$1,483.11, which is the sum of taxes and surcharges (\$212.75) and other charges (\$1,194.71).

Taxes & Surcharges	Total Charges
8.33 \$	58.32
169.23 \$	1,194.71
18.12 \$	118.07
17.07 \$	112.01
212.75 \$	1,483.11

- Unknown international caller IDs



- Unwanted calls and voicemails



Consequences of Telephony Fraud

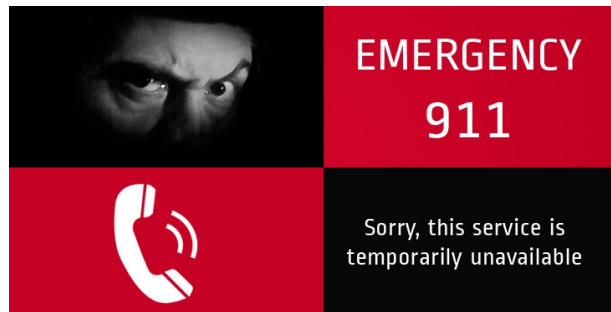


In 2015, estimated **financial loss for operators** was \$38.1 billion*

[*] CFCA Global Fraud Loss Survey, 2015



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

Telephony Fraud

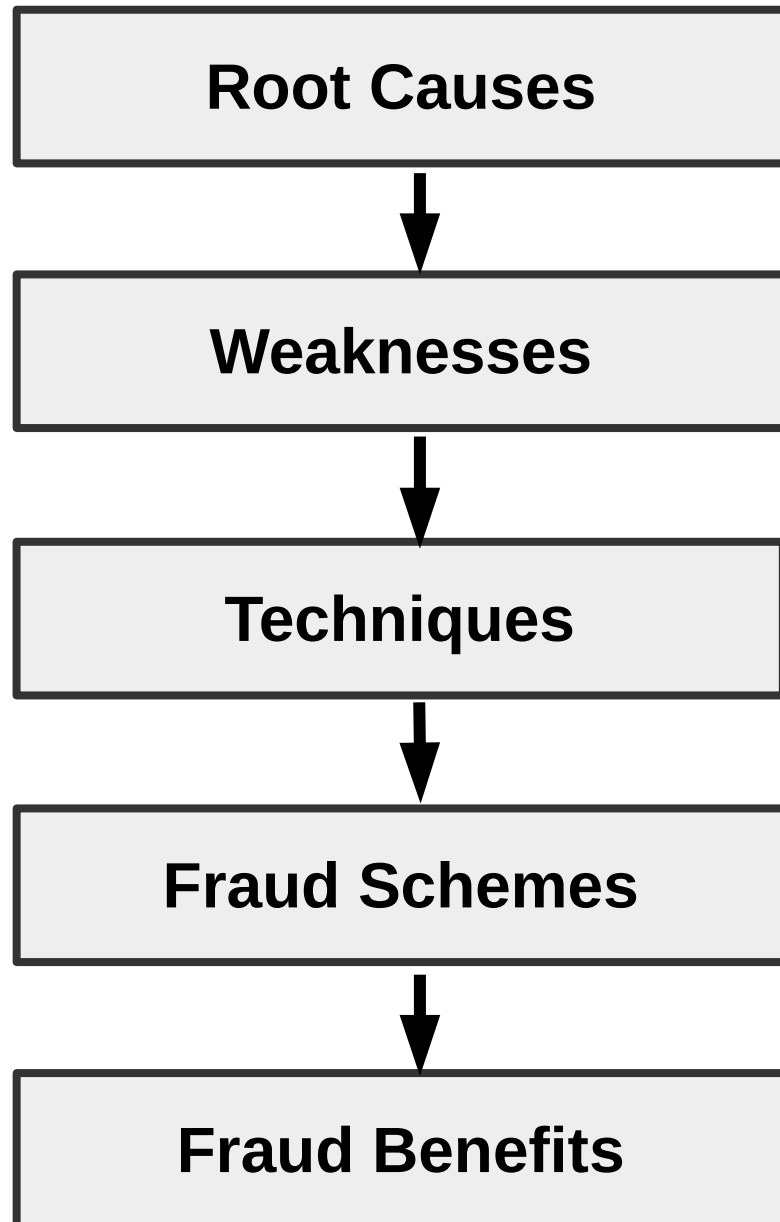
- Each new technology broadens the attack surface
- Performing fraud is easy and low risk
 - Massive volume of traffic
 - Obscure technologies
 - Remote and non-technical equipment/attacks

Fraud Taxonomy

Why do we need a taxonomy?

- Telephony fraud is a multi-dimensional problem (technology, environment, victim, techniques, impact...)
- Every actor has a different fraud experience
- Fraudsters have various skills and motivations
- Current fraud terminology can be confusing and misleading
 - Different terms for the same problem,
Same term for different problems

Defining telephony fraud



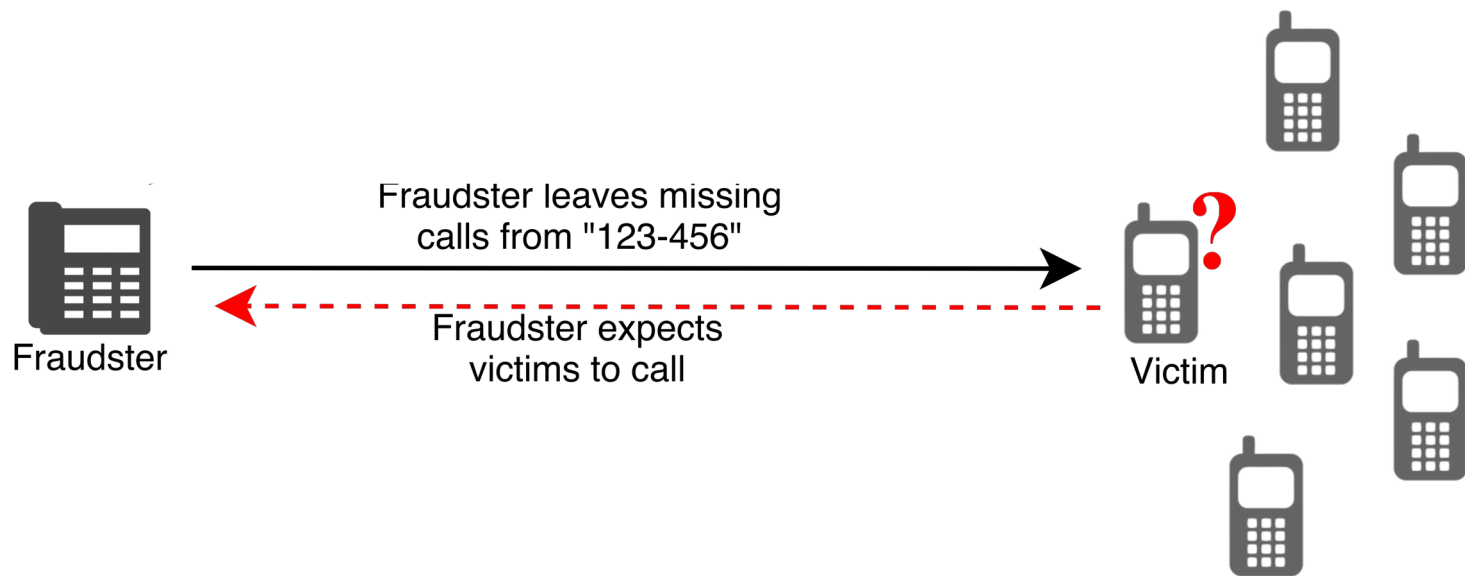
- A **fraud scheme** is a way to obtain an **illegitimate benefit** using a **technique**. Such techniques are possible because of **weaknesses** in the system, which are themselves due to **root causes**.

Example: Callback (Wangiri)Scam

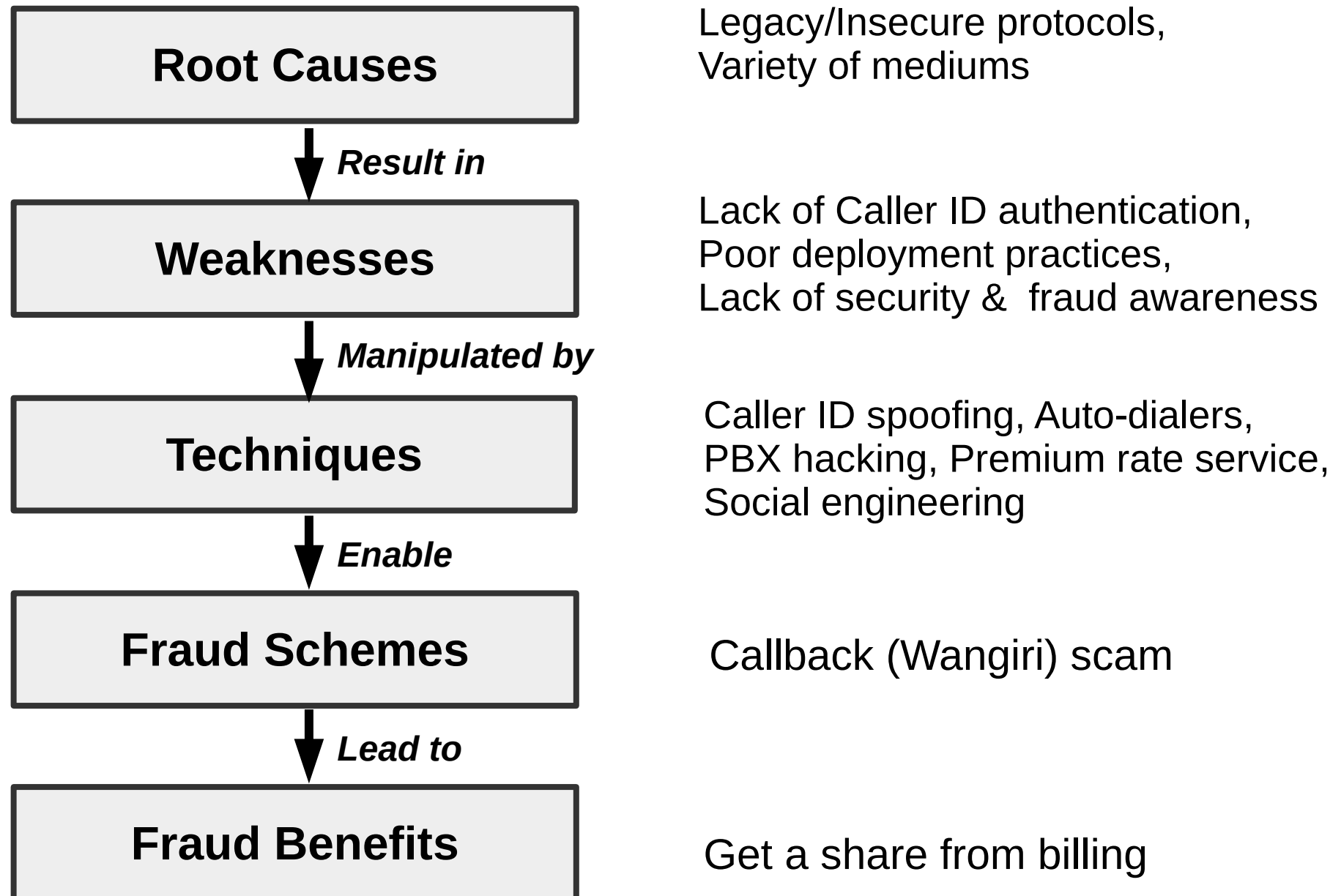


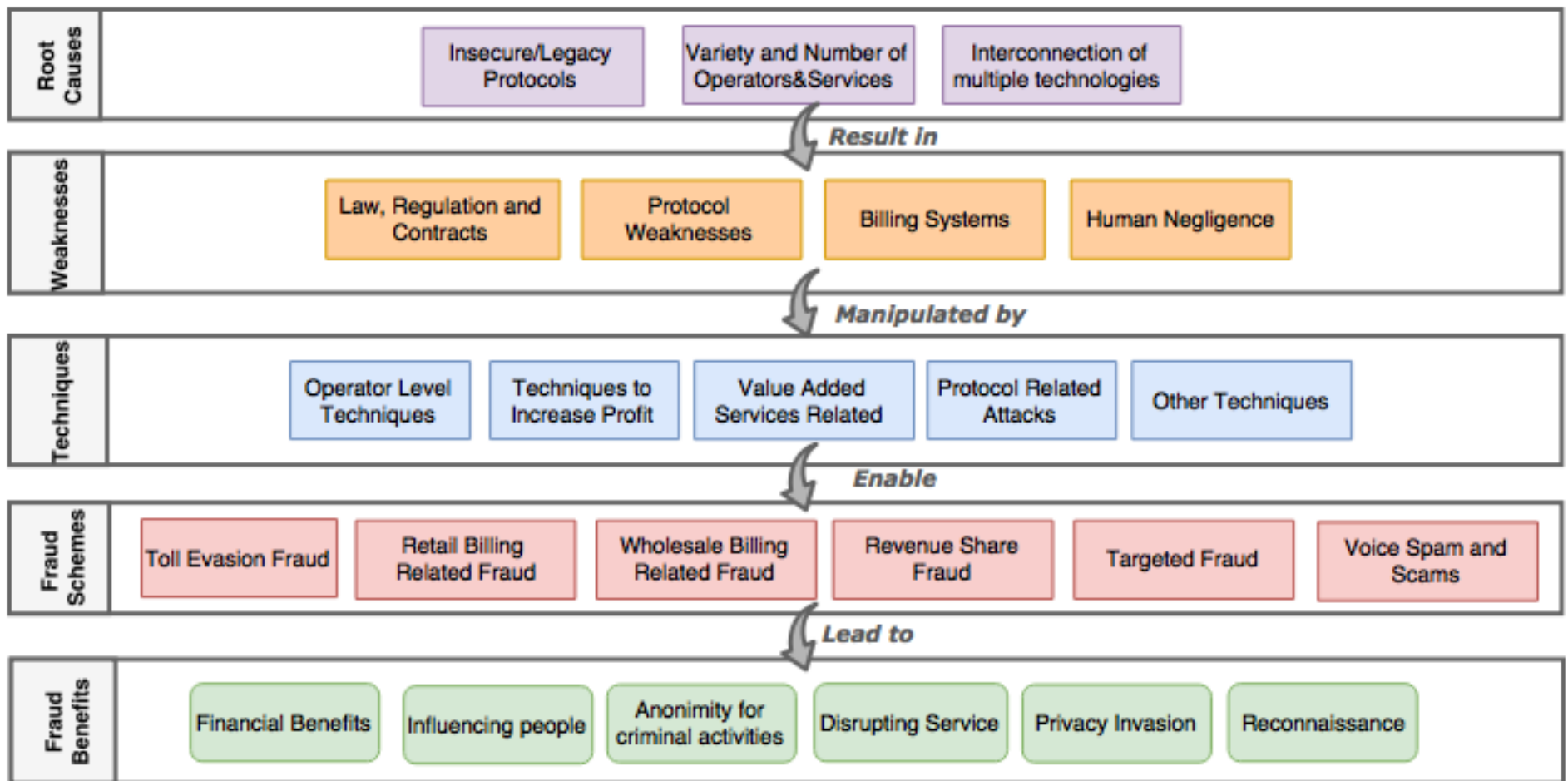
Example: Callback (Wangiri) Scam

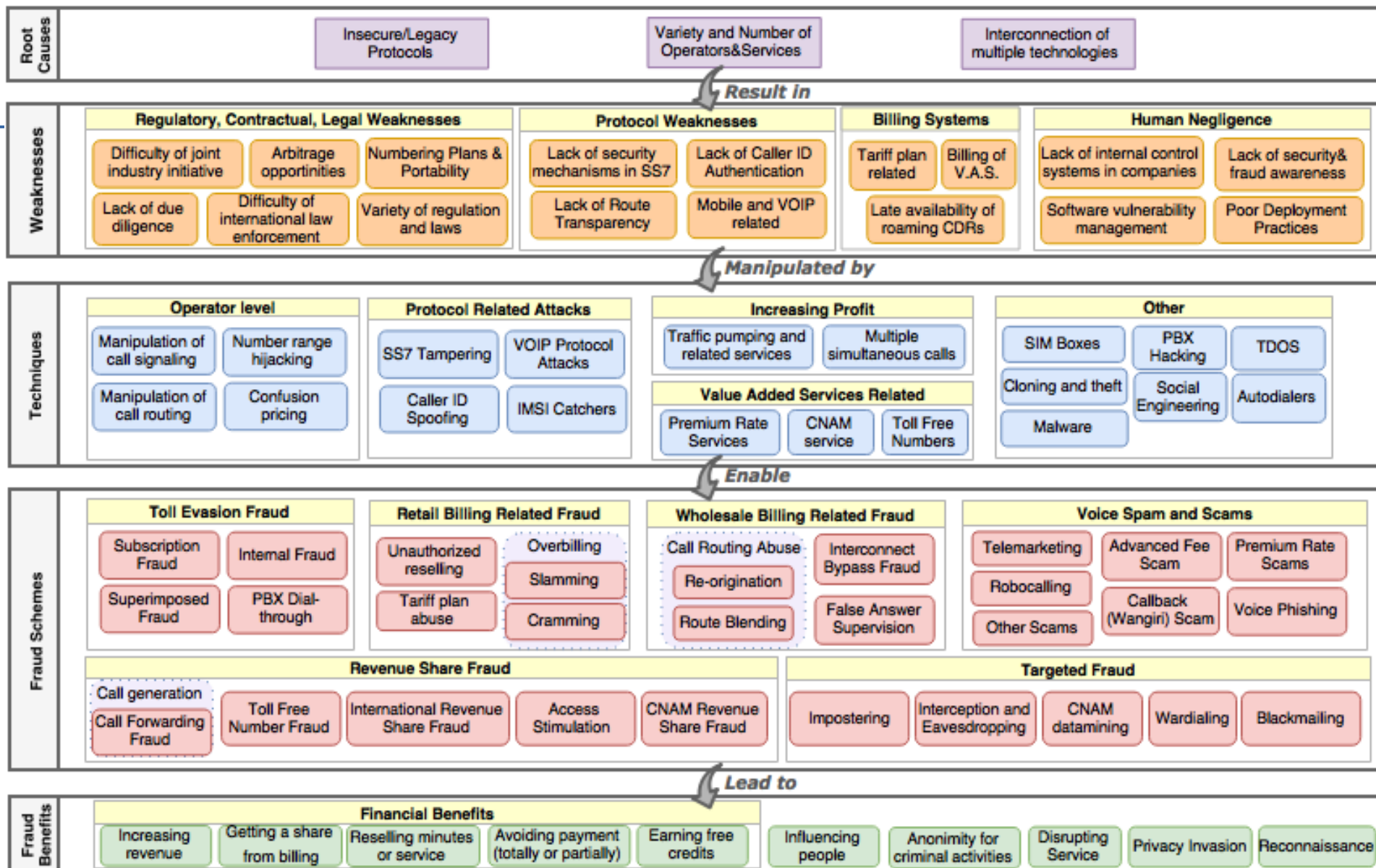
- Japanese word for “One (ring) and cut”



Example: Wangiri Scam







Fraud Taxonomy:

Root causes

Root causes

- Inherent characteristics that come from the initial design and evolution of the system
 - Legacy systems that are not designed with security in mind
 - Infeasible to upgrade in a global scale
 - Large variety and number of operators & service providers
 - Hard to identify parties with malicious intentions
 - Interconnection of multiple (poorly understood) technologies, services & products
 - Broadens the attack surface

Fraud Taxonomy: Weaknesses

Weaknesses

- A vulnerability or a feature of the system that can be manipulated in a malicious way
 - Regulatory & legal weaknesses
 - Protocol weaknesses
 - Billing related weaknesses
 - Human negligence

Regulatory&Legal Weaknesses

- Telecom regulations and laws vary largely across countries
 - Gray areas about legality of some actions
 - Operators are subject to various rules
 - Obligation to route calls to all numbers
 - Cannot block any calls without user permission
 - VOIP is usually not regulated
 - Should it be regulated?
Freedom and network neutrality discussions...

Regulatory&Legal Weaknesses

- Numbering Plans and number portability
 - Numbering plans allow to decode phone numbers to find the target operator and route the calls

Example:

COUNTRY	CC	NDC/SN	DESCRIPTION	TYPE	NET NAME	NET TYPE
"France"	"33"	"493"	"Cote d'Azur"	"FIXED"	""	""
"France"	"33"	"7806"	""	"MOBILE"	"Afone Mobile"	"VIRTUAL on SFR"
"France"	"33"	"7807"	""	"MOBILE"	"Lebara Mobile"	"VIRTUAL on Bouygues Telecom"
"France"	"33"	"7808"	""	"MOBILE"	"Lebara Mobile"	"VIRTUAL on Bouygues Telecom"
"France"	"33"	"781"	""	"MOBILE"	"Free Mobile"	"3G 900/2100 HSPA+, 4G LTE 2600"
"France"	"33"	"782"	""	"MOBILE"	"Free Mobile"	"3G 900/2100 HSPA+, 4G LTE 2600"
"France"	"33"	"783"	""	"MOBILE"	"Free Mobile"	"3G 900/2100 HSPA+, 4G LTE 2600"
"France"	"33"	"7840"	""	"MOBILE"	"Orange"	"GSM900/1800, 3G 2100 HSPA+, 4G LTE"
"France"	"33"	"7841"	""	"MOBILE"	"Orange"	"GSM900/1800, 3G 2100 HSPA+, 4G LTE"
"France"	"33"	"7846"	""	"MOBILE"	"La Poste Mobile"	"VIRTUAL on SFR"
"France"	"33"	"7847"	""	"MOBILE"	"La Poste Mobile"	"VIRTUAL on SFR"
"France"	"33"	"79"	""	"MOBILE"	""	""
"France"	"33"	"8"	"Value Added Services"	"SUPPLEMENTARY SERVICES"	""	""
"France"	"33"	"80"	"Freephone Services"	"SUPPLEMENTARY SERVICES"	""	""

Regulatory&Legal Weaknesses

- Numbering Plans and number portability
 - Global phone number allocation is regulated by ITU via E.164 standardization. Each country has its own regulatory body for further allocation.
 - **Numbering plans change frequently**, commercial databases try to keep updated information
 - **Number portability** allows to change your service provider without changing your phone number
 - Easy to know if a phone number belongs to an allocated number range, but hard to know if the number is currently assigned to a user and who is the operator responsible

Regulatory&Legal Weaknesses

- Difficulty of international law enforcement
 - Even though the fraudsters are identified, law enforcement is difficult across borders
- Lack of joint industry initiative to fight fraud
 - Some operators may not have the incentive to fight fraud
 - Fighting small scale fraud can be more expensive than the fraud loss

Protocol and Network Weaknesses

Telephony network is an interconnection of PSTN, cellular and IP networks, all of which have different weaknesses:

- Lack of encryption and authentication mechanisms in SS7
 - Access to SS7 network is no longer limited to small number of trusted operators (Operators providing commercial access to 3rd parties, femtocell hacking, etc.)
 - Anyone with access to signaling links can tamper with SS7 messages
 - SIGTRAN (SS7 over IP) protocol suite introduces encryption (TLS or IPSec), but only at transport layer.
- Lack of transparency on the call route
 - Signaling protocols does not provide a mechanism to trace the route of a call
 - Operators can only know the previous and the next hop of a call
 - IP gateways make call tracing even more difficult

Protocol and Network Weaknesses

- Lack of Caller ID Authentication
 - Caller ID (identification) information is transmitted between operators through the underlying signaling protocol
 - SS7 and most IP based signaling protocols do not authenticate the caller ID
- Lack of proper encryption and authentication in cellular and VOIP network protocols, vulnerabilities in software stacks
 - e.g., GSM (2G) networks only authenticates user, but not the network
 - Various attacks against A5/1 and A5/2 stream ciphers used in GSM
 - Vulnerabilities in 3G. 4G/LTE implementations
 - Legacy technologies lead to downgrade attacks

Weaknesses in Billing Systems

- Billing systems are complex and mistakes in billing process or tariff plans can be manipulated
- Operators cannot immediately detect fraudulent usage (High usage reports) for roaming CDRs
- Value Added Services (VAS) further complicates billing (complex networks of 3rd party service providers and number resellers, hard to identify malicious parties)
 - Operators have Revenue Assurance departments, usually working together with the Fraud Management department

Human Negligence

- People interacting with telecoms networks may not be aware of its vulnerabilities and possible fraud&abuse
- Some weakness on the enterprise level:
 - lack of internal control systems (such as access control)
 - poor deployment practices (weak passwords, ignoring updates)
 - lack of vulnerability management in software and hardware systems

Fraud Taxonomy: Techniques

Techniques

- Any attack vector that manipulates a weakness and enables a fraud
 - Operator level
 - Protocol related attacks
 - Abuse of Premium Rate Services
 - Techniques to increase profit
 - Other techniques

Operator Level Techniques

- Manipulation of call routing
 - Operators can manipulate the routing of calls that transit through their networks. E.g.,
 - by diverting the call to a fraudulent route
 - by terminating the call on an IVR, instead of sending it to legitimate destination (short-stopping)
 - Due to 'lack of route transparency', originating operator will not be aware of this

Operator Level Techniques

- Manipulation of call signaling
 - Operators can manipulate call signaling messages in order to:
 - fake the originating phone number (which will affect billing)
 - delay the call disconnect message or provide an early answer (which will increase call duration)

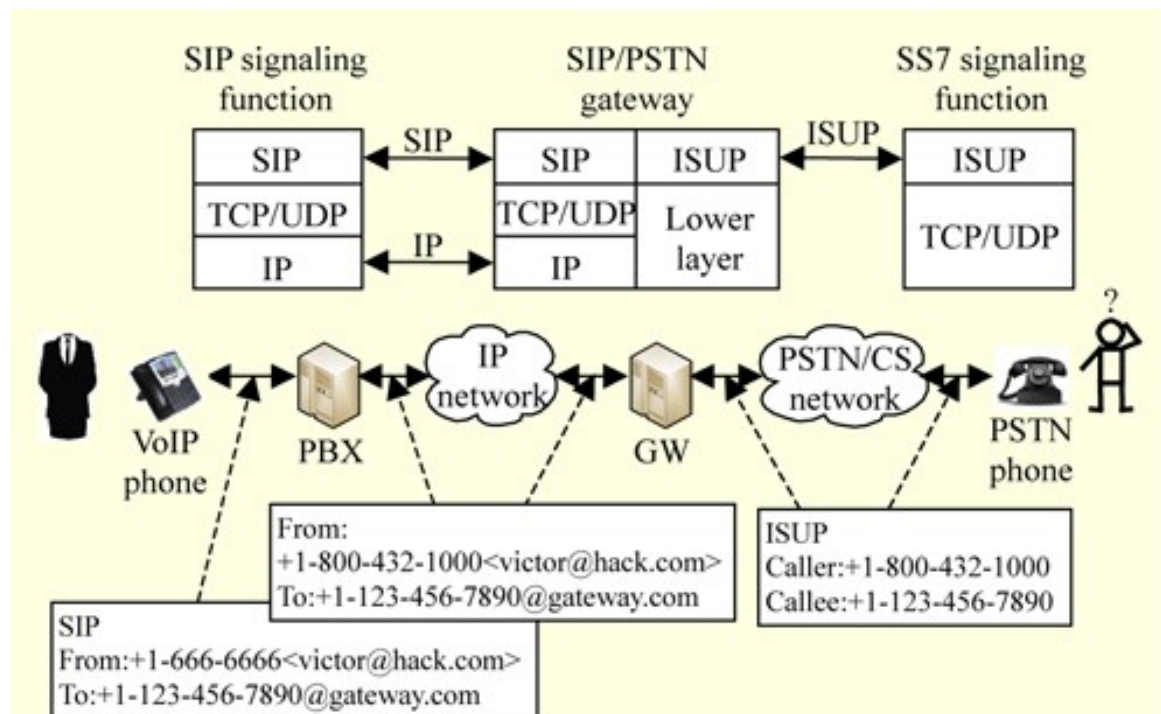
Operator Level Techniques

- Number Range Hijacking
 - Abuse of Least Cost Routing (LCR) policies
 - Operator advertises very cheap rates for a destination number range and attracts a lot of traffic from other operators, as they will choose the cheapest route
 - Calls to hijacked numbers may never reach the real destination, if a fraudulent transit operator hijacks and 'short-stops' the calls

Protocol Related Attacks

- Caller ID Spoofing

- Caller ID is supplied by the sender (originating party) and not authenticated. Most SIP providers allow spoofing
- More difficult to spoof caller ID in mobile networks, due to authentication of subscriber
- IP-to-GSM & IP-to-PSTN GWs makes spoofing easier
- Ex: <https://www.spooftel.com/>



Protocol Related Attacks

- SS7 Tampering
 - An attacker with access to SS7 network can use vulnerable SS7 messages to query a subscriber's status or change certain configurations
 - SS7 tampering allows
 - Call and SMS interception
 - Location Tracking
 - Call forwarding (e.g., to a premium rate number)
 - Denial of service

Protocol Related Attacks

- SS7 Tampering
 - Some vulnerable SS7 messages:

Message	Attack
sendAuthenticationInfo	Interception
registerSS, eraseSS	Interception (Incoming), Fraud
updateLocation	Interception(SMS), DoS
deleteSubscriberData, cancelLocation	DoS
provideSubscriberLocation	Tracking

[*]SANS Institute Whitepaper: "The Fall of SS7 How Can the Critical Security Controls Help?", 2015

Protocol Related Attacks

- IMSI catchers
 - Fake GSM base stations that are used to identify and locate phones in proximity (catch their IMSI), or intercept calls and communications
 - IMSI catchers manipulate the lack of network authentication in GSM protocol
 - 3G/4G networks are also vulnerable due to downgrade attacks, leaked authentication keys and implementation problems

Demo: SS7 attacks and IMSI catchers

- Use of PSI (Provide Subscriber Information) to get the location and TMSI
- Use of sendAuthenticationInfo to get the encryption key of the user

Karsten Nohl: Mobile self-defense CCC 2014

https://www.youtube.com/watch?v=nRdJ0vaQt0o&t=1109s&ab_channel=media.ccc.de
18:30 – 22:50

More techniques...

- PBX Hacking
 - Attackers can find vulnerable PBXs using SIP scanners or calling company phone numbers
 - Once they identify a PBX, they can compromise it via
 - Voicemail accounts
 - Maintenance interfaces
 - Social engineering, etc.
 - A compromised PBX can be used to commit many different fraud schemes
 - PBXs also allow creating multiple simultaneous calls, that will increase fraud profit

More techniques...

- SIM Boxes
 - devices that can act as a gateway between the mobile network (e.g., GSM) and the IP network or PSTN
 - can contain up to 64 SIM cards
 - both legitimate and fraudulent uses



Fraud Taxonomy: Fraud Schemes

Fraud schemes

- Actual methodology employed by the fraudster to commit fraud
 - Toll evasion
 - Retail billing related
 - Wholesale billing related
 - Revenue share fraud
 - Voice spam and scam
 - Targeted fraud
 - Let's see examples from each category

Toll Evasion Fraud

- Aims to make calls without the obligation of paying the call charges
 - Example: **Subscription Fraud**
 - Fraudster uses stolen or fake identity credentials to subscribe for a post-paid SIM card
 - All calls will be charged to the stolen/fake account

Retail Billing Related Fraud

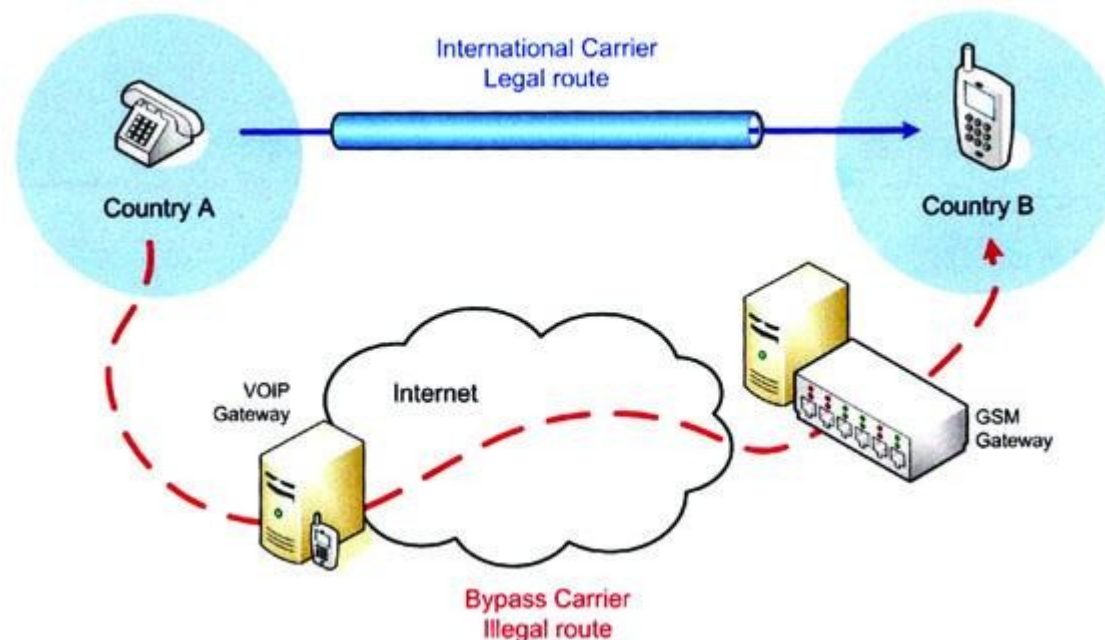
- Fraud schemes related to the billing of retail customers
 - **Over-billing:** Operators may place unauthorized charges on client's bill (e.g., when a customer unknowingly registers to a service)
 - **Tariff plan abuse:** Customers can abuse unlimited or flat rate tariff plans

Wholesale Billing Related Fraud

- Fraud schemes related to inter-carrier billing process
- **Ex.1 False Answer Supervision:** A transit operator fraudulently increase call duration or put extra charges on a call, by providing
 - False answer (call is charged while being short-stopped and diverted to a recorded message)
 - Early answer (call is charged while the callee's phone is still ringing)
 - Late disconnect (call is charged even after the disconnect message)

Wholesale Billing Related Fraud

- **Ex.2 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 calls and terminate them as domestic calls



Revenue Share Fraud

- Complex fraud scheme that targets value added services or high cost destinations
- Fraudster aims to earn a share of the call revenue
- Example: **International Revenue Share Fraud**

International Revenue Share Fraud

- Recap: Least Cost Routing mechanism

Rate sheet

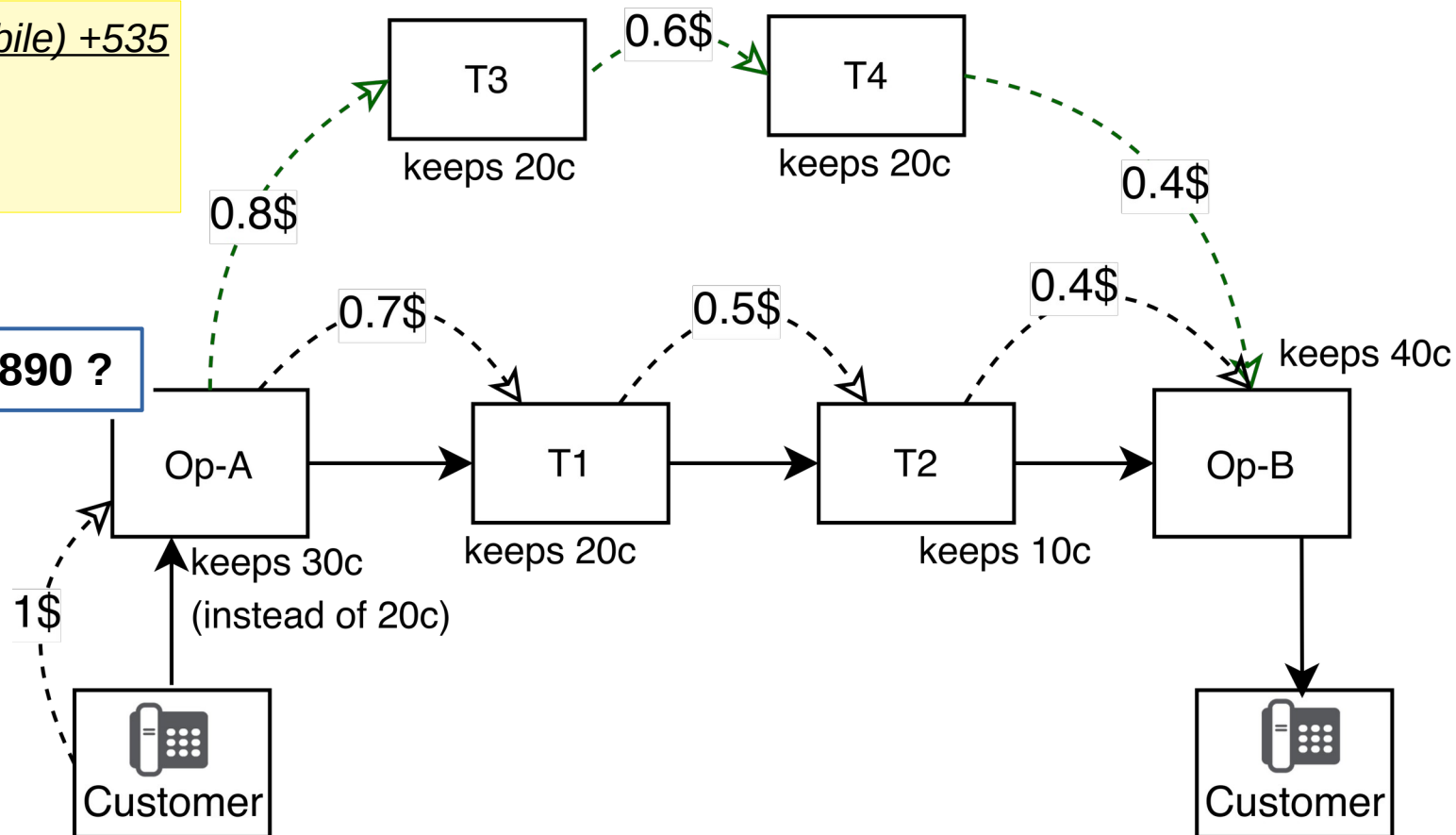
Cuba (mobile) +535

T1: 70 ¢

T3: 80 ¢

...

+53-5-67890 ?



International Revenue Share Fraud

- Recap: Lack of route transparency

Rate sheet

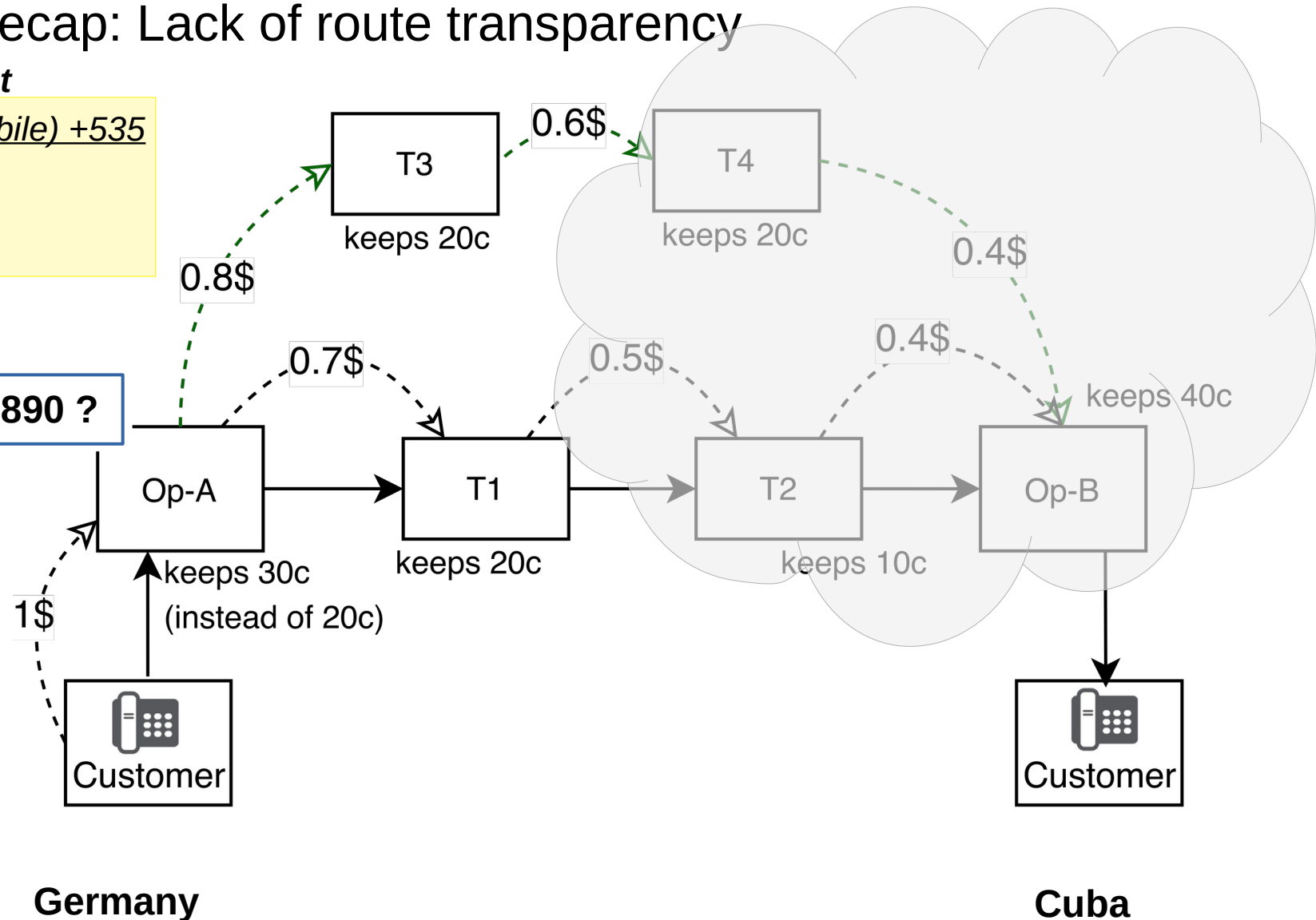
Cuba (mobile) +535

T1: 70 ¢

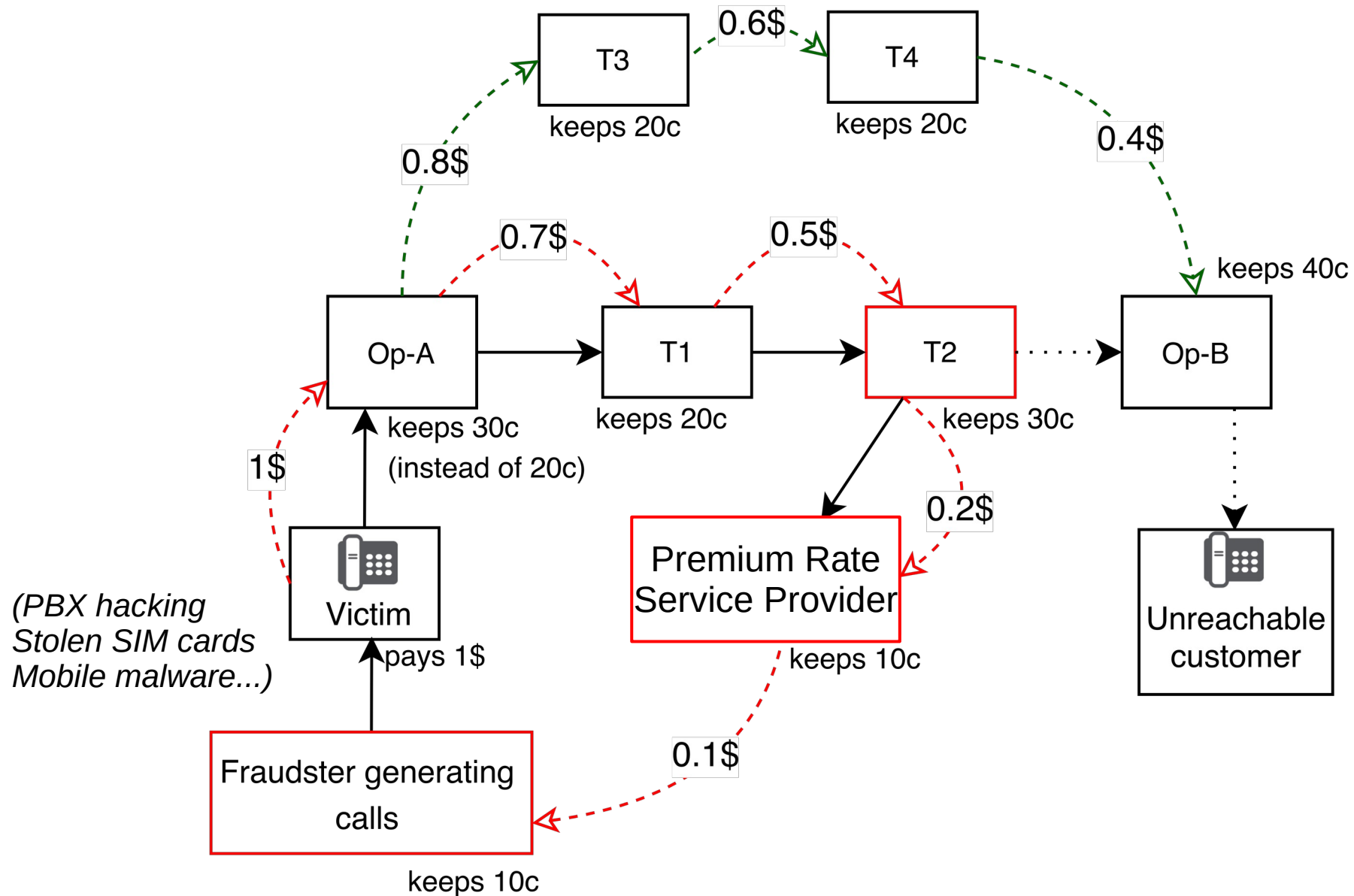
T3: 80 ¢

...

+53-5-67890 ?



International Revenue Share Fraud



International Revenue Share Fraud: Summary

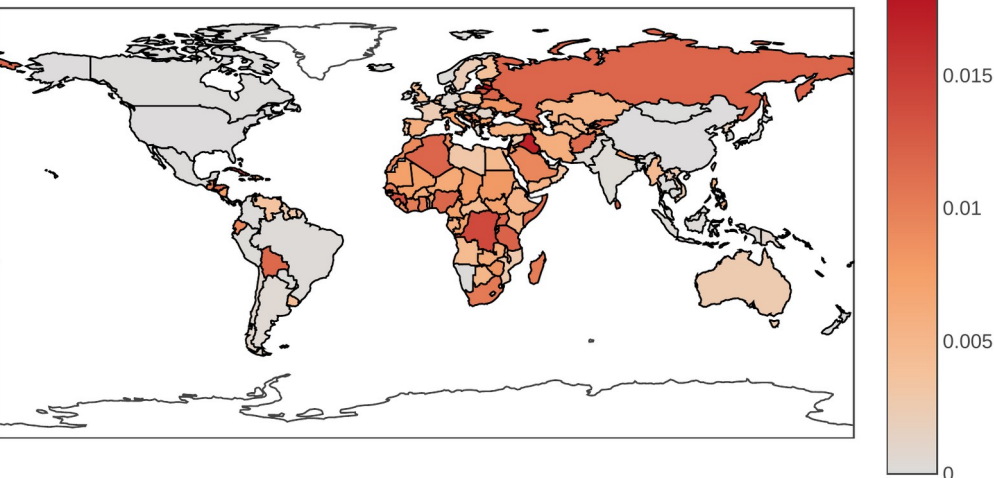
- The fraudulent transit operator
 - Hijacks and short-stops the calls
 - Keeps the termination fee
 - Re-routes calls to Premium rate service provider
- Premium rate service provider
 - Resells the high cost numbers as “Premium Rate Numbers”
- The fraudster
 - Gets a set of numbers from Premium rate service provider
 - Generates high volume of calls to these numbers (e.g., using a compromised PBX or stolen SIM cards...)

Our study of IRSF

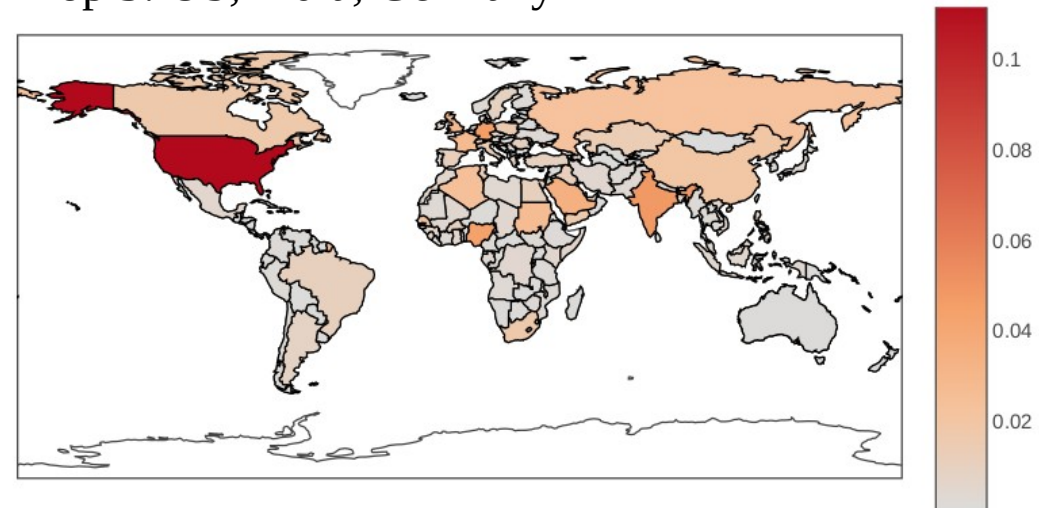
- We collected “International Premium Rate Numbers” for 4 years
 - 4M numbers
 - 200k test calls
- Built RF model for detection
- See our NDSS 2021 paper

Understanding and detecting international revenue share fraud
M. Sahin, A. Francillon, NDSS 2021

Ratio of advertised test IPRNs
Top 3: Latvia, Iraq, Cuba



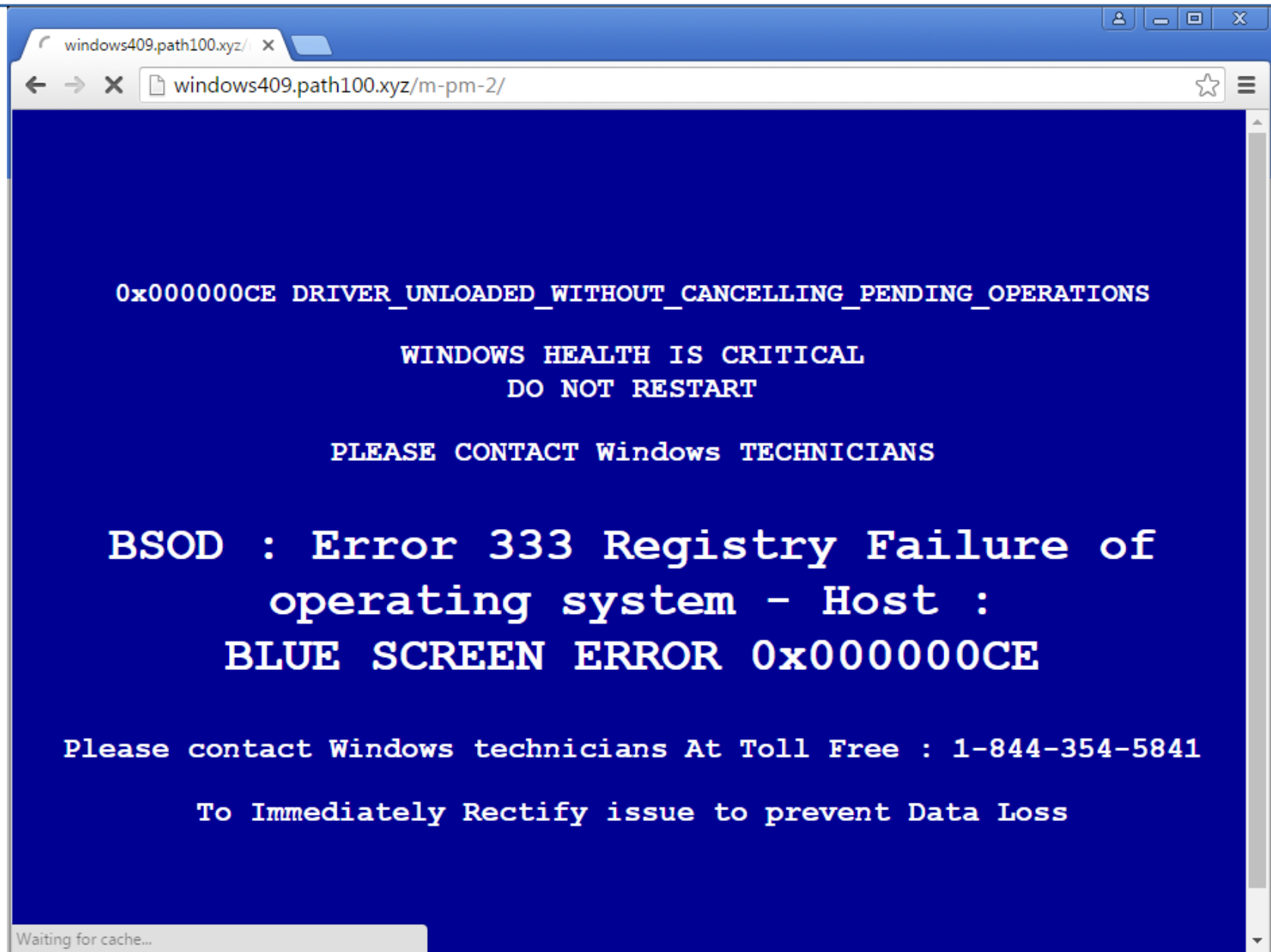
Ratio of test calls originations
Top 3: US, India, Germany



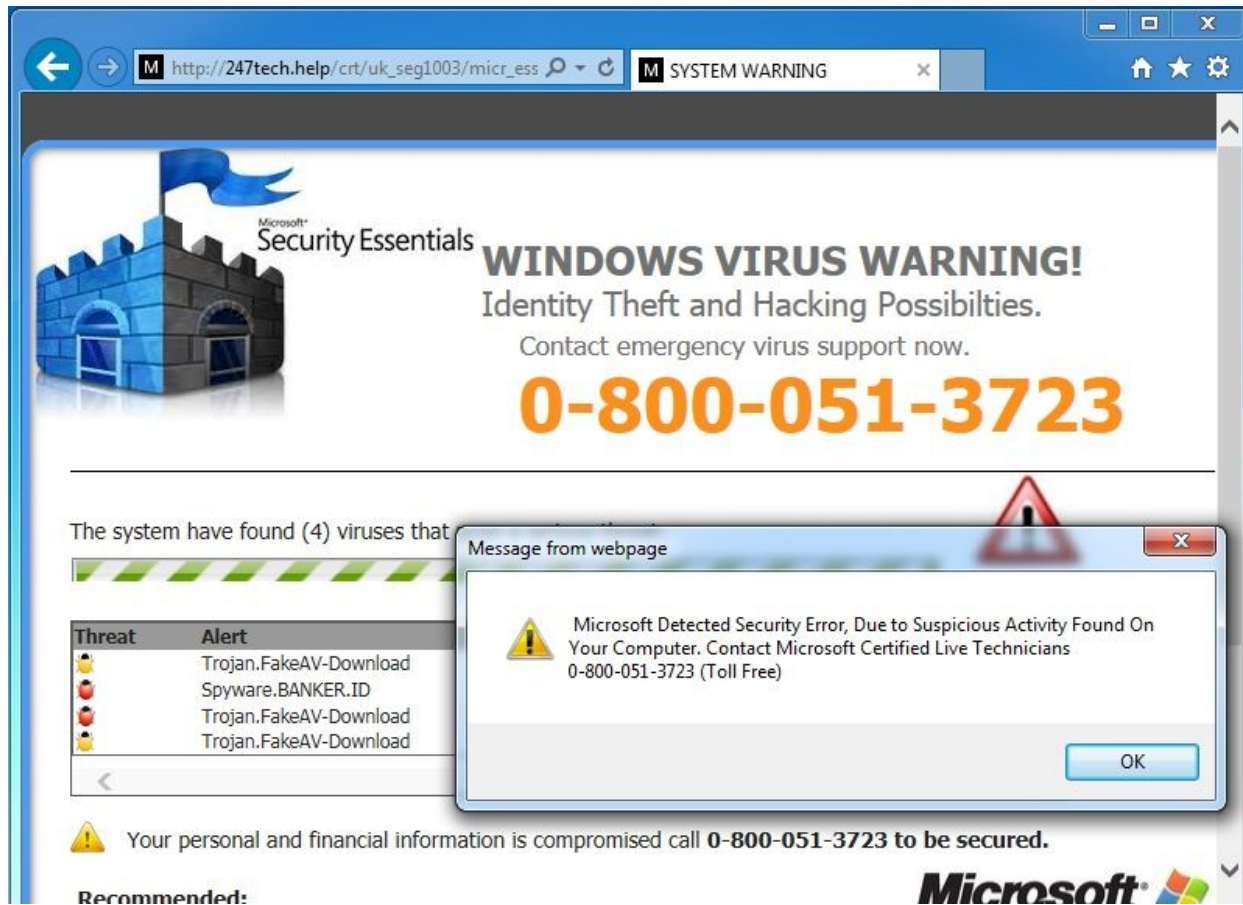
Voice Spam and Scams

- Voice spam includes all types of unsolicited and illegitimate calls
- Fraudsters obtain phone number lists from leaked databases, form submissions, etc.
- They can use auto-dialers are used to generate large number of calls
- Pre-recorded messages (robocalling) or call center agents interact with victims
 - to reveal sensitive information (e.g., credit card number) or
 - to convince victims to do certain actions (e.g., wire transfer to a bank account)
- Caller ID spoofing and social engineering techniques are frequently used
- Examples: Tech support scam, Free cruise scam

Ex. Tech support scam



Ex. Tech support scam



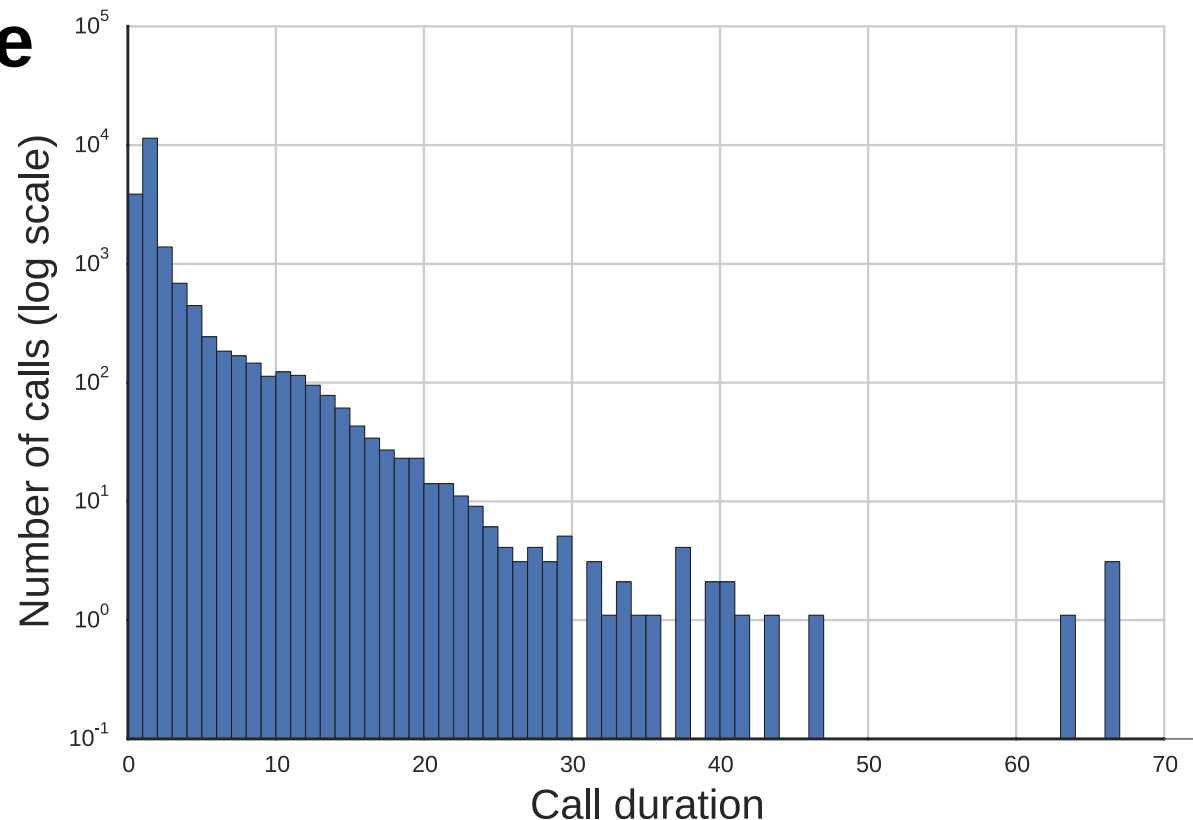
<https://www.youtube.com/watch?v=t7kSWvt3KXY>

Our study on a deceptive chat bot: Lenny

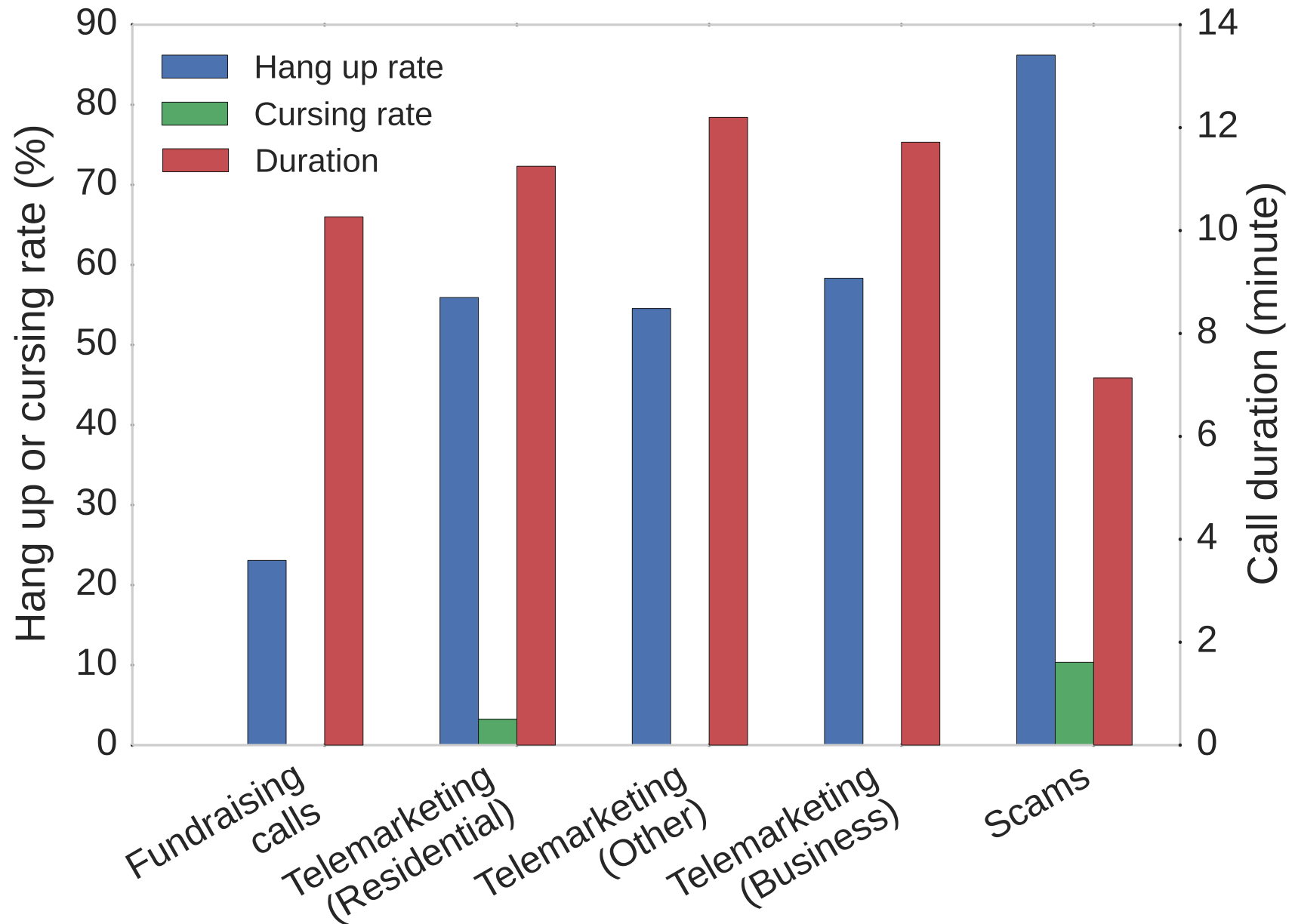
- Actor recording that is answering spammers automatically
- Voice spam includes all types of unsolicited and illegitimate calls
 - Total of 19k calls for 18 months (385 hours recorded)
- We analyzed the calls with conversation analysis
- Works so well because the construction of the
- [*]"Lenny!", Available at https://www.youtube.com/playlist?list=PLduL71_GKzHHk4hLga0nOGWrXlhl-i_3g

Analyzing call durations


- Lenny received 19,402 calls in 18 months
- 78% of calls < 2 minutes, 1 < 58% of calls < 2 min.
- Considering calls ≥ 2 minutes, Lenny wasted **more than 385 hours** of telemarketer time!



Spammers' Interaction With Lenny



Lenny the subtle chatbot

- Lenny is
 - a specialized chatbot &
 - a high interaction honeypot
 - *honey-bot*
 - *robo-callee*

to defend against spam calls.
- Lenny's smartness comes from its ability to fit in this **narrow context** of spam call conversations
- Use of Lenny-like chatbots may be an effective way of slowing down voice spam

Fraud Taxonomy: Fraud Benefits

Fraud Benefits

- Fraud benefit: The ultimate aim of the fraudster to commit fraud
 - can be financial:
 - Avoiding payment (totally or partially)
 - Reselling minutes or service
 - Increasing company revenue
 - or other benefits:
 - Anonymity for criminal activities
 - Disrupting service
 - Reconnaissance
 - Privacy invasion

Conclusion

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 > cost of detection/prevention)