THE EVOLUTION OF TELECOM FRAUD PREVENTION

Yaniv Rofé
Humbug Telecom Labs, Ltd.
BACKGROUND

In the 1960’s fraudsters tricked the phone systems of AT&T into providing free calls by whistling high-pitched sounds into their handset. These pranks would become known as phreak attacks. Ironically the founders of Apple made hardware for hacking into phone systems in what was their first commercial endeavor together. Although illegal, phreak attacks in the 60’s were relatively innocuous, affecting only carriers and causing no significant revenue loss.

The reality of telecom fraud today is frighteningly different. A 1983 insurance claim for a $382,000 telecom fraud attack on a Fortune 100 company presaged the enormity of the problem to come. According to the Communications Fraud Control Association 2011 Global Fraud Loss Survey, over $40.15 billion are lost each year to telephony fraud. The top three predominant sources are Subscription Fraud ($4.32 Billion), PBX/Voicemail Hacking ($4.96 Billion), and Premium rate Service Fraud ($2.24 Billion). According to the survey, 98% of participants felt that global fraud losses had increased or stayed the same, while 89% said fraud has trended upwards within their company.

In the past, only large companies could afford their own PBX, but the rise of inexpensive digital IP-PBXs have enabled smaller businesses to install their own in-house telecom networks. But with added convenience and functionality these companies unknowingly became susceptible to telecom fraud. Today organizations of all sizes, in the telecom business and otherwise, are susceptible to telecom fraud attacks that can cripple their business financially over a weekend.

Whereas hackers are community oriented, sharing and posting their methodologies and exploits online, companies are reluctant to speak of fraud attacks for fear of hurting their public image. This embarrassment only perpetuates the problem. Hackers are free to roam. As soon as a weakness is shored up in one location, the hacker is free to move to the next unsuspecting victim. Ideally organizations would reduce the collective risk of fraud attacks by sharing information anonymously.

For every telecom fraud related headline we see there are hundreds of other cases that go unreported. Those cases that do draw the media’s attention are salient reminders of the devastating consequences of an unsecure telecom network. However, outlets are beginning to raise awareness of the global telecom fraud epidemic:

- Company suffers $400,000 fraud in 2 days
- The U.S. government breaks up a toll fraud ring costing enterprises $55 million.
- A single company victim to an organized attack on their PBX and voicemail resulting in $2 M of damage.
- A music chain in Canada hit with $83,000 in fraudulent phone charges following a weekend attack.
- A small Perth, Australia business charged $120,000 for 11,000 fraudulent long distance calls made in the span of 46 hours via a phreak attack.
- AT&T customers are defrauded for $2 Million by a group of Filipino hackers operating on behalf of a Saudi terror group.

TOP 10 FRAUD ROUTING DESTINATIONS:

1. Cuba
2. Somalia
3. Sierra Leone
4. Zimbabwe
5. Latvia
6. Austria
7. Lithuania
8. Philippines
9. United Kingdom
10. Estonia

Source: CFCA 2011 Global Fraud Survey
TELECOM FRAUD EXPLAINED

MAJOR PROFIT DRIVEN ATTACK CATEGORIES

There are many types of attacks that can target an organization’s PBX, some more costly than others. The following represent the three overarching methodologies for infiltrating the organization’s defenses:

- **Crude** - exploiting voicemail security or trying default/common passwords are two of many crude techniques. Fraudsters may also directly contact employees to ascertain useful information that can be used to gain access to systems (phishing).

- **Sophisticated** - hacking the PBX to gain access privileges, much like hacking a computer network. This attack type may include denial of service (DoS) attacks, brute force attacks, etc.

- **Devious** - Hacking the PBX to gain access to internal computer systems via the link intended for connecting the PBX to the CRM system or an IT port. This allows the hacker to access customer data (including credit card information), insert viruses into the system, or otherwise disrupt business by bypassing the firewall.

Once the fraudster has gained access to the PBX, his crime may take several forms, which are listed below, in addition to other scenarios that should be considered.

**PREMIUM RATE FRAUD**
Owners of premium rate telephone numbers profit from hacking into PBXs around the world and routing calls to their own premium rate services.

**CALL SELL PBX FRAUD**
Online or offline call wholesalers hack into PBXs in order to sell calls to their customers without incurring any of the charges themselves; the more expensive the destination the better; the more calls the wholesaler can route out of an organization simultaneously the better. Destinations may be satellite phones that cost $8/minute to call, or countries that cost upwards of $2/minute to call. Obviously, the more lines the fraudster uses to perpetrate the attack, the more profound the financial loss.

**PBX DIAL-THROUGH**
Dial-Through fraud relies on DISA (Direct Inward System Access) features that exist on every PBX. These features allow employees to call into the switchboard or their voicemail and make outgoing calls after inputting a password or pin. Although this feature may be turned off upon installation, hackers will try to break in and create their own mailbox which will allow them to dial in and then make any calls they wish.

**CALLS TO KNOWN FRAUDULENT NUMBERS OR DESTINATIONS**
Telecom fraud is a well-known problem, and like the “Nigerian Bank Scam,” there are blacklists of phone numbers, area codes etc., that can be blocked or monitored if the right tools are at hand.

**OFF HOUR CALLS**
Calls originating from an organization’s PBX may be the result of Internal Employee Fraud, unauthorized visitors, or remote hackers accessing the system. Most significant telecom fraud attacks are perpetrated when the enterprise is unmanned at night, over weekends, bank holidays, religious holidays, etc.

**INTERNAL MISCONDUCT**
Telecom fraudsters are not always outside the confines of the organization. Internal Employee Fraud is a significant contributor to fraud affecting organizations. Employees may use company phones to make premium number, personal, and long distance calls. In the worst case scenario employees may actively enable toll fraud. It is possible to program an internal phone to auto-forward to an international destination or to create a mailbox with dial-out privileges allowing the employee to call it at local rates while forcing the company to pay the long distance charges.

**PHISHING ATTACKS**
Although phishing attacks focus on defrauding the business’ customers, they result in lower revenues and in ruined customer relations. A fraudster will call with partial information about an account and attempt to trick an agent into providing more information. The fraudster will call back continuously and speak to different agents and gain more crucial information each time, until he can convince an agent that he is the authorized customer. The fraudster can then make purchases, money transfers, incur charges, or otherwise defraud the customer and the business.

**EXAMPLE:**

100 lines are hijacked to call a Premium Number that charges $2/minute. The organization leaks $200/minute, which translates to $12,000/hour.

If undetected, the crippling cost of such an attack would reach **$288,000 in 24 hours.**

*Activating Humbug’s Premium Number Blacklist Alert identifies an attack of this nature at the very beginning.*
FIGHTING TELECOM FRAUD
THE OUTDATED MODEL

In the past decades the provision and usage of telecom services have been transformed beyond recognition. Hackers too have evolved from harmless pranksters into sophisticated and cunning criminals who can cause businesses considerable financial damage. Unfortunately, the prohibitively expensive customer premises based fraud solutions, running upwards of $170,000 for installation and costing more than $17,000 a month to operate and maintain, never evolved to cater to non-carrier customers.

The excessively high cost of customer premises based solutions is only part of the problem. The focus always has been and continues to be on carrier level traffic. Whereas anomalies in end-user traffic stick out like a sore thumb, they are lost in the sea of calls at the carrier level. Detecting anomalies in carrier level traffic naturally means that a negligible amount of fraud will occur before an alarm is sounded. Unfortunately what is negligible to carriers with deep pockets is hardly negligible to the vast majority of end-users. But the standard is that the end-user always pays.

Because customer premises based solutions are simply unaffordable, large businesses with sufficient resources may attempt to create in-house solutions and safeguards. As noted previously, organizations do not have a framework for sharing information on attacks, nor do they share information regarding solutions. This situation creates tremendous inefficiencies, not to mention the significant opportunity costs of diverting resources from core businesses as organizations improvise solutions to tackle the risk of telecom fraud.

THE EVOLUTION OF TELECOM FRAUD SOLUTIONS

To address the needs and concerns of the vast majority of telecom end-users, the following requirements must be met:

1. Affordability
2. Focus on the End-User
3. Anonymous Information Sharing
4. Shift from Customer Premises to Cloud Based

FIGHTING TELECOM FRAUD
HUMBUG TELECOM LABS

Humbug Telecom Labs provides organizations of all sizes with carrier-class telecom analytics as a free service, and fraud prevention and detection tools as an affordable paid monthly subscription. Both services are cloud based, installed within minutes, and may be accessed from any computer, anywhere in the world. Humbug Telecom Analytics boasts an elegant User Interface making it easy for marketing, finance, or IT staff to monitor the organization’s phone system(s).

Humbug modernizes the antiquated approach to fighting fraud in which each organization stood alone on the battlefield with a patchwork of contrived solutions. No need to reinvent the wheel; with a host of customizable alerts, users actively participate in setting up their defenses. This layer of proactive protection is driven by the philosophy that end-users understand their telecom traffic better than any algorithm. Whereas the traditional approach to fraud detection looks for fraud at the carrier level, Humbug’s focus is detecting fraud in end-user traffic where anomalies are more pronounced.

Finally, Humbug is changing the way telecommunications fraud is detected with anonymous information sharing; by correlating end-user traffic data with a community database of blacklisted numbers (compiled by the CFCA, law enforcement agencies, and industry players), Humbug creates the world’s largest fraud detection network and a vast repository of telecom data. Additionally, fraud methodologies and fingerprints are learned across the network, denying fraudsters the luxury of migrating from one user to another with the same schemes. Easily configurable safeguards alert the organization via email, SMS, or automatic phone call whenever an alert is triggered to forewarn of a pending telecom fraud attack.

THE COMPETITION | HUMBUG TELECOM LABS
--- | ---
Location | Customer Premises | Cloud Based
Focus On | Carrier Level Traffic | End-User Traffic
Installation Method and Time | Integration Team, 6 Months | Self Serve, 5 Minutes
Installation Cost | $170,000 + | Free
Monthly Cost | $17,000 + | Plans Range from $5 to $500*
Anonymous Information Sharing | No | Yes
Emphasis On | Detection | Prevention
Free Telecom Analytics | No | Yes

* Heavy traffic users, please contact us for a price quote.
HUMBUG ANALYTICS

The information Humbug analyzes is not only relevant in preventing fraud. Humbug Telecom Analytics provides your organization with tangible benefits in several ways:

MARKETING ACTIVITY OPTIMIZATION

Track marketing campaign effectiveness based on metrics, based on geography or by campaign specific phone numbers.

Track sales team(s) with metrics for number of calls inbound/outbound, average call duration, calls per location, department or employee, etc.

COST OPTIMIZATION

Real-time knowledge of telecom costs itemized details about calls per location, department or employee.

No bill shock, know your phone bill balance in real-time.

Improved bargaining position vis-à-vis the carrier enables detailed dispute resolution with itemized phone use details.

Optimize phone plan based on actual telecom utilization, to improve expenses.
Humbug’s fraud alerts were developed in collaboration with Carriers, major ITSPs, and high volume Call Centers. Alerts were designed to provide the heavy telecom user with flexibility. Alerts are as stringent as a user wishes. A single call to an unapproved destination, for example, might not be important enough to distract a manager with an alert. However, should that manager decide that five such calls in the span of an hour warrant an alert then he shall be alerted. Humbug Telecom Pro Threshold Alerts are configurable in different time resolutions and even according to geographical destination.

Humbug allows the user to reproduce the same configurations across dozens of servers without time consuming programming. Alternatively, the user may view all servers as one and apply alert configurations collectively. Moreover, the user interface was built so that it is enjoyable to use, visually pleasing, and requires very little technical understanding.

Decades of telecom fraud sciences teach us that no algorithm is as good as a few minutes of familiarization with the user. Why guess what the user already knows? Since no one knows the organization’s business activity patterns better than management, Humbug fraud alerts were designed with proactive protection in mind. Within 20 to 30 minutes of simple and intuitive work on the user interface, the organization is protected from a vast array of fraud possibilities.

### CARRIER CLASS TOOLS

Humbug’s Telecom Pro service is a game changer. The system is installed within minutes and any employee, regardless of his level of technical expertise, can configure fraud alerts, in the same amount of time it takes to eat lunch.

In terms of bang-for-the-buck performance, the Humbug solution is a no-brainer. However, the benefits to the organization begin before money changes hands. Once the Humbug Collector Agent is installed, users may access, within minutes, real-time carrier-class Telecom Analytics.

### CONNECTING TO HUMBUG

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TIME</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Humbug Collector Plugin</td>
<td>5 Seconds</td>
<td>Free</td>
</tr>
<tr>
<td>Install Humbug Collector Plugin</td>
<td>Less than 5 Minutes</td>
<td>Free</td>
</tr>
<tr>
<td>Start Receiving Carrier Class Telecom Analytics</td>
<td>At Conclusion of Installation</td>
<td>Free</td>
</tr>
<tr>
<td>Configure up to 48 Telecom Fraud Alerts to protect your organization</td>
<td>30 Minutes</td>
<td>Affordable Monthly Subscription</td>
</tr>
</tbody>
</table>

Install a cloud-based system to optimize your organization’s performance based on real-time, in-depth analytics within minutes. Protect your organization from costly telecom fraud in less than an hour.
HUMBUG FRAUD ALERTING TOOLS INCLUDE:

Technical - receive alerts when certain technical events occur; events that are strong indicators of pending fraud.

Blacklist - receive alerts when traffic to/from blacklisted sources is detected in your PBX:
- Number Blacklist - Set up your own list of blacklisted numbers.
- Community Blacklist - Protect your PBX from over 70,000 industry-confirmed blacklisted numbers.
- Country Blacklist - Receive alerts when traffic to/from specific countries you select are detected.

Timestamp - receive alerts when calls originate from your organization at suspicious times:
- User defined time ranges.
- Business hours.

Cost & Duration - receive alerts when individual calls exceed a specified cost per minute, total cost or duration.

Phishing & Threshold - receive alerts when hourly, daily or monthly costs, durations, or call volume thresholds are exceeded. Apply to specific numbers, to specific countries, or to overall traffic.

Statistical - User Specific Statistically Significant Anomalies, receive alerts when Humbug identifies traffic that is inconsistent with historic telecom usage.

Unique Community Based Information Sharing – Humbug Labs uses a secure cloud based system that learns of new fraud fingerprints in real time and spreads the information in the Humbug Network, ensuring that all Humbug users are protected. Customer premises solutions lack this important community feature.

Future Proof Solution – unlike solutions based on installing a physical box, the cloud-based nature of the Humbug solution is future proof for all technologies.

ABOUT THE AUTHOR

Yaniv Rofé, one of the founders of Humbug Telecom Labs, holds a BA in Economics from Emory University and an MBA from the University of Tel Aviv. Formerly of Merrill Lynch and Ernst & Young, Mr. Rofé was a member of a five-person transaction team that executed one of Israel’s largest real estate IPOs on the LSE (5970 million post-money valuation). Mr. Rofé is also the founder of a Due Diligence advisory firm that evaluated deals that closed in excess of $100 Million in 2010.

REFERENCES


2Communications Fraud Control Association (CFCA); Global Fraud Loss Survey for the year 2011, November 4, 2011 www.cfca.org/fraudlosssurvey


9Technical - receive alerts when certain technical events occur; events that are strong indicators of pending fraud.

Blacklist - receive alerts when traffic to/from blacklisted sources is detected in your PBX:
- Number Blacklist - Set up your own list of blacklisted numbers.
- Community Blacklist - Protect your PBX from over 70,000 industry-confirmed blacklisted numbers.
- Country Blacklist - Receive alerts when traffic to/from specific countries you select are detected.

Timestamp - receive alerts when calls originate from your organization at suspicious times:
- User defined time ranges.
- Business hours.

Cost & Duration - receive alerts when individual calls exceed a specified cost per minute, total cost or duration.

Phishing & Threshold - receive alerts when hourly, daily or monthly costs, durations, or call volume thresholds are exceeded. Apply to specific numbers, to specific countries, or to overall traffic.

Statistical - User Specific Statistically Significant Anomalies, receive alerts when Humbug identifies traffic that is inconsistent with historic telecom usage.

Unique Community Based Information Sharing – Humbug Labs uses a secure cloud based system that learns of new fraud fingerprints in real time and spreads the information in the Humbug Network, ensuring that all Humbug users are protected. Customer premises solutions lack this important community feature.

Future Proof Solution – unlike solutions based on installing a physical box, the cloud-based nature of the Humbug solution is future proof for all technologies.

REFERENCES


2Communications Fraud Control Association (CFCA); Global Fraud Loss Survey for the year 2011, November 4, 2011 www.cfca.org/fraudlosssurvey


9About the Author

Yaniv Rofé, one of the founders of Humbug Telecom Labs, holds a BA in Economics from Emory University and an MBA from the University of Tel Aviv. Formerly of Merrill Lynch and Ernst & Young, Mr. Rofé was a member of a five-person transaction team that executed one of Israel’s largest real estate IPOs on the LSE (5970 million post-money valuation). Mr. Rofé is also the founder of a Due Diligence advisory firm that evaluated deals that closed in excess of $100 Million in 2010.

ABOUT THE AUTHOR

Yaniv Rofé, one of the founders of Humbug Telecom Labs, holds a BA in Economics from Emory University and an MBA from the University of Tel Aviv. Formerly of Merrill Lynch and Ernst & Young, Mr. Rofé was a member of a five-person transaction team that executed one of Israel’s largest real estate IPOs on the LSE (5970 million post-money valuation). Mr. Rofé is also the founder of a Due Diligence advisory firm that evaluated deals that closed in excess of $100 Million in 2010.
Phone Hacking Tied to Terrorists

By SOMINI SENGUPTA
Published November 29, 2011

Four people in the Philippines hacked into the accounts of AT&T business customers in the United States and diverted money to a group that financed terrorist attacks across Asia, according to police officials in the Philippines.

According to the agency, the men were working with a group called Jemaah Islamiyah, a terrorist group linked to Al Qaeda and responsible for the 2002 bombings in Bali, which killed 202 people.

The suspects remotely gained access to the telephone operating systems of an unspecified number of AT&T clients and used them to call telephone numbers that paid on revenue to the suspects.

The company declined to say how much it cost AT&T. The Philippines is known as a “remote toll fraud” weak password region.

Security Manager's Journal: Slammed with a $100,000 phone bill

The way VoIP works, the company will have to pay for calls made by hackers, but it doesn't want that to happen again.

J.F. Rice

October 29, 2010 (Computerworld)

Last week, my company got a $100,000 phone bill. Turns out, some enterprising types have been bouncing their calls off our voice network. This allowed them to make numerous calls to a foreign country, using our equipment. And it looks like we're stuck with the bill.

Man gets 10 years for VoIP hacking

Edwin Pena was the first person charged by US authorities for VoIP hacking.

Robert McMillan (ODG News Service) — September 29, 2010 05:34

Edwin Pena, 27, was convicted in February of breaking into 15 AT&T telecommunications companies and then reselling their accounts without permission. He must also pay more than $1 million in restitution, and will be deported once his sentence is served.

Pena was sentenced by Judge Susan Wigenton in U.S. District Court for the District of New Jersey on computer hacking and wire fraud charges.

The scam cost the victims, including VoIP sellers Net2Phone, Vonage and Skype, more than $1.4 million in losses.

Man Gets 7 Years For Forcing Modems to Call Premium Numbers

A New Hampshire man who made US$8 million by installing unwanted dial-up software on computers and then forcing them to call expensive premium telephone numbers...

By Robert McMillan

Mar 1, 2011 3:40 PM

A New Hampshire man who made US$8 million by installing unwanted dial-up software on computers and then forcing them to call expensive premium telephone numbers was handed down an 80-month sentence on Monday.

Prosecutors say that between 2003 and 2007, Asu Paus and others put together a lucrative business by setting up premium telephone numbers in Germany —