SecureLogix

Voice & Unified Communications

# State of Security Report 2014

CISCO DEVELOPER Solution

The scale and scope of UC is far too large, and the potential damage to the enterprise too severe, for real-time communications to be left unmonitored and unprotected.

SecureLogix

# Voice & Unified Communications

# State of Security Report 2014


Introduction . . . . . 2

Executive Summary . . . . . 6

Threats Overview . . . . . 10

Threats Taxonomy . . . . . 14

Detailed Threat Analysis and Data . . . . . 20

Threat Forecast . . . . . 58

# Introduction

## What is the actual state of real-time communications security in 2014?

## Which are the most serious threats to your enterprise and customers, and which are still, at this stage, more distant prospects?

In this report, we discuss the current, real-world state of security in the scope of enterprise Voice and Unified Communications (UC). Leading security experts from SecureLogix, including Mark Collier, author of the authoritative Hacking Exposed: UC and VoIP book, present real-world findings drawn from documented and observed operational attacks against US corporations over the past year, and compare them with data observed over the past 15 years where relevant.

# Why did we write this report?

Several industry reports have emerged since the late 1990s detailing real-world, measured security issues and threat levels associated with data networks and IP-based communications. Examples of such reports include the "State of Enterprise Security Annual Report" by Symantec, the "Annual Computer Crime and Security Survey Report" by the Computer Security Institute, and similar reports from vendors such as Cisco and McAfee. These reports play an important role in profiling and measuring IP and data network threats and incident levels to help guide enterprise security decision-making, while educating the public at large.

However, a lack of attack and threat data for voice/VoIP/UC communications exists, even though voice technologies pre-date IP systems by more than 100 years. This may partly be explained by the fact that network-based crime is a fairly recent phenomenon. However, the primary explanation is the lack of real-time network monitoring tools capable of identifying and characterizing UC attacks. Note that for the remainder of this report, we use the term "UC" to describe voice, VoIP, and its related communications forms.

In the absence of real-world data, the industry has turned to prognosticating. Most UC security papers, presentations, and discussions available today focus on potential vulnerabilities discovered in laboratory environments that may or may not be a real threat in the future as UC networks evolve. Meanwhile attacks like Telephony Denial of Service (TDoS) are exploding and affecting many enterprises. Virtually no real-word, observable data or public reports illustrate the laboratory-based, potential threats actually occurring today. There simply isn't an incentive for attackers to exploit these vulnerabilities. While academic debates over future threats can be interesting, they are not what is needed to understand the attacks and fraud schemes that may be causing substantial damage to enterprises today.

# Why is it important to understand current threats to UC environments?

At one level, it is important for the same reasons it is critical to track traditional IP and data network-based threats. The ability to protect against attacks begins with identifying them and understanding which are the most severe and frequent. Further, this understanding is critical because real-time, interactive communications such as UC represent a large quotient of enterprise interactions, networks, and systems and applications. This is especially true for contact centers within enterprises. The scale and scope of UC is far too large, and the potential damage to the enterprise too severe, for real-time communications to be left unmonitored and unprotected.

At a global level, the goal of this report is to account for this blind spot. We aim to complement existing IP/data network security reports. We will help fill in this critical visibility gap surrounding UC threats so that industry and the public better understand the types of attacks that are prevalent today, how they manifest themselves, which attacks pose the greatest threat to your enterprise, and which threats should be priorities for your corporate security teams and programs. As future threats emerge over time, these will be observed in operational enterprise networks and become relevant information included in this annual report.

# What does the report contain?

We begin with a general overview of the major categories of threats to enterprise communications based on a simplified of the threat taxonomy. Each of the major threats is described giving you a clear understanding of the most important near-term threats to your enterprise and how these attacks can be mechanically executed.

The report then focuses on the summarization of real-world data regarding actual UC attacks observed against US enterprises in recent months and years. Scientific modeling is used to illustrate a UC Threats Trending Model that shows which threats are currently trending as the most frequent and severe. These are the UC attacks that enterprises should be prioritizing and guarding against today. We conclude the report with a look ahead that provides a brief security threats forecast for the next 12-24 months.

# Who wrote this report?

UC security experts, analysts, and service engineers from SecureLogix Corporation collected and summarized the information contained in this report. Founded in 1998, SecureLogix pioneered the voice security industry with the invention of patented solutions to actively monitor voice and UC networks for security attacks and vulnerabilities in real time. SecureLogix monitoring and protection solutions are currently deployed across more than five million enterprise UC devices. Through a host of network assessment and monitoring services on operational corporate networks, SecureLogix has complied more than 14 years of UC network attack and security data. The presentation and interpretation of this data forms the basis for this industry report, the only one of its kind.

# Executive Summary

This 2014 report on the State of Voice and UC Security presents a perspective developed from 15 years of real-world experience and data. In this report, based on the 2013 calendar-year time period, we present a comprehensive review of UC network threats, provide a threat taxonomy, and discuss the impact of technological advances, such as public/private SIP. Where possible, we contrast results, indicate trending, and identify new findings as compared to the results presented in the 2013 edition.

## Summary of Threats

UC security has always been a serious issue in legacy voice networks and the adoption of VoIP has made it an even larger problem. VoIP itself is not the real target; rather, VoIP has made some attacks practical and also made it easier to execute the same sort of attacks that have been around for years, namely application level UC threats, such as Telephony Denial of Service (TDoS), financial fraud/social engineering, call pumping and toll fraud, harassing calls, voice SPAM and phishing. Also, illicit use of modems persists as an issue.

The Public Voice Network will continue to get more hostile and is starting to look like the Internet in terms of threat level. This public network used to be the most trusted medium for communications, but now it has become one of the least trusted. It is unlikely to be the source of packet-attacks, but rather the source of many different types of malicious inbound calls. Also, as long as it costs money to make calls to premium numbers, outbound toll fraud will continue to be an issue.

Talk about vulnerabilities with internal/campus VoIP deployments While vulnerabilities indeed exist, the threat to these systems is low. Attacks require insider access, and there is no great financial incentive to attack these systems.

Enterprises are beginning to migrate to SIP trunks, but because the majority of these trunks are dedicated connections to private service provider networks, SIP-specific packet attacks over these trunks are unlikely. However, the migration to centralized SIP trunks creates a choke point, where TDoS attacks can be much more disruptive. Whereas historically these attacks might affect one site, with centralized SIP, they may "bleed over" and affect an entire enterprise.

Free IP PBX software such as Asterisk/Trixbox, call generation tools, and SIP access have greatly lowered the barrier of entry for attackers. Call generation can be set up quickly and used to generate TDoS, call pumping, harassing calls, voice SPAM and phishing. Call generation can also be used to brute-force probe IVRs for account information and IP PBXs/voice mail for vulnerable Direct Inward Services Access (DISA). This information can then be used for financial fraud and social engineering attacks. Social networking sites such as Facebook and Twitter can be used to gather information about individuals for fraud and even to organize TDoS attacks against enterprises.

The ability to spoof the calling number and make anonymous calls makes many of these attacks more effective—the attacker can imitate a real user, cover their tracks, or mutate the calling number for every call, making attacks such as TDoS more difficult to detect and mitigate.

Many types of malicious inbound calls are possible. The threat increases every day. This is true whether the enterprise is using TDM or SIP trunks. It is critical for enterprises to deploy call-level, application-level, policy-based security to detect and block these sorts of attacks.

The continued move to UC and collaboration will increase the threat of voice security breaches. Integration of video, instant messaging, social networking/media, BYOD, Internet UC, and WebRTC will introduce new vulnerabilities.

# Summary of Trends

Telephony Denial of Service (TDoS) — 2013 was the year of TDoS. The frequency and impact of attacks increased significantly. For example, the "Payday loan scam" TDoS attack involves the attacker calling a victim, usually at a hospital, public safety organization, or other enterprise with critical UC lines. The attacker would often state that the employee owed money on a "payday loan" and if they did not pay, their place of business would experience a TDoS attack. Government sources have reported almost 650 attacks since March of 2013 and this upward trend is continuing. One group responsible for the attacks collected over $4,000,000 in extortion funds. The attacks were generated with what appears to be a combination of labor pools and automated call generation.

TDoS was such a major issue this year that it was covered in the mainstream media, in many technical publications, and was mentioned in a number of bulletins from federal and local governments. A few selected links are provided below:

New York Times 1/2014
http://www.nytimes.com/2014/01/20/technology/swindlers-use-telephones-with-internets-tactics.html?ref=business&_r=0

Los Angeles Times
http://articles.latimes.com/2013/jul/18/business/la-fi-phone-hacking-20130719

Krebs on Security 4/2013
http://krebsonsecurity.com/2013/04/dhs-warns-of-tdos-extortion-attacks-on-public-emergency-networks/

DHS TDoS Warning 3/2013
http://www.securelogix.com/tdos/dhs---nccic-ncc-telephony-denial-of-service-tdosinformation-bulletin.pdf

FBI Warning on Call Pumping (TDoS)
http://voipsecurityblog.typepad.com/files/toll-free-traffic-pumping_11-7-13-.pdf

For many more links, see
www.securelogix.com and www.voipsecurityblog.com

Automated TDoS — attacks increased in frequency, call volume, and sophistication in 2013. These attacks included outright TDoS, call pumping and harassing calls, which created TDoS conditions.

Social TDoS — Facebook, Twitter and other social networking vehicles continue to be used as a means for organizing vast numbers of callers to make harassing calls to victim organizations with the express intent of shutting down operations. The attacks were motivated by a number of social issues occurring around the globe, such as the "Occupy" movements.

Financial Fraud and Social Engineering — This threat is accelerating for a variety of reasons, including the ease of gathering basic Personal Information (PI) from social networking sites, the ability to spoof the calling number, and the increased level of security for Internet-based financial transactions, which has pushed attackers to target voice contact centers, which are soft targets.

Service Theft and Call Pumping — two types of fraud that affect enterprises. Call pumping is a relatively new form of attack, where inbound calls are made to 1-800 contact centers to collect connection and per-minute charges. Toll fraud continues to be an issue, but often now involves automated calls to International Revenue Sharing Fraud (IRSF) numbers.

Harassing or Restricted Callers — a class of inbound calls, which may be manual or automated, with the intention of annoying, harassing, or threatening the victim. The ability to spoof the calling number makes these attacks more effective. Examples are bomb threats and SWATing attacks.

Robo-calling Scams, Voice Phishing, and Spam — the same automatic call generation methods make "robocall" call generation easier. More than 80% of these callers were attributable to telemarketing, debt collection, credit rating, and auto warranty scams. The number of robocalls received by our enterprise customers continues to increase, with an average increase of 4% over the past two years. We maintain a managed blacklist built from a variety of sources, and are seeing 4-5% of inbound calls match this list.

Modem/ISP Calls and Fax Abuse — We have discovered modem traffic at every customer facility we have assessed or monitored; no enterprise has been modem free. We have detected calls to ISPs at more than 91% of all of our customers. While the average number of ISP calls in our measured 10-year averages has decreased, the 3-year averages have been trending up slightly and now both averages are approximately the same. Like modem duration, the total ISP call duration has decreased by approximately 50% compared to the 10 year average. Since legacy business use of ISP and employee personal use have declined, what is left is a static population of users who are connecting to ISPs for illegitimate purposes.

In summary, perpetrators of UC attacks and fraud have not varied the end targets with the advent of VoIP. However, features provided by VoIP technologies and Social Networking tools have increased the ease with which a single attack or a coordinated attack campaign can be carried out. Although discussion abounds in the industry about Private SIP and Carrier SIP Attacks, we have not seen evidence that such attacks are widespread or significant; instead, traditional voice-application vulnerabilities unrelated to the transport medium continue to be the primary threat vector.

Encouragingly, best practices are available in the industry to mitigate UC network threats, and technologies are available to lessen the impact of or entirely stop most exploits. Only a limited number of companies are performing R&D in this field, but they continue to innovate in order to offer solutions to all of the threats discussed in this report.

# Threats Overview

UC network security has been an issue for years for enterprises, with voice application threats such as toll fraud, financial fraud/social engineering, harassing calls, and modem abuse posing the largest threats. However, with the proliferation of UC in both the service provider and enterprise networks, the threat to UC networks has dramatically increased.

This is not because UC itself is being attacked through packet vulnerabilities, but rather that UC creates many new vectors of attack and makes the overall UC network more vulnerable and hostile. Attackers do not target UC per se; they leverage UC to perform the same voice-application attacks they have been perpetrating for years. Even the Public Switched Telephone Network (PSTN), which used to be primarily a closed network, has become much more hostile due to the proliferation of UC call origination, causing it to increasingly experience the security threats common to the Internet. The PSTN used to be the most trusted communications medium, but has now become one of the least trusted networks.

The primary way in which VoIP is changing the threat to enterprise UC networks lies in the increasingly simple and inexpensive ability for attackers to originate Session Initiation Protocol (SIP) calls into the Public Voice Network. The diagram illustrates this point.

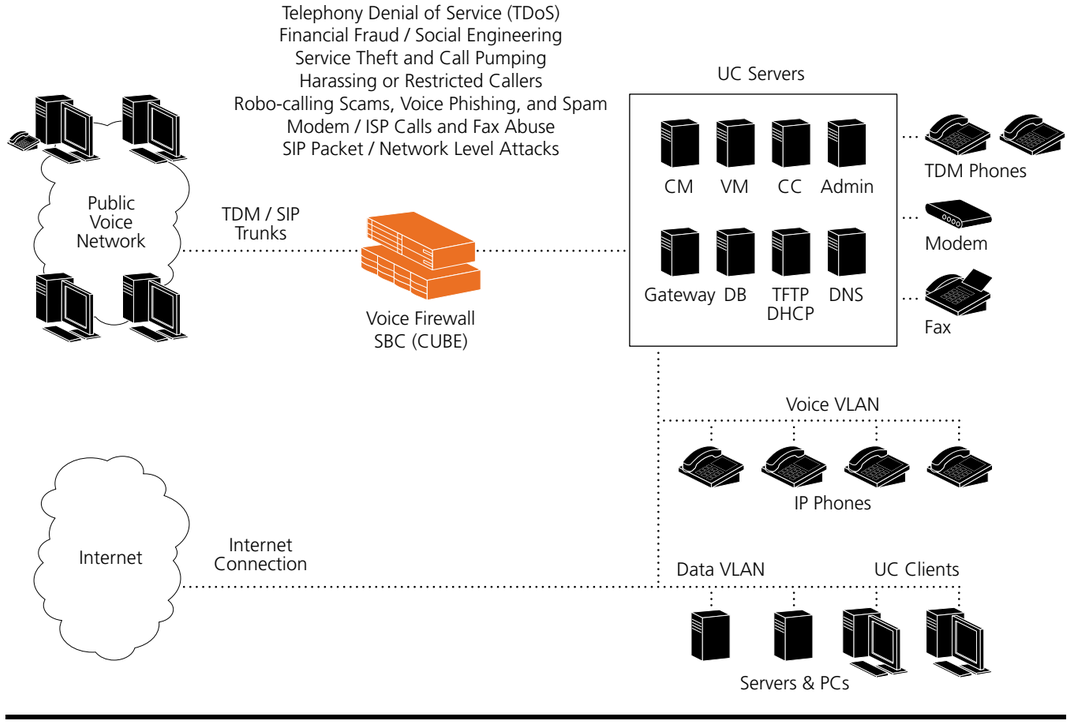
As the Public Voice Network continues to migrate to UC, with SIP being the dominant protocol, it has become easy and inexpensive to originate large numbers of concurrent calls (or floods) into this network. While the trunking entry point into enterprises remains primarily TDM, the call origination point is often SIP. On the origination side, the Public Voice Network looks more like the Internet every day from a call generation and threat point of view. This change is accelerating and is out of the control of the enterprise. Service providers are in the business of delivering calls and are neither incented nor equipped to address attacks based on call floods. These automatically generated calls are often referred to as "robocalls." This transition represents the most significant threat to enterprise networks.

SIP trunks, consumer/cable SIP offerings, Internet-based SIP services, softphones, and smart phones all combine to make call origination with spoofed/anonymous calling numbers easy and commonplace. It is simple to use free software, such as the Asterisk IP PBX, sipp call generator, and other freeware tools, to automatically generate robocalls. A call generation capability can be set up in a matter of hours or days to enable TDoS, financial fraud/social engineering, call pumping, harassing calls, voice SPAM and phishing. These tools make it possible to generate hundreds or even thousands of concurrent calls. A UC-aware botnet can fire up and generate tens of thousands of simultaneous calls, and the threat increases with each passing day. Commercial services to generate robocalls are even available.

Internal/Campus UC systems are complex and involve many servers and components. The major IP PBX and VoIP vendors are progressively doing a better job of securing these systems, including improving default configurations and offering security features, such as encryption. However, security is often not the primary consideration during deployment of new UC network systems, and quite a few vulnerabilities exist. This is especially true for highly critical voice applications, such as contact centers, and for critical devices such as call control, media gateway, and support servers.

An attacker with internal network access and the right motivation and tools can attack these devices. However, if an attacker has internal access to a corporate network, there are broader security issues other than just UC security. The good news is that other than disruption and selected eavesdropping scenarios, no significant financial incentive exists to exploit these internal vulnerabilities. Virtually no publicized, real-world attacks have occurred on internal/campus VoIP networks.

## Public Voice Network








SIP is a standards-based protocol for controlling voice calls. SIP can be used for internal handset communications, but its security issues are similar to those for other handset protocols. SIP is also commonly used for enterprise SIP trunks, which are a means to connect enterprise voice networks to the Public Voice Network. Many enterprises are transitioning to SIP trunks. Enterprises use SIP trunks both for one-to-one replacement of TDM trunks and to consolidate the traffic from smaller branch or retail sites to a centralized trunk model. Centralized SIP trunk deployments offer a number of advantages, but also increase the threat of certain types of attacks, such as TDoS, since all or most of an enterprise's public access is now consolidated through one or a few sites.

The vast majority of enterprise SIP trunk deployments are provisioned by large service providers who provide a private SIP connection between their networks and the enterprise. This is a separate, managed, private connection, where security and Quality of Service (QoS) can be assured, as opposed to the Internet, where they cannot. While it is technically possible for SIP-specific packet attacks to be seen on these private SIP trunks, such attacks are unlikely. Also, SIP trunks primarily use SIP for signaling and RTP for audio, as opposed to the complexity of the multitude of protocols used on an internal/campus VoIP network.

If an enterprise uses SIP over the Internet, the threats rise considerably. While uncommon now, such access may occur more often as enterprises seek to enhance the rich communications experience they enjoy inside their networks with Instant Messaging (IM), presence, and other Unified Communications and Collaboration applications that may not be available with dedicated Service provider SIP trunks. In fact, we have seen several SIP-based Internet video systems exploited, but the motivation for these exploits was toll fraud, rather than the video application itself.

But while SIP-specific attacks represent a low threat, UC application-level attacks/threats such as TDoS, financial fraud/social engineering, call pumping and toll fraud, harassing calls, and voice SPAM/voice phishing are still prevalent. None of these threats decrease with the transition to SIP trunks.

Hosted IP is a UC deployment where the service provider hosts the IP PBX and other UC application servers. The enterprise simply deploys IP phones or softphones. This deployment offers the classic advantages and disadvantages over an enterprise-deployed IP PBX. However, unlike classic Centrex, Hosted IP can be delivered, expanded, and reduced much more quickly and cost effectively.

From a security standpoint, Hosted IP offers some advantages over an enterprise IP-PBX, removing the concerns with securing the complex IP PBX, its devices, services, and supporting applications. However, the enterprise should still be concerned about threats such as eavesdropping and possibly malware delivered to softphones from the service provider. The enterprise also has many connections open to the service provider that should be secured, especially if the Internet is used to deliver the Hosted IP service.

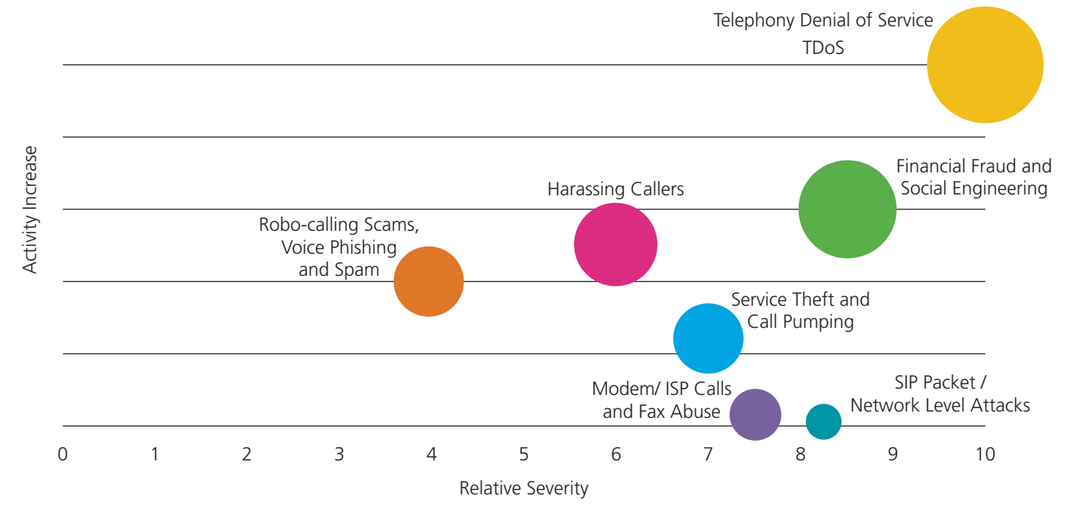
More importantly, the enterprise is still as vulnerable to inbound voice application attacks, such as toll fraud, social engineering, harassing calls, and TDoS, as before but now depends upon the service provider to address these threats.

# Threat Taxonomy

SecureLogix proposes a simplified UC threat taxonomy that is prioritized based on the real-world threat to enterprises. Other useful threat taxonomies exist, such as that provided by the Voice Over IP Security Alliance (VoIPSA) (www.voipsa.org), but they are more complex and heavily weighted towards VoIP-specific, data-oriented attacks. These taxonomies and vulnerabilities are certainly relevant, but do not represent the highest priority threats to enterprises. SecureLogix has developed a Threat-Risk Trending model to provide an all-at-once visual summary of the voice security risk environments enterprises face. It represents recent relative trending (last 6-12 months from MSSV customers and recent assessments) and illustrates the relative severity of well known and new-risks areas. The following diagram illustrates the primary threats to enterprise voice networks.

The chart shows the primary UC threats to enterprises. Each threat is represented by a "bubble", the size of which is a measure of the impact to the enterprise, coupled with the difficulty of detection and mitigation. This chart is based on real-world data assembled from hundreds of SecureLogix assessments and managed service efforts. More information on this chart is provided later in this report. The Threat-Risk Trend graphs a subset of an index of leading indicators derived from a Six-Sigma Failure Modes and Effects Criticality methodology. Briefly, the chart is read as follows:

## Voice Security Threat-Risk Trending 2013




The vertical axis is a relative measure of the increase in activity we have observed. Items low on this scale may have plenty of activity but little or no increase over the last 6-12 months.

The horizontal axis is the relative severity posed by each threat.

The size of each bubble combines several metrics, but primarily reflects the difficulty of detection. This means a larger bubble indicates a difficult threat to detect, possibly due to the novelty of the threat, or that the threat is rapidly changing, meaning that constant attention must be paid to tracking the threat.

Threats up and to the right are trending upwards in growth and are more severe risks. They tend to be new and tend not to be mitigated by an established best practice. Enterprises probably do not know whether they have been impacted by this threat and need to change their practices and technology to detect and mitigate these attacks and vulnerabilities.

Threats to the lower left are neither increasing nor declining. These may either be sporadic events or continuous commonplace threats, much like port scanning as a constant threat in the data world. Operationally, enterprises need to stay on top of these threats as part of best practices or attackers will note the vulnerability and exploit a lack of vigilance.

Threats in the middle of the graph are typically either of high severity or high growth or a mix of each. These threats are the most worrisome from an enterprise perspective because they are becoming widespread, are severe, and are probably on the more innovative edge of enterprise best practices. They are, however, mature enough that technology does exist to effectively measure and mitigate the risk posed.

# Taxonomy and Overall State

## Telephony Denial of Service (TDoS)

Very strong growth and high severity. TDoS is increasingly common among smaller enterprises, with limited, high criticality contact center lines because they are easy to flood and attractive targets for extortion. TDoS itself, as well as call pumping and harassing calls, which can create TDoS conditions, is becoming much more common in large contact centers as well. TDoS can be generated through cheap labor pools of callers. It can also be generated by organizing callers through social networking sites, such as Facebook and Twitter. However, most TDoS is generated with automation. This provides much more control, volume, and the ability to generate a persistent attack. These attacks can vary in sophistication and volume, by combining multiple SIP origination points. TDoS is detectable via cutting-edge technology that has limited availability. TDoS is a threat which can be detected and mitigated with real-time detection technologies and voice-intrusion prevention.

## Financial Fraud and Social Engineering

This is not a new issue, but becoming a bigger and bigger problem. We are seeing more and more companies become victims of attempts at various types of voice fraud via Social Engineering schemes, especially as transactions over the phone with contact centers have become commonplace. Detection activity must be continuous, not a one-time exercise; attackers constantly change methods and numbers. This is high severity due to financial and brand-reputation loss.

## Service Theft and Call Pumping

A combination of a new issue and old issue which still plagues enterprises. Call pumping schemes are on the rise, due to the ease of automatically generating inbound calls to 1-800 numbers. Toll fraud remains an issue, which has become more acute due to IRSF schemes, where the attacker uses automation to generate inbound or internal calls that terminate to IRSF numbers. Wangiri attacks causing people to inadvertently call premium-rate toll numbers are a common practice. Incidents are regularly reported in the media. Call pumping can be a challenge to detect and mitigate, depending on the sophistication of the attacker. Toll fraud is relatively easily quantified and mitigated in real time.

## Harassing or Restricted Callers

Increased as an issue in 2013. Harassing calls, which intend to annoy targeted users, continue to be an issue. Threatening and dangerous calls such as bomb threats and SWATing calls have become more of an issue due to the ability to spoof the calling number and make anonymous calls.

## Robo-calling Scams, Voice Phishing, and Spam

Continued large upswing in 2013. While often considered a consumer issue, these calls are being received more and more by enterprises. These calls may occur in large burst calling campaigns, wasting user time, bandwidth, and possibly even creating TDoS-like conditions.

Voice SPAM, Phishing, and Robocalls are dominated by collection agencies and businesses, more eager than ever to sign up new customers, relying on mass phoning as the cheapest way to reach new customers/prospects. Calling campaigns affect employee productivity and cause circuit congestion. Continuous vigilance is required to maintain accurate blocking lists.

## Modem/ISP Calls and Fax Abuse

Reduction in modem call duration over the last 10 years. ISP calling rates static over 3-year averaging window. ISP and Modem Calls are a persistent trend where people continue to completely bypass a company data security policy by calling ISPs directly from within the enterprise network. Risk posed equals turning off all network-based data security devices. Modems are still in wide use, though fewer than 10 years ago. They are typically found in IT management, SCADA, telemetry and logistics operations where IP technologies are not yet deployed.

## SIP Packet/Network Level Attacks

While this is spoken about in security forums and publications, it is not a phenomenon we have observed, nor is it an issue affecting enterprises.

TDoS activity was so prevalent in 2013 that it became a topic addressed in national media.

## Summary of What Changed in 2013

TDoS activity was so prevalent in 2013 that it became a topic addressed in national media such as the New York Times and the Los Angeles Times. The DHS, FBI, and public safety organizations have produced numerous bulletins warning of the issues. The reason for this was the widespread use of TDoS as a tool for extortion of everyday people while at work. The result was that enterprises became inadvertent victims of this criminal activity, as their UC services were subject to crippling TDoS attacks.

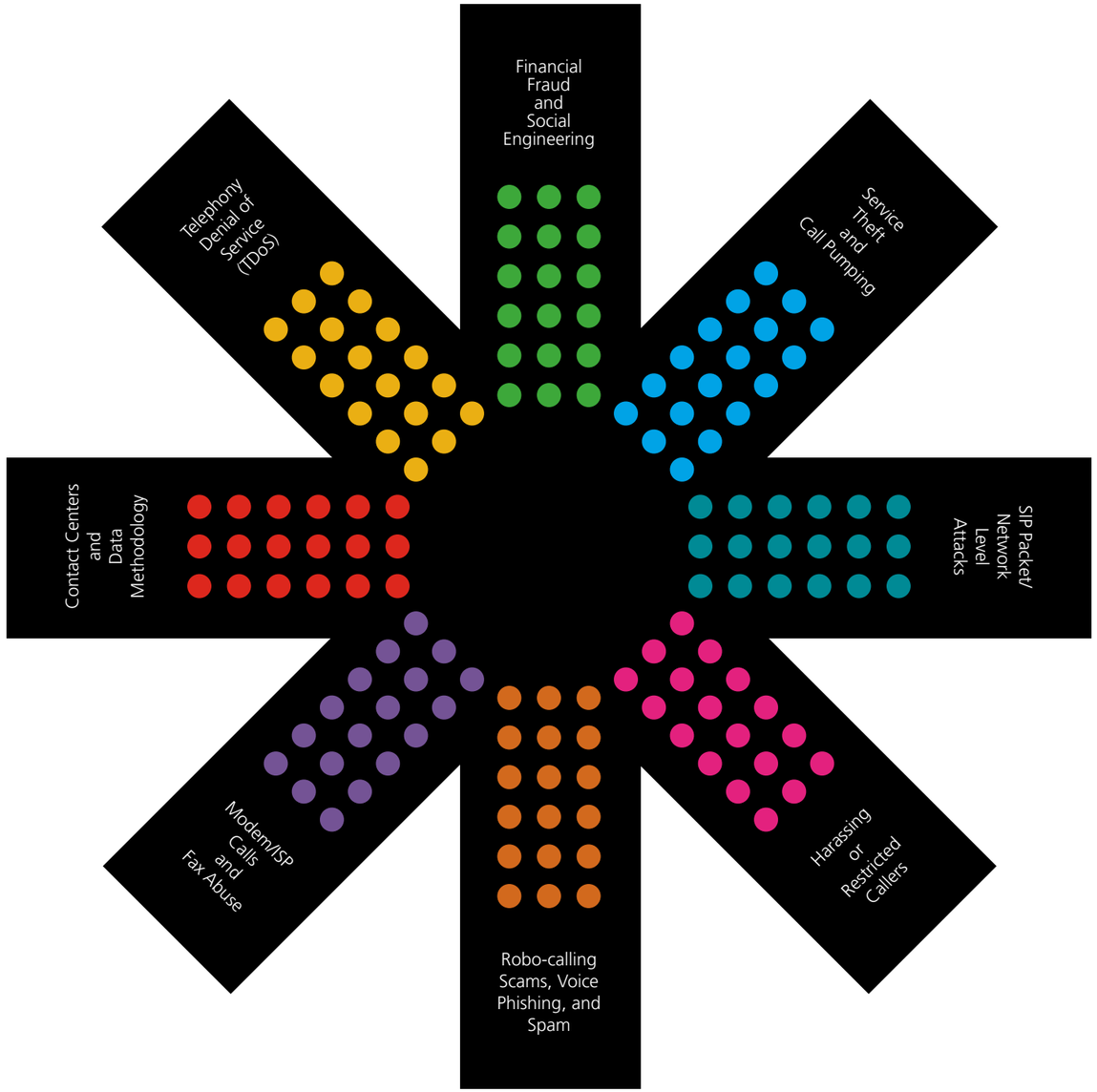
Fraud and Social Engineering attempts increased substantially, and we continued to see this activity targeted at Contact Centers. Motives include financial gain or personal information phishing. We have seen telephone-based Social Engineering incidents involving calls coordinated across several countries. Establishing and following best practices for authenticating callers, as well as having proper voice policy, alerts and analytics are effective measures to combat this.

Robocalling for voice SPAM and phishing is also a threat, which increased to such an extent, in 2013 the FCC issued new legislation to try and control it. The FTC has begun aggressively pursuing litigation and fines against robocallers. The current economic climate is creating more demand for collection agents and credit/debt services. Telemarketers continue to benefit from lower per/call costs and automation to increase their reach. Detection and blocking of these callers requires continued vigilance, but is straightforward with the right technology.

Modem usage and ISP calling is declining but is by no means extinct. We still find modems and ISP calling in our assessments. ISP call attempts are flat over 3 years, while duration of completed calls is dropping. We are continuing to monitor usage of this back-door data leakage vulnerability, as we do not expect it to disappear.

# Detailed Threat Analysis & Data

We now present detailed information for each threat covered above. We first cover why many of these threats are such an issue for contact centers. We also cover our methodology for gathering data. We follow this introductory material with detailed information about each threat.



# Focus on a High-Value Target: Contact Centers

Contact Centers represent a critical transaction-processing function for businesses of all sizes. Contact center infrastructure is costly to deploy and operate, with the fully loaded operating cost per answered call in the $5-10 range for a North American or European insourced facility. Because of this cost, it is important that only the highest-value calls be answered by a person, and that staffing levels be sufficient to accommodate the high-value caller volume.

So how does UC security figure into contact centers? Contact center operations managers have told us that, in general, calls to contact centers can be categorized by form of double 80-20 rule: 80% of the calls generate 20% of the transaction revenue/value and 20% of incoming calls generate 80% of revenue/value.

According to this double 80-20 rule, contact center operators categorize calls as high-value or low-value. Automated technologies like IVRs are used to service low-value calls, thereby allowing high-value calls to be addressed by as few human agents as possible.

However, two other categories of calls come into contact centers daily for which no industry-wide names exist; we refer to these as: “No-Value” and “Negative-Value” calls

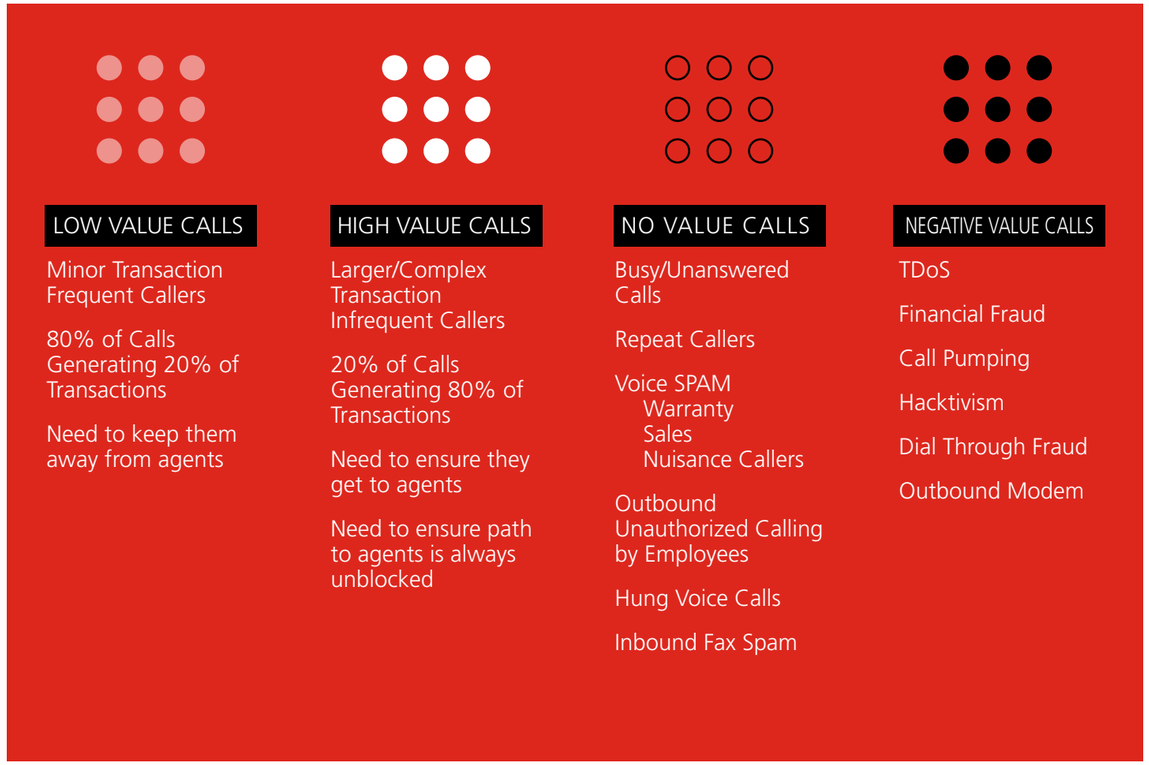
No-value calls are calls to the contact center in which the individual (or device) making the calls have no intent to engage in any form of legitimate transaction with the company. The calls are made for a variety of reasons, such as harassment, telemarketing, and so forth. These calls serve to intentionally or inadvertently consume contact center resources, which is felt most acutely at peak calling times.

Negative-value calls are a more malicious type of call than no-value calls. These calls are specifically aimed at disruption or stealing money from the business or its customers via TDoS, financial fraud/social engineering, call pumping, and toll fraud.

No-value calls tend to be a constant, continuous presence, while negative-value calls tend to come in organized campaigns or in spurts of activity around a specific financial fraud opportunity. Reducing these categories of calls with an effective UC security policy can protect the most desirable and valuable high-value transaction traffic.

People seeking to harm an organization have come to understand that attacking contact centers, and more specifically, occupying the scarcest resource-- the agents--is a highly effective way to stop high value business transactions through fully legal telephone calling.

Throughout this year’s report, we emphasize where particular case studies or threats are of particular concern to contact centers.



# Data Sources, Methodology, and Analysis

For more than 15 years, SecureLogix has monitored the latest trends in UC application threats, attacks, and vulnerabilities, and has delivered unique security solutions to protect customers from these activities and weaknesses. In addition to its research efforts, SecureLogix has accumulated real-world metrics and insight into enterprise voice application issues from the following sources:

- One-time assessments of customer networks using real-time attack monitoring tools.
- Technical support in use of SecureLogix® solutions to mitigate threats and attacks.
- Continuous Managed Security Services for Voice (MSSV) engagements.

UC network assessments provide valuable, raw snapshots of the state of UC security, performance, and usage management across a base of enterprise users. While these assessments typically evaluate only part of a customer's network for an average length of about 60 days, they are carefully designed in consultation with customers to capture a representative sample of overall enterprise traffic.

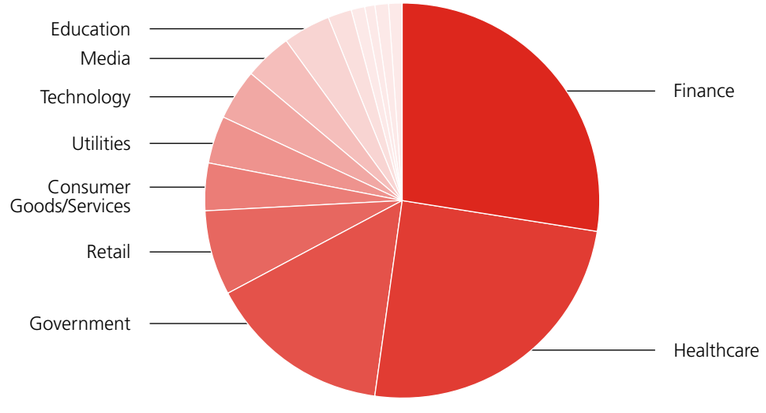
Our data is scientifically collected via our patented ETM® Solution, which sits inline on customer trunks to analyze multiple attributes in the signaling and media of each call, along with call patterns.

The methodology used for this report is to normalize all data into a per span-year value, wherein a span represents a connection with a capacity of 24 to 31 concurrent calls over various circuit types, including SIP trunks and legacy TDM trunks (T1 PRI or CAS, E1 PRI or CAS, SS7 and analog).

For macro-level trending analysis, we have chosen to calculate averages over both a long-term, ten-year dataset and a short-term, most recent three-year dataset.

SecureLogix assessment data comes from a diverse set of vertical segments, as illustrated in the graphic.

## Assets by Vertical 2001-2013



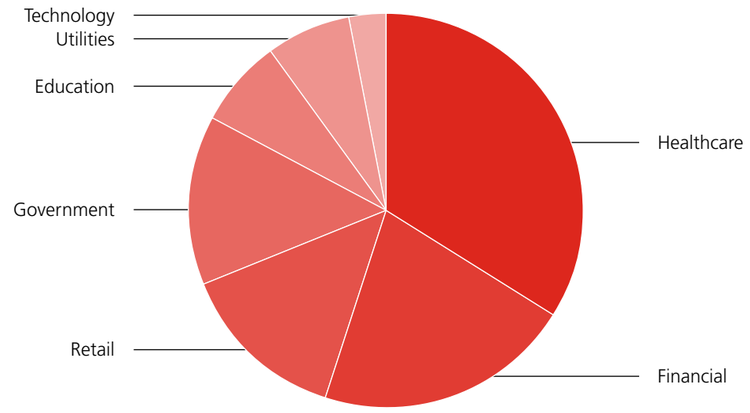





Our unique visibility into real-time traffic across our entire MSSV customer base allows us to see and protect against specific attackers as they attempt to infiltrate multiple customers, whether simultaneously or serially. Data derived from SecureLogix MSSV customers provides a continuous view into their UC security and performance environment, affording us the unique opportunity to track security threats as they start, mature, mutate, and eventually are replaced with new attacks.

The vertical segment distribution of our MSSV customers is shown below. We currently have visibility into several thousand TDM and SIP spans across our MSSV customer pool.

## Managed Customers by Vertical 2001-2013




The SecureLogix MSSV service has been in operation for more than six years. The data derived from our overall MSSV customer base is particularly useful for near-term trending analysis.

SecureLogix actively pushes attack-mitigating security policies, adds signatures to our detection databases, and makes performance improvement recommendations on a continual basis. These changes affect collected MSSV data over time. That is, in many instances, attackers stop attacking, fraudsters cease attempting long-distance fraud, and ISP users realize their calls are blocked and stop dialing. We are aware of this effect and are careful about how we present data in this report collected in such circumstances. Nevertheless, we present MSSV data in numerous places throughout this report, typically as real-life customer examples, and we do highlight where a policy has been applied that is causing an observable change in the data. In some cases, we show that a policy simultaneously protects the customer from an attack while allowing us to retain visibility into attempts to continue attacks.

# Telephony Denial of Service (TDoS)



## Telephony Denial of Service (TDoS)

TDoS attacks follow the same model as the more traditional data network denial of service—an attacker floods the target with too many access requests and prevent legitimate users from accessing the system. With TDoS, the objective is to make a significant number of calls and to keep those calls up for as long as possible, to overwhelm all or a portion of the enterprise. This could be trunk circuits, an IVR, specific phone numbers, agents, or some other choke point.

The impact to an organization where attackers tie up every available voice session can be a catastrophic loss of the ability to conduct business at even the most basic level; the subsequent loss of service, business, and revenue can be devastating.

TDoS is often thought of as an overwhelming number of calls that completely saturate a target. While this is possible, a TDoS condition can also occur even with an attack that only includes a few simultaneous calls. The "payday loan scam" TDoS attack is a good example. The attacker isn't overwhelming the entire site or enterprise, simply a few critical numbers and phone lines into an Emergency Room (ER), Intensive Care Unit (ICU), public safety point, or other critical resource.

## Automated TDoS

As we have discussed in this report, there are multiple forms of TDoS. The most significant is where the attacker is using automation, IP PBX, SIP trunks, and call generators to create the calls. There are also turnkey TDoS tools available that can be used to do this: see http://www.webroot.com/blog/2014/01/16/new-tdos-market-segment-entrant-introduces-96-sim-cards-compatible-custom-gsm-module-positions-market-disruptor/ for more information. These systems have a GSM module, with 100 non-attributable SIM cards, allowing them to completely anonymously generate moderate scale TDoS attacks. For more information on this tool, see http://www.webroot.com/blog/2014/01/16/new-tdos-market-segment-entrant-introduces-96-sim-cards-compatible-custom-gsm-module-positions-market-disruptor/

SIP-based automated TDoS, while not quite as turn-key, offers more control and the potential for a greater number of concurrent calls. To execute a SIP-based automated TDoS, the attacker will perform the following simple steps:

- Select the phone numbers that are to be targeted. Since the numbers are generally public facing (often 1-800 numbers), they are very easy to source from the target's website. For a large contact center, it is also possible to locate some portion of the contact center, which has limited resources and/or is a choke point.
- Install and configure the Asterisk or other open source/free PBX software. These systems require nothing more than a capable Linux server. There are many resources on the Internet which describe how to set them up.

- Set up a call generator, which uses the underlying Asterisk software to make the calls. During this process, the attacker can chose to spoof the calling number, decide what audio to play, etc.
- Execute the attack, during the time when it will be the most effective. This may be during the busiest part of the year (think tax season, any holiday, peak shopping time, etc) and/or the busiest time of the day.

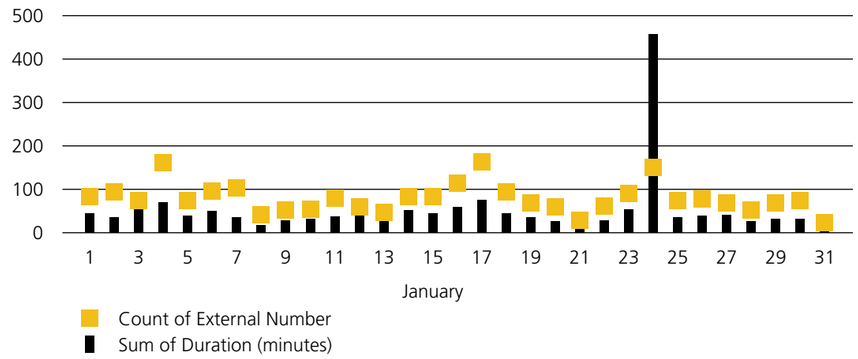
TDoS attacks can use simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns, which attempt to cause calls to dwell in IVRs. These are simple techniques, with future attacks likely using other types of mutating audio.

TDoS attacks are sometimes difficult to detect because the attacker may change the calling number frequently. This makes it very difficult even for service providers to detect the attacks. Unless these attacks can be quickly traced back to an originating carrier that typically does not generate many calls to the contact center, they are very difficult to differentiate from legitimate calls. The attacks also typically move through multiple service providers, making them time consuming to trace back to the source. Since the service providers are not allowed to examine the audio, they are forced to look for attacks based the limited information they do have available.

While not an attack per se, it has also become very easy to make anonymous calls or calls with a spoofed calling number. This has become easy with popular UC applications such as Skype, spoofing services such as Spoofcard, applications on certain smart phones, and of course, free IP PBXs such as Asterisk. This ability makes all of the inbound call attacks covered in this document even more effective and dangerous.

We have discussed the "Payday loan scam" TDoS attack. We have seen this attack at several of our managed service customers. The following diagram shows an automated attack and the impact it had on a hospital ICU contact center.

Inbound Calls to ICU

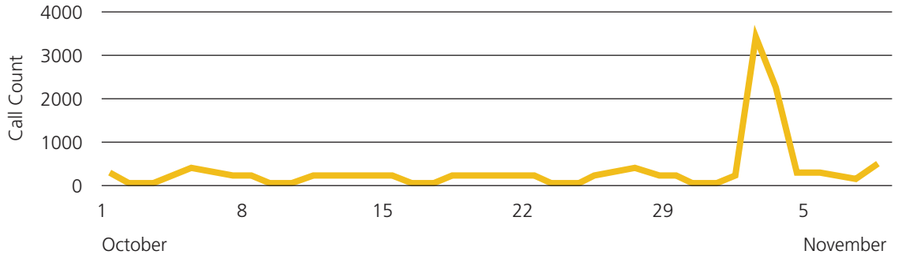



In the example above, a nurse working in the Intensive Care Unit (ICU) of a major metropolitan hospital was the target of the publicized payday loan repayment extortion scam. The nurse was informed by the perpetrators that they had acquired a list of people who had taken payday loans (and who were presumably financially vulnerable) and were threatening to disrupt her place of employment and get attention focused on her as the "cause" of the disruption. The intent was to make her fear for her job. They then requested payment of a modest sum of money to leave her alone.

The nurse refused payment and consequently the perpetrators initiated an automated TDoS attack against her telephone number. The attack caused a huge spike of over 450 calls in a single day. Unfortunately, the nurse worked in the ICU where call capacity was limited; they typically receive 30-50 calls per day. The call volume severely disrupted operations within that critical section of the hospital, causing the hospital's telecom team to temporarily take the ICU number out of service until they understood the nature of the problem. Analysis determined that the calls were the result of just three discrete harassing callers making repeated calls into the ICU. Once we were engaged by this enterprise, the harassing caller's numbers were added to a their voice firewall policy and calling levels and work in the ICU returned to normal.

Also shown is another real-world example. In this instance, it was noticed that a customer was receiving an abnormal number of calls, which generated multiple simultaneous matches against our TDoS rule set. The rule set was designed to detect high call volume with matching audio signatures. The call pattern of these suspicious calls can be seen in the graph. The spike indicates the combination of high call volume and matching calls against the TDoS rule set.

Call Count




Our audio analytics software indicated that all of the calls were from an identical source recording—the attacker played an identical audio recording on each call to keep the calls up.

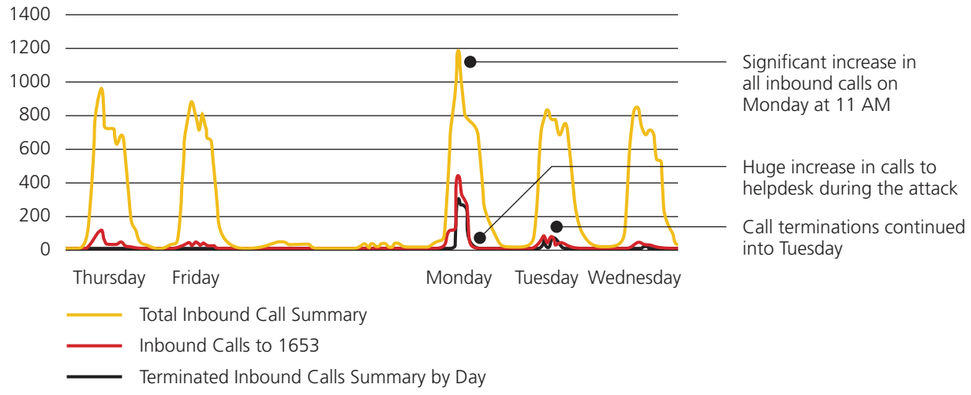
# Social TDoS

Social networking technologies such as Facebook and Twitter are increasingly used to coordinate vast numbers of people to take particular actions, usually as protest movements and in some instances riots. We continue to see events being organized to specifically disable enterprise UC systems.

Examples are rapper, The Game's request on Twitter for followers to call the Los Angeles County Sheriff's Office: more than 500,000 people received the message and created a call volume that shut down emergency services. Facebook has been used to coordinate TDoS attacks on Bond Rating Agencies relating to national credit ratings, Twitter searches show "Occupy" movements requesting followers to call banks, lobbyists, and so forth.

This method is favored for two main reasons: 1) calling an organization or individual is legal and inexpensive and 2) organizers have realized that they do not need a participation rate so massive as to overwhelm circuits (or a web server in an IP DoS case) but that they only need to overwhelm a single individual or a relatively small number of agents in a contact center. So, it is an inexpensive, legal and effective method.

Inbound Calls — 7-Day View








In this example, the attack was organized on Facebook, wherein date, time and list of numbers to which to concentrate calls was published. Instructions were given to keep agents on the phone as long as possible. The traffic chart above shows call volumes to one location for the attack day and two days on either side. Also shown are call volumes to a targeted victim number. It can be seen that the attackers managed to drastically increase overall and specific-number inbound call attempts at the called-for attack time.

The attackers called from landline, cellular and VoIP sources, and a large proportion of callers restricted their Caller ID. This meant that simple mechanisms to stop such attacks would have only been partially effective. In this instance, we deployed several proprietary call blocking methods and policies to counter the attack. The effect of these policies is also shown on the chart above as the "terminated calls" line and shows that essentially all the inbound attack calls were terminated. The net effect was that the organization would have been completely disrupted had protections not been put in place. In reality, operations were barely affected and callers soon stopped trying once they realized they had been blocked.

We have seen this attack method become very popular. In fact, there are several services now that will automate a TDoS attack of this type for an hourly or daily fee.

# Financial Fraud and Social Engineering



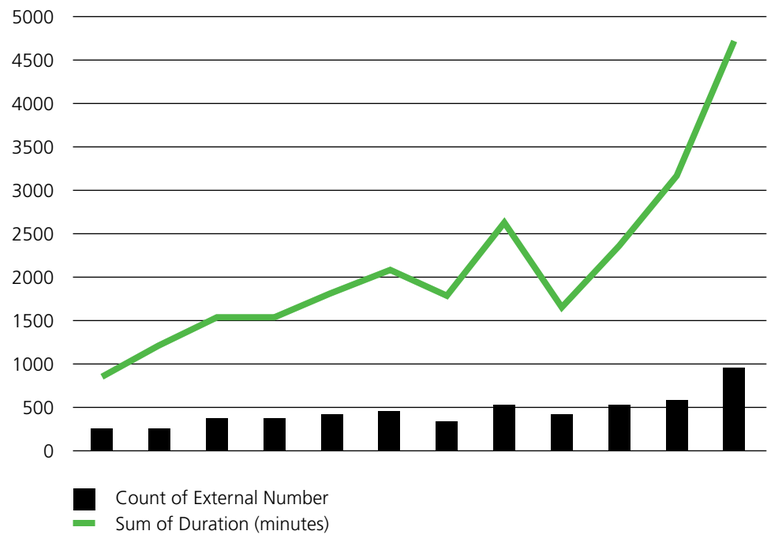
Social Engineering within the IP world is well known. However, perpetrators increasingly use the UC system to exploit people within enterprises for monetary gain. Financial services organizations are a primary target of social engineering attacks, in particular, the elements within those financial organizations that actively process payments, credit cards and other liquid financial transactions. Attackers often call with partial information, such as an account number, a customer name, or the amount of a previous bill and then attempt to talk the representative into divulging additional information that eventually allows the perpetrator to access the account and extract money. This type of attack relies on a convincing attacker and a less-than-vigilant representative. Attackers continue to be better armed for this process, as it is getting easier and easier to gather basic Personal Information (PI) from social networking.

In a recent example, a contact center for a large financial services organization had been continuously targeted by social engineers due to the type of financial transactions that it processed and the high-value accounts accessed through this contact center. An analysis of calling patterns associated with social engineering indicated that many of these suspect calls originated from a specific area code.

Analysis of calls from that area code to the call center showed an upward trend in the count of calls along with a dramatic increase in total call duration towards the end of the year, indicating the perpetrators had gained an increased level of confidence from their success, leading to more frequent and in-depth attacks.

A call recording policy was established to record all calls from that area code to this contact center. Additionally, a real-time alert was sent to the organization's security and loss prevention team each time a suspicious call was detected. This enabled them to identify social engineering attempts in early stages, thereby allowing policies to be implemented automatically directing subsequent suspect calls to specially trained agents.

## Call Count Duration



# Anatomy of a Social Engineering Call Session

For those not familiar with the extent to which a social engineer can trick a helpful contact center agent to fully and completely compromise a victim's account and perpetrate theft, we present the anatomy of what took place during a recorded Social Engineering session at one of our customer's sites.

The Social Engineers were a male-female pair who masqueraded as a married couple. They had clearly managed to get a paper copy statement for the victim's home-equity line of credit. They used the account-holder information to get Social Security Numbers. As the call proceeded they:

- Passed the authentication questions by giving address, SSN, statement balance and birth date.
- Established a set of security questions for the account for both the male and female.
- Got the most recent available funds balance.
- Discovered how to transfer funds directly out of the account, by first leading the agent with a ruse about transferring payment funds into the account.
- Got international wiring instructions for Bangkok.
- Discovered that wiring would require a call to the home phone number for verification.

During the call, a lot of background noise and many requests for information to be repeated created a very tiring and difficult environment for the contact center agent's ability to concentrate, and gave an impression that the customer needed an extra degree of helpfulness. The call length was also very long, and most of the suspicious information-gathering occurred late into the call when the agent was made most malleable.

On the second call the following day:

- Attempted to wire funds.
- Had worked with the local telephone company to have the customer's home phone forwarded to the Social Engineer's cell phone.
- Accepted the funds transfer verification call.

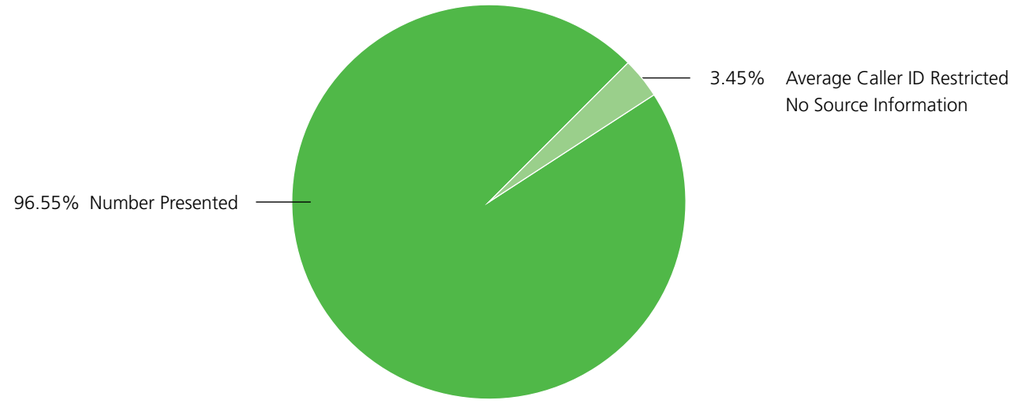
This attempt at theft was fully tracked by the financial institution and all calls that met special criteria were recorded and also transferred to specially trained contact center agents for handling based on the voice firewall policy protecting this contact center.

The recommended "best practice" to successfully identify and defend against Social Engineering attacks via voice lines is having the capability to analyze calling patterns and correlate them to known or suspected fraudulent Social Engineering activities. Once suspicious activity is detected, the ability to record and analyze those calls to determine whether they represent Social Engineering is key. Confirmed or suspected Social Engineering calls can then either be redirected to a senior agent or the Security team, or a policy can be established to block future calls from telephone numbers known to be associated with Social Engineering.

Low sophistication Social-Engineering callers can be stopped by our database of static numbers because they usually present legitimate caller ID. However, more sophisticated callers either restrict their caller ID to hide their identity or spoof their caller ID to further their efforts. We analyzed 2013 traffic to quantify the proportion of inbound calls that have no source information (caller ID restricted or carrier-stripped), and the proportion of calls that present a spoofed or suspect caller ID number.

The graph illustrates the proportion of inbound voice calls to enterprises for which no source number is presented, as measured on a cross-section of our customers. On average, 3.45% of inbound voice calls have no source information. Of these, 75% have caller ID intentionally removed by the caller and the remaining 25% have no source information from the originating carrier. We note that in our financial customers, the average is 6-7% no source, and in non-financials, the rate is 1.5-3%.

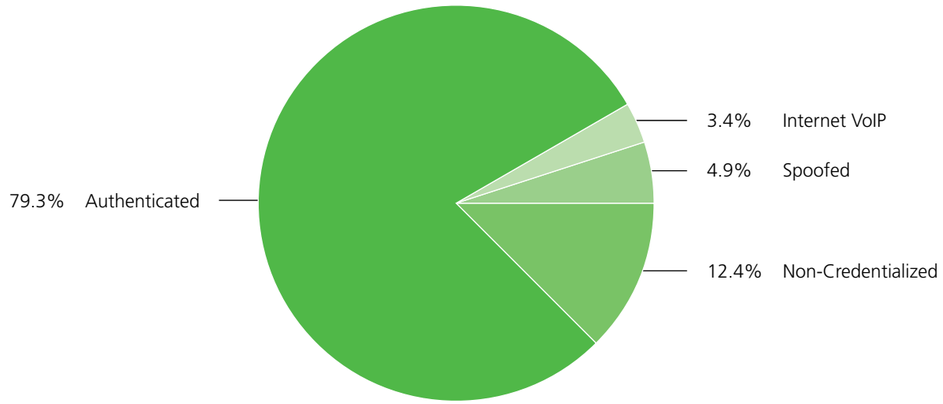
## Proportion of Calls with No Caller ID




Caller-ID restricted call volumes increase during particular types of attacks on enterprises, such as TDoS attacks, so regular monitoring for these calls can help identify the onset of such an attack and mitigate risk.

Of the remaining calls where a proper Directory Number (DN) is presented, we have worked with TrustID, a partner, to analyze the proportion of calls for which the reported DN is authentic versus spoofed or otherwise modified, as shown (the call sample size was in the millions).

## Caller Authentication




The data show that approximately 80% of the calls were authenticated to be coming from the presented DN at the time of the call and were not spoofed. The remaining 20% of calls could not be authenticated. Of the calls that could not be authenticated, 3.4% are Internet VoIP and 12.4% present a DN which is legitimate, but not authenticated because it is masked by an enterprise or is a carrier-injected source number. The remaining 4.9% of calls are spoofed.

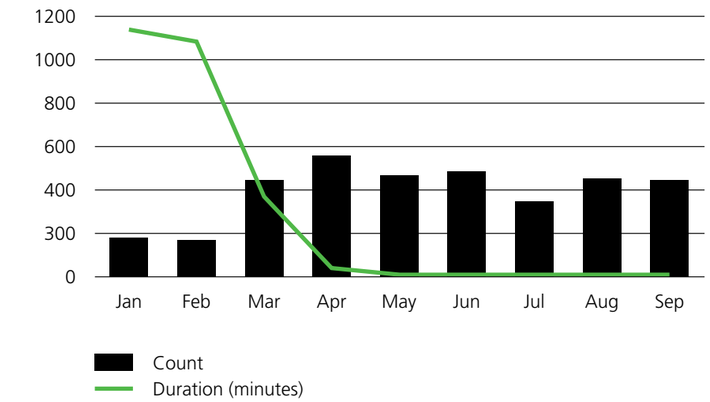
To cast this in a real-world scenario, a call center in the financial services sector receiving 300,000 calls per day would experience up to 50,000 no-source calls and 12,250 spoofed calls per day. This is why Social Engineering calls sit in a high-concern position on the Threat-Risk Model discussed earlier and why we recommend all organizations have risk-mitigation measures such as intelligent call blacklisting, caller authentication, and call blocking/redirection in place.





More troubling for organizations that are attacked, the frequency of attack remains consistent month-over-month, with attacks continuing even after a policy is implemented to terminate calls from those known Social Engineering telephone numbers. In the example below, a termination policy, driven by our Social Engineering Caller Database, was applied in February and tuned over a 2 month period. While the total duration of these calls dropped to zero (meaning all calls were blocked), the number of attempts increased and then remained consistent month-over-month. Perpetrators commonly continue to probe for weakness even though they are not currently able to exploit vulnerability.

## Customer ABC — Social Engineering Calls by Month



# Service Theft and Call Pumping



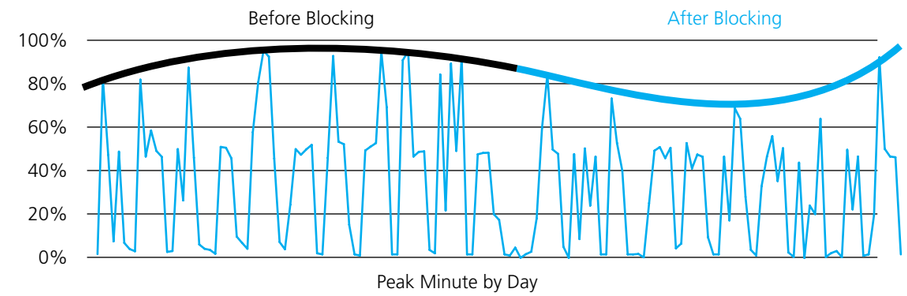
Call pumping is an inbound attack focused on 1-800 contact centers. The attacker uses automated call generation, similar to TDoS, with the intention of collecting a portion of the call connect and per-minute charges. The connect charges are generally less than 1 cent, with the per-minute charges around 1 cent. The attacker may "spray" many 1-800 numbers across many enterprises and/or focus on large contact centers and pump a moderately large number of calls into the contact center's IVR. The goal is to generate revenue, but not make so many calls that the attack is noticed. Also, the calls need to be designed to only dwell in the IVR because if they exit out (are too long), they will be noticed by the contact center agents.

Call pumping attacks can use simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns, which attempt to cause calls to dwell in the IVRs. The calling number may also be spoofed to random values, to make the calls more difficult to detect.

We have seen call pumping attacks affect many contact centers. In some cases, the attacker got "greedy" or "sloppy" and the calls affected a critical part of a large contact center, such as a set of agents who work with high-wealth customers. In this case, an unintended, but significant TDoS attack occurred.

In an example, one of our managed customers was experiencing a call pumping attack. In this instance, the victim asked us to analyze several circuits supporting an advertised contact center. The circuits showed much higher peak utilization than was anticipated or expected and they were concerned that customer traffic was being affected. The left hand side of the graph shows an example of the traffic on these circuits, and it can be seen that peak utilization regularly exceeded 90%. We determined that 4 callers were automatically generating calls which matched our call pumping profile logic, all of which were also found to be presenting spoofed caller ID information. We designed a blocking policy and implemented it on the customer lines. The right portion of the graph shows the post-policy implementation peak usage.

## Resource Utilization Before & After Blocking Policy



Thousands of calls per day were being blocked by our firewall, resulting in a noticeable reduction in peak trunk utilization, as can be seen in the graph. Overall, available circuit capacity was increased 60%. This eliminated the need for the customer to purchase extra circuits. Furthermore, as can be seen on the right-hand side of the graph, the contact center still had days where legitimate-caller peak utilization was above 80%. Without our firewall blocking in place, the additional illegitimate robo-traffic generated by the perpetrators would have resulted in an outage for legitimate customers.

Toll fraud has long been and continues to be a significant threat to enterprises. This threat is financial and can range from relatively minor abuse to full-scale Dial Through Fraud (DTF), in which losses in excess of $100,000 are not uncommon. Toll fraud is a very commonly reported real-world voice threat, as evidenced by the many publicized real-world attacks. According to the Communications Fraud Control Association (CFCA) Telecom Fraud Survey, annual global telecom fraud losses amount to an estimated $40.1 billion (USD). The 33% decrease in fraud loss since 2008 is primarily due to increased awareness and effectiveness of anti-fraud programs as a result of increased collaboration and communication between anti-fraud professionals within the industry. Toll fraud is an easy and profitable crime, both because it often goes undetected until large amounts of money are lost and because the perpetrators are hard to identify, minimizing their sense of risk. These factors increase the likelihood of such attacks.

Minor long-distance abuse occurs when enterprise users abuse unrestricted extensions, use fax lines for voice, or abuse corporate policy and use services to which they are not entitled. This abuse is relatively minor, but still costs enterprises money.

Major long-distance abuse/toll fraud occurs when an attacker obtains access to a service such as Direct Inward Services Access (DISA) and sells this access to external consumers. The CFCA (www.cfca.org) reports this type of toll fraud is responsible for 13% of all telecom fraud reported annually. Once access is found, access/passwords are sold to illicit consumers, who abuse enterprise service until the attack is detected. Attacks can go unnoticed for weeks, until the enterprise reviews CDR or receives a bill from the service provider.

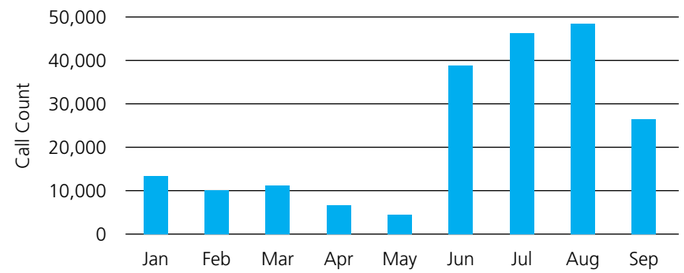
It is still very expensive to dial certain destinations and countries. In fact, some destinations are specifically established so that traffic can be intentionally generated to create revenue. An example of this type of fraud is International Revenue Sharing Fraud (IRSF), in which the attacker establishes premium rate services and phone numbers and then generates traffic from enterprises to generate revenue. New forms of toll fraud involve automatically generating inbound calls (using the same techniques we have been describing in previous sections), which exploit the same DISA issue, and then "hair pin" out to outbound calls to the IRSF numbers.

UC architectures have also made toll fraud easier to perform, because it creates additional vectors of attack into the IP PBX. A non-secured IP PBX or separate media gateway can be used to generate outbound calls. A user with the right piece of easily obtained software, such as a softphone or traffic generator, can easily generate calls. In fact, SecureLogix performed a UC security assessment where an internal attacker exploited a non-secure media gateway and an H.323 call generator to create some $250,000 of traffic over a three-week period.

Because they represent premium telephone services with associated fees that vary by destination, long distance (LD) and international (INTL) calling patterns are of interest to the enterprise from both a financial perspective and a business perspective. Enterprises need to determine whether calls to those destinations have legitimate business purposes.

Although many enterprises today have negotiated nominal and reasonable rates for LD service, it is still an area that can result in increases in costs due to changing calling patterns or theft of service, so enterprises should be ever vigilant. In the example shown, the customer had a significant increase in total LD calls in a very short time, which dramatically increased their LD costs.

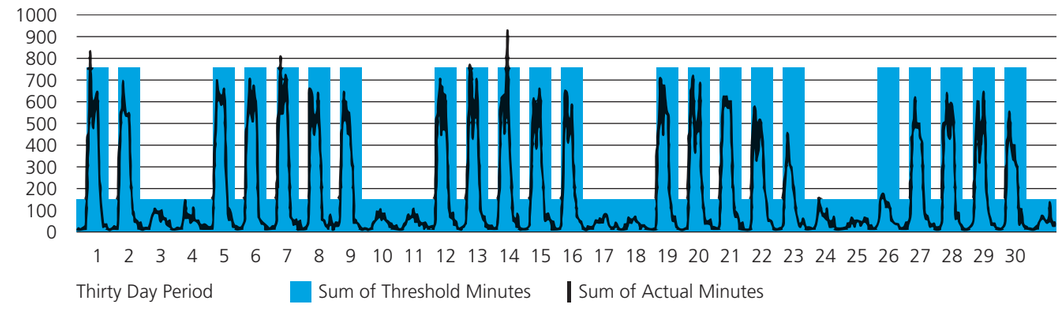
Investigated Long Distance Calling Issue




Also shown is an example of an enterprise with a very well managed long distance monitoring and alerting program, a "best-practice." Through detailed analysis, this organization was able to determine the typical variation in their long distance calling patterns. Several months of contiguous data were used to identify fluctuations in LD calling patterns brought on by any seasonality effect of this organization's business. As a result of this analysis, they were able to establish reasonable thresholds for total long distance minutes for the business day, nights, and weekends. These thresholds were entered into a our voice Intrusion Prevention System (IPS) that monitors and can alert and take corrective actions in the event that long distance calling exceeds these thresholds.

In the graph, you can see actual daily long distance minutes in red and the established thresholds in blue. Over the course of several weeks, a few brief breaches of the threshold levels occurred; however, none of these breaches lasted a significant length of time and the organization suffered virtually no additional long distance charges. In this example, the organization had their IPS system tuned to notify on first breach and take additional action if the breach was sustained.

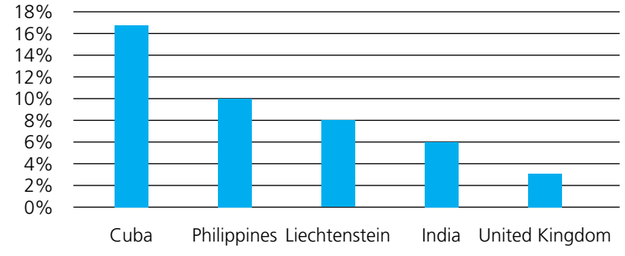
## IPS Stats — Long Distance Usage and Thresholds




Without this ability to continuously monitor and alert on long distance calling patterns, a typical enterprise would have a window of vulnerability to extended long distance fraud of around thirty (30) days or until the next invoice arrived from their provider. By intelligently monitoring, alerting, and taking action in real time, that window of vulnerability shrinks from 30+ days to mere hours.

The current best practice for combating IRSF includes blocking calls to known IRSF countries or specific telephone numbers within those countries. The current CFCA list1 of IRSF numbers contains over 61,000 discrete numbers worldwide (up over 50% from the previous year) known to have a connection to this fraudulent practice. The countries most frequently called as part of this fraud include Cuba, the Philippines, Liechtenstein, India, and the United Kingdom.

## Predominent Destination Countries for IRSF

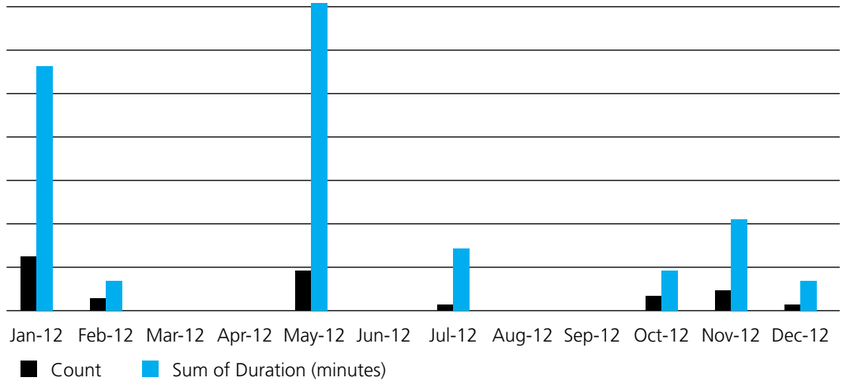



A particular concern regarding international calling for many enterprises involves calls to and from countries that have been identified by the Office of Foreign Assets Control (OFAC). The OFAC administers and enforces economic and trade sanctions against targeted foreign countries, regimes, companies and individuals with ties to terrorism, narcotics trafficking, weapons proliferation and other threats where controlling the movement of money can restrict their ability to operate. We have noted that many organizations, particularly those in the financial vertical, are interested in calls to or from countries identified by the OFAC because they cannot be associated with those types of organizations or be involved in financial transactions with them.

In a recent example, a financial organization asked SecureLogix to perform a study of calls to and from a number of countries including Nigeria, Indonesia, Albania, Philippines, and others and they were surprised when we identified nearly 100 calls made to or received from countries on that list in a short three-week period. More troubling to the organization was that the calls were not misdials: the duration of the calls was measured in hours. This particular organization chooses to be aware of and investigate these calls individually to determine whether they have a legitimate business purpose. Alternatively, they can choose to be alerted whenever one of these calls takes place or choose to block those calls outright.

In another recent example, SecureLogix was monitoring international traffic for an organization in the Utilities vertical and noted calls to countries known for toll fraud, particularly Nigeria, Ghana, and Cameroon. After being made aware of the phenomenon, the organization chose to allow and monitor the calls to see if they were an anomaly or an increasing threat.

## International Calls to Nigeria Trend




Although the quantity of calls to Nigeria decreased, continued vigilance in monitoring paid off when the calling patterns later returned. Analysis of the calls indicated that they were originating from only two extensions: an employee's line and a conference room phone. Since calls to countries like Nigeria are known to be linked to toll fraud and other types of fraud, the initial detection of calls to these countries propelled the enterprise to develop and implement a written policy regarding calls to countries known for toll fraud. They were able to analyze their calling patterns and establish thresholds for abnormal calling patterns worthy of notifications via alerts and thresholds at which to begin call terminations. This enterprise continues to monitor calls to suspicious countries and compares them regularly with their normal international calling patterns.

# Harassing or Restricted Callers



Many types of calls can be considered harassing calls, including TDoS, intentionally harassing, threatening, and then the broad class of voice SPAM and phishing calls. In general harassing calls whether intended to annoy, trick, or sell, are not a new issue but are getting much worse. UC in the Public Voice Network has made it very easy and cheap to anonymously and automatically generate any type of calls, a boon for harassing callers.

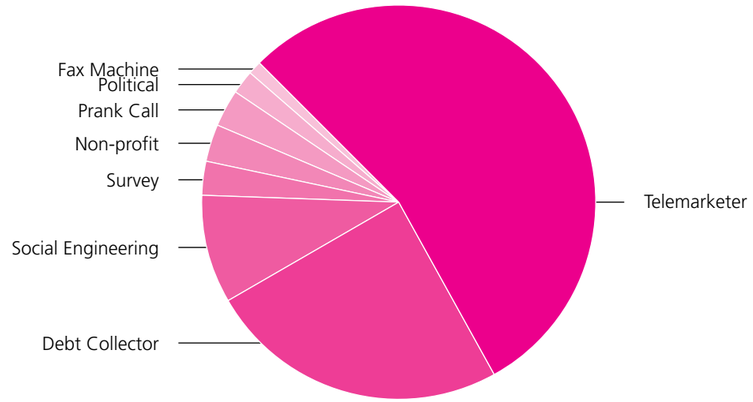
Unwanted or harassing calls continue to be a large problem for most enterprises. Harassing callers include ex-spouses, disgruntled former employees, dissatisfied customers, and businesses targeting their local market. At the national level, harassing callers are typically companies or scam perpetrators that have well-organized, persistent, high-volume campaigns. National harassing callers focused on voice SPAM and phishing favor companies with direct inward dialing and those for which they have managed to discover or deduce a large portion of the DID phone number range, making it easier to generate a large number of calls to a specific enterprise.

The use of automated call generation turns an annoying harassment campaign into one that can be overwhelming, especially when calls are intended to threaten the recipient. One example is bomb threats. Organizations and sites that interact with the public must take these threats seriously and empty retail sites and offices when a threat is made. Imagine an attack, in which 1000+ retail sites are automatically called at the same time with a bomb threat. The financial impact to the target would be overwhelming.

Another very dangerous type of harassing call is SWATing, wherein the attacker uses a spoofed calling number and then calls the authorities, claiming that there is a dangerous situation (robbery, hostage, etc.) at the target's location. The authorities scramble emergency resources and arrive at the target's facilities, expecting to deal with a volatile situation, only to discover that there is no emergency, after having caused major disruption. This normally affects individuals, but can affect enterprise sites as well.

SecureLogix maintains a carefully verified National Harassing Callers database used in our MSSV service. The breakdown of the list as of year-end 2013 is represented in the graph.

## Harassing Caller Types — 2013




The relative proportion of harassing callers by type remained largely the same as reported for 2012. Again this year, a massive increase in the number of harassing callers was reported and detected via our data collection processes, resulting in a database that is 8.6x larger than in 2011. Over the last three years, the size of our harassing callers database has increased by over 100x!

2013 was again a year where many more organizations and suspect callers turned to the phone system to try to increase end-user contact. The effect of this is shown later in the 2012 — 2013 trending analysis of harassing calls to enterprises. Because our customers use our harassing caller database for call termination, phone numbers must meet strict criteria to be included in that database.

Because most of these calls are designed for voice SPAM or phishing, we cover that separately in the next section.



SecureLogix maintains a carefully verified National Harassing Callers database used in our MSSV service.

# Robo-calling Scams, Voice Phishing, and Spam

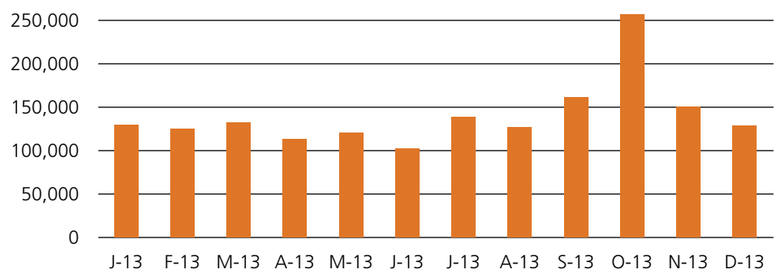


These automatically generated calls are also known as robocalls. Voice SPAM or SPAM over Internet Telephony (SPIT) also leverages VoIP-based automatic call generation for the purpose of selling some product or service. Similar techniques are used as with vishing: setting up automatic call generation, using SIP access, spoofing caller ID and the like, to quickly set up an easy and inexpensive operation. This is the voice equivalent of email SPAM. Voice SPAM is becoming increasingly prevalent and problematic for enterprises.

Independently operated public web sites that collate complaints about voice SPAM/phishing callers have reported an average of 200 new phone numbers each day, providing evidence of just how prevalent and persistent harassing callers have become. Also in 2012, the US Federal Trade Commission highlighted its desire to stop robocallers by initiating a contest to find solutions. Visit http://robocall.challenge.gov/ for details.

The primary negative impact of calls is the loss of employee productivity; the secondary impact is the tying up of telecommunications resources for non-business purposes. As an example of the growth of these callers, consider the customer sample data shown here.

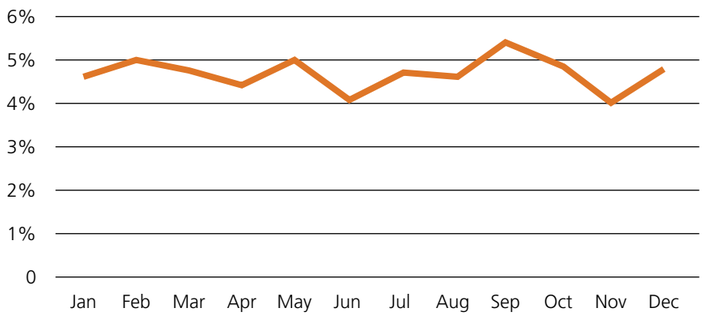
Voice SPAM/Phishing Call Attempts: Single Enterprise — 2013




This graph depicts the number of call attempts to one of our customers from phone numbers in our harassing callers database for the 2013 calendar year. The attempted harassing calls distribution seen here is indicative of what was observed in our managed service customers in 2013.

To help illustrate the magnitude of the number of harassing call attempts, we examined harassing calls as a percentage of all inbound calls to enterprises. This graph shows an example for a single customer. An average of 4.69% of all inbound calls this customer received matched our harassing callers blacklist. Across our dataset, the average number of harassing call attempts across an entire enterprise is 4.17%.

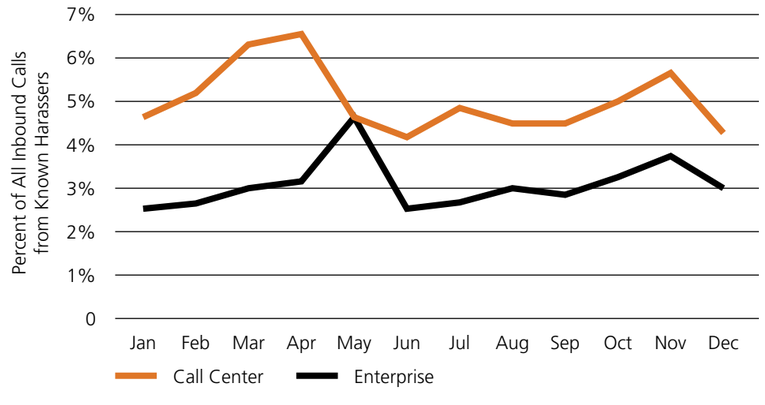
## Harassing Call Attempts as a Percent of All Inbound Calls




As noted earlier, Contact Centers are an attractive target for certain types of malicious callers, one of which is harassing callers. We have the ability to analyze known harassing caller attempts to call all numbers in an enterprise or call attempts to select numbers. Our data shows very clearly that advertised contact center numbers receive on average more harassing call attempts than the overall enterprise average.

The graph shows a single customer example that illustrates what we have observed more generally. For all but one month, the advertised "main line" for the customer saw many more harassing caller attempts as a percentage of inbound calls than the enterprise as a whole. The target number in this case was not even answered by a human; a combination of IVR and ACD system handled the incoming calls. Harassing callers navigate IVR systems to get to a human (as we illustrate in a case study below) or are simply interested in dwelling in the IVR to consume resources.

## Harassing Call Attempts to Contact Center vs All Enterprise








On average, across our dataset, our customers' contact center lines see 43% more harassing call attempts than the enterprise as a whole for these reasons:

- The numbers are easily discoverable since they are published.
- Staff are trained to be helpful and are an excellent source of information for Social Engineering attacks.
- It is easy to hide in a large IVR for certain types of revenue-share fraud attacks.
- They are a high value target for organized complaints and TDoS attacks.

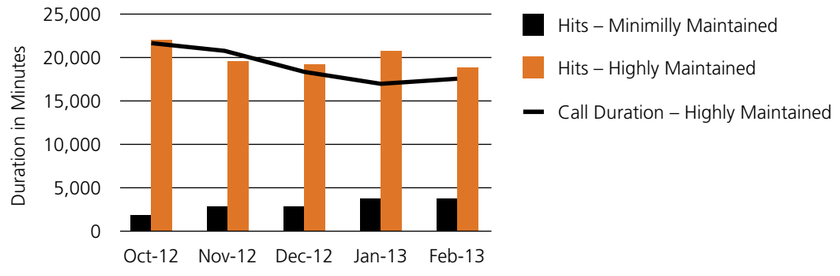
Unfortunately for the enterprise, each zero-value caller that occupies a session on a contact center number consumes a revenue or customer-satisfaction/loyalty resource that is costly to operate.

Across a sample of our dataset, 5.52% of inbound calls to contact center numbers are from known harassing callers.

Finally, we show the importance of maintaining a comprehensive harassing caller blocking list. Shown is a study depicting the number of harassing calls that were detected and blocked by an enterprise that occasionally maintained their own blocking list versus the number that would have been blocked by our managed service blocking list.

The best-effort list detected and blocked 14,920 calls in the analysis period. In the same period, SecureLogix's list would have detected in excess of 100,000 additional harassing calls. We also managed to measure that the total time employees spent talking to the unblocked harassing callers was in excess of 95,000 minutes.

## Comparison of Harassing Caller Blocking Effectiveness



# Modem / ISP Calls and Fax Abuse



## Inbound Modem Access and Outbound ISP Modem Access

Modems are still commonly used in enterprises to provide remote access to critical infrastructure systems. This access is present for vendor maintenance and/or failsafe access. Many of these modems are poorly protected—if an attacker finds these modems through a war-dialing process, he can often easily break in and access the critical system. War dialing is not a new process, but again, it has been made more efficient and inexpensive with the availability of VoIP access and VoIP-based war dialing tools such as WarVOX, which are dramatically faster than traditional war-dialing tools.

Another issue with modems is their use to dial Internet Service Providers (ISPs). Users who want to use the Internet for illicit purposes often resort to using modems and ISPs because this behavior bypasses all Internet-based firewall, IPS, and content monitoring software. This activity wastes time and bandwidth, and creates a serious, unmonitored back door into the enterprise data network.

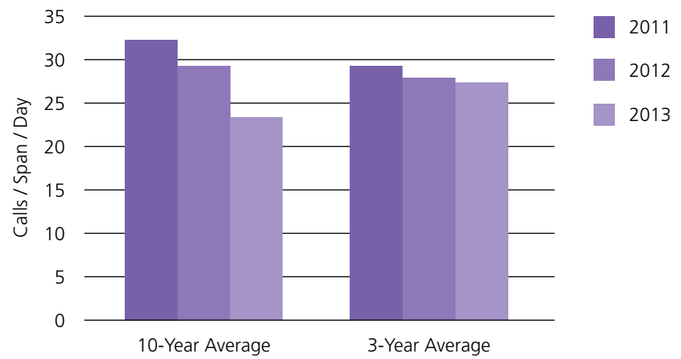
We have discovered modem traffic at every customer facility we have assessed or monitored: no enterprise is modem free. While properly secured, authorized modems are not a risk in and of themselves, illegitimate uses of unsecured or unauthorized modems present a serious risk.

Both inbound and outbound modem calls present a security risk because they involve external connections to data systems inside the enterprise via the phone line, a connection not protected by a typical firewall.

Modem use trends from our ten-year database are presented below:

- Ten-year average: 23.55calls/span/day (8,596/span/year)
- Three-year average: 27.62 calls/span/day (10,080/span/year)

### Modem Daily Calls Trend



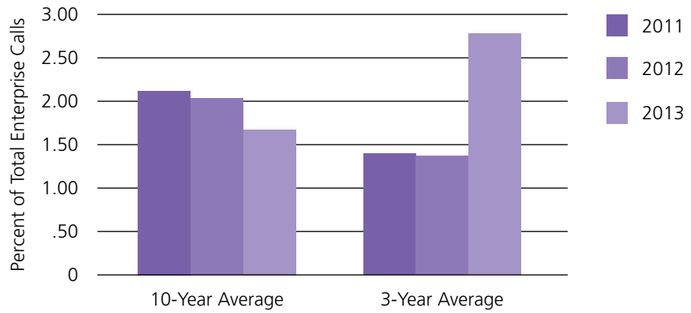
Typically, modems are used in IT departments, SCADA, telemetry and remote diagnostics and logistics applications. Many uses in these application areas have shown progression to IP or proprietary wireless, but modems are still prevalent (e.g., automated meter reading).

Modem use as a fraction of total enterprise calling:

- Ten-year average: 1.70% of all calls
- Three-year average: 2.80% of all calls

Modem calls increased slightly as an overall percentage of enterprise call traffic over a ten-year sliding scale. While modem calling was more prevalent ten years ago, a three-year sliding scale shows a flat trend, showing that modem use is still common and appears to be approaching a steady state.

## Modem Proportion of Overall Enterprise Calls




Modem Duration Trending:

- Ten-year average: 190.35 minutes/span/day
- Three-year average: 91.35 minutes/span/day

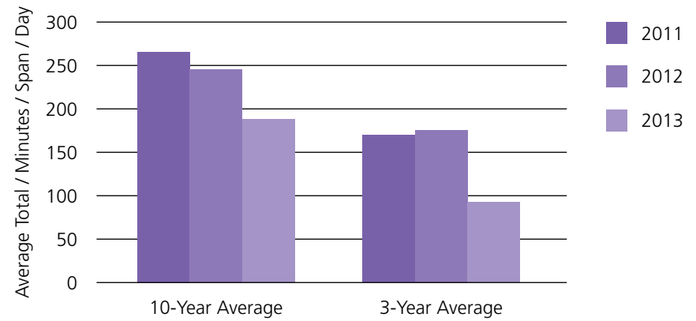
Specifically, in the last three years, modems have been found in use for an average of 1.5 hours per span/day.

These trends are most likely due to continued call generation from entrenched modem-based applications (typically short duration calls), coupled with a large reduction of relatively low call volume business-to-business data transfer and remote access (long duration calls). The ISP section below also sheds light on why modem duration is changing.





## Modem Daily Duration Trend




The three-year rolling average of modem call minutes/span/day decreased from 176.4 minutes to 91.35. The proportion of modem calls to all calls increased from 1.4% to 2.80%.

Many enterprises attempt to use war dialing to mitigate the modem threat. While this can be somewhat effective for always-on, always-connected modems set to receive inbound calls, it does not detect modems in use or modems that are turned off, and it is an insufficient means in today's world of laptops and the ad-hoc dial-out threat. Real-time, in-line detection of modem use offers complete coverage and is a mature technology.

The current best practice for modem remediation is to require all modem users with legitimate business reasons to register the source and destination numbers with the enterprises telephony firewall team. Other unregistered or unauthorized modem calls can then be simply blocked. At a minimum, the organization should maintain a list of local ISP access numbers and block them, because they are essentially unmonitored data connections.

## ISP Calling

As mentioned above, unauthorized outbound calls to ISPs represent one of the greatest threats to the integrity of an enterprise's data security perimeter.

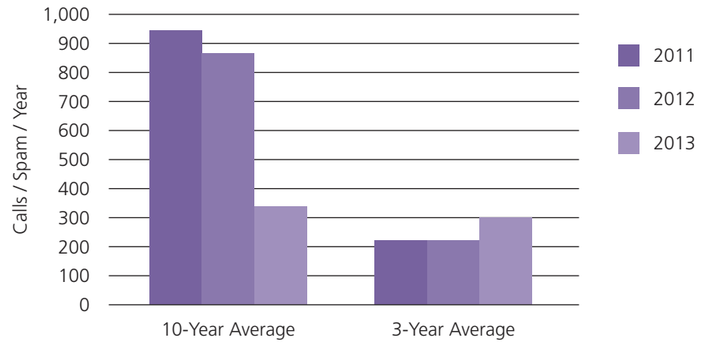
ISP calling trends from our ten-year database are presented below:

- 8.7% of customers had no ISP calls discovered during the approximately 60-day assessment window, while about 91% had ISP calls.

ISP Calls:

- Ten-year average: 0.9 ISP calls/span/day (347/yr/span)
- Three-year average: 0.84 ISP calls/span/day (305/yr/span)

### Annual ISP Call Trend




Many enterprises still complete business-to-business data transfer via ISP connections, and provide employees the ability to access personal communication services via the web. That said, approximately one ISP call per span every two working days still occurs, which equates to the risk of one data security breach per span every two working days for the average enterprise.

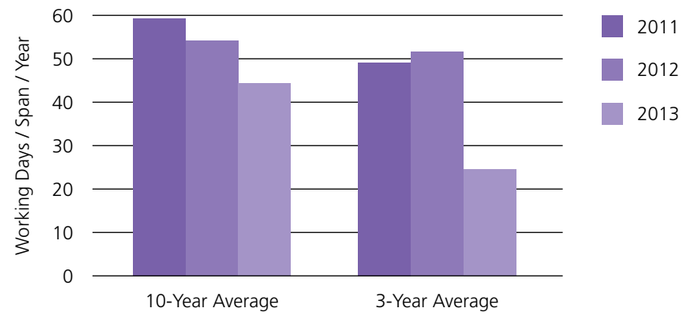
ISP Call Total Duration:

- Ten-year average: 58.5 minutes/span/day (14.82 days/span/yr)
- Three-year average: 32.02 minutes/span/day (8.11 days/span/yr)



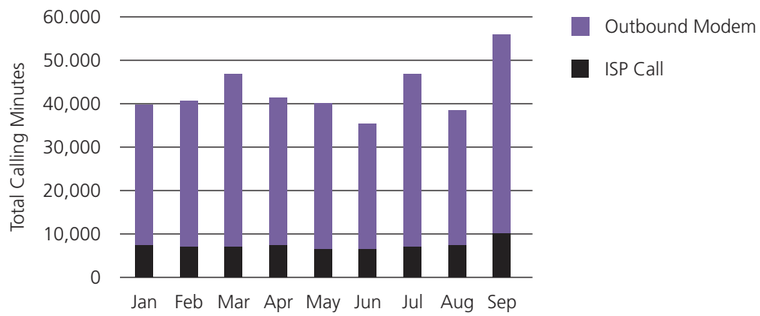


### ISP Duration




Presented is a graph illustrating this phenomenon in a nine-month study we undertook for a customer. In this instance, ISP calls consistently average about 20% of all modem call duration.

### Modem Calls to Known ISPs




ISP calling remains an issue as reported in our 2013 report. As expected when looking at a rolling 10-year average, the number of ISP calls has dropped; however, when compared to the rolling 3-year average, the number of ISP calls has remained fairly constant. Both the 10-year and 3-year averages highlight the same issue: ISP calling continues and is being used to bypass security controls.

Voice and VoIP systems continue their migration towards UC and collaboration, which integrates other forms of communications, including messaging, video, and social networking. Presence is an integral part of these communications.

One huge trend is the move to mobility and smart phones, which allow constant robust access to the Internet. While these devices are called smart phones, the voice application has become one of the least used features of the devices. These devices allow users to be constantly connected and communicating. They are changing the way we communicate and are moving much of the enterprise voice communications to mobile and different forms such as SMS messaging, instant messaging, and other applications. Since most users expect enterprises to support a Bring Your Own Device (BYOD) policy, the user's device is often used for both enterprise and business use. From a UC point of view, the device is now used for many forms of communication, most of which are outside the control of the enterprise. However, since the enterprise may be paying for the user's service, they can be affected by various fraud issues. They are obviously affected if the user's behavior puts corporate data at risk.

Whether it is on mobile devices or on the enterprise desktop, many voice conversations are being replaced with text and instant messaging. Texting is ubiquitously supported across mobile devices, and various instant messaging applications are commonly used as well. Text messaging brings with it a number of issues, including text SPAM (SPIM), text phishing (SMISHING), and types of toll fraud, where the attacker generates text messages to premium numbers.

The various applications that provide Over-The-Top (OTT) communications are not necessarily secure. These are generally closed systems, so they don't have the same issues with SPAM and phishing, but are only as secure as the application; they may not encrypt the data being sent, may allow data leakage by sending files, and are a target of malware. Remember that they are an application running on the mobile device or desktop, with a direct connection to the Internet. Consider applications such as Whatsapp, which amassed almost 500 million users in a few years of existence. Skype, iMessage, Viber, etc. are other examples.

Video is becoming increasingly common. Video can range from very high quality telepresence level systems, to lower end ad-hoc calls from phones, or collaboration software/services such as WebEx and Google Hangouts. When video is used on the internal/campus network, the security issues with it are very similar to those for voice and use the same signaling and media protocols; most often SIP for signaling and RTP for media. The security issues with these protocols for video are essentially the same as they are for voice. Video is similar to voice in that it is intolerant of latency/jitter, although one can argue that users are more used to choppy video because of the nature of video over the Internet. The biggest difference with video is that it consumes much more bandwidth, especially with high quality systems, and can be a bigger DoS issue. If attackers can one day generate a large number of video sessions, they can easily create a DoS condition against their target. Also, because video uses so much bandwidth, it is a more lucrative way of exfiltrating data.

Video is starting to be used over the Internet to enable enterprises to federate and collaborate. Video systems are often accessible over the Internet and left in default security states.

Users continue to make heavy use of social networking services, such as Facebook, Google+, Twitter, Instagram, LinkedIn etc. The security issues with using these services are well known. Most of these services have their own built-in messaging (and video) capabilities. Facebook just purchased Whatsapp for this function. The main issue with these services is that it is very easy and common for users to exchange information and data, via an uncontrolled cloud, which greatly increases security risk.

There is also a general movement of applications to utilize the public cloud. In fact, many of the applications described so far exist in the public cloud. Also, more enterprises, especially smaller ones, are looking to move the UC application/IP PBX to the cloud. This is often described as Unified Communications as a Service (UCCaaS). In this case, the enterprise is no longer responsible for securing the UC application/IP PBX, but is still vulnerable to the call-level attacks discussed in this document.

As noted earlier, the greatest threats to enterprises occur because the Public Voice Network will continue to allow more UC-based access, will become hostile, and will therefore increasingly be the source of malicious calls. This network will continue to look more like the Internet from a call-generation standpoint. While packet attacks remain unlikely, even when using enterprise SIP trunks, voice-application level threats, including TDoS, financial fraud/social engineering, call pumping and toll fraud, harassing calls, and voice SPAM/phishing will still be present.

TDoS will continue to be a critical issue. Attacks against smaller sites will continue, because it has been established that there is a proven financial incentive. Also it will become progressively easier to generate thousands or even tens of thousands of calls, overwhelming IVRs, agents, and other parts of enterprises. TDoS attacks will also get more sophisticated in terms spoofing the calling number and audio content, making it more difficult to differentiate TDoS from legitimate calls. Attackers will update botnets to be UC-aware and will generate massive numbers of calls from many locations, making attacks very difficult to detect and mitigate.

TDoS will become the largest threat to enterprises. Social networking-originated TDoS will become a bigger issue. Careless celebrities with many Twitter followers can create a harassing caller/TDoS condition by encouraging their followers to call an enterprise/group of numbers. An anonymous individual can create Facebook pages that incite, educate, and organize a group of individuals to flood an enterprise with harassing calls.

Financial Fraud/Social Engineering will continue to get worse. This is exacerbated by the fact that UC makes it easier to probe IVRs for basic PI, while spoofed calling number and other cheaply and readily available means facilitate masking real identity. The increased use of social networking will also make it easier and easier for attackers to get basic PI about their victims.

Call pumping and toll fraud issues will continue to grow. As long as there are charges for 1-800 numbers, call pumping will continue to be an issue. Some predict the elimination of voice usage costs, where enterprises will only pay for bandwidth/capacity and not the cost of calls based on destination. However, this is unlikely to be common in the near to mid-term. As long as it costs money to call certain countries





and premium numbers, long distance abuse and toll fraud will continue to be issues. The increasing complexity of VoIP systems will continue to introduce new vectors of attack for toll fraud.

Harassing calls will continue to be an issue. Bomb threats and other threatening calls will continue to occur. Automation will only make these issues more acute.

As it becomes even easier and cheaper to generate calls, voice SPAM and phishing will gradually become bigger issues. With each passing day, enterprise users and consumers will receive progressively more SPAM and phishing calls, soon getting to the point where enterprises are receiving as many “robocalls” as consumers.

Modem abuse will remain an issue. Authorized modems will remain in enterprises for maintenance, backup, and failsafe access. ISP modems will remain because they are a relatively safe way for users to illicitly access the Internet.

Enterprises may start to see attacks occurring on internal/campus VoIP networks. As enterprises deploy more VoIP and use UC to blend with data networks, the threats to VoIP systems will increase. The most likely attacks are different forms of DoS for disruption, toll fraud, and eavesdropping on calls, IM, presence, and video. Wider use of mobile devices, smart phones, and remote workers will allow more hostile endpoints to connect to key VoIP systems. Fortunately, encryption can be used to mitigate some of these attacks.

Enterprises may start to see some SIP-specific attacks on trunks, but this is unlikely. With more use of SIP for handsets, video, IM, etc., it is likely that some internal or new attacks will be seen.

Enterprise VoIP traffic will start to migrate to the Internet. Enterprises will want the rich communications experience users get with modern VoIP/UC systems for communications with other enterprises. This may start the movement of traffic to the Internet, thereby increasing the threat of VoIP-specific attacks. Instant messaging already uses the Internet and video is likely to do the same.

TDoS will become the largest threat to enterprises. Social networking-originated TDoS will become a bigger issue.

SecureLogix®

We see your voice™

SecureLogix Corporation
13750 San Pedro Ave.
Suite 820
San Antonio, TX 78232

PHONE 210 402 9669
TOLL FREE 1 800 817 4837
INT 001 210 402 9669
FAX 210 402 6996

EMAIL info@securelogix.com
WEB SecureLogix.com
BLOG voipsecurityblog.com

© Copyright 2014 SecureLogix Corporation. All Rights Reserved.

ETM, TeleWatch Secure, TWSA, We See Your Voice, SecureLogix, SecureLogix Corporation, the SecureLogix Emblem and the SecureLogix Diamond Emblem are trademarks and/or service marks or registered trademarks and/or service marks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

SecureLogix technologies are protected by one or more of the following patents:

US 6,226,372 B1, US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 B2, US 6,760,421 B2, US 6,879,671 B1, US 7,133,511 B2, US 7,231,027 B2, US 7,440,558 B2, US 8,150,013 B2, CA 2,354,149, DE 1,415,459 B1, FR 1,415,459 B1, & GB 1,415,459 B1.