BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Whether the Commission's Rules Concerning	)	ET Docket No. 04-35
Disruptions to Communications Should Apply to	)	WC Docket No. 05-271
Voice Over Internet Protocol Service Providers	)	GN Dockets 09-47, 09-51, 09-137

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net Coalition (VON Coalition)[1] hereby submits these comments in response to the Commission's Public Notice concerning whether the Commission's network outage reporting requirements should apply to interconnected Voice over Internet Protocol (IVoIP) service providers.[2] The VON Coalition does not support extending outage reporting requirements to IVoIP providers for a variety of reasons.

Service outages could be caused by multiple factors, all of which may be out of the control of and unknown to the IVoIP provider, including the unavailability of third-party provided broadband connections or electrical power failures. As many of the causes of service outages may not be within the control of IVoIP providers, mandating outage reporting for IVoIP providers would be a burdensome endeavor that diverts necessary resources away from serving consumers. Moreover, the competitive market for IVoIP services incents providers to make their services as reliable as possible. Additionally, Congress and the FCC have committed to imposing a light regulatory burden on IVoIP providers in order to promote innovation within the industry. The FCC

[1] The VON Coalition works to advance regulatory policies that enable Americans to take advantage of the promise and potential of VoIP. VON Coalition members are developing and delivering voice innovations over the Internet. VON Coalition members include AT&T, Broadvox, Cisco, Google, iBasis, Microsoft, Skype, T-Mobile, Vonage and Yahoo.

[2] See *Public Notice*, DA 10-1245, ET Docket No. 04-35, WC Docket No. 05-271, and GN Docket Nos. 09-47, 09-51, and 09-137 (released July 2, 2010).

should maintain that light touch regulatory policy by refraining from requiring outage reporting at this time.

If the FCC does impose outage reporting requirements on IVoIP providers, however, reports should only be required when (1) there has been a service outage caused by a failure of equipment provided by the IVoIP provider and not the underlying Internet Service Provider; and (2) where that outage impacts five percent or more of an IVoIP provider's customer base. Also, any reports should be for information purposes only, rather than to penalize IVoIP providers.

BACKGROUND

The Commission first implemented outage reporting requirements in 1992 for wireline telephone networks, extending these requirements to wireless and satellite communications networks in 2004.[3] According to these regulations, providers must notify the Commission and provide initial and final reports in a timely manner whenever they experience a service outage that exceeds a certain threshold of user-minutes.[4] These requirements are intended to give the Commission "rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of our Nation."[5] The Commission also uses this information to analyze the capabilities and vulnerabilities of communications networks and to develop industry best practices.[6] In its National Broadband Plan, released in

[3] See *Report and Order and Further Notice of Proposed Rule Making*, FCC 04-188, ET Docket No. 04-35 (2004) ("*New Part 4 Order*").
[4] 47 C.F.R. §§ 4.9, 4.11.
[5] *New Part 4 Order*, ¶ 1.
[6] *Id.* at ¶ 12.

March 2010, the Commission recommended extending outage reporting requirements to broadband and IVoIP.[7]

DISCUSSION

I. MOST OUTAGES WILL NOT BE CAUSED OR CONTROLLED BY THE IVOIP PROVIDER

IVoIP cannot be characterized as a single technology; it can vary by service, by service provider, and by end user. In all cases, the end user must have a broadband connection to access the IVoIP service. This broadband connection mayor may not be provided by the customer's IVoIP provider; it could also be provided by a cable television company, a telephone company, an electric company's broadband over power-line service, or a wireless company through a subscription service or as an occasional user through Wi-Fi at hot spot. IVoIP customers also need a handset or other equipment that facilitates the communication between two or more parties. Again, that equipment may or may not be provided by the IVoIP provider. Finally, IVoIP providers rarely, if ever, provide the electricity necessary for the operation of broadband service and other IVoIP equipment.

Failure of the customer equipment, the broadband service, or an electrical power will likely result in a complete IVoIP service outage. A major outage by a broadband provider or an electric company throughout a large geographic area could result in the unavailability of IVoIP service for a sizeable portion of an IVoIP provider's service territory. Unfortunately, in most of these cases, the IVoIP provider will likely not be aware of the outage (unless contacted by one of its customers) and will not have any

[7] Federal Communications Commission, "Connecting America: The National Broadband Plan," 320-21, available from http://download.broadband.gov/plan/national-broadband-plan.pdf ("National Broadband Plan").

ability to fix the problem. These types of outages should not require reports by the IVoIP provider.

There may be rare occasions when the equipment used by the VoIP provider, or network connections under the control or supervision of the VoIP provider, fail and lead to an outage. In these cases, when the VoIP provider is responsible for, or should be responsible for the service availability, it may be appropriate, as discussed below, for the IVoIP provider to file an outage report with the Commission.

II. THERE IS NO EVIDENCE THAT IVOIP CREATES CYBERSECURITY RISKS

The National Broadband Plan recommended extending outage reporting requirements to IVoIP providers because of the need for stronger cybersecurity to protect the nation's commercial and Internet infrastructure. However, despite the incredible growth in IVOIP services with governmental, commercial, and residential consumers, there is no evidence that the services present unique cybersecurity problems or that there have been security breaches. In fact, many providers are making special effort to protect security.

AT&T published a White Paper detailing the robust security mechanisms it has deployed to secure its IVoIP service.[8] Other companies are providing guidance to customers that are thinking about moving to VoIP but that are concerned about end-to-end security.[9] Indeed, companies are now touting the security of VoIP as a selling point

---

[8] See, AT&T Voice DNA Voice over IP Security Overview, copy attached.

[9] See "Securing Enterprise VoIP," at http://www.nortel.com/support/news/articles/newsarticle080301a.html. See also, "VoIP Security: The Basics," at http://computernewsme.com/technology/security/voip-security-the-basics.html.

to new users.[10] Thus, with IVoIP providers taking their own security measures, even in the absence of a noted problem, the FCC need not extend outage reporting requirements to IVoIP at this time.

III. REQUIRING IVOIP PROVIDERS TO REPORT OUTAGES IS NOT NECESSARY OR APPROPRIATE GIVEN THE MARKET INCENTIVES TO PROVIDE INNOVATIVE AND RELIABLE SERVICE.

Extending reporting requirements to IVoIP providers is further unnecessary since competition within the IVoIP market motivates providers to ensure high-quality, secure, reliable service. The Commission recently reported that 13% of local telephone connections are now IVoIP subscriptions, for a total of 21 million IVoIP subscriptions in the United States.[11] VoIP has also emerged as a major provider of international communications; Skype, for example, is by far the largest provider of cross-border communications worldwide.[12] Furthermore, this growing market is divided among a large and ever-increasing number of providers. One online source of VoIP comparisons identified more than 1,400 international VoIP services as of January 2008.[13] These providers have been competing not only against each other, but also with non-VoIP wireline and wireless communications services, and these competitive pressures have caused the price of communications services to drop significantly.[14]

---

[10] See, Officescape offers new Secure VoIP solution as part of latest UC server release, at http://www.forbes.com/feeds/businesswire/2010/06/01/businesswire140491646.html.

[11] Federal Communications Commission, "Local Telephone Competition: Status as of December 31, 2008," 3 (2010), available from http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-299052A1.pdf.

[12] TeleGeography, "TeleGeography Report Executive Summary," 6 (2009), available from http://www.telegeography.com/product-info/tg/index.php.

[13] MyVoipProvider.com, available from http://www.myvoipprovider.com/index.php?option=content&task=view&id=92.

[14] *See* Matt Richtel and Ken Belson, *Online Calling Heralds an Era of Lower Costs*, N.Y. Times, July 3, 2006, available from http://www.nytimes.com/2006/07/03/technology/03phone.html; "TeleGeography Report Executive Summary," 7; Voice on the Net Coalition, "Unleashing the Full Promise and Potential of Internet Voice Communication," 5 (2004), available from http://www.von.org/usr_files/Whitepaper%20Final.pdf.

To earn and retain a share of the market in this competitive arena, IVoIP providers must constantly monitor and improve the quality of their services. If they do not provide reliable service, their customers will soon abandon them for one of the many other possible providers. IVoIP users can turn to a multitude of websites and Internet forums to help compare products before purchasing them and report on the services after using them.[15] Given the potential for instantaneous feedback, competitors who offer unreliable service are likely to be identified and eliminated rapidly. Recognizing the importance of high-quality services, many IVoIP providers have voluntarily taken cooperative improvement measures (e.g. meeting with experts to improve access to emergency numbers) years before this policy was mandated by the Commission.[16]

Imposing outage reporting requirements on IVoIP providers is not only unnecessary, it is also difficult to reconcile with previous commitments by Congress and the Commission to encourage innovation in Internet services. Congress has written that "the policy of the United States [is] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[17] The Commission, meanwhile, "has worked to create an environment promoting competition and innovation to benefit consumers," only imposing regulations on IVoIP when necessary.[18]

In light of these policy priorities promoting innovation in IVoIP services, the Commission should avoid imposing outage reporting regulations on IVoIP providers.

---

[15] *See, e.g.,* VoIP User Forum, available from http://www.voipuser.org/forum_index.html.
[16] *See* Federal Communications Commission, "Voice Over Internet Protocol: FCC Consumer Facts," available from http://www.fcc.gov/cgb/consumerfacts/voip.html; "Unleashing the Full Promise and Potential of Internet Voice Communication," 13.
[17] 47 U.S.C. § 230(b)(1) & (2).
[18] "Voice Over Internet Protocol: FCC Consumer Facts."

Given the variety of ways in which IVoIP can be used, it may be difficult for providers and for regulators to identify the root causes of service outages. Imposing such burdensome regulations may have a chilling effect on innovators looking for new and improved ways to provide IVoIP. Furthermore, customers can currently choose IVoIP providers to fit their needs, based on cost, quality, and available services. New regulations not only increase costs, they also mandate greater uniformity and thereby restrict consumer choice. Imposing outage reporting requirement on IVoIP may also deter potential investors from funding research into innovative services and technologies.

IV. IF IMPOSED, OUTAGE REPORTING REQUIREMENTS MUST BE ADMINISTRABLE AND LIMITED TO INFORMATION-GATHERING

If the Commission imposes outage reporting requirements on IVoIP providers, the requirements must reflect the realities of IVoIP and the purpose of the regulations. First, "outage" must mean exactly that, a complete outage, -- i.e., a failure of equipment of the IVoIP provider that results in no available service -- rather than service degradation or congestion, or an outage caused by the customer's ISP. Tracking all instances of brief delays or congestion in IVoIP service would impose untenable burdens on providers, if it is even technically possible. Moreover, IVoIP customers may be unable to access their services if there is a failure of their underlying ISP or a power failure, both of which may be out of the control of the IVoIP provider. Limiting outage reporting solely to instances of complete outage is also more in line with the goal of the regulations since this alone will help the Commission understand "how to prevent future outages" and "analyze information on outages."[19]

[19] *See* National Broadband Plan, 321.

Moreover, from a process perspective, outage reports should be presumptively confidential, as they are for other services covered by the rules, and shared only with the Department of Homeland Security.[20] IVoIP providers should not have to be concerned about misuse of the data or about revealing commercially sensitive subscriber or network information. Reports should only be required if the outage affects five percent or more of the IVoIP providers' customer base. Many of these companies serve niche markets and should not be required to report if only a handful of customers are affected. Finally, reports should be due no earlier than five days after the IVoIP provider discovers the outage. This will provide the IVoIP provider adequate time to troubleshoot the problem and conclusively determine whether the outage was caused by the IVoIP provider or another service provider of the customers.

In addition, procedures for outage reporting must focus on gathering information, not imposing punitive measures on providers. For years, the Commission carried out investigations and made enforcement decisions to ensure that companies were capable of meeting their outage reporting requirements. For instance, it required non-compliant companies to create compliance plans and to implement training programs for employees, internal controls, and periodic compliance reporting.[21] In these enforcement decisions, the Commission recognized that companies were admitting no violation or liability by agreeing to undertake these reforms.[22] In contrast, in two decisions from July 2010, the Commission has issued notices of apparent liability for forfeiture, imposing penalties on companies for willfully disregarding reporting requirements.[23]

---

[20] *Public Notice* at 5.
[21] *See, e.g., Bluegrass Cellular, Inc.*, DA 10-237 (2010), ¶ 8; *Verizon*, FCC 07-124 (2007), ¶ 12.
[22] *See Verizon*, FCC 07-124, at ¶ 10.
[23] *Alpheus Communications, LP*, DA 10-1258 (2010), ¶ 1; *Verizon*, DA 10-1268 (2010), ¶ 1.

Punitive measures are contrary to the intent of the reporting requirements. The Commission has repeatedly stated that the goal of these requirements is gathering information to monitor and improve services.[24] Imposing penalties and liability for non-compliance does not comport with this information-gathering intent. Using the reporting requirements to issue penalties may also create uncertainty and inefficiencies for IVoIP providers, who, even if they submit all reports on time, could still face punitive retribution for not meeting other of the Commission's criteria despite the best intentions.[25] Instead, the Commission should use the reporting requirements as they were intended, to gather data on network outages.

[24] *See Verizon*, DA 10-1268, at ¶ 2; *see also New Part 4 Order*, ¶ 1 ("We made this proposal because we recognized the critical need for rapid, complete, and accurate information on service disruptions . . . .").

[25] *See Verizon*, DA 10-1268, at ¶ 5 (imposing liability for a forfeiture on a wireless provider for its failure to "completely and accurately describe" an outage, notwithstanding the provider's protest that its report was accurate).

CONCLUSION

For the foregoing reasons, the VON Coalition respectfully requests that the Commission decline to extend outage reporting requirements to IVoIP providers at this time. If the Commission deems it necessary to impose these requirements, it should require IVoIP providers to report only complete outages caused by failures in the IVoIP providers' equipment and not by outages in the users' underlying ISP services, and it should use the reports solely for information-gathering rather than punishment.

Respectfully submitted,

VOICE ON THE NET COALITION

/s/

Glenn S. Richards
Pillsbury Winthrop Shaw Pittman LLP
2300 N Street NW
Washington D.C. 20037
(202) 663-8215

Its Attorney

August 2, 2010

AT&T Voice DNA℠ Voice over IP Security Overview

AT&T Security Center of Excellence

Overview: This white paper highlights the key security differentiators for the AT&T Voice DNA Voice over Internet Protocol (VoIP) Service and discusses the robust security mechanisms that AT&T has deployed to secure the service.

Executive Summary — Key Security Differentiators

AT&T Voice DNA (Dynamic Network Applications) is a new network-based Voice over IP service that provides advanced telephony features and flexible local and long distance calling along with web-based tools that provide control and convenience to IT administrators and individual employees.

AT&T has developed a security architecture for AT&T Voice DNA that strengthens potentially vulnerable points. This security architecture deploys a "Defense In-Depth" approach to provide a multi-layered secure environment. Security mechanisms are deployed throughout the elements of the service in order to provide seamless and effective security.

AT&T's world class experience in both IP and telephony security provides the following key security differentiators:

- AT&T Labs has designed an effective "Defense In-Depth" security architecture that seeks to provide protection to AT&T Voice DNA in the areas of Denial of Service, Theft of Service / Fraud and Abuse, Data Confidentiality, and Privacy.
- AT&T Voice DNA leverages the unique capabilities of the AT&T Converged IP/MPLS Network to provide Security and Quality of Service (QoS). AT&T has designed its IP Network to be an effective security device to detect, isolate, and eliminate security threats before they become a security breach.
- AT&T Managed Security Services including AT&T Professional Services can be leveraged by AT&T Customers to secure their enterprise networks. These are the same services that AT&T uses to secure its own IP networks and services.

As a leader in enterprise networking, AT&T constantly evaluates and updates security mechanisms to ensure a continued high-level of secure communications for AT&T Voice DNA.

Introduction

The very nature of VoIP places telephony traffic on IP data networks. This potentially subjects VoIP services to threats known to IP data networks. The AT&T Voice DNA Security Architecture leverages AT&T security innovations and other IP and telephony security procedures and best practices, and it hardens the service and infrastructure at potential points of vulnerability. These points of vulnerability are places where the service or infrastructure may be susceptible to known or presumed attacks.

AT&T is working to meet the security needs by building upon the following security cornerstones:

- Service Function and Availability Assurance:

  Preserve proper functional behavior and availability of the service in the face of software, protocol, bandwidth, memory, or CPU denial of service attacks.
- Service Integrity Assurance:

  Preserve the integrity of system functions and data; prevent theft and fraudulent use of service.
- Service Confidentiality and Privacy Assurance:

  Preserve the confidentiality of signaling, voice, and web communications; preserve the privacy of customer information.

This paper discusses the AT&T Voice DNA Security Architecture in detail. First, an overview is presented of the AT&T Voice DNA Service and the AT&T VoIP Functional Architecture. Then, the primary threats against VoIP are summarized. Next, the overall AT&T Voice DNA Security Architecture is discussed. The security architecture

provides protection that is integrated throughout the AT&T VoIP Functional Architecture. Finally, the mechanisms that make up the security architecture are discussed in detail.

AT&T Voice DNA Service Overview

AT&T Voice DNA provides the flexibility, control and reduced capital expenditures inherent in network-based IP services. AT&T Voice DNA has several advantages. It uses the global AT&T Converged IP/MPLS Network, interoperates with AT&T's industry leading VPNs and leverages AT&T's award-winning web portal BusinessDirect.

AT&T's Voice DNA provides Local, US Long Distance and International calling between an enterprise's VoIP sites (on-net) as well as between an enterprise site and any PSTN connected site (off-net). With AT&T Voice DNA Flexible Reach, customers get an array of calling plans to best meet their business requirements. There is a long distance only plan, a local and long distance plan (with long distance being billed on a per-minute basis) and a flat rate package of combined local and long distance calling. The local plan includes carrier-class primary local service and features (e.g., Local numbers, N11, 8YY, DID/DOD, etc.).

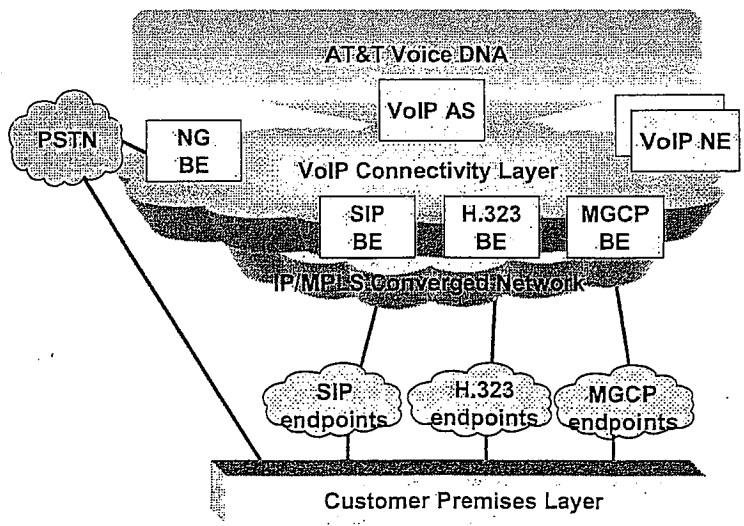
For customers looking for an alternative to a premises-based PBX or IP PBX, AT&T Voice DNA also provides network-based IP telephony features (e.g., Call Hold, Call Waiting, etc.), and advanced features such as Find Me/Follow-Me, Switch phone, etc. Web-based administration and end-user tools are provided for IT managers and employees. Customers have options for different types of Customer Premises Equipment (CPE), including SIP-enabled IP phones, black (analog) phones along with a Telephone Adapter, and a PC-based soft phone.

AT&T's Flexible Reach Service also provides emergency calling capability (911/E911) as required by FCC rules. Note that 911/E911 service through AT&T VOIP services may be ineffective or unavailable due to reasons such as (i) broadband connection failure, (ii) loss of electrical power, (iii) use of the service at a location other than the address registered with AT&T, or (iv) delays in updating emergency agency records for a changed or new location.

Additional information about AT&T's VoIP Services can be found at http://www.att.com/voip.

AT&T VoIP Functional Architecture

AT&T has designed a VoIP Functional Architecture to provide an array of VoIP services for businesses. The functional architecture is an open architecture that enables best-of breed Plug 'n Play components. This functional architecture is shown in the figure below.



In the AT&T VoIP Functional Architecture, VoIP Application Servers (VoIP AS) provide the standard and advanced VoIP features. VoIP Network Elements (VoIP NE) provide a number of functions such as call control and routing. VoIP Border Elements (BE) provide the interface to the various types of CPE and to the Public Switched Telephone Network (PSTN).

Summary of Threats to VoIP Services

In this section we summarize the threats to VoIP. Threats to VoIP can be grouped into three primary areas:

- Denial of Service
- Theft of Service / Fraud and Abuse
- Data Confidentiality and Privacy

Denial of Service Attacks

A service provider must be able to provide continuously available service to its subscribers. Denials of Service attacks on the Internet have been well documented. These attacks, often due to vulnerabilities in software or insecure configurations, attempt to interfere with service protocols and processes so that the proper level of service is denied to subscribers. They are aimed primarily at network elements, but they can target the CPE as well.

Denials of service attacks take several forms. One method is to force the operating system (OS) of a network element to fault, either disrupting service or presenting some other undesirable customer experience. Another method is to trick the network element or CPE into accepting false messages for the various protocols used in the service. These false messages can interfere with the correct operation of the service. A third method, the so-called "flood" or Distributed Denial of Service (DDoS) attack, is intended to overwhelm network resources. These attacks attempt to force the network element to divert resources such as CPU power or memory to handle false requests for service, leading to a degradation of service.

Theft of Service / Fraud and Abuse Attacks

Theft of service, also known as fraud, is used to describe cases where people are able to use more services or resources than they are entitled to use. Theft of Service can cover the spectrum from complete theft (where service is used without authorization by non-subscribers) to partial theft (where more service is used by a subscriber than permitted or paid for). In general, any behavior against the Acceptable Use Policy for the service is considered to be abuse.

Fraud and abuse may also occur if new, advanced features are not adequately protected. Because VoIP is a relatively new technology, new fraud and abuse techniques may be discovered that will need to be counteracted.

Data Confidentiality and Privacy Attacks

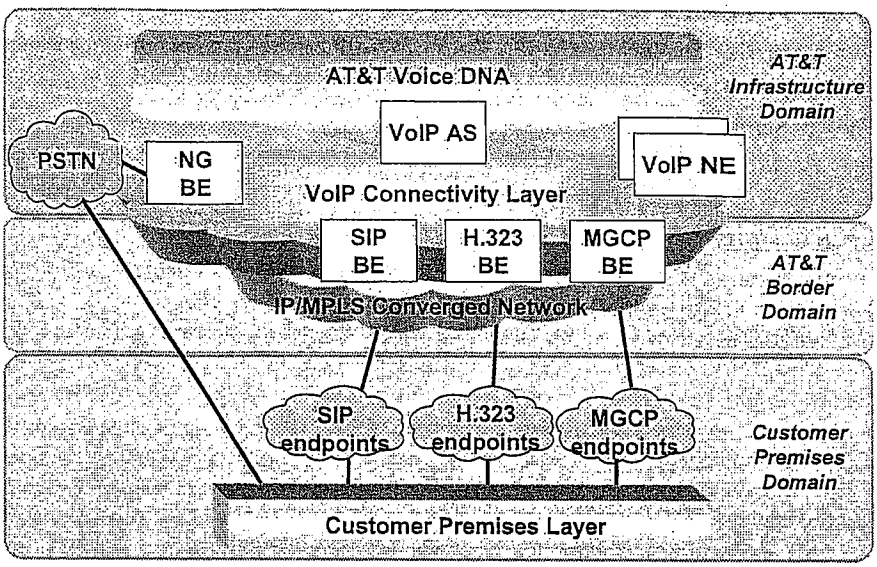
Data Privacy issues are concerned with protecting the rights of subscribers by maintaining the confidentiality of their data. Subscriber data (information that authenticates an individual as a client on AT&T Voice DNA – not details of individual calls placed) are stored within AT&T databases. Traditional IP attacks against privacy are directed toward compromising the network elements or databases that contain customer data.

Information that subscribers would consider private is also transported within the voice conversation and the signaling protocol. Unprotected data (including voice) transported over public or shared IP networks may be susceptible to confidentiality and privacy attacks. IP voice messages may be at risk for eavesdropping. Additionally, any private data within the signaling packets may be at risk for eavesdropping. Private data may include, for example, the phone numbers being called by a given subscriber.

at&t

AT&T Voice DNA Security Architecture

To counteract threats to AT&T Voice DNA, AT&T Labs has designed a security architecture to protect the VoIP Functional Architecture described above. The security architecture is shown in the figure below.



The security architecture segments the functional architecture into three security domains — the AT&T VoIP Infrastructure Domain, the AT&T Border Domain, and the Customer Premises Domain. The AT&T VoIP Infrastructure Domain contains the VoIP network elements and application servers that control the VoIP calls, provide VoIP advanced features, and act as the gateway to the PSTN. The AT&T Border Domain is the interface to the Customer Premises (Enterprise) Domain. The Border Domain protects the AT&T VoIP Infrastructure Domain against external attacks.

An effective security architecture seeks to provide protection in the areas of Denial of Service, Theft of Service / Fraud and Abuse, and Data Confidentiality and Privacy. Within the Infrastructure and Border Domains, AT&T Voice DNA deploys a "Defense In-depth" strategy. Many integrated mechanisms are deployed to provide security. So that an attack against one mechanism may still be blocked by other supporting mechanisms. These security mechanisms are described below.

Security Policy and Process

At AT&T, security begins with the AT&T Security Policy and Requirements (ASPR). This family of policies governs security in AT&T IP Services in everything from Operating Systems to Network Operations. Building on this foundation, all AT&T IP Services also follow the AT&T OneProcess℠ Service Realization Process. For each new and enhanced feature, the AT&T IP Security Team works closely with the service realization teams to build security into the feature, service, or network itself. Also, AT&T maintains strict customer information privacy policies including the AT&T Online Privacy Policy (http://www.att.com/privacy/).

Denial of Service Protection

Because these problems will continue to plague the Internet, AT&T has designed its IP Network to be an effective security device to detect, isolate, and eliminate security threats before they become a security breach. One AT&T security innovation, AT&T Internet Protect™, monitors the AT&T Converged IP/MPLS Network looking for early warning of new Denial of Service attacks such as those which are caused by worms and viruses. AT&T Internet Protect is supported by advanced algorithms developed at AT&T Labs and is monitored 24x7 by AT&T security personnel. If data indicate that a potential attack is brewing, the AT&T

Computer Security Incident Response Team (A-CSIRT) is called into action. A-CSIRT takes pro-active steps to ensure that any adverse effect on AT&T assets is minimized.

AT&T deploys other mechanisms throughout the infrastructure. Border Elements provide further protection against flood and other Denial of Service attacks. Border Elements are VoIP-aware network elements that block malicious or other misbehaving traffic that is destined for the AT&T VoIP infrastructure.

Other security mechanisms also protect against Denial of Service attacks. Network security rules only allow access to specific services and from specific IP addresses. Configuration settings within firewalls, routers, switches, and servers minimize the impact of flood and other DoS attacks. Regular and frequent audits of all network elements help ensure their security is up-to-date. When an attack is suspected, action is taken quickly to investigate and mitigate the effect. Network element software provides the capability to limit the amount of resources allocated to servicing requests. This is particularly important to maintain service in the presence of an elevated number of requests.

Security of AT&T Voice DNA Advanced Features

A key advantage of VoIP is the integration of Voice and the Web. For example, AT&T Voice DNA users can manage their accounts, provision advanced features, and access their accounts remotely via the Web. Access to these advanced features is authenticated and protected using standard and well-known security protocols. Access to web servers is protected by SSL, a technology that provides secure transmission over the Internet. Furthermore, all advanced features are reviewed for potential security, fraud, and abuse vulnerabilities.

Voice and Signaling Security

The very nature of VoIP places telephony traffic on data networks. This now exposes VoIP services to threats known to IP data networks. AT&T Voice DNA logically separates voice and associated signaling from general data traffic to provide enhanced security.

At the access point to AT&T VoIP network elements, AT&T deploys VoIP-aware Border Elements that filter VoIP traffic from data traffic and also filter malicious VoIP traffic. Other network-based mechanisms are used to further separate VoIP and data traffic. For example, AT&T deploys an MPLS Voice Aware Network VPN on its IP network to provide both security and QoS.

Fraud (Theft of Service) Prevention and Detection Mechanisms

AT&T Voice DNA leverages the extensive fraud detection and prevention mechanisms that are used by the AT&T Switched Telephone Network. As part of its security practices, AT&T is working to adapt the AT&T Global Fraud Management System to protect against fraud in AT&T Voice DNA. This system includes numerous fraud-detection algorithms that have been developed over the many decades that AT&T has been providing telephony service. In addition, new algorithms will be developed to counteract new threats in IP as well as to protect new features such as web-enabled advanced services.

Infrastructure Security

AT&T Voice DNA deploys many different infrastructure security mechanisms in a layered, defense-in-depth approach so that failures or breaches in one security mechanism do not necessarily affect the entire service. These mechanisms are discussed in the following sections.

Server-based Security

For hardened OS configurations, AT&T Voice DNA follows the AT&T Security Policy and Requirements (ASPR) and other vendor and industry recommendations. These recommendations are implemented in a package that automatically configures the servers for a consistently secure configuration.

Network-based Security

AT&T Voice DNA is supported across several geographically dispersed AT&T facilities. These AT&T facilities and the connecting IP networks are designed using the following measures.

The AT&T facility architecture includes several zones for network security. Each zone has different requirements for security and is segmented so that traffic cannot leak between zones. The zones are enforced by using a variety of industry standard network security elements including firewalls, access control lists (ACLs), Virtual Local Area Networks (VLANs), and separate physical LANs.

All access to the AT&T network elements passes through Network Security elements to ensure that only acceptable traffic reaches AT&T Network Elements.

Software Security Patch Updates

AT&T Voice DNA adheres to a strict and regular patch update policy. AT&T monitors internal, industry, and vendor advisories for Recommended and Security patches, tests the patches in production support labs, and deploys the patches.

Pre-production and Production Vulnerability Scans

Vulnerability scans identify known vulnerabilities in applications and the underlying operating system that may be exploited by an attacker. AT&T performs security scans before services are deployed to help ensure the network elements are secure before they are exposed to any malicious traffic. AT&T network servers are also scanned on a regular basis after the service is operational to help maintain high security.

Network Operations and Lifecycle Security

The Network Operations function is critical to maintaining security throughout the service lifecycle. Network Operations security includes physical security, strict access control, continuous security monitoring, and fraud and security incident response. Access from Network Operations to AT&T Voice DNA network elements is controlled according to policies prescribed by AT&T's Security Policies and Requirements.

Systems, networks, and applications are fully monitored 24x7. System resources are monitored and compared to expected use, and abnormal activity is investigated to determine the root cause including the possibility of an attack. Alarms are generated based on unusual network activity. Network element logs are monitored to determine unusual activity.

In the event of a suspected security incident, AT&T Voice DNA is supported by A-CSIRT. This specialized technical group of senior security specialists is available 24x7 to support AT&T's computer and network infrastructure, and minimize damage to AT&T assets.

Customer Premises (Enterprise) Security

Ultimately, the security of a customer's VoIP services depends not only on the security measures that AT&T deploys in its network and services, but also by the security that the enterprise customer implements at its own locations. Many of the security measures taken by AT&T to secure VoIP must also be deployed by an enterprise on its own devices to be fully effective. For example, an enterprise should have a security policy in place that serves as the foundation of its security. An enterprise must secure its infrastructure by providing server-based and network-based security mechanisms. The enterprise must also maintain its servers and personal computers up to date with patches and anti-virus software to mitigate against Denial of Service attacks. Monitoring for security events through the use of logging and intrusion detection, and following up with investigations to determine cause and response, are needed so that an enterprise can reach more quickly to suspected security incidents and hopefully reduce potential damage.

AT&T can support customers in their efforts to provide security on their customer premises for VoIP through the AT&T Managed Security Services discussed below.

AT&T Managed Security Services

AT&T offers a family of managed security services that can be used either as an extension of a customer's security capability or to completely implement and operate large portions of a customer's security environment. AT&T's managed security services include:

- AT&T Internet Protect with Distributed Denial of Service (DDoS) Defense
- AT&T Managed Network-Based Services such as the AT&T Network-based Firewall Service and the AT&T Secure E-mail Gateway
- AT&T Managed Firewall Service Premises-Based
- AT&T Personal Firewall Service
- AT&T Managed Intrusion Detection Service

AT&T Professional Services can provide further customized security support beyond the AT&T Managed Offers discussed above.

Summary

At AT&T, security is an integral element of all services. Security for AT&T Voice DNA flows from AT&T's world-class experience in IP and Telephony Security. Security is integrated from the beginning of the AT&T OneProcess Service Realization Process and maintained throughout Lifecycle Management. AT&T has developed an AT&T Voice DNA Security Architecture that strengthens the service at potentially vulnerable points. This security architecture deploys a "Defense In-Depth" approach to provide a multi-layered secure environment. Security mechanisms are deployed throughout the service to provide seamless and effective security.

Customer-premises security is a critical component of end-to-end VoIP security. Customers can leverage AT&T Managed Security Services including AT&T Professional Services to secure their enterprise networks.

At AT&T, security is on-going process requiring constant vigilance, and AT&T Voice DNA is constantly monitored for new threats that could impact service.