OVERVIEW

VoIP and Security

Preserving the Integrity, Availability and Confidentiality of VoIP Communications

As businesses converge their voice and data networks to support their business applications, new security challenges are introduced. Integration of automated business functions and real-time collaboration – while great for productivity – increase risk and exposure. Add to that, the growing number of "outsiders" in the supply chain who need access to the network – and all the day-to-day details involved in their clearance and validation.

Networks are fast becoming the corporate central nervous system, playing a role few analysts could have predicted a decade ago. When voice traffic is merged into the data network; call servers, gateways and telephones are now potentially subject to security breaches common in the IP world. Businesses need to know that conventional measures taken to secure the data network are inadequate for voice traffic and specialized security solutions are needed. Each endpoint, IP telephone or softphone is susceptible to attacks – call servers, media gateways, signaling gateway routers and firewalls all need to be secure as well.

VoIP is Subject to New Security Threats

The unification of voice and data on IP networks brings advanced features, savings and also potential security attacks such as:

- Denial of Service attacks on signaling or media traffic
- Compromised systems revealing confidential information or being used to break into others
- Eavesdropping on conversations or signaling traffic
- Interference with service functionality and advanced features
- Connection requests from non-subscribers
- Cloning of CPE

Without proper security, the exposure of the VoIP service to malicious attacks from external and internal sources is increased. AT&T has a comprehensive set of VoIP specific security systems, procedures and services enabling us to provide extensive VoIP security. AT&T deploys a number of state-of-the-art security mechanisms on its IP network to protect against denial of service, eavesdropping and theft or fraudulent use of services. For example, AT&T can rapidly identify threats, such as worms and viruses, on its IP network and respond before they impact the customer.

AT&T VoIP Security Objectives

As in our switched network, AT&T's VoIP security efforts help ensure the availability, integrity and confidentiality of our customer's VoIP service while simultaneously maintaining quality of service.

- To preserve the availability of the VoIP environment is to stop the denial or even deterioration of service functionality.
- To preserve the integrity of the VoIP environment is to prevent system functions or data from being either maliciously or accidentally corrupted and to prevent theft and fraudulent use of VoIP.
- To provide confidentiality in VoIP is to keep customer information secure and private.

External and Internal Protective Measures Protect the VoIP Services

AT&T has identified three security domains for VoIP. First, there's a protected domain within the AT&T core IP/MPLS infrastructure with detection and monitoring mechanisms that are proactive and innovative. A second domain, edge security, provides the interface between the protected AT&T core infrastructure and the external domain. Finally, there's the external domain that exists in the client enterprise where security protection is the obligation of the business.

AT&T's Core IP/MPLS Infrastructure Security: AT&T VoIP infrastructure elements such as the Call Control Element (CCE), Application Servers (AS), Media Servers (MS) and the OAMP servers are protected by state-of-the-art security mechanisms.

AT&T's VoIP Edge Security includes the application-aware border elements. The major security function of these border elements is to protect the infrastructure. The border elements help prevent DoS attacks, and also provide authentication, authorization and encryption services.

AT&T's VoIP Client Enterprise Security configures a customer specific solution to address security requirements and provides engineering of customer premises equipment for IP PBXs, LAN and WLAN access points. AT&T has certified interoperability with leading IP PBX manufacturers who provide significant security capabilities in their platforms. AT&T's Managed Security Services for customer networks can be leveraged for firewall security, intrusion detection, token authentication and security alerting services. AT&T Professional Services can also provide customized support.

A Preventative Approach to Security

- AT&T Security Policy and Requirements (ASPR) and the AT&T OneProcess Service Realization Process provide the security foundation for AT&T VoIP Services.
  - ASPR and AT&T OneProcess ensure that security is integrated into AT&T VoIP from the beginning.
- AT&T IP/MPLS security architecture provides:
  - State-of-the-art mechanisms to protect voice and multimedia services and applications and the VoIP network infrastructure from potential compromises.
  - Continuous monitoring of its IP Network to rapidly identify potential threats and respond with security measures.
- Based on work at AT&T, we've learned it's possible to spot unusual network patterns and security threats on our IP backbone well before attacks occur. By sampling the public Internet data that crosses our network daily – about 6.767* petabytes – we can monitor and track unusual traffic patterns that could be the early stages of an attack.

In an era when everything is networked, the network is truly the best front line for security.

*As of July, 2006.