NEW PRODUCT/ PRESS RELEASE

FOR IMMEDIATE RELEASE

http://www.adaptivedigital.com
Adaptive Digital Technologies, Inc., 525 Plymouth Road, Suite 316
Plymouth Meeting, PA 19462
Contact: Tina Marcinek, Marketing Coordinator, 610-825-0182 x115
Email: tina.marcinek@adaptivedigital.com

Adaptive Digital Technologies Announces Support for the VoIP Encryption Protocol SRTP

Secure Real-Time Transport Protocol (SRTP) Performs Authentication and Encryption of RTP Packets Providing Protection for IP Voice and Video Packet Traffic

Plymouth Meeting, PA, June 11, 2009 - Adaptive Digital Technologies, the leading provider of telecom and Voice over IP DSP software solutions and voice quality enhancing algorithms, today announced optimized support for the Secure Real-time Transport Protocol (SRTP). Through the use of encryption, SRTP enables secure, confidential real-time voice and video communication over IP networks, including networks that are otherwise unprotected such as the public Internet. SRTP has been adopted as a standard by the Internet Engineering Task Force (IETF) and is designated RFC-3711.

A VoIP system is essentially a data network, based upon shared media communication. When a voice call is transmitted over an IP network, it is susceptible to the same security threats as is normal data traffic. These threats include interception, eavesdropping and snooping, call hijacking and spoofing, call tracking, and toll fraud. Once a victim is hijacked, he or she may also be subject to denial of service.

A call originating from a VoIP phone is converted from an analog signal into a series of digital, IP packets, which are transmitted across the network, and reassembled into voice at the receiving end. When a voice (or data) packet travels from its source to its destination over the public Internet, it travels from the source's Local Area Network (LAN) through the public Internet to the destination's LAN, and then to its final destination. In the case of voice, the source and destination may be VoIP phones. In the case of data, the source and destination tend to be computers and servers.

There are many access points within a LAN and within the public Internet where voice and data packets can be intercepted and exploited. A packet may pass through a dozen or more routers at as many different locations before reaching its destination. It is therefore far easier to eavesdrop on an unprotected VoIP phone call than it is on a traditional analog telephone call. The reason is that physical access to the traditional telephone network is more limited and better controlled.

Since there is little control over the routing of voice packets through the Internet, the best way to prevent eavesdropping and other exploitation is to encrypt the data in the voice packets. Even if encrypted packets are intercepted, it is extremely difficult for the interceptor to decode the voice without having the security codes that are required to do so.

SRTP is a security profile for RTP (Real-time Transport Protocol), another IETF standard. Through the use of its default encryption type, 128-bit AES, SRTP adds confidentiality, message authentication, and replay protection to RTP voice and video data. SRTP can be used in conjunction with RTP header compression.

A significant technical issue with VoIP security has been the tradeoff between protection and performance. With standard data encryption, the latency caused by the encryption/decryption process would degrade voice quality. SRTP performs the authentication and encryption of RTP packets in such a way that latency and voice quality are unaffected, and payload overhead is only minimally affected.

As VoIP services experience a healthy growth rate, unfortunately so do online threats; they are becoming more treacherous and destructive each day. The VoIP market is demanding robust security features to protect online interactions and personal privacy. Product developers and equipment manufacturers must meet or exceed those expectations while maintaining the performance that VoIP users demand.
Product page: http://www.adaptivedigital.com/product/protocol_stacks/srtp.htm

About Adaptive Digital Technologies – (www.adaptivedigital.com)
Adaptive Digital continues to meet and exceed the current and future requirements of service providers, equipment manufacturers, system integrators and developers by bringing superior voice quality to speech-based applications. Adaptive Digital's highly optimized DSP Algorithms/Solutions include network, line, and acoustic echo cancellation, high-density conferencing, speech compression, telephony, and voice quality algorithms. Recognized internationally for its quality software, Adaptive Digital's customers include British Telecom, Cisco Systems Inc., Cantata Technology, Digium®, General Dynamics, Motorola, Northrop Grumman, Sonus, and Texas Instruments.
Adaptive Digital is a member of the Texas Instruments' Third Party Developer Network and is located in suburban Philadelphia, Pennsylvania (USA).

###