liberty-i

Strategies for Lawful Intercept

Contents

Introduction

Public access venues like guest networks, HotSpots and Digital Cites pose a unique security challenge to the industry. As the number of public access venues and the number of nomadic users continue to increase dramatically, the requirement for new security mechanisms and the ability to aid law enforcement officials in their duty to protect society has become a paramount concern.

Security for network operators and subscribers to those networks has always been a key part of Liberty-izone Ltd"s technology. Our Wireless/Wired Intelligent Network Gateways (W.I.N.G.) supports both user and network security features to address a variety of issues being faced in such networks.

Our Gateways safeguard the user by employing features like Dynamic Address TranslationTM (DAT) and intelligent NAT (iNAT). These features translate the users" IP addresses thereby making it impossible to attack their computers from the Internet. W.I.N.G also support SSL login pages and VPN technologies that allow users to encrypt traffic.

In order to secure the network itself, W.I.N.G provides secure management interfaces and IPSec tunnels. It also provides network self-preservation and virus mitigation by employing session rate limiting and automatic MAC address blocking. User access to the network is moderated by features like Home Page Redirection, support for RADIUS, Credit Card and Property Management Billing Systems that enable enforcement of a variety of authentication methods like UAM, Smart Clients and 802.1x

To address liability issues for Venue Owners and Public Access Service Operators (PASOs), Liberty-i W.I.N.G. units support Terms of Use/Agreement pages that can be displayed to the Users. This forces the user to acknowledge the code of conduct they are expected to follow while using the network.

Though all the features stated above adequately address the security requirements of the users and the networks, they fall short of the unique requirements for lawful intercept (LI). The remainder of this paper outlines our LI strategy.

Whatis.com defines Lawful Intercept as follows "Lawful interception (LI) is the legally sanctioned official access to private communications, such as telephone calls or e-mail messages. In general, LI is a security process in which a network operator or service provider gives law enforcement officials access to the communications of private individuals or organizations. Countries around the world are drafting and enacting laws to regulate lawful interception procedures; standardization groups are creating LI technology specifications."

Definition

Requirement of LI in Public Access Networks

Most public access technologies rely on some kind of Network Address Translation (NAT) while providing access to visitors. This is done primarily to save public IP addresses, which tend to be expensive. NAT offers security to the end user by restricting access to the end user computer from the Internet and in the process offers anonymity to a public user. This anonymity presents challenges when Lawful Intercept is required.

There is a huge concern that public access networks will provide a safe-haven for users who want to carry out illegal activities on the Internet. These activities include illegally downloading copyrighted material from the Internet, sending threatening emails or engaging in illegal activities in chat rooms. Additionally, venue owners who offer public access networks and utilize them as a marketing vehicle do not want to have their brand associated with any negative activity on the Internet or be exposed to the potential liabilities associated with not taking the appropriate measures to safeguard such activities.

Liberty-i provides a range of public access Gateways that use the W.I.N.G. Service Engine Software to provide seamless access to public users. Our solutions enable any kind of user with varied client configurations to get onto the network without making any changes or adding client side software to their laptops or handheld devices. While our technologies simplify the process of getting access, we are acutely aware of the Lawful Intercept issues and requirements. Liberty-i has a detailed set of solutions and strategies that enable Public Access Service Operators and Venue Owners to comply with Lawful Intercept requirements.

LI using Public Address Assignment

The NSE provides features that enable automatic provisioning and assignment of publicly routable IP addresses. With the IP-Upsell feature, all users accessing the public access network can be forced to have a public IP address. The traffic of such users does not undergo Network Address Translation and can be traced back to the original user. Additionally, the NSE can also be configured to turn its Dynamic Address TranslationTM (DAT) feature OFF, allowing users with DHCP option enabled to access the network.

liberty-i

LI using Trace-Back Logs

The tracking logs carry the following information. The NSE provides tracking logs, which can be enabled to monitor all the port assignments for the users accessing a public network. These tracking logs enable you to trace-back to a particular MAC address and Username based on port and IP information available to an external site that has been attacked, hacked or used in an illegal fashion.

. 1) Time Stamp

. 2) Source IP

. 3) Source Port

. 4) Destination IP

. 5) Destination Port

. 6) Translated IP

. 7) Translated Port

. 8) Translated Destination IP

. 9) Translated Destination Port

. 10) User Details   a. MAC Address b. Local IP assigned c. Subnet d. Type of user (RADIUS, PMS, Credit Card, XML, Admin Added…) e. Username (if available)

liberty-i

LI using Tunneling

The L2TP Tunneling feature enables the W.I.N.G device to act as an L2TP Access Concentrator (LAC) and initiate single or multiple L2TP tunnels to different L2TP Network Servers (LNS). This capability can be used very effectively with the RADIUS Realm Routing feature to initiate tunnels based on the user Realm or Network Access Information (NAI). Realm specific traffic can be routed to a private network specific to that realm through these tunnels.

L2TP tunneling requires authentication with the „home" RADIUS server and since all the subscriber traffic is tunneled to the ISPs „home network", all the traffic can be monitored for Lawful Intercept purposes.

LI using Standard Protocol

There are numerous Lawful Intercept standards and numerous Lawful Intercept Forums. A short list of these can be accessed on the Global LI Industry Forum.

LI is a sensitive issue since it involves issues pertaining to privacy rights. There is a debate on whether LI strategies help protect privacy rights by enabling methods to isolate and precisely target specific users or whether these strategies provide a tool to invade on privacy rights. As this debate continues, PASOs and Venue Owners are faced with providing solutions dictated by current, local legislation.

There are quite a few "standards" in place today and Liberty-i feels that there isn"t a commonly accepted or widely used standard. Liberty-i continues to track these standards bodies and will work with the industry to incorporate widely accepted standards and practices applicable to a public access Gateway.

Conclusion

As Internet usage and the introduction of new applications like VoIP in a public access environment continues to increase, Service Providers will be required to provide more tools to aid law enforcement officials in tracking criminal activity over the Internet. Public access Gateways play a critical role on connecting nomadic users to public access networks, and are the ideal place to start the process of tracking illegal activity.

Lawful Intercept is important and Liberty-i W.I.N.G already has several features in place to aid PASOs and Venue Owners in supporting LI requirements. Liberty-i is committed to tracking this part of the industry and providing new LI features as standards solidify and market requirements dictate additional techniques approaches.