Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 3, Issue 11

Are Lawful Intercept Standards and Solutions in Denial about Denial-of-Service attacks?

by Dr. Supranamaya “Soups” Ranjan

With the May 2007 deadline for CALEA compliance getting closer, debates surrounding the social and moral ramifications of Lawful Intercept (LI) have begun raging once again. However, an issue that has neither been initiated nor discussed at length is whether the LI solutions are sophisticated enough to handle a clever adversary. Are LI solutions and standards in denial about denial-of-service attacks? The short and scary answer is yes, since a clever adversary can either launch attacks that thwart successful interception or exploit vulnerabilities in an LI system to launch other attacks. In the first case, an adversary can prevent Law Enforcement Agencies (LEAs) and ISPs from successfully intercepting targeted events and traffic data by simply launching a denial-of-service attack on the ISP's infrastructure. Secondly, a poorly architected LI solution may introduce new points of vulnerability within an ISP's network, leading to much larger attacks against the ISP’s infrastructure post-compliance. The picture may appear gloomy, but ISPs can proactively address the challenge either by deploying LI solutions with built-in security capabilities, or by complementing LI deployments with proven network security solutions.

LI Solutions

All LI solutions can be characterized either as active, passive or hybrid. Active LI solutions consist of an intercept device interacting directly with network equipment such as media gateway control servers to obtain all the flows that match the user/service targeted by an LEA. In contrast, passive LI solutions sniff traffic off the wire, and the traffic is then analyzed offline by the intercept device and matched against the target. A hybrid LI solution is one that performs the initial target match passively against sniffed traffic, and on successful match, it configures the network equipment actively to intercept the media streams corresponding to the target.

Attacker Model

Irrespective of whether the intention is to deny successful interception or to exploit LI infrastructure to launch other attacks, attackers have access to an extensive and bewildering set of techniques that they can use to achieve their goal.

To illustrate the ease with which an attacker may thwart successful interception, consider an attacker who learns of an impending warrant against his VoIP phone number. His first reaction would probably be to stop all VoIP communication. Next, however, he could begin a "spam flood" attack targeted at the ISP(s) most likely to execute the warrant. In order to bring down the LI infrastructure, the attacker could launch a layer-7 SIP flood with his VoIP phone number as the originating number. In order to execute the warrant, the ISP would begin intercepting all the packets in the flood, and depending on which portion of the LI infrastructure is the least provisioned in terms of resources, one or all of the following components could be affected:

- Access link between the routers and intercept device can be congested since the routers start forwarding the entire packet storm.
- System resources of the intercept device may be exhausted during a SIP flood for constructing in-memory the association of SIP control channels with the corresponding RTP sessions.

Moreover, the agility and flexibility with which Internet identities can be obtained allows an attacker to launch a "smoke gas" attack. Consider an attacker who has learned of a warrant issued against him. Owing to the prevalence of dial-up VoIP solutions such as those offered by AOL and Netzero, and soft-phone software such as Skype, the attacker could quite easily obtain several new accounts, and initiate phone calls from each of these new accounts to himself. Alternatively, the attacker could lease out botnets, install soft-phone software on the zombie machines and commandeer them to dial his phone number simultaneously. In contrast to the aforementioned attack, each phone call would originate from a unique phone number and the LI systems would parse these calls to build the detailed call graph. Some botnets have been known to consist of as many as 200,000 machines. Even if, under a conservative assumption, each of these machines were behind dial-up access (64 Kbps), the attacker would be able to create a flood of 1.28 Gbps — enough to congest an OC-12 or GigE link in an ISP. In addition, building a call graph with that many identities may stress the CPU and memory resources of the intercept device itself. Lastly, the call quality of legitimate callers would certainly suffer, since the media gateway controllers within the ISP would be expected to stop admitting new calls during the call storm.

The publicly addressable components of an LI system such as the reporting portals also introduce new vulnerabilities into an ISP's infrastructure. An attacker could initiate a buffer overflow exploit against the Web portal in order to gain backdoor entry into the ISP's infrastructure. Exacerbating this is the fact that the tools and resources for achieving such exploits are quite easily available. The attacker could begin with ICMP pings to determine publicly accessible machines and continue with port scans and OS fingerprinting techniques to determine open services on a machine, and then install malware known to exploit those services. Once the attacker has gained backdoor entry into the ISP's infrastructure, he could eavesdrop on all communications and parse all of the traffic. He could determine if a subpoena has been initiated against him, and thereby stay a step ahead of LEAs in the intercept battle.

Why exactly would this be important for carrier networks and ISPs? Well, a lot of the DoS, DDoS, scan and worm attacks seen to date on the Internet have been launched by thrill-seeking script kiddies, cyber extortionists looking to make a quick buck, or by spammers looking for un-patched, vulnerable machines so that they could add them to their bot armies. However, once ISPs become compliant with CALEA and ETSI in 2007, the scenario will very likely change as “cyber mafias” could gain yet another customer. In fact, criminals or terrorists who, upon learning of impending intercept warrants against them, could be expected to approach cyber mafias to prevent successful interception. The results could be disastrous, with cyber attacks launched as fast as warrants are issued.

Unfortunately, ISPs and carriers will bear the brunt of such a mafia nexus. Imagine being an ISP that suddenly starts fielding a huge number of phone calls from disgruntled customers who couldn’t check their e-mails, couldn’t access their banking accounts and couldn’t order lifesaving drugs online, all because they were being DDoSed for opening up a cyber warrant against a particular target.

LI Security Solution

Fortunately, solutions and techniques that have been developed to solve the general problem of Internet security can be applied to securing LI infrastructure as well. The pertinent requirements of such a security solution would call for visibility across all the layers of the OSI stack as well as scalability to the high-speed links found in carrier-class networks. It is imperative to point out that, since every network has different traffic characteristics, an effective carrier-class security solution must adapt on the fly to subtleties in traffic patterns to provide a high detection rate while minimizing the false-positive rate (defined as the instances where legitimate traffic is classified as malicious).

Once an attack is discovered, it can be mitigated before it affects the LI infrastructure or even the ISP’s network, thereby protecting the integrity of the intercept. Common mitigation methodologies such as Access Control Lists and Blackholing or null-routing can be used to drop all attack traffic at the edge routers of the ISP, before it affects the rest of the network. However, in some cases, it may be desirable to further investigate the attack traffic, which can be achieved via mitigation solutions such as Sinkholing or re-routing attack traffic to a different part of the network where it can be scrubbed and further analyzed. This can serve as an important tool for LEAs, who can then inspect the attacks to look for circumstantial evidence that can further implicate a target for interfering with investigation.

In summary, the deployment of a Lawful Intercept solution without a corresponding carrier-class security solution can not only compromise an ISP's ability to comply with a warrant from an LEA, it can also increase the risk of attack on core service and routing infrastructure.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.