DHS Science and Technology (S&T) Directorate
Telephony Denial of Service

Convergence of Telephony Denial of Service

The public voice network has become the target of many attacks, including Telephony Denial of Service (TDoS), robocalls (automated telephone calls), SWATing (anonymously filing police reports to provoke a police raid) and bomb threats. TDoS is a flood of malicious inbound calls that target public-safety response systems such as 911. If these were coordinated with a physical terrorist attack, a TDoS incident could be particularly disruptive, resulting in a large number of victims unable to connect with emergency services. TDoS also could affect other organizations such as financial services entities by denying consumers access to voice contact centers. If synchronized with a Distributed Denial of Service (DDoS) attack against a financial service entity's internet and mobile presence, a TDoS attack could prevent customers from contacting their banks.

DDoSD
Distributed Denial of Service Defense

911 Call Center Impacts

The underlying enabler for TDoS attacks is the ability to use automation to cheaply and easily generate hundreds or thousands of simultaneous calls. Also, it is very easy to spoof calling numbers and other attributes, making it very difficult to differentiate legitimate calls from malicious ones. This issue makes other attacks more severe and difficult to mitigate such as robocalls, SWATing and bomb threats. Robocalls—in the form of telemarketing and scams—will become worse as attackers use spoofing to bypass the simple "blacklist" applications used by consumers and enterprises. SWATing and bomb threats will become more common with services such as those from the "Evacuation Squad," which can be used anonymously through websites and Bitcoin. Further, the shift from traditional "land lines" to mobile phones and Voice over IP and new features in the Next Generation 911 system such as text and video could create new ways for attackers to generate disruptive calls. The DHS S&T Cyber Security Division (CSD) and SecureLogix are focused on solving these issues and applying solutions.

Emergency Management Systems: TDoS 911

The project's goal is to shift the advantage from a DDoS attacker to the network administrator by developing the capability to authenticate callers and detect fraudulent call spoofing. SecureLogix is working in multiple research areas to solve TDoS-related issues and applying the results to these voice system security concerns. These solutions—based upon a series of filters that assign a risk-threat score to every call—will enable 911 systems administrators to better respond to and manage TDoS threats.

Accomplishments to Date

- Defined and tested attack signatures that identify legitimate and fraudulent calls
- Developed a Proof of Concept based on SecureLogix's PolicyGuru
- Identified multiple partners who have agreed to pilot results and are currently in contract negotiations (source selection is sensitive)

Performer

SecureLogix
13750 San Pedro Avenue, Suite 820
San Antonio, Texas 78232
SecureLogix Website

Homeland Security
Science and Technology

To learn more about Telephony Denial of Service Attacks, contact Dan Massey, program manager, at Daniel Massey's email address

2014-mm-dd