DHS Science and Technology Directorate

Distributed Denial of Service Defense (DDoSD)

Distributed Denial of Service (DDoS) Attacks

DDoS attacks are used to render key resources unavailable. Hackers accomplish a DDoS attack by literally sending so much web traffic at a target that it is unable to function. A classic DDoS attack disrupts a financial institution's website and temporarily blocks the ability of consumers to conduct online banking. A more strategic attack makes a key resource inaccessible during a critical period. Some examples of this type of attack may include rendering a florist's website unavailable on Valentine's Day, slowing or blocking access to tax documents in mid-April or disrupting communication during a critical trading window. Prominent DDoS attacks have been conducted against financial institutions, news organizations, Internet security resource providers and government agencies. Any organization that relies on network resources is considered potential targets.

DDoS Attacks Are Becoming More Damaging

Over the past five years, the scale of attacks has increased tenfold. In 2008, one of the largest DDoS attacks to date was a few tens of megabits per second. By 2016, DDoS attacks have grown an order of magnitude to hundreds of megabits per second. It is not clear if current network infrastructure could withstand future attacks if they continue to increase in scale. Further, DDoS attacks have made use of the rapid growth in Internet of Things devices that often with limited security.

Shifting the Advantage to Defenders

The DDoSD project is working to increase deployment of best practices that would slow attack scale growth, specifically a technique called Internet Best Current Practice 38 that blocks forged packets at or near the source. It also is seeking to defend networks against one terabit per second (Tbps) scale attacks through development of collaboration tools suitable for medium-scale organizations. Last, the project is working to defend emergency management systems—both current 911 and Next Generation 911 systems—from Telephony Denial of Service (TDoS) attacks.

Accomplishments to date

Spoofer Tool Released—The University of California San Diego has released a toolset that allows an organization to test if it properly blocks spoofed addresses.

DDoSD
Distributed Denial of Service Defense

Demonstration of defense against 250 Gbps simulated attacks—All of the one Tbps DDoSD teams have demonstrated an initial capability to withstand a 250 Gbps attack through several different techniques. Many of the techniques rely on new network services such as software defined networks.

Prototype to detect invalid telephony calls released—The SecureLogix Policy Guru prototype was enhanced to provide new capabilities to detect and block spoofed calls sent to a 911 system or other critical phone system.

Upcoming milestones

- Wide-scale measurement of source address validation and network configuration changes to block spoofing in multiple networks.
- Demonstration of defense against 500 Gbps simulated attacks from the one Tbps defense teams.
- Pilot results from deploying TDoS protection at two major 911 emergency management centers—Miami/Dade County and City of Houston—and a top bank.

Performers

- Colorado State University, Fort Collins, Colorado
- University of California San Diego, San Diego, California
- University of Southern California Information Science Institute, Los Angeles, California
- Waverley Labs, Waterford, Virginia
- Galois, Portland, Oregon
- University of Oregon, Eugene, Oregon
- SecureLogix, San Antonio, Texas
- University of Houston, Houston, Texas

Homeland Security
Science and Technology

To learn more about DDoSD, contact Program Manager Daniel Massey at sandt-cyber-liaison@hq.dhs.gov

2016-11-21