Camouflage of Network Traffic to Resist Attack (CONTRA)

William Weinstein
Janet Lepanto
The Charles Stark Draper Laboratory, Inc.

Overview

By monitoring Internet traffic in the vicinity of a given host—which can be a single computer or a gateway device with multiple computers behind it—an attacker can observe communications originating from and destined to this host. Even if the message contents are encrypted, the IP addresses must remain visible for the packets to be properly routed throughout the open Internet. So the attacker can eventually discover the identity of all of the hosts with which this host communicates. In particular, if this host belongs to a collaborating set, such an attacker would be able to identify the remaining members of the set from simply observing the traffic in and out of this host. Moreover, by analyzing the traffic patterns the attacker may be able to glean useful information and also identify “high-value” hosts within the collaborative against which to mount a denial-of-service (DOS) attack.

The CONTRA system camouflages traffic among a set of collaborating hosts, and camouflages critical hosts by spreading the identity of each across multiple IP addresses. One realization of this system comprises a virtual network topology and supporting protocols that operate on top of the network transport layer. The protocol employs a synergistic combination of multipath relay transmissions, K-out-of-N message encoding, packet encryption, heteromorphic packet relay and dynamically changeable IP addresses. The characteristics of the virtual network topology and protocols together impede the attacker’s ability to analyze traffic patterns, limit the visibility of real IP addresses to those cooperating hosts that are topologically adjacent to a host whose traffic is being monitored, and allow hosts to spread their IP identities and to modify the IPs associated with a host. These system characteristics will reduce the ability of a hostile entity to mount a successful denial-of-service attack against the operations among the set of hosts.

Problem

In the Internet environment it is relatively easy to mount a distributed denial-of-service attack against a specific host, often associated with a specific IP address. There is currently no good, easily-deployable mechanism for preventing such targeted attacks, and no good way to overcome the effect of such an attack in the short run, i.e., a few hours.

Because real IP addresses are used to route traffic they are necessarily visible to anyone capable of monitoring traffic over a link on the public Internet. By looking up network assignments at a domain registry, an attacker could identify the set of hosts assigned to a particular organization; and by analyzing traffic patterns among specific set of IP addresses, an attacker could identify “high-value” hosts within the set that would make good targets for a DOS attack.

Furthermore, even if the contents of messages are encrypted, the attacker may observe the traffic pattern variations in response to known network activities, which could be initiated by the attacker, among the set of IP addresses and deduce the relevant information with regard to the organization within the set.

Approach

CONTRA spreads the identity of critical hosts over multiple IP addresses and transmits data to those hosts using K-of-N threshold encoding. To impede traffic to the host an attacker needs to flood more than N-K of the addresses. In order to prevent an attacker from associating the addresses that define the host, CONTRA employs multipath relay transmissions, packet encryption, heteromorphic packet relay and dynamically changeable IP addresses in order to camouflage the traffic pattern and the organization among the set of cooperating CONTRA hosts.
CONTRA prevents an attacker who is sniffing the Internet near a CONTRA-equipped host from analyzing the content, distribution, and actual volume of traffic between that host and other CONTRA hosts. It limits the exposure of real host IP addresses to those CONTRA-equipped hosts that are topologically adjacent, in the CONTRA virtual network (Vnet), to the host being observed. In addition to camouflaging the organization within the set of CONTRA equipped hosts, it prevents an attacker sniffing outside of a site that contains a “high-value” host from determining the real IP addresses used by that host at any specific time.

Finally, even if denial-of-service (DOS) attacks are launched against some CONTRA hosts—such attacks will have to be launched in the absence of the knowledge of the value of the targets—the remaining CONTRA hosts will be able to continue their operations.

Although CONTRA operates as a closed virtual network, it is possible for outside users to access services provided by the set of hosts if some of the CONTRA hosts are designated as access gateways. Interaction between such an outside user and a CONTRA gateway may range from being totally anonymous to being encrypted with user authentication. In any case, the set of CONTRA hosts can provide such services without revealing its internal organization. However, while an outside user can interact with CONTRA hosts across the CONTRA Vnet in this manner, these users and their hosting systems are not afforded the full protection provided by CONTRA.