TARP: Ticket-based Address Resolution Protocol

Wesam Lootah, William Enck, Patrick McDaniel

Abstract

•IP networks fundamentally rely on the **Address Resolution Protocol (ARP)** for proper operation.

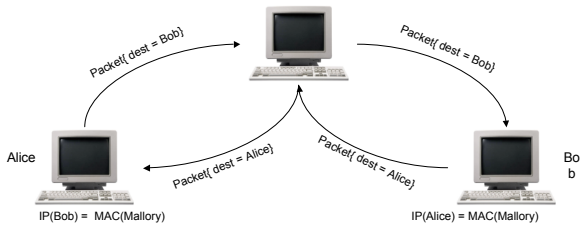
•Unfortunately, vulnerabilities in the ARP protocol enable a raft of IP-based impersonation, man-in-the-middle, or DoS attacks.

•Proposed countermeasures to these vulnerabilities have yet to simultaneously address backward compatibility and cost requirements.

•**TARP, Ticket-based Address Resolution Protocol** implements security by distributing centrally issued secure MAC/IP address mapping attestations through existing ARP messages.

•TARP improves the costs of implementing ARP security by as much as **two orders of magnitude** over existing protocols.

ARP Poisoning



Example of a Man-In-The-Middle attack in progress. Both Alice and Bob believe they are talking directly to each other.

Protocol Overview

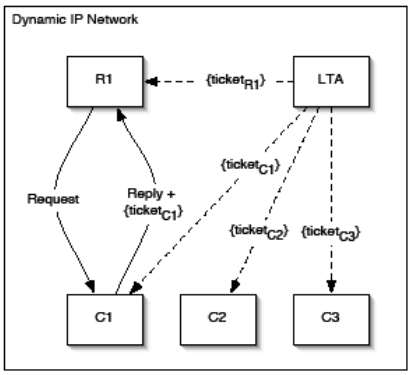
•TARP implements security by distributing centrally generated attestations.

•These attestations, called *tickets*, authenticate the association between MAC and IP addresses through statements signed by the Local Ticket Agent (LTA). Each ticket encodes a validity period.

•To securely perform address resolution using TARP,

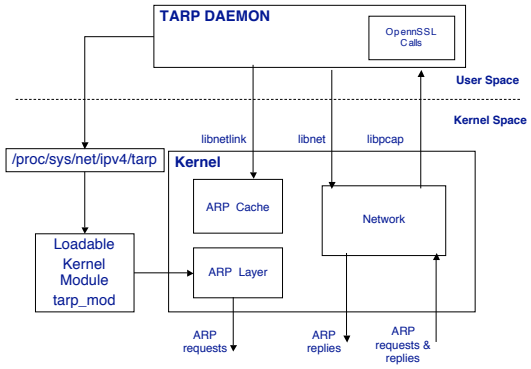
- •a host broadcasts an ARP request. The host with the requested IP address sends a reply, attaching previously obtained ticket.
- •The signature on the ticket proves that the LTA issued it,
- •The requesting host receives the ticket, validating it with the LTA's public key. If the signatures is valid, the address association is accepted; otherwise, it is ignored.

TARP in action



Hosts receive TARP tickets during the initial DHCP exchange, and include them with each ARP reply.

Implementation Architecture



TARP was implemented as Linux Loadable Kernel Module and a userspace daemon

Results

Protocol	Average (µs)	Std. Deviation (µs)	Overhead (µs)
ARP	1178.59	259.98	N/A
S-ARP	6579.57	415.99	5401.02
TARP	**1276.54**	**262.47**	**97.95**

Roundtrip delay for ICMP echo requests with caching (1000 requests).

Protocol	Average (µs)	Std. Deviation (µs)	Overhead (µs)
ARP	1178.59	259.98	N/A
S-ARP	12479.71	571.47	11319.12
TARP	**1364.21**	**253.93**	**185.62**

Roundtrip delay for ICMP echo requests with caching (1000 requests).

This work has been accepted and will appear in ACSAC 2005