CSCI 5271 Exercise Set 4

Alex Biedny

November 23, 2020

Problem 1. ARP By Other Means

(a) To first consider confidentiality, the trusted authority method provides much more confidentiality than the traditional method. By only transmitting ARP queries to the trusted host, traffic between any host that needs an ARP query and the trusted host is sent only between those two parties. As the traditional method broadcasts ARP queries to the entire network, the whole network will learn that a host is looking for the MAC of another host, rather than keeping it confidential like the trusted authority method. This method is also a boon to integrity, as there is no chance that a host on the network disobeys protocol and improperly responds to the ARP query.

Availability wise, so long as the trusted host remains operational not much will change from the traditional method. However there will be an accountability benefit, as the trusted authority is the one host responsible for recieving and replying to ARP queries.

(b) Considering confidentiality, this method is similar to the traditional method. The ARP queries are still broadcast across the network, so that data is available for all hosts to see. This method also does not improve integrity. Despite requiring a consensus of host responses to resolve an ARP query, it must be assumed that an adversary would have the ability to create a number of malicious hosts (perhaps a colelction of virtual machines on the same physical device). This would make it trivial to have all malicious hosts reply to the query in an adversarial manner, and have the host that sent the ARP query accept the adversarial reply.

This also negatively affects availability. As responses from every host are now required for every ARP query, there is much more data to process, and many more hosts to communicate with. This means that if a host is malfunctioning or behaving slowly, it would have a more severe effect here than in the traditional method. Similar can be said about accountability; as the hosts replying to the ARP query are many machines, if there are problems it is much harder to pin down what may have gone wrong, as the responsibility of replying to ARP queries is spread out.

Problem 2. TCP-Unfriendly

(a) Security wise, the problem is that adversarial hosts have no obligation to follow protocol. Under this system, an adversary could send packets as fast as they like. The router would likely see this and send the RST packet, but the host can simply not obey the RST packet and continue sending packets really fast.

The mechanism could possibly be adjusted so that it would be more effective against hosts that don't follow protocol. For example, the router could refuse to send packets from that host until the RST packet is obeyed and it sees that a new TCP conenction is being opened. Any effective mechanism would likely have to be implemented by the router, because the host does not have to obey protocol.

(b) Because adversaries control the content of the entire packet, an adversary would still be able to get around a blacklist by simply using another IP address in the src field of the packet header. Even if one IP address is blacklisted, the malicious host can just change the IP whenever it wants.

In addition, having this blacklist creates an availability vulnerability for everyone on the network. All an adversary has to do is send packets using the IP of another host on the network as the packet src, and then not respond to dropped packets appropriately. The router would blacklist the IP in the packet, and through this an adversary could get any IP blacklisted.

Problem 3. BGPSec Around the World

(a) The only security guarantee that this gives is making sure that the route follows the "expected" ASes. Becuase the originating AS does not use BGPSec, it would not pass on a ROA, and without a ROA there is really no mechanism to guarantee that the AS advertising a route actually owns those IPs. It would be possible for an adversary in this system to lie and advertise that they own a certain IP range for example, because without the ROA signed by IANA there is no way to verify this.

(b) This provides some level of security because so long as the ROA is forwarded along, every AS in the path that uses BGPSec is able to verify that the IPs advertised for that path do actually belong to the AS advertising it. This does not guarantee the integrity of the path itself however, and an adversary could take advantage of the non-rejection for missing signatures in the path to route traffic wherever they wish, possibly through a compromised AS.