

Denial of Service or Denial of Security?

How Attacks on Reliability can Compromise Anonymity

HY558- Roman Čížek

The authors aimed to the connection between reliability and security. Instead of blanket denial-of-service (DoS) attack, an adversary may selectively affect reliability of the system in those states that are hardest to compromised, thereby causing the system to enter less secure states. They explore an attack where DoS is performed whenever the communication cannot be compromised. Selective DoS is easier to carry out than an attack to whole system, and can be more effective. Faced with poor reliability, many users will naturally attempt the communication again, presenting more opportunities for attack.

They analyzed success of this attack on these systems:

- Conventional anonymity systems
 - Low-latency – Tor
 - High-latency – Mix networks (Mixmaster, Mixminion)
- Systems featuring reliability
 - Cashmere
 - Hydra-Onions
- Salsa

Tor

Communication over Tor happens through tunnels that are sent via multiple (default 3) Tor routers. Tor routers are picked in proportion of their advertised bandwidth. The tunnel is compromise if attacker controlled first and last router in the tunnel. If the adversary has not have dishonest nodes in the first and last position of the tunnel, but in another position he will use selective DoS attack to stop the traffic in this tunnel. This will give to the adversary another chance to compromise tunnel. Under this attack, a tunnel is reliable only if the first and last nodes are compromised, or if it is composed of only reliable honest nodes.

Examples of results if in tor will be 50% of malicious nodes, than conventional analysis suggests that 75% of all paths should be secure, whereas under the selective DoS attack, only 33% of the successful paths are uncompromised.

Possible defense against selective DoS is used guard nodes. Guard nodes are honest nodes which are always used like a first node in a tunnel. Users with honest guard nodes may suffer in terms of reliability but their anonymity will never be compromised. However, in another way, guard nodes actually make the selective DoS attack more powerful, since the probability that a single successful tunnel will be compromised is actually higher using guard nodes.

Mix networks

Mix-Net systems consist of a series of such mixes and provide unlink ability between a sender and recipient. Each message is sent through a sequence of mixes that is chosen randomly from available mixes. Only when the adversary controls every mix in the forwarding path will the anonymity of a message be compromised.

The issue of reliability became apparent as volunteer-run nodes were often unavailable or offline, one approach was to introduce pingers to keep track of the reliability of nodes. Pingers attempt to relay traffic through all mixes and keep track of the messages. To avoid malicious nodes manipulating the rankings, the pinging traffic is forwarded through the anonymous network itself. Mix clients then select routes based on these reliability rankings. Alternative strategy is to send copies of the messages, or fragments thereof, through independent paths.

Authors analyze security and reliability using conventional analysis and after using DoS selective attack. For example in conventional analysis, with length of the path 5, even if 50% of all mixes are compromised, only 3% of all messages can be read. In DoS attack the result is the same, but to achieve the same level of reliability, a sender has to send the messages more times, which in turn provides more opportunities for the adversary to capture the message.

One response to increase security under the DoS attack may be to use longer paths. But the results show that, when reliability, and not just security, is taken into account, mix networks have a fundamental limit on the number of compromised mixes. When a majority of nodes are corrupt, mix networks are “unsafe at any path length.”

Cashmere

Cashmere is an anonymous routing layer that uses relay groups instead of single-node mixes to provide increased connection reliability. Each group is composed of a set of nodes that share a common public/private key pair. Each node is assigned a unique nodeID and each relay group a unique groupID. The node that receives the message is named the relay group root. The root decrypts the message, broadcasts the payload to all members of his relay group, and then sends the message to the next relay group in the forwarding path. Node recognizes itself as the destination when it can decrypt the message payload.

To compromise message anonymity, the adversary needs at least one malicious node in the each relay group leading up to destination. Finally, the destination itself must be malicious for the route to be compromised.

To affect cashmere routing by DoS attack is only necessary to compromise relay group root. If the adversary will control relay group root he is able to drop any connection that goes through.

Hydra-Onions

Hydra-Onion system was designed to resist active adversaries dropping onions during transmission. Copies of Hydra-Onion are sent in cascade and in each step, a mix will forward two copies to two different mix servers at the next step.

To compromise the path it is enough to have at least one dishonest node at each step. If the adversary will not have dishonest mix in each step he will perform a denial of service and drop all traffic sent to them.

Salsa

It is an anonymous communication system designed to overcome the scalability problems in traditional mix systems. As in Tor, a tunnel is built between the initiator and the recipient via proxy routers for anonymous communication. Layered encryption ensures that each node knows only its previous and next hop in the tunnel. The nodes used for the tunnels are randomly selected from the global pool of nodes, even though each node has only local knowledge of a small subset of the network.

Salsa is based on a distributed hash table (DHT) that maps nodes to a point in an ID space corresponding to the hash of their IP address. There are two basic mechanisms in the Salsa architecture: (1) a node lookup mechanism and (2) a tunnel building mechanism. The former returns the IP address and public key of node in the DHT closest to a given point in the ID space. The latter is used to build a Tor-like tunnel. Both schemes use redundancy to avoid attacks and both are susceptible to the selective DoS attack.

To build a tunnel the initiator chooses r random IDs and looks up the corresponding nodes (first set of nodes). Keys are established with each of these nodes. Each of the first set of nodes does a lookup for r additional nodes (second set of nodes). A circuit is built to each of the nodes in the second group, relayed through one of the nodes in the first group. Again, the initiator instructs the second set of nodes (via the circuits) to do a redundant lookup for a final node. One of the paths created between the first and the second set of nodes is selected and the final node is added to the tunnel.

A tunnel can be compromised if there is at least one attacker node in every stage of the tunnel. Also by end-to-end timing analysis, the tunnel will be compromised if the first and last forwarding nodes are compromised. Tunnel building process is subject to a public key modification attack. If all r nodes in a particular stage are compromised, they can modify the public keys of the next set of nodes being looked up.

The idea of selective DoS attack is to deny service to trustworthy nodes so that user traffic moves toward compromised nodes. The compromised nodes will try to abort the tunnel building process whenever the tunnel cannot be compromised. The attackers should deny service in two cases. First, if the last node is honest, and there is an attacker in the second

last stage, that attacker will perform DoS, unless all r nodes in that stage are malicious. Also, if the attacker nodes are selected to forward traffic in a tunnel, they can deny service if the tunnel has not been compromised.

They compare the performance of three attack methodologies on the Salsa building mechanism. First one consists of conventional passive attacks in which the tunnel is compromised whenever there is an attacker in every stage or via end to end timing analysis. The second methodology involves action modification of the public key of nodes being looked up whenever the attackers have compromised an entire stage. And the third methodology, nodes try to selectively DoS the tunnels which are likely not to be compromised.

They find that the public key modification attack does not yield a significant advantage over conventional attacks. Their analysis shows that Salsa design is extremely vulnerable to DoS attack. If they have 20% dishonest nodes in Salsa network they get 6.82% compromised tunnels for conventional security analysis, but for selective DoS attack it was 19.14% of compromised tunnels.

Conclusion is that they have shown that in anonymous communications systems, denial of service attacks reduce anonymity considerably. This shows that availability and anonymity are linked and reliability must be assured against adversaries and not just random failures. They show that routes with few honest nodes will be subject to DoS, and only fully honest or fully compromised paths will survive. Their work strongly demonstrates that mechanisms to address reliability, as well as preventing denial of service, must be designed and evaluated with criteria from security engineering and not merely network engineering.