Computer Security II Project Proposal
Woo Young and Nathan Dautenhahn
September 3, 2009

Group Members: Woo Young (3 credits) and Nathan Dautenhahn (4 credits)

We propose to develop a method that will identify malicious edge nodes performing a correlation attack in a Tor network. At this point, the first step is to determine the feasibility of different approaches to the problem. One potential method would be to perform a correlation analysis of edge nodes in the internal Tor network. If one could identify that two nodes were communicating with each other, it could be deduced that these two nodes are communicating for the purpose of performing a correlation attack. Another possibility is to use a centrally stored set of auditing systems within the Tor network that determine if a node's bandwidth claims are false. Another way is to insert a trust mechanism into the network in order to perform analysis on which systems are performing malicious activities. The basic idea is that we propose to determine a mechanism by which to identify nodes performing a correlation attack.

A previous approach has been developed to detect nodes that have lied about there bandwidth capabilities [1]. This is useful because by claiming high bandwidth a node will be selected by the Tor routing algorithm with greater probability. Therefore, detecting that a node does not have the capable bandwidth it claimed, it can be deduced that that node is malicious. The approach used to detect these malicious nodes is to use an observation based reputation system. Meaning that each end user (i.e. Tor client) performs statistical analysis of each circuit it uses to determine if a node in that circuit is being untrustworthy in its bandwidth claims. It is important to note that this method is dependent upon malicious nodes providing false bandwidth claims. If a node has high bandwidth and is malicious this method will not work. Additionally, this approach requires a lot of data to be captured by end nodes and a statistical approach, which can take some time to aggregate into a decision on whether a node has lied about its bandwidth claims.

Success will be determined by whether or not we can determine a successful and reliable method to perform malicious edge node identification. It will be too resource intisive to develop a complete Tor testbed to evaluate this method. Therefore, success will be measured by the ability to detect two nodes communicating with each other inside a small simulated Tor network.

Bibliography

1: Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker, Low-Resource Routing Attacks Against Anonymous Systems, 2007