

Intern Requirement

No. of students required	1-2
Preferred Discipline	<ul style="list-style-type: none">• Computer Science• Computer Engineering
Prerequisites/ Skills Required	<ul style="list-style-type: none">• Strong interest in computer and security• Preferably with experience in C Programming• Foundational knowledge in networking principles

Project Details

Title	Security of Tor Public Infrastructure
Overview/Background	<p>Tor is an anonymity network which hides the origin of web traffic by routing it through a series of nodes. Since each Tor node only has knowledge of the previous and next nodes, Tor makes it difficult for other network nodes to detect the source of web traffic.</p> <p>Although Tor employs various security mechanisms to protect the anonymity and privacy of its users, it is not invulnerable. The traffic could be monitored at the exit node where it leaves the Tor network to be forwarded to its final destination.</p>
Objectives/Scope/ Deliverables	<p>The aim of this project is to assess the method(s) in which a rogue Tor server could be used to trace back the originating IP address of the web traffic.</p> <p>Scope:</p> <ul style="list-style-type: none">• <u>Proof-of-concept for trace back</u>. The interns will be tasked to demonstrate how a Tor server node could be circumvented to trace back the origin of web traffic.• <u>Detection of rogue servers</u>. The interns will research into mitigation methods to detect rogue Tor servers performing trace backs on the web traffic. <p>Deliverables:</p> <ul style="list-style-type: none">• a set of source codes to demonstrate the method(s) to perform the trace back on a rogue Tor server• method(s) to detect rogue Tor servers.
Project Duration	<input checked="" type="checkbox"/> 2-4 months, or <input checked="" type="checkbox"/> 6 months