Aufgabenstellung

Modul:	Dept I BAA FS26

Titel:	Praktische De-Anonymisierung im Tor-Netzwerk: Einfluss von Circuit Padding auf Website-Fingerprinting im Shadow Netzwerk Simulator
Ausgangslage und Problemstellung:	Mit dem Tor Netzwerk kann der eigene Internetzugang anonymisiert werden. Verschiedene Gegenmassnahmen wurden entwickelt um diese Anonymisierung wieder rückgängig zu machen. Mit Website Fingerprinting (WF) werden Muster von Websites aufgezeichnet, wie die Anzahl der ein und ausgehenden Paketen. Damit können Rückschlüsse auf die aufgerufenen Webseiten gezogen werden. WF Angriffe können auf einem kompromittierten Tor Entry Node oder einem passiven Beobachter wie dem ISP ausgeführt werden (3). 2018 wurde als Gegenmassnahme Circuit Padding eingeführt, welches adaptive Dummy-Pakete zwischen Client und Middle Node einfügt. Damit wird das Traffic Muster gegenüber WF verschleiert. Im Tor-Client kann das circuit padding konfiguriert werden und ist standardmässig aktiviert. Mit dem 2011 vorgestellten (1) Shadow Netzwerksimulator können Tor-Netzwerke lokal und reproduzierbar simuliert werden. Website Fingerprinting Attacken können damit zuverlässig simuliert werden (2). 1: https://apps.dtic.mil/sti/tr/pdf/ADA559181.pdf 2: https://petsymposium.org/popets/2023/popets-2023-0125.pdf 3: https://petsymposium.org/popets/2016/popets-2016-0027.pdf
Ziel der Arbeit und erwartete Resultate:	- Wie verändert sich die Erkennungsrate der DF Angriffe mit unterschiedlichen Circuit Padding Settings? - Welche bekannten Limitationen simulierter und laborbasierter WF Angriffe sind in der Literatur dokumentiert, und wie sind die experimentellen Ergebnisse dieser Arbeit einzuordnen? - Aufgebaute Shadow Simulationsumgebung in einer VM von labservices.ch - Ein Website Fingerprinting Dataset wurde erstellt - Deep Fingerprinting (DF) WF Angriff durchgeführt mit dem Tool WFlib DF: https://github.com/deep-fingerprinting/df WFlib: https://github.com/Xinhao-Deng/Website-Fingerprinting-Library
Gewünschte Methoden, Vorgehen:	- Literatur und Technologieanalyse (Aufarbeitung aktueller Stand der Technik) - Experiment. Versuchsaufbau einer Tor Network Simulation im Shadow Tool. Durchführung von Website Fingerprinting Angriffen.
Kreativität, Methoden, Innovation:	Den Einfluss von Circuit Padding auf Website Fingerprinting Angriffe unter reproduzierbaren lokalen Bedingungen testen können.

Sonstige Bemerkungen:	

Projektteam

Student:in 1:	Oliver Staub
Betreuer:in:	Eskhita

Auftraggeber

Firma:	HSLU
Ansprechperson:	Dr. Radwan Eskhita
Funktion:	Dozent
Strasse:	
PLZ/Ort:	
Telefon:	0796657472
E-Mail:	radwan.eskhita@hslu.ch
Website:	