Published on *University of Colorado* (https://www.cu.edu)

Security and Privacy in TOR Network [1]

About This Specialization

In this MOOC, we will learn about TOR basic concept and see how they protect the security and privacy of users and resist censorship. We will examine how TOR realize the anonymity and utilize its service by downloading and using Tor browser software. A recent attack on TOR's application flow control called sniper attacks is analyzed. We introduce the hidden service provided by TOR and show how it can be denonymized. We will learn how to setup a hidden server to provide web service on AWS instance. We will also learn the best practices and operational security in providing the hidden services. We will learn how to manage the hidden server using Tor circuit and configure the web server not to reveal the software version information. We also show how it can be defended. To improve TOR's performance, we discuss the cloud based TOR and their implementation. By the end of this course, you should be able to utilize TOR browser to protect your privacy, set up hidden service on current interface that protect your servers and make it anonymous, you will choosing entry guards wisely since your adversary will try to attack them with DDoS traffic and force you to choose their relay as your entry and exit router. We will also learn the basic components of both censorship and censorship resistance systems, and the scheme deployed by these systems and their attacks.

Language
English

Level
Intermediate

Commitment?
9 hours/week

For More Information or to Enroll

Created by:

Groups audience:
MOOCs
Right Sidebar:
MOOC: DDos Attacks and Defenses

Source URL:https://www.cu.edu/mooc/security_and_privacy_tor_network2.0

Links
[1] https://www.cu.edu/mooc/security_and_privacy_tor_network2.0