COPPE
UFRJ

PESC
Programa de Engenharia de Sistemas e Computação

Ciclo de Seminários

Matt Wright

Director of the Center for Cybersecurity, Rochester Institute of Technology

Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning

Website fingerprinting enables a local eavesdropper to determine which websites a user is visiting over an encrypted connection. State-of-the-art website fingerprinting attacks have been shown to be effective even against Tor. Recently, lightweight website fingerprinting defenses for Tor have been proposed that substantially degrade existing attacks: WTF-PAD and Walkie-Talkie. In this work, we present Deep Fingerprinting (DF), a new website fingerprinting attack against Tor that leverages a type of deep learning called Convolutional Neural Networks (CNN) with a sophisticated architecture design, and we evaluate this attack against WTF-PAD and Walkie-Talkie. The DF attack attains over 98% accuracy on Tor traffic without defenses, better than all prior attacks, and it is also the only attack that is effective against WTF-PAD with over 90% accuracy. Walkie-Talkie remains effective, holding the attack to just 49.7% accuracy. In the more realistic open-world setting, our attack remains effective, with 0.99 precision and 0.94 recall on undefended traffic. Against traffic defended with WTF-PAD in this setting, the attack still can get 0.96 precision and 0.68 recall. These findings highlight the need for effective defenses that protect against this new attack and that could be deployed in Tor.

segunda-feira

5 de novembro

11:00hs

Sala H324B

http://www.cos.ufrj.br/seminarios