BSides Ume 2025

Contribution ID: **25**

Type: **not specified**

Bypassing Dynamic Taint Analyzers

Tuesday 10 June 2025 13:00 (45 minutes)

Dynamic taint analysis (DTA) is widely used to detect information flow vulnerabilities by tracking the propagation of taint tags at runtime. However, existing DTA approaches rely on the assumption that the underlying type system is secure. In reality is it often not the case. In this presentation we will look at how attackers can manipulate object types and directly alter taint labels, effectively bypassing taint tracking mechanisms.

Length

Optional: Speaker / convener biography

Yufei Wu, PhD student at Umeå, researches software security, focusing on program analysis, software vulnerabilities, and taint tracking.

Primary author: WU, Yufei

Presenter: WU, Yufei

Session Classification: Talks

Track Classification: Talks and presentations