The Tigress Endpoint Protection Tool

Transition to Practice

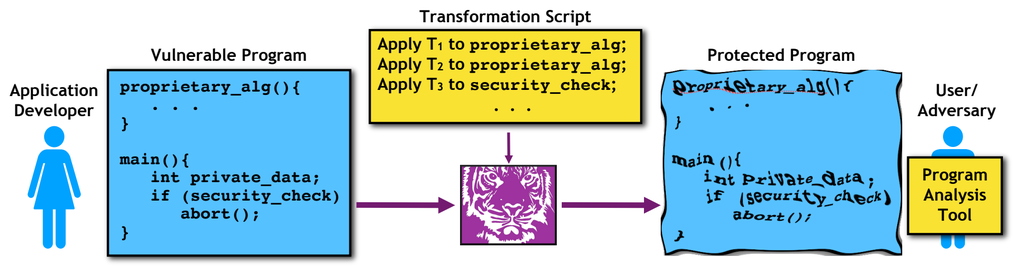
Christian Collberg

University of Arizona

https://tigress.wtf

https://grand-re-challenge.org

In a prototypical MATE (Man-At-The-End) scenario an application developer protects an asset (keys, IP addresses, media, security checks, intellectual property) from discovery or tampering by a malicious end user. The developer uses an end-point protection tool to apply a sequence of code transformations to slow down attacks.

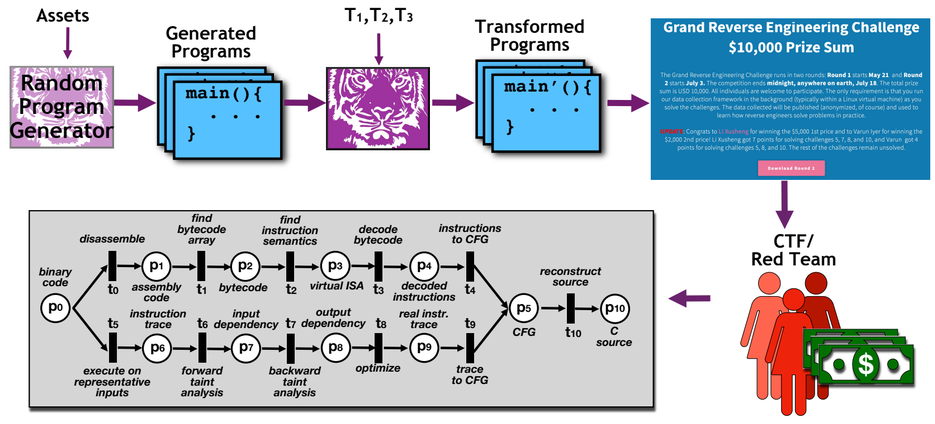


The goal of the *Tigress* tool is to provide a complete set of code transformations that protect any asset, in any application, on any platform, against any attack, while balancing performance vs. level of protection.

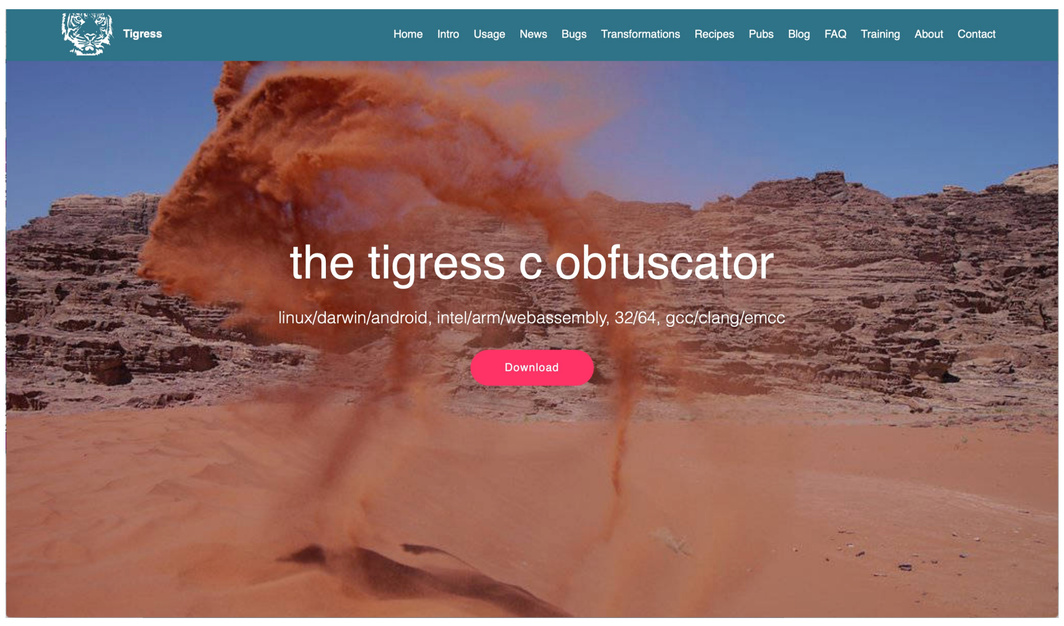
Key Problems to be Addressed

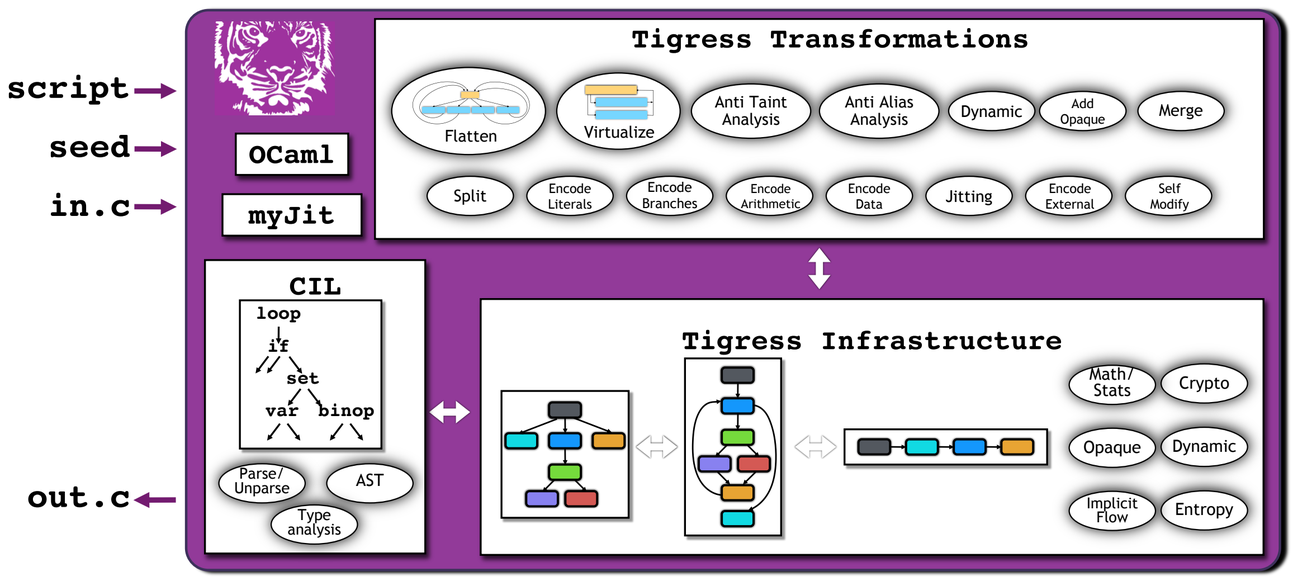
- Comprehensive set of **protective transformations** allowing any asset to be protected
- Comprehensive **platform coverage** (X86/ARM/Wasm, Linux/MacOS/Windows, 32/64, …)
- Comprehensive **correctness** testing to ensure real programs can be protected
- Comprehensive **security evaluation** giving users confidence in the level of protection afforded their applications
- **Performance** improvements allowing low-power platforms (IoT devices) to be protected

Tigress has been developed to serve both the academic and industrial communities as we believe learning from both will best drive progress in the field.



A key issue in the MATE scenario is how to evaluate the protection afforded by a sequence of transformations. We are running CTF-like events where we collect gigabytes of highly granular data showing how reverse engineers attack protected software. The goal is to use this data to build detailed attack models. Without access to the Tigress tool it would be impossible to generate realistic challenges.

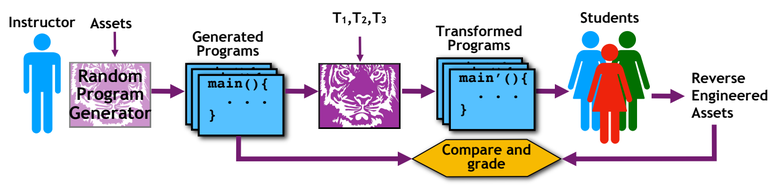




Societal Impact

- Academics use Tigress as an adversary to evaluate how novel program analysis/malware detection algorithms fair against highly obfuscated code
- Industry uses Tigress to experiment with software protection before investing in commercial tools
- Strong endpoint protection is necessary to protect IoT devices against end-user attacks (extracting proprietary data including P and user credentials)

Impact on Education



- Tigress has been used in Computer Security courses to generate reverse engineering assignments
- We are working on auto-grading solutions

Broader Impact

Achieving a trusted cyberspace requires securing all components: server-side components, networking components, user-facing endpoint components (web-browsers, cars, smart meters, home IoT devices). Attacks on endpoints by those who (often legitimately) operate them are frequently ignored when doing security analysis, yet they often form an easily penetrable part of the attack surface. Freely available endpoint protection tools is a step in solving this problem.