HITBSECCONF AMSTERDAM - 2021

emproof Safeguard what counts

Workshop: Semi-automatic Code Deobfuscation

Tim Blazytko

@mr_phrazer

tim@blazytko.to

https://synthesis.to

Personal Details

co-founder of *emproof GmbH*, binary security researcher and former PhD student

- **trainings:** reverse engineering and trainings
- **full-time:** design and evaluation of obfuscation techniques
- **research:** code deobfuscation, fuzzing and root cause analysis

Today

- code obfuscation in APT malware
  - opaque predicates (X-Tunnel)
  - mixed Boolean-Arithmetic (FinSpy)
- semi-automated code deobfuscation
  - symbolic execution and SMT solving
  - program synthesis

Slides and Code

https://github.com/mrphrazer/hitb2021ams_deobfuscation

Automatic Detection and Removal of Opaque Predicates

- opaque predicates in X-Tunnel (APT128 malware)
- symbolic execution
- SMT solver
- identification of opaque predicates
- removing/patching opaque predicates

Task #1: Detection and Removal of Opaque Predicates

Try it on your own with `remove_opaque.py`.

- Reproduce the identification and patching.
- Try it also on other functions like `0x40b4a0` or `0x40bc50`.
- Find more functions with opaque predicates on your own.

Automatic Simplification of Mixed Boolean-Arithmetic

- MBAs in FinSpy (commercial spyware suite, sample based on Obfuscator-LLVM)

- MBA simplification via program synthesis

- verification of MBA simplifications

- symbolic exploration

- synergy of symbolic execution and MBA simplification

Task #2: Automatic Simplification of Mixed Boolean-Arithmetic

Try it on your own with `simplify_finspy.py`.

- Reproduce the symbolic exploration and MBA simplification.
- Try it also on other functions or basic blocks like `0x405374` or `0x4097a0`.
- Find more functions and basic blocks with MBAs on your own.

3-day Training: Software Deobfuscation Techniques

- state-of-the-art code (de)obfuscation techniques
- deep dive into topics demonstrated in the workshop
- next virtual training (more will come)
  - 23-25 August 2021
  - 09:00-17:00 SGT/GMT+8

https://sectrain.hitb.org/courses/software-deobfuscation-techniques-hitb2021sin/

Conclusion

- opaque predicates and mixed Boolean-Arithmetic
- slides, code and samples: `https://github.com/mrphrazer/hitb2021ams_deobfuscation`
- next training: `https://sectrain.hitb.org/courses/software-deobfuscation-techniques-hitb2021sin/`

Thank you very much for your active participation!