Reverse Engineering for Ethical Hackers

CAE Tech Talk 20 FEB 20

Dr. Bryson Payne, GREM, GPEN, CEH, CISSP
Director, Center for Cyber Ops Education
Professor of Computer Science

UNG | UNIVERSITY *of* NORTH GEORGIA
THE MILITARY COLLEGE OF GEORGIA

About Me

- Dr. Payne: Ph.D. in computer science from Georgia State University, 6 years as a CIO, 22 years teaching CS/IS/Cyber in the University System

- Author of *Teach Your Kids to Code*, 3rd book *Hacking for Kids* comes out in June

- CISSP, CEH, GPEN, SANS/GIAC Reverse Engineering Malware (GREM)

- Coach for the #1 NSA Codebreaker Challenge team UNG Cyber Hawks (2019)

1ˢᵗ Place 2019 (532 schools)

Our Story

- *UNG built an NSA Codebreaker-winning cyber operations team by introducing a special topics course on Reverse Engineering from an ethical hacker's point of view, now a regular part of the course catalog.*

- *From reverse-engineering Solitaire and CMD.exe to disassembling Windows, Linux and Android malware with Ghidra and the FLARE VM, all the way to creating keygens to defeat ransomware and get users' files back, I will share UNG's "secret recipe" for getting students excited about reverse engineering and the Codebreaker Challenge.*

How to Win @ NSA Codebreaker in 6 easy steps

- Create a Reverse Engineering course
- Make it fun
- Place in top 10 (#3 in 2018)
- Add more to the RE Course
- Win (#1 out of 532, in 2019)
- Repeat (hopefully)

The flow of the course

- Day 1: Hack Solitaire and CMD.exe
- Demo RE of malware using all the tools (brbbot: IDA, ProcMon, RegShot, etc.)
- Tackle progressively tougher malware/ ransomware starting with strings/floss, then Ghidra/IDA, OllyDbg/WinDbg/x64
- [then x64, Linux, Android, based on pref.]
- Ghidra+python to create decryptors
- Circle back to advanced malware w/tools

Reverse Engineering Resources

- Textbook: Practical Malware Analysis – Michael Sikorski et. al.

- Supplemental Texts:
  - Practical Reverse Engineering, Bruce Dang et.al & Reversing: Secrets of Reverse Engineering, Eldad Eilam et. al.

- Two awesome resources: Point3 Escalate and NSA Codebreaker Challenge

- Team communication: Discordapp.com

Free Virtual RE Environment

- Virtualbox.org
- Win10 + FLARE VM, REMnux, Kali
- Modern.ie for FREE Win10 VM
- FLARE setup (includes Ghidra): https://www.fireeye.com/blog/threat-research/2018/11/flare-vm-update.html
- Options: Volatility, CheatEngine (min install), mimikatz, Solitaire from WinXP…

Demo Day 1: Hook 'Em

Day 2: Hack CMD.exe

Progressing through levels of RE

- Start with static analysis: strings and floss
- Progress to IDA/Ghidra for disassembly/decompiling
- Move to Dynamic analysis (debuggers, changing values in memory, changing program flow, rewriting code in memory)
- Build back up to Behavioral analysis with ProcMon, ProcessHacker, RegShot, ProcDot

Payne's Pyramid of RE

Automated

- HybridAnalysis.com, Malwr.com, Cuckoo Sandbox

Behavioral

- ProcHack, ProcMon, RegShot, ProcDot
- Wireshark, fakedns, INetSim

Dynamic Analysis

- x64dbg, WinDbg, OllyDbg, edb, IDA debugger, Android Studio and adb, etc.
- Volatility, Redline

Static Analysis

- Quick: strings, floss, PE Studio, VirusTotal
- Slow: IDA, Ghidra

One option: Point3 ESCALATE

- Paid CTF platform with Win, Linux, Android, x86/x64, ARM and more
- Academic discount w/reassignable seats
- Start with static analysis: strings and floss
- Progress to IDA/Ghidra, then debuggers, tools, then disassembly, decompiling
- Can build your own 'malware' by hiding flags, but ESCALATE has all the levels

Malware Reversing: Decryptors

- Most firms/individuals won't be able to do REM, so one goal is to write a key generator (keygen) or decryptor (especially for ransomware)

- Once we reverse a malware (disassemble or decompile first with automated tools), we can use Python to automatically search for the key/password/flag and decode it

- Then, anyone can run it ☺

Next Steps/Staying up to Date

- Previous years' Codebreaker Challenges
- BleepingComputer, ID-Ransomware
- REM mailing lists/forums
- Consider joining **Bugcrowd** and **Hackerone** and other bug bounties
- Firmware RE, Car Hacking, IoT, Medical Devices, Exploit development…

Thanks!

- Thanks to the NSA, CBC and CAE teams!
- Thank you for attending today, and see you in Codebreaker 2020!
- Q&A
- Bryson.payne@ung.edu
- [small book plug: *Hacking for Kids* is on presale now at Amazon ☺]