Understanding arbitrary code execution: a case study

Sasha Toscano

Advisors: Marc Langheinrich, Carlo Alberto Furia

GitHub repository:
https://github.com/Fireblast9/ACE

Project activities

1) Explanation of what Arbitrary Code Execution (ACE) is

Definition, Vulnerabilities examples, Possible threats

2) Analysis of the case study (Pokémon Emerald, 2004)

“Pomeg glitch”, Study of the consequences (analysis of decompiled code)

3) Discussion about advancements in protections against ACE

Recent scenarios analysis, Current “State of the art” protection against ACE

Schedule

Week 1-2: finish ACE definition (project activity 1) and start analyzing the decompiled code to prepare the case study section (https://github.com/pret/pokeemerald) + study and learn Assembly

Week 3-7: complete the case study (project activity 2): explain what happens when the "pomeg glitch" occurs, understand and show off what exactly happens on a code level, analyze the risks on the market perspective (exploits, dangers, etc.)

Week 8-11: examine what is considered a "state of the art" protection against ACE with recent papers and studies, elaborate on what can, should and has to be done to prevent ACE and ACE-like attacks (project activity 3)

Week 11-12: reviews and corrections