

Vulnerability of Simulation Executables

Brian Eoff



Introduction

“Remember that hiding secrets is hard” – Gary McGraw

Simulation executable security raises a great concern. Simulations by their very nature are large complex pieces of software containing proprietary algorithms and sensitive numerical data. Far too often the executables of Simulations are shared with other bodies without concern for the safety of the executable

How to Compromise an Executable

- Disassemblers
- Decompilers
- Behavior Monitoring
- Buffer Overflows

How to Protect an Executable

- Good Coding Standards
- Code Obfuscation (Layout, Data, Control)
- Encryption
- Client-Server Model
- Attacking Debuggers/Disassemblers
- Watermarking
- Tamper-Proofing
- Removal of Trade Secrets

Conclusion

“Given enough time, effort and determination, a competent programmer will always be able to reverse engineer any application.” – Christian Colberg