Tutorial Proposal for SIN 2009

Title: Secretes of Reverse Engineering Software

Abstract

Software reverse engineering is a two-edge sword. On one hand, it can be used for debugging, analysis of malware and viruses, and the discovery of any vulnerabilities, trapdoors, and illegally integrated code. On the other hand, it can be used for cracking software with the intent of breaking the licensing verification and copyright protection. Software products with weak copyright protection mechanism can jeopardize the existence of the software development companies. In this tutorial, popular techniques and tools for reverse engineering software will be presented. A number of examples and demonstrations will be shown on how reverse engineering tools can be used to expose and crack real software in order to bypass licensing and copyright protection schemes. In addition, the tutorial will present the most effective anti-cracking techniques that can be used to develop a tamper-resistant and unbreakable software.

Proposed Duration

Half day or three hours.

Intended Audience

Software developers, virus and malware analysts, developers of AV (AntiVirus) products, debuggers, and researchers or investigators interested in examining code infringement, illegal software use, pirated software, or copyright violations.

Prerequisite Knowledge

Basic software development and programming experience.

Detailed Outline

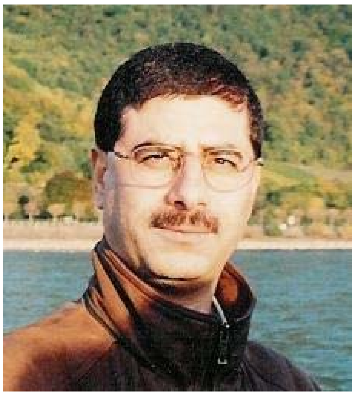
- What is Reverse Engineering?
- Why Reverse Engineering?
- What is Software Cracking?
- Legality and Ethics
- Approaches to Reverse Engineering
- Reversing Tools
- Executable Binaries: Structure and Format
- Types of Copyright Protection Schemes
- Anti-Reversing Techniques
- Most Effective Copyright Protection Schemes
- Beyond Disassembly and Decompilation
- Real Demos: Reversing Malware, Breaking Copyright Protection, Ripping Keygen Algorithms, Reversing JAVA Bytecode

Tutorial Goals

The primary goals of this tutorial are numerous. Here is a brief listing of some of the goals:

- Understand what is meant by reverse engineering and software cracking
- Explain the pros and cons of reverse engineering
- Present the laws and recent issues and legalities surrounding reverse engineering: when is it legal and when is it not?
- Present a brief and fundamental background needed for understanding reverse engineering such as binary executable formats, structure, platforms, and assemblers and disassembles as well as compilers and de-compilers.
- Teach how to browse and read efficiently and understand quickly compiler-generated assembly language code for IA-32 compatible processors, and explain the run-time and debugging environment of an application.
- Present popular tools used to reverse engineer software, and discuss in detail their features and differences
- Expose widely-used reverse-engineering techniques that are used by security malware and virus analysts as well as crackers
- Present the general principles behind modern-day malicious programs and how reverse engineering is applied to study, detect and neutralize such programs
- Show how to use reverse engineering to decipher an undocumented file format, APIs, or network protocol
- Show how reverse engineering is applied by crackers to defeat copyright protection technologies
- Present most effective techniques for preventing competitors and crackers from reverse engineering your code
- Demonstrate how to evaluate the effectiveness of copyright protection schemes used in software products
- Show how to use reverse engineering in finding the misuse of any shareware and open source code
- Explain what is meant by keygenning and show how reverse engineering can be used to rip keygen algorithm from protected code
- Explain the basic overview, strengths, and weaknesses of copyright protection technologies including DRM, watermarking, online activation, dongles, and cryptoprocessors.

Short Biography of Presenter



Khaled H. Salah is an associate professor of Computer Science. He received the B.S. degree in Computer Engineering with a minor in Computer Science from Iowa State University, USA, in 1990, the M.S. degree in Computer Systems Engineering from Illinois Institute of Technology, USA, in 1994, and the Ph.D. degree in Computer Science from the same institution in 2000. He has over ten years of industrial experience in embedded systems and software and firmware development of network protocol stacks and device drivers for ATM and Ethernet. He joined King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in September 2000. Dr. Salah is currently with the department of Information and Computer Science, teaching graduate and undergraduate courses in the areas of computer and network security, operating systems, VoIP, computer networks, and performance evaluation. Dr. Salah is an Editorial Board member of seven prestigious international journals including IET Communications, Elsevier JNCA, Wiley IJNM, and J.UCS. Over the past four years, Dr. Salah published 20 research articles in reputable international journals. He was the recipient of the departmental awards of Best Research and Best Teaching. His research interests are in computer and network security, computer forensics, malware analysis, Linux networking subsystem, VoIP deployment, performance analysis and design of computer systems and networks. Dr. Salah has a number of research projects and consultations on network firewalls, intrusion detection, and network security assessment and auditing. He is leading activities of the *Saudi Honeynet Project* to detect and analyze malware and viruses in KSA Internet. He has given a number of public talks and seminars on network and software security. He has also a number of recent articles which appeared in Saudi national newspapers and in international conferences on the subject of IT and network security. Dr. Salah is the founder and leader of the Security Research Group (SRG) at KFUPM. **Web Page:** http://faculty.kfupm.edu.sa/ics/salah

Technical Talks & Tutorials on Security

Below is a list of at least two-hour tutorials and talks given by the presenter. These are limited to talks related to security topics.

Title	Date	Place
Saudi Honeynet Project	March 15, 2009	College of Computer Science and Engineering, KFUPM.
Software Reverse Engineering	March 20, 2008	College of Computer Science and Engineering
Intelligent Firewall DoS Attacks and Countermeasures	Mar. 27, 2007	College of Computer Science and Engineering, KFUPM.
Effective Techniques against Software Cracking	Mar. 2006	College of Computer Science and Engineering, KFUPM.
Analysis of Internet Worm of August 2003	Sept. 2003	**KFUPM Auditorium, attended by more than 250 people, broadcasted live on KFUPM TV Channel, and video tapped.**