UNIVERSAL UNPACKER OF EXECUTABLE FILES

Jan Marek
Master Degree Programme (1), FIT BUT
E-mail: xmarek44@stud.fit.vutbr.cz

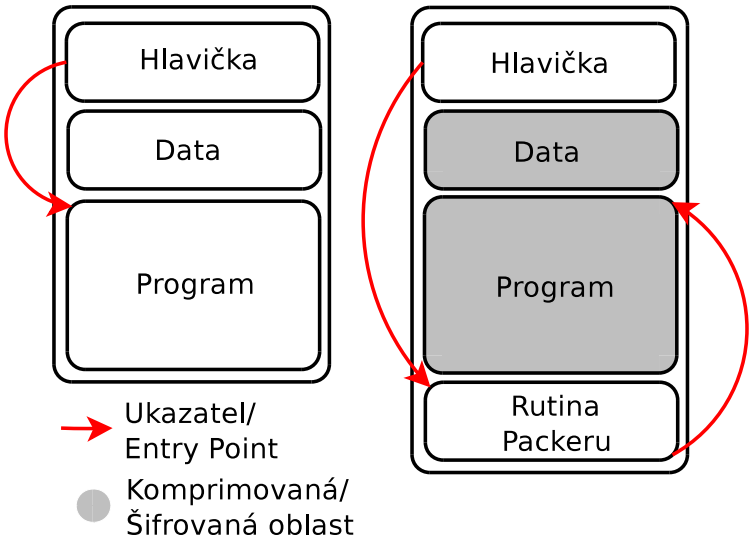
Supervised by: Jakub Křoustek
E-mail: ikroustek@fit.vutbr.cz

Abstract: The Goal of this work is to build universal unpacker of executable files aimed for robustness, extensibility and modularity. This work has several outputs, the first is C++ library designed for creating new unpackers and manipulation with executable files, the second one is an application for managing unpackers as plugins and the last one are several unpackers/plugins for use with this application. This work is created as a part of the project Lissom at FIT BUT.

Keywords: Unpacker, binary file, executable file, PE, ELF, library

1 ÚVOD

Packing spustitelných souborů se zabývá komprimováním, šifrováním a ochranou dat v souborech, a to bez změny jejich funkčnosti. Je hojně rozšířen mezi autory škodlivého softwaru, neboli malware, kteří ho využívají pro skrytí pravé podstaty jejich škodlivého kódu. Jak může vypadat jednoduše packovaný soubor ilustruje obrázek 1. V roce 2003 bylo packingem ochráněno asi 29% škodlivého softwaru, v roce 2007 již 80% [1]. Je tedy zřejmé, že obliba packingu mezi autory škodlivého softwaru stoupá a tím roste i poptávka po nových packerech. V roce 2007 vznikalo každý měsíc 10-15 nových packerů [1]. Z pohledu bezpečnosti je tedy nutné umět tyto ochrany účinně odstraňovat a mít prostředky, které umožní rychle a efektivně reagovat na nové packery. Tím se zabývá unpacking.



Obrázek 1: Ukázka funkce packeru.

Metody unpackingu se dělí na statické a dynamické. Dynamický unpacker komprimovaný program spustí, monitoruje jeho běh a snaží se najít místo, ve kterém program ukončí svoji unpackovací rutinu

a spustí původní kód, který je v tomto okamžiku umístěn v paměti. Unpackeru ho už stačí jen extrahovat a uložit [4]. Takové unpackery zpravidla nelze realizovat v přenositelné podobě. Je také možné je obelhat pomocí tzv. dynamických obran. Statický unpacker se snaží programy unpackovat staticky, tedy bez nutnosti komprimovaný program spouštět.

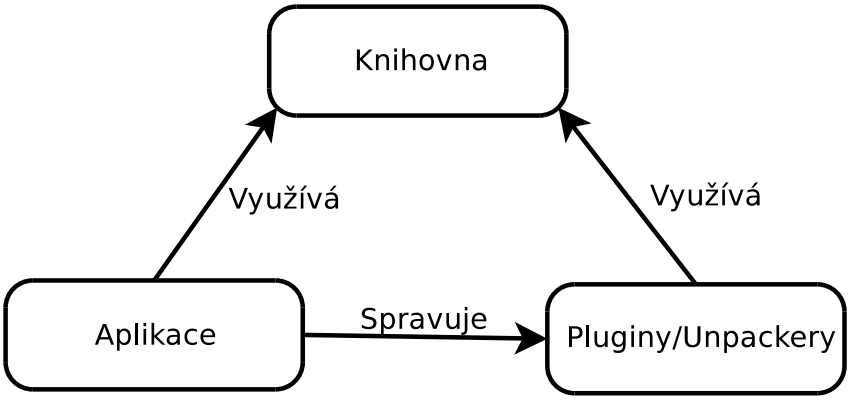
Specifickou oblastí unpackingu jsou tzv. Generické unpackery. Většina unpackerů je reakcí na některý konkrétní packer a je tedy jednoúčelová. Generické unpackery se snaží o dekompresi vstupního souboru bez znalosti konkrétních použitých metod nebo packeru, který byl k jeho kompresi použit, a vytvořit tedy zcela univerzální unpacker. Existuje řada takovýchto unpackerů, ale žádný zatím není zcela univerzální a vzhledem k neustálému vývoji packerů je pravděpodobné, že toho dosáhnout nelze. Zpravidla se jedná o rozsáhlé a komplikované programy, které jsou pomalé a obtížně modifikovatelné či rozšiřitelné. Většina metod generického unpackingu spadá do metod dynamických a k tomu patří i všechny jejich nevýhody.

Účelem této práce je návrh a implementace unpackeru, který bude do značné míry univerzální, a bude poskytovat prostředky pro udržování a prohlubování této univerzality.

2 UNIVERZÁLNÍ UNPACKER

Naším cílem není generický unpacker, ale vytvoření nástroje usnadňujícího tvorbu nových unpackerů a umožňujícího jejich snadnou správu. Výsledný unpacker, přestože bude složený z dílčích unpackerů, bude robustní a bude nabízet prostředky pro aktualizaci, vytvoření a doplnění nových unpackerů. Náš návrh řešení se skládá ze tří hlavních částí viz obrázek 2.

První částí je knihovna v jazyce C/C++. Ta nabízí objektové rozhraní pro práci s binárními soubory formátu PE a ELF a sadu metod a funkcí reprezentujících běžně používané operace, postupy a techniky pro unpacking. Tyto metody jsou vytvářeny na základě podkladů získaných jak při tvorbě nových, tak z analýzy již hotových unpackerů. Rozhraní pro práci se soubory vychází a využívá volně dostupných knihoven PeLib [2] pro PE a ElfIO [3] pro formát ELF. Knihovna poskytuje nad souborem jistou míru abstrakce, ale umožňuje a podporuje i práci na nízké úrovni. Je navržena tak, aby byla přenositelná přinejmenším mezi Unixovými OS a operačními systémy na jádru Windows NT. Z tohoto vyplívá, že její zaměření je téměř výhradně na statický unpacking.



Obrázek 2: Struktura unpackeru.

Druhou částí je aplikace pro jednoduchý managment unpackerů jako pluginů, a tím jejich snadné a efektivní využití zejména při automatickém zpracování. Pluginovací systém je založený na dynamických knihovnách v jazyce C/C++. Od autora nového unpackeru/pluginu se tedy očekává pouze vytvoření jednoduchého rozhraní dynamické knihovny skládajícího se z inicializační funkce, volitelné funkce poskytující podrobnější informace o pluginu a hlavní funkce tvořící unpacker. Řídící

aplikace poté takto vytvořené pluginy načítá a umožňuje jejich spuštění.

Poslední částí je sada zpravidla jednoúčelových unpackerů vytvářených při tvorbě knihovny. Jedná se o unpackery pro běžně využívané packery, přičemž řada z nich je vhodná pro demonstraci možností a funkčnosti knihovny.

3 VYUŽITÍ A AKTUÁLNÍ STAV

Unpacker je vyvíjen jako součást decompileru v projektu Lissom na FIT VUT v Brně. V současné době je k dispozici čtveřice unpackerů s řídící aplikací a základní stukturou knihovny. V rámci projektu byl také rozbalen Malware Psyb0t, packovaný pomoci UPX a upravený tak, aby nebylo možné ho unpackovat standardně. Další využití projektu může být v oblasti bezpečnosti, zejména jako předstupeň před analýzou spustitelného souboru (např. antivirový program). V kombinaci s aplikací pro detekci použitého překladače či packeru, která je také vyvíjena v rámci projektu Lissom, je pak možné unpacker využívat automaticky, bez nutnosti zásahu člověka.

4 ZÁVĚR

Výsledný nástroj nebude umožňovat univerzální unpackování jakéhokoli souboru, ale nabídne prostředky pro snadnější tvorbu unpackerů ve vyšším programovacím jazyce (C/C++) a jejich správu. A tedy využívání celé sady unpackerů jako jednoho, kde tato sada může obsahovat škálu různých unpackerů od jednoúčelových až po generické. Výsledkem je potenciálně silný unpacker s širokými možnostmi aplikace.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory grantu TAČR TA01010667 a výzkumného záměru MSM0021630528.

REFERENCE

[1] Babar, K., Khalid, F.: Generic Unpacking Techniques, National University of Science and Technology, Pakistan, 2009, ISBN: 978-1-4244-3313-1

[2] Porst, S.: PeLib An open-source C++ library to modify PE files [online], [cit. 2012-02-02], Dostupné na World Wide Web: <http://www.pelib.com>

[3] Finch, A.: ELFIO [online], [cit. 2012-02-02], Dostupné na World Wide Web: <http://elfio.sourceforge.net/>

[4] Bilge, L., Lanzi, A., Balzarotti, D.: Thwarting real-time dynamic unpacking, Proceedings of the Fourth European Workshop on System Security (EUROSEC '11), ACM, New York, NY, USA, 2011, Dostupné na World Wide Web: <http://www.syssec-project.eu/media/page-media/3/unpacking-eurosec11.pdf>