УДК 004.056.53

ЄФІМЧЕНКО Анастасія
КАПЛУН Валентина

РОЛЬ РЕВЕРСИВНОЇ ІНЖИНЕРІЇ У ЗАХИСТІ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація. *У статті проаналізовано проблеми, пов'язані з реверсивною інжинерією, досліджено зв'язок між реверсивною інженерією та захистом інформації. Аналіз інформаційних джерел показав, що зворотний інжиніринг може бути використана як для захисту інформації, так і для зламу ресурсів інформаційних систем. Зворотне проектування може допомогти виявити вразливості у програмному та апаратному забезпеченні для посилення безпеки.*

Ключові слова*: зворотний інжиніринг, вразливості, безпека, програмне забезпечення, апаратне забезпечення, захист інформації.*

Abstract. *The article analyzes the problems associated with reverse engineering, explores the relationship between reverse engineering and information protection. Analysis of information sources showed that reverse engineering can be used both to protect information and to hack the resources of information systems. Reverse engineering can help identify vulnerabilities in software and hardware to enhance security.*

Keywords: *reverse engineering, vulnerabilities, security, software, hardware, information protection*.

Вступ

Захист інформації є критично важливою складовою інформаційної безпеки. У сучасному цифровому світі, де зростає кількість загроз і атак на інформаційні системи, необхідно розробити ефективні заходи безпеки для забезпечення конфіденційності, цілісності та доступності інформації. У цьому контексті зворотне проектування, процес аналізу деталі, вузла або системи, є важливим для захисту інформації.

Зворотний інжиніринг (англ. reverse engineering) – аналіз компонентів, деталей або систем для виявлення їх структури, функцій та принципів роботи. Цей процес широко використовується для зворотного проектування програмного, апаратного забезпечення, електроніки, механізмів та інших складних систем, щоб зрозуміти їх функції та можливості.

Зв'язок реверсивної інжинерії з захистом інформації

Зворотний інжиніринг може використовуватися як засіб захисту інформації, так і як засіб зламу інформаційних систем.

З одного боку, зворотне проектування може бути корисною для інформаційної безпеки, оскільки вона дозволяє дізнатися, які заходи безпеки використовуються програмними та апаратними пристроями. Основними функціями реверсивної інженерії в захисті інформації є такі:

- *виявлення вразливостей*. Зворотне проектування можна використовувати для виявлення вразливостей у програмному забезпеченні, апаратному забезпеченні та інших складних системах. Аналізуючи структуру та функції об'єктів, зворотне проектування дозволяє виявити потенційні слабкі місця та вади, якими зловмисники можуть скористатися для несанкціонованого доступу або атак;
- *захист від несанкціонованого доступу*. Зворотне проектування можна використовувати для розробки механізмів безпеки, які ускладнюють або унеможливлюють несанкціонований доступ до системи. Аналізуючи протоколи зв'язку, механізми шифрування та автентифікації, зворотне проектування допомагає виявити потенційні слабкі місця та розробити ефективні заходи безпеки для запобігання несанкціонованому доступу.

З іншого боку, зворотна розробка може використовуватись для злому систем з метою викрадення або модифікації інформації. Захист від зворотного проектування, такого, як обфускація коду та використання шифрування, дає змогу захистити конфіденційну інформацію та запобігти розголошенню алгоритмічних і структурних рішень. Для запобігання зворотній інженерії розробники

можуть використовувати різні методи, як то: шифрування коду, захист від декомпіляції, віддалені служби захисту,ускладнення структури програмного забезпечення та інші.

Таким чином, зворотне проектування може допомогти розробникам підвищити рівень захисту власного програмного або апаратного забезпечення від злому та несанкціонованого втручання.

Застосування реверсивної інженерії в захисті інформації

Застосування реверсивної інженерії в захисті інформації може мати безліч конкретних прикладів. Нижче наведено перелік деяких із них:

1. *Аналіз шкідливих програм*. Зворотне проектування можна використовувати для розбирання та аналізу шкідливих програм, таких, як віруси, троянські програми або шпигунське програмне забезпечення. За допомогою цього аналізу можна зрозуміти їх структуру, функцію та метод впровадження у програмний продукт. Озброївшись цими знаннями, можна розробити ефективні антивірусні програми та заходи безпеки для запобігання атакам.
2. *Виявлення вразливості програмного забезпечення.* Зворотний інжиніринг дозволяє аналізувати програмне забезпечення для виявлення потенційних уразливостей, якими зловмисники можуть скористатися для несанкціонованого доступу абодля здійснення атак. Розкривши структуру програми та проаналізувавши взаємодію зовнішніх компонентів, можна виявити слабкі місця та вжити відповідних заходів для підвищення безпеки.
3. *Розшифрування криптографічних протоколів*. Реверс-інжиніринг може використовуватися для аналізу криптографічних протоколів з метою зрозуміти їх структуру та потенційні уразливості. Це дозволяє покращити якість шифрування та підвищити стійкість до атак зловмисників.
4. *Відновлення втрачених даних*. Реверс-інжиніринг може використовуватися для відновлення втрачених даних, які пошкоджені або недоступні через технічні проблеми, і тому можуть бути відновлені з зовнішніх пристроїв, де вони зберігаються. Аналіз структури диска або файлової системи може допомогти відновити ці дані і відновити їх для подальшого використання.

Висновок

Зворотне проектування відіграє важливу роль в інформаційній безпеці, виявляючи вразливості, розробляючи контрзаходи та оптимізуючи безпеку програмного та апаратного забезпечення. Однак, враховуючи потенційну небезпеку, пов’язану з неправильним використанням реверсивної інженерії, важливо звернути увагу на безпеку та етичні міркування під час її застосування. Забезпечення інформаційної безпеки вимагає постійного вдосконалення та співпраці між фахівцями з зворотного проектування, розробниками та правоохоронними органами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Reverse-engineering? [Електронний ресурс] : URL: https://www.techtarget.com/searchsoftwarequality/definition/reverse-engineering
2. Що таке зворотна розробка й де вона застосовується [Електронний ресурс] : URL : https://robotdreams.cc/uk/blog/274-chto-takoe-obratnaya-razrabotka-i-gde-ona-primenyaetsyaReverse
3. Engineering in Cybersecurity [Електронний ресурс] : URL: https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-reverse-engineering

ЄФІМЧЕНКО Анастасія – студентка групи 1БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 14estasyf09@gmail.com

КАПЛУН Валентина, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

YEFIMCHENKO A. – student of group 1BS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

***KAPLUN* V**. – Lecturer of the Chair of Safety of Infomation and Communication Systems, NTU, Vinnytsia.