На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.,** ректор ОНАХТ.

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

Крім іншого, при композитингу є можливість роботи з масками (коли необхідно прибрати, вставити або виділити якусь певну частину зображення), кеінг (заміна однотонного яскравого фону на щось інше), трекингом (визначення місця розташування об'єктів за допомогою камери і подальша робота з отриманими точками). Зображення, що отримується безпосередньо після рендеру – далеко не фінальний результат. Величезна кількість роботи над зображенням ведеться на етапі постобробки – композитинга.

Візуалізація в *Blender* змушує постійно шукати «золоту середину» між тривалістю обробки сцени і прийнятною якістю фінальної картинки. Тому цілком очевидно, що в арсеналі тривимірного редактора присутній цілий ряд інструментів, призначених для компоитинга.

Список літератури

1. 3D blender[электронный ресурс]/01.04.2015. Режим доступа http://www.3d-blender.ru, свободный – Яз.Рус.
2. Короткометражная 3D анимация [электронный ресурс] /01.04.2015. Режим доступа https://habrahabr.ru/post/256683/ , свободный – Яз.Рус.
3. Основы анимации и композитинга[электронный ресурс]/07.04.2015. Режим доступа http://render.ru/books/show_book.php?book_id=634, свободный – Яз.Рус.

АНАЛІЗ І КЛАСИФІКАЦІЯ СУЧАСНИХ КІБЕРНЕТИЧНИХ АТАК

Дьяконов Д.М. студент ОКР „бакалавр” факультету ІТ та КБ
Одеська національна академія харчових технологій, м. Одеса
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

1. Атаки

Перехоплення і прослуховування переданих по мережі даних називається пасивної атакою, т. К. Атакує не впливає на протокол, алгоритм, ключ, саме повідомлення, будь-які частини системи шифрування. Пасивну атаку дуже складно виявити, в більшості випадків простіше спробувати запобігти її, ніж виявити і зупинити. Активними атаками є зміна повідомлень, зміна системних файлів, спроби видати себе за іншу людину. При виконанні активних атак атакуючий щось реально робить, а не просто збирає дані. Пасивні атаки зазвичай використовуються для збору інформації перед проведенням активної атаки, які можна розділити на кілька видів:

1.1. Атака «Тільки шифротекст». При виконанні атаки цього типу, атакуючий має шифротекст кількох повідомлень. Кожне з повідомлень зашифровано одним і тим же алгоритмом. Метою атакуючого є розтин ключа, використаного в процесі шифрування. Якщо атакуючий зможе розкрити ключ, він зможе розшифрувати всі інші повідомлення, зашифровані на тому ж ключі. Атака «тільки шифротекст» (cipher-only attack) - це найпоширеніший тип активних атак, оскільки отримати шифротекст досить просто, наприклад, прослуховуючи чийсь мережевий трафік. Однак це дуже складна атака, в якій вкрай складно домогти-

ся успіху, оскільки атакуючий має занадто мало інформації про процес шифрування.

1.2. Атака «Відомий відкритий текст». При виконанні атаки типу «відомий відкритий текст» (known-plaintext attack), у атакуючого є відкритий текст і відповідний йому шифротекст одного або декількох повідомлень. Метою також є розтин ключа, використаного при шифруванні цих повідомлень, щоб розшифрувати і прочитати інші повідомлення. Зазвичай повідомлення починаються і закінчуються одним і тим же текстом. Наприклад, атакуючий може дізнатися, що більшість повідомлень співробітників компанії починається з певного вітання і закінчується підписом, в яку входить ім'я співробітника, посаду і контактна інформація. Таким чином, атакуючий має певний обсяг відкритого тексту (однакові дані в кожному повідомленні) і може перехопити зашифроване повідомлення і витягти з нього шифротекст. Це дозволить розкрити кілька частин цієї головоломки, а для завершення атаки потрібно буде провести зворотний інжиніринг, частотний аналіз або брутфорс-атаку. Атаки типу «відомий відкритий текст» використовувалися США проти Німеччини і Японії у Другій Світовій війні.

1.3. Атака «Обраний відкритий текст» При виконанні атаки типу «обраний відкритий текст» (chosen-plaintext attack), у атакуючого також є відкритий текст і відповідний йому шифротекст, але він має можливість самостійно вибирати відкритий текст і отримувати його в зашифрованому вигляді. Це дає атакуючому додаткові можливості для більш глибокого вивчення механізмів роботи процесу шифрування, а також для збору більшого обсягу інформації про використаний ключі. Якщо йому вдасться розкрити ключ, він зможе розшифрувати інші повідомлення, зашифровані на цьому ключі. Як це робиться? Наприклад, атакуючий може підготувати спеціальне повідомлення, яке змусить одержувача переслати його комусь ще. Атакуючий відправляє це повідомлення користувачу, той пересилає його своєму колезі, а поштова програма на його комп'ютері автоматично зашифровує повідомлення перед відправкою. Після цього атакуючий перехоплює трафік користувача і отримує копію шифротекста до написаного ним самим відкритого тексту.

1.4. Атака «Обраний шифротекст» При виконанні атаки типу «обраний шифротекст» (chosen-ciphertext attack), атакуючий може вибирати шифротекст для розшифрування і має доступ до одержуваному в результаті відкритого тексту. Метою знову ж є розтин ключа. Це більш складна атака в порівнянні з попередньою. Для її реалізації атакуючому може знадобитися контроль над системою, що містить криптосистему.

2. Відкриті і секретні алгоритми

В даний час в світі в основному використовуються добре відомі і зрозумілі криптографічні алгоритми, а не секретні. Криптографи знають, наскільки стійким і добре спроектованим повинен бути алгоритм, представлений на суд громадськості. Тисячі умів краще, ніж п'ять, і часто це допомагає знайти в алгоритмі проблеми, які не помітили розробники. Саме тому різні виробники і компанії влаштовують змагання по злому їх кодів і процесів шифрування. Якщо

комусь вдається їх зламати, розробники повертаються до креслярської дошці і підсилюють ту чи іншу частину алгоритму. Однак не всі алгоритми зроблені загальнодоступними, наприклад, деякі алгоритми, розроблені Агентством національної безпеки США, є секретними. Оскільки рівень критичності даних, з якими працюють шифри АНБ, настільки великий, вони хочуть максимально зберегти процес в секреті. АНБ не проводить публічних тестів і досліджень своїх алгоритмів, проте це не говорить про слабкість алгоритмів АНБ. Ці алгоритми розробляються, досліджуються і тестуються кращими криптографами, мають дуже високу кваліфікацію.

3. Атаки з використанням побічних каналів

Усі розглянуті раніше атаки, засновані в першу чергу на математичних аспектах криптографії. Використання відкритого тексту і шифротекста, а також застосування потужних математичних інструментів, направлено на розтин ключа, використаного в процесі шифрування. Але існують і інші методи.

ПЛАНИРОВАНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ ДИНАМИКИ ТЕХНОЛОГИЧЕСКИХ СИСТЕМ РЕЗАНИЯ

Евсюкова Д.Ю., Коваленко В.И.
Одесский национальный политехнический университет

Возможность получать информационные сигналы в реальном времени работы технологического оборудования, оснащенного измерительной системой NI-DAQmx с программным обеспечением NI-LabVIEW, позволяет выявить влияние режимных параметров обработки на виброхарактеристику упругой системы металлорежущего станка [1]. Экспериментальные исследования проводили на станке мод. 500 V/5 (обрабатывающий центр) при фрезеровании специальных призматических образцов из конструкционной стали марки Ст.3 (рис.1).

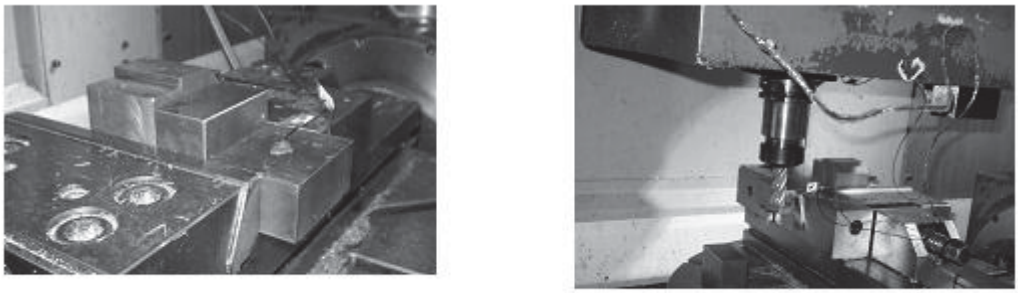

Рис. 1 Расположение вибродатчиков АР 2019 (по осям *z* и *x*) на призматическом образце (слева) и настройка на выполнение рабочего хода фрезерования (справа) на станке мод. 500 V/5.

Фреза из быстрорежущей стали Р6М5 диаметром 18 мм, исследованы 4-х и 6-ти зубовые концевые фрезы. План проведения двух двухфакторных экспериментов позволяет установить влияние режимных параметров фрезерования