Семинар "Вокруг запутывания программ"

Представление индивидуальных тем в рамках проекта "Запутывание программ".

Юрий Лифшиц

16 декабря 2004 – лаборатория Intel

Сегодня

- Принципы организации проекта, его цели и сроки
- Индивидуальная работа над темой
- Презентация тем
- Время для вопросов

Анкета слушателя

- Степень мотивации?
- Какие направления представляют наибольший интерес?
- Что важно при выборе темы?

Этапы работы над темой

- Чтение литературы (статьи или документация софта);
- Постановка исследовательских задач;
- Написание индивидуального отчета (курсовой);
- Доклад на семинаре;
- Коллективные обсуждения (мозговые штурмы).

Аспекты исследовательских тем

- Новизна;
- Внутренняя интересность;
- Применимость на практике;
- Связь с другими разделами математики;
- Доступность;
- Открытость/закрытость информации.

Проектный подход

- Коллективные или индивидуальные исследования?
- Планирование результатов.
- Контроль деятельности.

Общее направление: обнаружение новых «сильных» технологий, выявление математической сути темы и установление связи между запутыванием программ и другими областями математики и Computer Science.

Анкета темы

- Характеристики темы;
- Пример исследовательской задачи;
- Литература;
- Время для вопросов.

Список тем

- Программы, нуждающиеся в запутывании
- Математические модели защиты программ
- Архитектурный подход к защите программ
- Запутывание в системах взаимодействующих программ
- Защита на ассемблерном уровне
- Инструментальная тема
- Техники распутывания
- Качество запутывающих преобразований

Use cases

Характеристика: абсолютно необходимая и совершенно неисследованная тема.

Общая задача: классификация use cases.

Конкретная постановка: составить контактный лист программистских фирм России, использующих обфускацию для своих ресурсов. Выяснить, что именно они защищают и какую оценку дают используемому софту.

Литература для Use cases

- Мой обзор;
- L. D'Anna, B. Matt, A. Reisse, T. Van Vleck, S. Schwab and P. LeBlanc. Self-protecting mobile agents obfuscation report. June 2003;
- Digital Rights Management.

Математические модели защиты программ

Характеристика: основа всей области запутывания программ.

Общая задача: получить методы с доказанной (измеримой) секретностью.

Конкретная постановка: сформулировать математические модели для различных типов защит и атак. Составить список модельных программ и искать запутывания этих конкретных программ.

Литература для Математических моделей

- B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang. On the (im)possibility of obfuscating programs, 2001;
- B. Lynn, M. Prabhakaran and A. Sahai. Positive Results and Techniques for Obfuscation, 2004;
- Nikolay P. Varnovsky and Vladimir A. Zakharov. On the Possibility of Provably Secure Obfuscating Programs. 2003;
- C.S. Collberg and C. Thomborson. Watermarking, tamper-proofing, and obfuscation - tools for software protection, June 2002.

Архитектурный подход к защите программ

Характеристика: ведущее направление запутывания программ, одно из самых актуальных для Intel.

Общая задача: разработать среду, в которой можно создавать исполнимые, но не анализируемые (не изменяемые) программы.

Конкретная постановка: Выяснить подробности про патент Intel. Изучить возможности архитектурного подхода по отношению к JVM.

Литература для архитектурного подхода

- C. Wang. A Security Architecture for Survivability Mechanisms, Oct. 2000;
- D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell and M. Horowitz. Architectural support for copy and tamper resistant software, 2000;
- Y. Ishai, A. Sahai, and D. Wagner. Private circuits: Securing hardware against probing attacks, 2003;
- P. Gutmann. An open-source cryptographic co-processor. 2000;
- R.J. Anderson and M.G. Kuhn. Low cost attacks on tamper-resistant devices, 1997;
- W.A. Arbaugh, D.J. Farber and J.M. Smith. A secure and reliable bootstrap architecture, 1997;

- S. Forrest, A. Somayaji and D. H. Ackley. Building diverse computer systems, 1997.

Запутывание в системах взаимодействующих программ

Характеристика: новое направление в запутывании программ. Эта технология развивается в среде клиентских программ, работающих с денежными потоками.

Общая задача: разработать технологию создания программ, состоящих из нескольких компонент, которые контролируют друг друга.

Конкретная постановка: найти практический пример, установить контакт и поставить конкретный исследовательский вопрос.

Литература для запутывания в системах

- J. Algesheimer and C. Cachin and J. Camenisch and G. Karjoth. Cryptographic security for mobile code, May 2001;
- T. Sander and C.F. Tschudin. Towards mobile cryptography, 1998;
- L. D'Anna and B. Matt and A. Reisse and T. Van Vleck and S. Schwab and P. LeBlanc. Self-protecting mobile agents obfuscation report, June 2003.

Защита на ассемблерном уровне

Характеристика: один из способов затруднить анализ программ.

Общая задача: реализовать максимально мощные методы по защите от дизассемблирования.

Конкретная постановка: установить потенциал запутывания программ на уровне машинного кода и ассемблера.

Литература для ассемблерного уровня

- C. Linn and S. Debray. Obfuscation of executable code to improve resistance to static disassembly, 2003;
- B. Schwarz and S. Debray and G. Andrews. Disassembly of executable code revisited, 2002;
- C. Cifuentes and K.J. Gough. Decompilation of binary programs, 1995;
- Gregory Wroblewski. General MEthod of PRogram Code Obfuscation, 2002.

Инструментальная тема

Характеристика: изучение софта для защиты и взлома программ.

Общая задача: научиться писать софт по защите программ, превосходящий современные аналоги, изучить текущие и предсказать будущие возможности хакерских инструментов.

Конкретная постановка: изучить несколько образцов хакерского и запутывающего софта и применить его к построенным в математической модели программам.

Литература для инструментальной темы

- SandMark;
- Доклад Саши Пименова – `http://logic.pdmi.ras.ru/ yura/of/jvm.ppt`;
- J.G. Steiner and C. Neuman and J.I. Schiller. Kerberos: An authentication service for open network systems, 1988;
- C. Cifuentes and T. Waddington and M. Van Emmerik. Computer security analysis through decompilation and high-level debugging, Oct 2001;
- J.R. Nickerson and S.T. Chow and H.J. Johnson and Y. Gu. The encoder solution to implementing tamper resistant software, Oct. 2001;
- J. Vinciguerra and L. Wills and N. Kejriwal and P. Martino and

R. Vinciguerra. An experimentation framework for evaluating disassembly and decompilation tools for c++ and java, 2003;

- J. Wilander and M. Kamkar. A comparison of publicly available tools for dynamic buffer overflow prevention. Feb. 2003.

Техники распутывания

Характеристика: изучение возможностей для взлома программ. Как ни странно, довольно хорошо освещена в литературе.

Общая задача: найти такие задачи для анализа программ, которые не под силу современным методам распутывания.

Конкретная постановка: выяснить практическую устойчивость основных опубликованных методов запутывания программ. Написать критику всех этих методов.

Литература для распутывания

- E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems, 1997;
- D. Bleichenbacher. Chosen ciphertext attacks against protocols based on rsa encryption standard pkcs #1, 1998;
- M. Jacob and D. Boneh and E. Felton. Attacking an obfuscated cipher by injecting faults, 2003;
- D. Boneh and R.A. DeMillo and R.J. Lipton. On the importance of eliminating errors in cryptographic computations, 2001.

Качество запутывающих преобразований

Характеристика: совершенно не систематизированная область. Результаты важны для продвижения новых методов и сравнения методов.

Общая задача: найти механизм оценки качества запутанности программ.

Конкретная постановка: построить оценку качества для запутывания одной *тестовой программы*.

Литература для оценок качества

- Никакая – вся.

Запомнить/записать

- Интернет-страница – `http://logic.pdmi.ras.ru/~yura/of.html`;
- Лифшиц Юрий – `yura@logic.pdmi.ras.ru`, +79043310563;
- Сайт лаборатории – `http://se.math.spbu.ru/setlab/`
- Запишитесь ко мне на листок! Перечислите темы, которые вас заинтересовали.

С чего начать?

- Главное – принять внутреннее решение;
- Сделать выбор темы и начать самостоятельную работу;
- Не пропустить начало спецкурса и спецсеминара в марте.
- Подать заявку на какую-нибудь студенческую школу.

ВРЕМЯ ДЛЯ ВОПРОСОВ

СПАСИБО ЗА ВНИМАНИЕ!