ВМК МГУ им. М.В. Ломоносова
Кафедра информационной безопасности

Некоторые научные проблемы информационной безопасности

СОКОЛОВ Игорь Анатольевич

18 мая 2015 г.

Научные проблемы информационной безопасности

Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации *(СБ РФ 7 марта 2008 г.):*

- гуманитарные проблемы;

- научно-технические проблемы;

- проблемы кадрового обеспечения.

Научные проблемы информационной безопасности

Определение информатики:

Информатика (computer science) – наука о методах, процессах и средствах сбора, хранения, обработки, передачи и анализа информации (данных).

Составные части информатики:

- теоретическая информатика;
- программная инженерия (разработка программ);
- разработка аппаратных компонентов вычислительных систем;
- социальная информатика;
- информационная безопасность (пересекается со всеми другими областями).

Научные проблемы информационной безопасности

Определение информационной безопасности:

Информационная безопасность (Information Security) – междисциплинарное научное направление, изучающее вопросы защиты целостности, доступности и конфиденциальности информации.

Основные научные разделы информационной безопасности:

- **криптография и теория кодирования;**
- **модели и методы анализа протоколов;**
- **методы выявления уязвимостей и вредоносных компонентов в программах и системах;**
- **модели сетевых атак, методы распознавания сетевых вторжений и контроля доступа к сетевым ресурсам.**

Основные категории ИБ

Целостность (integrity) – невозможность несанкционированной модификации информации.

Доступность (availability) – невозможность временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Конфиденциальность (confidence) – возможность доступа к информации имеют только пользователи с соответствующими правами.

{неотказуемость, подотчетность, достоверность, аутентичность, …}

Причины нарушения ИБ

- ошибки разработчиков (несоответствие предъявляемым требованиям);
- действия злоумышленников (вредоносные программы, сетевые атаки);
- сложность современных информационных технологий (объем кода, информации, субъектов; сложность протоколов).

Ошибки разработчиков

Теория верификации:

- построение математических моделей анализируемых компьютерных систем;
- математическое доказательство соответствия предъявляем требованиям.

Основные математические разделы:

- теория автоматов;
- теория алгоритмов;
- теория графов;
- теория сетей Петри;
- алгебра исчисления процессов;
- математическая логика;
- семантика языков программирования.

Действия злоумышленников

Задачи:

Поиск уязвимостей:

- знание общих закономерностей работы современного ПО;
- знание протоколов обработки информации;
- усилия компьютерного сообщества.

Выявление вредоносного кода:

- сигнатурный анализ;
- разработка метрик близости программ к классу вредоносных;
- выявление аномалий поведения систем.

Действия злоумышленников

Сигнатурный анализ:

$$M(A, B) < m$$

A – эталонный набор сигнатур;
B – наблюдаемый набор сигнатур;
M – метрика (решающее правило).

Методы теории распознавания образов (ак. Журавлев Ю.И., чл.-к. Софер В.А., чл.-к. Рудаков К.В., чл.-к. Арлазаров В.Л.).

Действия злоумышленников

Выявление аномалий

Проактивная технология защиты – HIPS (Host-based Intrusion Prevention Systems):

- статистический анализ;
- ДСМ метод (Финн В.К.);
- теория алгоритмов, методы распознавания, прогнозирования, принятия решений (школа ак. Журавлева Ю.И.).

Криптография

$$Y = T(x, k)$$

X – исходный текст;
Y – зашифрованный текст;
T – правило преобразования x в y (шифр);
K – параметр шифра T (ключ).

Простой шифр – шифр простой замены (шифры Атбаша, Цезаря, Виженера и т. д.)

Сложный шифр – суперкомпозиция простых.

Основные задачи:

- криптоанализ (расшифровка);
- разработка криптографических протоколов, устойчивых к криптоанализу.

Криптография

Основные разделы математики:

- теории конечных групп, колец, полей;
- теория булевых функций;
- теория конечных автоматов;
- теория чисел (факторизация, конечное логарифмирование);
- теория вероятностей и математическая статистика).

Вычислительная техника в криптографии:

- суперкомпьютеры 10^{15} flops (МГУ – 10^{12})
- параллельные вычисления (ак. Четверушкин Б.Н., чл.-к. Воеводин В.В.)

Криптографические протоколы

Применения:

- аутентификация;
- электронная цифровая подпись;
- распределение ключей;
- электронное голосование;
- электронная коммерция;
- электронные финансы

…

Математические модели протоколов:

- разработка;
- доказательство стойкости (математические методы криптографии, теория верификации).

Многое другое

- Стенография;
- Скрытные каналы;
- Побочные каналы;
- Сетевые атаки;
- Исследование инцидентов;
- Политики безопасности;
- Системы противодействия;

…

Современные информационные технологии

- облачные вычислительные системы (cloud computing);
- работа со сверхбольшими объемами данных (Big Data);
- Интернет вещей (Internet Things);
- беспроводные мобильные системы (>10 Гбит/с).

Облачные вычислительные системы

Особенности:

- обработка информации в неконтролируемой среде;
- использование технологии виртуализации.

Следствие – потеря контроля над информацией на всем жизненном цикле.

Задачи:

- разработка новых методов разграничения доступа и противодействия;
- гомоморфное шифрование.

Научные проблемы информационной безопасности

Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации *(СБ РФ 7 марта 2008 г.):*

- гуманитарные проблемы;

- научно-технические проблемы;

- проблемы кадрового обеспечения.

ВМК МГУ им. М.В. Ломоносова
Кафедра информационной безопасности

Некоторые научные проблемы информационной безопасности

СОКОЛОВ Игорь Анатольевич

18 мая 2015 г.