ЗАЩИЩЕННЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ: МИФ ИЛИ РЕАЛЬНОСТЬ?

Иванов М.А.

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)

Введение. Важнейшей характеристикой любой компьютерной системы, независимо от ее сложности и назначения, является безопасность обрабатываемой в ней информации. Информационная безопасность давно стала самостоятельным направлением исследований и разработок. Однако, несмотря на это, проблем не становится меньше. Это объясняется появлением всё новых компьютерных технологий (суперкомпьютерных, мобильных, радиочастотной идентификации (RFID) и пр.), которые не только создают новые проблемы информационной безопасности, но и представляют, казалось бы, уже решенные вопросы совершенно в новом ракурсе. Кроме того, появление новых компьютерных технологий, новых математических методов дают в руки нарушителей и создателей *разрушающих программных воздействий* (РПВ) (malware) все новые и новые возможности. Главная причина трудоемкости решения задачи обеспечения безопасности информации в современных условиях – всё большее отстранение пользователей от процессов управления и обработки информации и передача его ПО, обладающему некоторой свободой в своих действиях и поэтому очень часто работающему вовсе не так, как предполагает пользователь.

С развитием суперкомпьютерных технологий (СКТ) ситуация принципиально изменилась, причем на первый взгляд в худшую сторону. С появлением суперкомпьютеров стало намного проще решать задачи полного или частично-полного перебора, а именно таковыми являются задачи, связанные с компрометацией систем защиты информации, в частности задачи взлома криптоалгоритмов и криптопротоколов, задачи поиска уязвимостей программных систем. Полный перебор вариантов это универсальный метод решения подобных задач, вероятность его успеха всегда равна единице. Именно с появлением суперкомпьютеров получила широкое распространение простая и эффективная технология *фаззинга*, суть которой – автоматический поиск уязвимостей атакуемой системы методом грубой силы. Такая атака, основанная на модели «чёрного ящика», хотя и не всегда является наилучшим выбором, практически всегда возможна. Ее основными преимуществами являются доступность, простота и воспроизводимость, которые невозможно получить при использовании других методов [1].

Новый стимул в развитии получают атаки, основанные на использовании криптографии против криптографии. Многие скрытые каналы утечки информации из криптосистем для своего использования требуют именно решения задач частично-полного перебора. С появлением суперкомпьютеров требования к пропускной способности таких каналов существенно снижаются [2, 3]. РПВ, использующие скрытые каналы воздействия на объект, а также приема и передачи информации, уже появились. Совершенствование методов поиска уязвимостей программных систем, создающих предпосылки для проведения атак, основанных на вставке кода, привело к увеличению фактов обнаружения РПВ, использующих *уязвимости нулевого дня* (Zero day vulnerabilities). Совершенно очевидно, что в самое ближайшее время будут обнаружены РПВ, которые при функционировании для затруднения своего выявления и нейтрализации применяют СКТ, в частности, гибридные. В результате антивирусы, использующие традиционные реактивные методы защиты, окажутся не в состоянии справиться с новой угрозой.

Ситуация тяжелая, но не безнадежная. Надежду вселяет знание основных ошибок, которые были сделаны в недавнем прошлом и которых вполне можно избежать в будущем:

- Решение вопросов ИБ по остаточному принципу уже после создания новой системы или новой компьютерной технологии. В результате в большинстве случаев все сводится к «латанию» все новых и новых «дыр», а не к кардинальному решению проблемы;
- Большинство существующих алгоритмов защиты информации и протоколов защищенного информационного взаимодействия исходят из модели «черного ящика» (Black Box) и именно в условиях действия такой модели они обеспечивают требуемый уровень ИБ. В действительности же действует либо модель серого ящика (Grey Box), ко-

гда возможны утечки по побочным каналам (Side Channels) и соответственно надо думать о временных, мощностных и др. атаках на реализацию (Timing, Cache timing, Power, Differential Power Attacks и др.), либо «белого ящика» (White Box), когда компьютер, где программно реализованы методы защиты информации, полностью доступен злоумышленнику и в его распоряжении огромный набор хакерских утилит, позволяющих мгновенно нейтрализовать любую защиту.

Следует выделить три важнейших направления при движении в сторону создания защищенных компьютерных технологий:

- Разработка и исследование криптографических методов защиты информации;
- Выявление тенденций развития РПВ, исследование механизмов проведения атак на компьютерные системы в защищенном исполнении и опережающее совершенствование методов и средств защиты от них;
- Создание методики комплексного анализа защищенности компьютерных систем, и в первую очередь критически важных.

Рассмотрим эти направления более подробно.

Криптографические методы защиты информации. Анализ угроз информационной безопасности, тенденций развития компьютерных технологий позволяет сделать однозначный вывод о постоянно возрастающей роли криптографических методов защиты информации. В некоторых случаях криптография – это единственно возможный механизм защиты.

Однако криптография имеет много, мягко говоря, интересных особенностей. Можно озвучить в качестве примера следующие истинные утверждения, на первый взгляд противоречащие друг другу:

- Криптография может решить практически любую задачу, связанную с защитой информации;
- Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана;
- Криптография сложнее, чем кажется;
- Криптография опасна тем, что очень часто создает лишь видимость безопасности;
- Криптография – технология двойного назначения и может использоваться не только для защиты, но и для нападения.

Тем не менее, имеются следующие криптографические механизмы, в совокупности решающие весь спектр задач, связанных с информационной безопасностью:

- Криптосистемы с открытым ключом, не требующие наличия надежных каналов связи для обмена ключами;
- Протоколы выработки общего секретного ключа;
- Протоколы электронной цифровой подписи (ЭЦП): классическая ЭЦП, мультиподпись, групповая подпись, слепая подпись и пр.;
- Протоколы аутентификации (проверки подлинности) удаленных абонентов, в том числе протоколы доказательства с нулевым разглашением знаний (Zero Knowledge Proofs);
- Протоколы привязки к биту (Bit Commitment);
- Протоколы правдоподобного отрицания;
- Протоколы разделения секрета и ряд других, менее известных.

Двумя главными «врагами» современной криптографии являются квантовые компьютеры и РПВ.

Квантовый компьютер в состоянии эффективно решать многие трудности математические задачи, на сложности решения которых основывается стойкость всех современных криптоалгоритмов и протоколов. Имеются в виду, в первую очередь задачи факторизации целых чисел, дискретного логарифмирования и дискретного логарифмирования на эллиптических кривых, которые лежат в основе соответственно криптосистем RSA, Эль-Гамаля и ECCS. Последняя, к слову, используется во всех существующих государственных стандартах на ЭЦП. Таким образом, появление полноценного квантового компьютера «поставит крест» на современной криптографии. Пока до наступления этой неприятной ситуации далеко, однако направление, связанное с созданием криптоалгоритмов, которым «не страшны» квантовые компьютеры, уже активно развивается, в том числе и в России. Это направление получило название *по-*

стквантовая криптография (Code-based Cryptography, Lattice-based Cryptography, Hash-based Signature Schemes, Multivariate Public Key Cryptography и др.) [4].

Разрушающие программные воздействия, скрытые каналы передачи информации. Программы, изначально предназначенные для выполнения деструктивных действий, получили обобщенное название разрушающих программных воздействий. Типы РПВ: *компьютерные вирусы* (КВ), *сетевые черви*, *закладки*, *троянские программы*, *дропперы* (droppers), *эксплойты* (exploits), различные *хакерские утилиты* (конструкторы РПВ, сканеры уязвимостей, утилиты удаленного администрирования и «заметания следов» (rootkits) и др.).

Например, эксплойты – это обобщенное название вредоносных программ, которые используют *уязвимости* ПО (vulnerabilities) для проведения удаленных атак на компьютерные системы. При этом под уязвимостями понимают не ошибки программирования, а дефекты безопасности, наличие которых не влияет на вычисления, а это значит, что эти дефекты не выявляются на традиционных этапах тестирования и отладки программ. Примеры уязвимостей: Buffer Overflow, Race Condition, Integer Overflow, Heap Overflow, Format String Errors, Double Free и др., всего более 10, если считать разновидности в первых трех случаях. Обнаружив одну из таких уязвимостей, злоумышленник может провести атаку, основанную на вставке произвольного кода (Code Injection). В результате появляются возможности для повышения своих полномочий в системе, подмены алгоритмов функционирования средств защиты и пр. [5].

Наиболее опасные типы РПВ:

- РПВ, использующие криптографические методы для выполнения деструктивных функций или затруднения своего обнаружения;
- РПВ, создающие или использующие скрытые каналы (Covert, Subliminal, Side Channels) утечки информации или воздействия на объект.

"Лекарства" даже от простейшего вида РПВ, компьютерных вирусов, не существует. Всегда можно создать вирус, который не сможет нейтрализовать ни одна из существующих антивирусных программ. Основная идея в том, что если разработчик КВ знает, что именно ищет антивирусная программа, он всегда способен разработать РПВ, незаметное для нее. Конечно, после этого создатели антивирусных средств могут усовершенствовать свои продукты, чтобы они определяли уже и новый вирус, таким образом, возвращая ситуацию в исходное положение.

Можно выделить следующие принципиальные недостатки существующих средств защиты от РПВ:

- при их разработке в большинстве случаев используются методы, при реализации которых нападающие всегда находятся в более выигрышном положении, чем защищающиеся;
- отсутствие оперативной реакции со стороны разработчиков средств защиты от РПВ на появление принципиально новых методик создания РПВ, требующих таких же принципиально новых методов защиты.

Злоумышленник не может нанести вред системе в двух случаях, когда (1) он ее «не понимает» или «понимает неправильно», либо когда (2) он ее вообще «не видит». Именно в этих ситуациях защита может получить преимущество перед нападением, в отличие, например, от таких традиционных методов, как межсетевое экранирование и обнаружение атак. Поэтому чрезвычайно перспективными методами следует признать методы внесения неопределенности в работу средств и объектов защиты, создание ложных объектов атаки (ЛОА) (по сути приманок) и стеганографические методы.

Внесение неопределенности в работу средств и объектов защиты на порядок увеличивает стойкость защитных механизмов, метод предполагает использование генераторов псевдослучайных или случайных чисел для:

- управления последовательностью выполнения шагов алгоритма (пермутация и полиморфизм);
- обеспечения независимости времени выполнения отдельных шагов алгоритма от исходных данных (для защиты от временных атак на реализацию);
- внесения непредсказуемости в результат преобразований (рандомизации), например, реализации концепции вероятностного шифрования;

– реализации «плавающих» протоколов взаимодействия программных и аппаратных средств (обычно устройств ввода-вывода);
– обеспечения для каждой программы индивидуальной среды исполнения (рандомизация среды исполнения, Instruction Set Randomization).

Внесение неопределенности в работу средств и объектов защиты – это пример так называемого стохастического метода защиты информации. Стохастические методы являются универсальными и могут использоваться совместно с любыми другими методами, автоматически повышая их качество.

Комплексный анализ защищенности компьютерных систем. Традиционный системный подход к решению проблемы информационной безопасности в принципе не применим, необходим процессный, а еще лучше эволюционный подход. Иначе говоря, эффективная система защиты – это не какой-то фиксированный набор методов и средств защиты, это непрерывный процесс, который включает в себя:

– Постоянный анализ защищенности системы на всех ее уровнях (элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО),
– Опережающее совершенствование методов и средств защиты.

Таким образом, важнейшую роль в обеспечении информационной безопасности играет разработка методики комплексного анализа защищенности компьютерных систем (Ethical Hacking), и в первую очередь проведения важнейшего его этапа – теста на проникновение (Penetration Testing) [6, 7].

Заключение.

Таким образом, можно выделить следующие важные направления исследований:

– Разработка методологии криптографии «серого» и «белого ящика» (grey and white box cryptography), иначе говоря, криптографии, свободной от утечек по побочным каналам; разработка методов запутывания программной реализации симметричных и асимметричных криптоалгоритмов;
– Исследование вопросов безопасной реализации симметричных и асимметричных криптоалгоритмов на GPU; исследование вопросов безопасной реализации симметричных и асимметричных криптоалгоритмов на ПЛИС;
– Поиск путей создания минималисткой (легковесной, Light-Weight) криптографии для RFID-систем;
– Исследование новых методов криптоанализа симметричных криптоалгоритмов: Cube Attack, Rebound Attack, Biclique Attack, XSL Attack и др.;
– Разработку и исследование методов постквантовой криптографии;
– Разработку и совершенствование проактивных методов защиты от РПВ, разработку методов обнаружения ранее неизвестных РПВ (эвристический анализ, мониторинг и блокировку потенциально опасных действий; контроль целостности файлов и системных областей в фоновом режиме);
– Разработку стохастических методов защиты информации, основанных на использовании непредсказуемых алгоритмов генерации ПСЧ и хеширования;
– Выявление тенденций развития РПВ и механизмов проведения атак на компьютерные системы, основанных на использовании стохастических методов и скрытых каналов передачи данных;
– Разработку базы моделей наиболее опасных РПВ для анализа эффективности создаваемых средств защиты от вредоносных программ;
– Создание и внедрение методики комплексного анализа защищенности критически важных информационных систем.

Литература

1. Kozirsky B.L., Komarov T.I. Fuzzing – a perspective method of searching software vulnerabilities. Proceedings of REDS-2013, Moscow, pp. 160-163.
2. Разрушающие программные воздействия / А.Б. Вавренюк, Н.П. Васильев, М.А. Иванов и др. Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. http://www.aha.ru/~msa/razrushayuschie.pdf
3. Chepik N.A. Kleptographic attacks on ECDSA. Proceedings of REDS-2013, Moscow, pp. 163-166.
4. Post-Quantum Cryptography. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen Editors. http://www.e-reading.by/bookreader.php/135832/Post_Quantum_Cryptography.pdf.
5. Jon Erickson. Hacking: The Art of Exploitation, 2nd edition. – No Starch Press, 2008.
6. Ethical Hacking & Countermeasures. Threats & Defense Mechanisms. COURSE TECHNOLOGY, CENGAGE Leaning. http://greymind.ir/ebook/Ethical.Hacking.Countermeasures.Threats.Defense.Mechanisms_%5Bwww.Graymind.ir%5D.pdf.
7. Kimberly Graves. Certified Ethical Hacker STUDY GUIDE. http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf.

Защищенные компьютерные технологии: миф или реальность?

Рассматриваются причины трудоемкости решения задачи защиты информации в компьютерных системах и сетях. Выделяются три направления движения в сторону создания защищенных компьютерных технологий.

Ключевые слова: криптография, разрушающие программные воздействия, рандомизация, анализ защищенности.

Сведения об авторе

Автор доклада – профессор, заведующий кафедрой Компьютерных систем и технологий факультета Кибернетики и информационной безопасности НИЯУ МИФИ.

Контактная информация: тел. 8-926-558-60-99, email: MAIvanov@mephi.ru.

Secured Computer Technologies: Myths versus Reality

The article deals with causes of complexity of securing data in computer systems and networks. Three ways of getting closer to secured computer technologies are described.

Keywords: cryptography, malware, randomization, ethical hacking.