ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-СЕРВЕРА МЕТОДОМ ЗАЩИТЫ ОТ ИССЛЕДОВАНИЯ

Е.С. Семенкин, д.т.н.; М.А. Стюгин (Сибирский государственный аэркосмический университет имени академика М.Ф. Решетнева, styugin@rambler.ru)

Рассматривается подход к обеспечению информационной безопасности на основе информационного управления нарушителем. Приводится алгоритм технологии защиты от исследования систем. Подход иллюстрируется на примере двух технических реализаций технологии для защиты веб-сервера от преднамеренных атак.

Ключевые слова: информационная безопасность, информационное управление, защита от исследования, сдерживание несанкционированной активности.

Введение

В данной статье рассматривается подход к обеспечению информационной безопасности принципиально отличающийся от существующих. Современное развитие средств обеспечения безопасности серверов, приложений, баз данных и пр. строится на выявлении уязвимостей и перекрытии их. Каждый день в области программных средств открываются новые «дыры», которые открываются и реализуются настолько быстро, что настройка безопасности любого приложения состоит, практически, в процессе непрерывного «латания дыр». Здесь мы сформулируем иную точку зрения на проблему обеспечения безопасности компьютерных систем.

Для атак на компьютерные сети, как и для любых других активных действий, необходима информация. Чем стереотипнее система – тем меньше нарушителю необходимо собрать информации вплоть до реализации стандартных эксплойтов. Отклонение системы от стереотипного состояния принуждает нарушителя к ее исследованию. Получение новой информации – это исследование системы, при котором нарушитель интерпретирует получаемую информацию в соответствии с его гипотезами относительно структуры этой системы[1]. Т.е. даже в исследовании некая информация всегда априорно предшествует действиям, иначе не может быть интерпретирована получаемая от системы обратная связь. На этом основывается принцип защиты от исследования систем: *чтобы сохранить функциональную структуру системы от несанкционированных воздействий, надо ее разнообразить до такой степени, чтобы для непосвященного исследователя она представляла хаос, относительно структуры которого трудно сформулировать однозначную гипотезу*[2].

Таким образом, технологии защиты от исследования не накладывают каких-либо ограничений на действия злоумышленника, а задействует неиспользуемый на данный момент ресурс систем безопасности – информационное управление нарушителем. Это дает снижение риска сразу по всему множеству (даже не открытых) уязвимостей, т.к. блокирует информативную обратную связь при попытке исследования системы.

Технология защиты от исследования систем

[1] Стюгин, М.А. Создание «хаоса» с целью защиты от исследования // М.А. Стюгин / Труды XVI Международной конференции «Проблемы управления безопасностью сложных систем» – М.: РГГУ, 2008.

[2] Стюгин, М.А. Защита от исследования и ее применение в системах безопасности // Е.С. Семенкин, М.А. Стюгин / Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – Вып. 2 (23). – 2009.

Любые кибернетические системы (в том числе и человек) распознают объекты, основываясь на неразличимости восприятия. Это единственный способ получения информации об объектах реального мира. Любой идеальный объект строится на основе множества упрощений. Очень редко эти упрощения можно сразу выразить в определении идеального объекта. «Точно» зафиксировать объект в исследовании невозможно, что очень хорошо показано на примере истории развития теоремы Эйлера и понятия «правильного многогранника» в книге И. Лакатоса «Доказательства и опровержения»[3]. Поэтому проектирование систем строится на стереотипных схемах, отклоняться от которых можно, вводя в определения идеальных объектов дополнительные параметры[4]. Человек всегда мыслит в пределах идеальных объектов, т.к. это единственный способ строить цепочки логических суждений. Способность мыслить нестереотипно, а, следовательно, создавать что-то принципиально новое, присуща лишь гениям с неординарным типом мышления. Проблема построения нестереотипных систем, принципы и структура функционирования которых выходила бы за рамки способности восприятия других субъектов конфликта, уже встречалась в научных исследованиях. Интересный подход к этой проблеме был предложен Денисовым А.А.[5], который выявил ранжирование сегментов сознания человека в соответствии с доминирующим типом квазипсихичекой активности и определил сегмент, связанный с генерацией новых классификаторов. К сожалению, столь интересная работа, так и не привела к практически значимым результатам. Технология, о которой идет речь в данной работе, основана на искусственном усложнении системы путем введения в нее «бессмысленных» параметров[1,4]. Однако результат, которого мы достигаем в результате реализации этой технологии заключается в отклонении структуры системы в область нестереотипных шаблонов вплоть до полного хаоса для стороннего наблюдателя.

Предлагаемая технология защиты от исследования заключается в функциональном изменении процессов в системе в соответствии с некой концепцией уникальности. Данный процесс показана на рис.1.

[3] Лакатос, И. Доказательства и опровержения. Как доказываются теоремы. // И. Лакатос – М.: Наука, 1967.
[4] Стюгин, М.А. Планирование действий в конфликте на уровне функциональных структур // М.А. Стюгин / Информационные войны - №2, 2009.
[5] Денисов, А.А. Проблемы и задачи новой кадровой политики // А.А. Денисов / Рефлексивные процессы и управление - № 2, том 8, 2007.

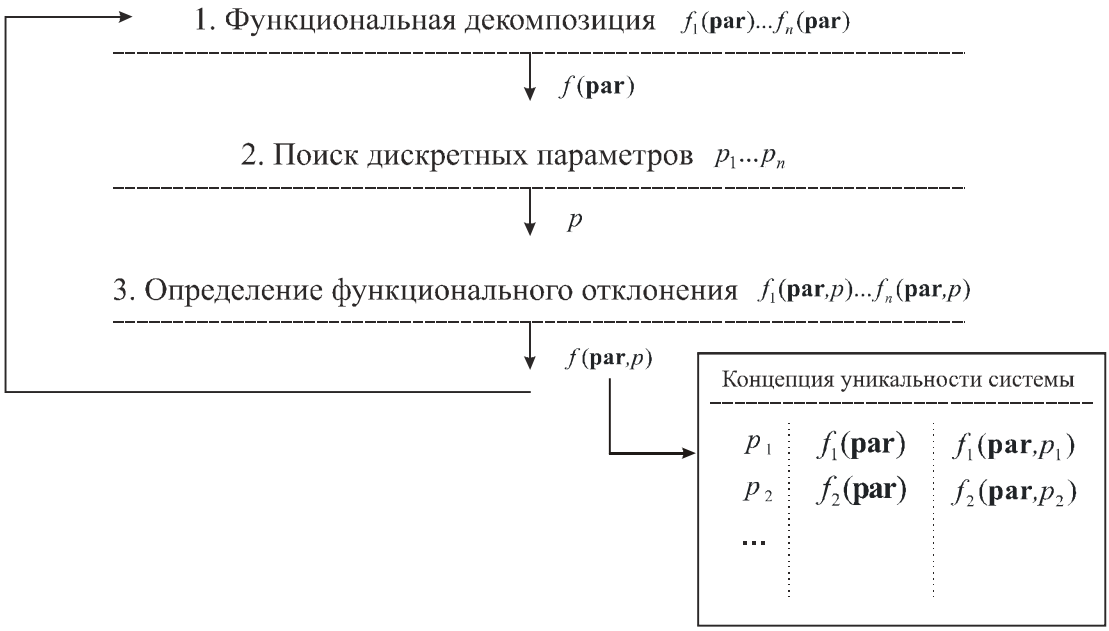


Рис.1. Алгоритм построения «уникальной» системы

На первом шаге производится функциональная декомпозиция системы, целью которой является выделение подпроцессов для конкретной цели ($f_1(\mathbf{par})...f_n(\mathbf{par})$), где **par** - любые параметры процесса. Например, доступ к базе данных – это последовательная аутентификация, соединение с базой данных и формирование запроса. Аутентификацию в свою очередь можно разбить на ввод логина и пароля и т.д.

Второй шаг – для конкретных процессов, полученных в ходе функциональной декомпозиции, определяются возможные дополнительные параметры, имеющие дискретный характер ($p_1...p_n$). Например, время в минутах, позиция символов, номер сессии и т.д.

После определения дискретных параметров вводится "бессмысленное" отклонение исходного процесса по его значению ($f_1(\mathbf{par},p)...f_n(\mathbf{par},p)$). Например, для ввода пароля – это смещение символов на клавиатуре в зависимости от их позиции в строке, для коммутации – это перераспределение портов и адресов хостов в сети в зависимости от номера сессии и пр. Функция отклонения должна быть отражена в концепции уникальности системы. Зная ее, можно восстановить исходную функциональную структуру.

Что это дает? Исходное значение функции $f(\mathbf{par})$ является стереотипной схемой, относительно которой злоумышленник пытается произвести атаку. Если функция изменена, то стандартные действия нарушителя не дают ожидаемого им результата, что склоняет его к исследованию атакуемой системы. Но исследование возможно только в том случае, если злоумышленник правильно определит гипотезу (дополнительные параметры) новой функции. В противном случае он не сможет получить информативной обратной связи от «черного ящика». Для случая одного дополнительного параметра $f(\mathbf{par},p_1)$ зависимость уловить достаточно просто, а следовательно и сформулировать правильную гипотезу. Но параметров в процесс можно ввести сколь угодно много - $f(\mathbf{par},p_1,p_2,...,p_n)$, тем самым уводя систему в состояние некоторого «хаоса» для потенциальных злоумышленников.

Защита от исследования систем как элемент информационной безопасности

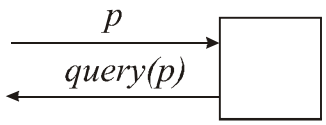
Усложняя процессы в информационных системах, необходимо точно осознавать возможную область для таких модификаций. Многие процессы, такие как стек протокола в операционной системе, принципы коммутации и пр. не поддаются усложнению (или по-другому можно сказать что их усложнение является чрезмерно затратным), но в целом в любые процессы можно вводить дополнительные параметры и формировать для них «концепцию уникальности».

Изложенные идеи легли в основу разработки комплекса программных модулей для защиты от исследования систем (Protecting from Research – PR). В области безопасности рациональнее закрывать от исследования самые популярные уязвимости, совершая атаку по которым нарушитель не получал бы информативной обратной связи. Сценарий такого подхода достаточно прост – пытаясь реализовать простые уязвимости, злоумышленник не наблюдает «сопротивления» системы, и, следовательно, тратит много времени на «распутывание» логики ее работы. Можно сказать что он «вязнет» в системе, т.к. будучи не в состоянии правильно интерпретировать обратную связь, он не совершает действий в рамках поставленной им цели. В то же время приложение легко протоколирует несанкционированную активность, т.к. обнаруживает действия нарушителя по стереотипным схемам атаки.

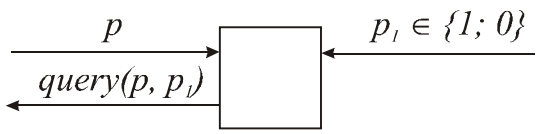
Разработанные в настоящее время приложения для веб-сервера относятся к защите сервера от SQL-инъекций. Это наиболее популярный вид уязвимостей, а поэтому и наиболее оправданный с точки зрения защиты от исследования. Каждый программный модуль написан на PHP и подключается к началу программного кода сайта конструкцией *require_once()*. Далее мы рассмотрим принципы работы этих модулей.

Переадресация несанкционированной активности (PR-HoneyPot)

Первый пример достаточно прост в реализации, так как является функцией всего одного фиксированного параметра и не требует настройки «концепции уникальности». Принцип работы модуля схож с сетевым устройством HoneyPot («горшок с медом») по европейскому патенту EP1218822. Как известно, данное устройство эмулирует несуществующую сеть, как часть реальной, и используется в качестве приманки для нарушителя. Оно сдерживает несанкционированную активность и позволяет изучить нарушителя на «безопасной территории». Само устройство HoneyPot можно интерпретировать как защиту от исследования системы с отклонением по единственному параметру. В нашем случае создается копия структуры базы данных, которая выдается за реальную при обнаружении несанкционированной активности.



а.



б.

Рис.2. Обращение к базе данных

Стандартный запрос к базе данных показан на рис.2.а. Параметр ***p*** представляет собой запрос к базе данных формируемый системой на основании информации передаваемой через массивы ***$GET*** и ***$POST***. Система управления базой данных (MySQL) обрабатывает запрос и выдает ответную реакцию – ***query(p)***.

Мы вводим в этот процесс дополнительный параметр – p_1 (рис.2.б). Он может принимать всего два значения – 0 и 1. Значение единицы он принимает в случае, когда регулярные выражения, проверяющие массивы ***$GET*** и ***$POST***, обнаружили характерные символы для атак ISS и SQL-инъекций.

Формирование запроса к базе данных показано на рис.3.

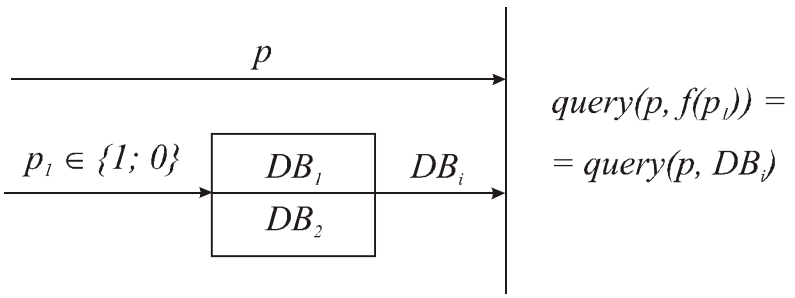


Рис.3. Формирование запроса к базе данных

DB_1 – исходная (оригинальная) база данных сайта. На ее основе создается копия – DB_2, из которой можно убрать (подменить) нужную информацию. Кроме того, не представляет риска удаление и модификация информации в данной БД. Если по регулярным выражениям модуль опознает атаки ISS и SQL-инъекций, то параметр p_1 принимает значение 1 и система переподключается к базе данных DB_2, а так же протоколирует данные массива ***$_SERVER***, содержащего IP-адрес злоумышленника, версию браузера, тип операционной системы и т.д.

Пытаясь реализовать атаку, злоумышленник не встречает сопротивления системы, а поэтому попадается на ту же самую приманку, что и в системе HoneyPot. Для исследования системы ему необходимо получить информативную обратную связь, а это в свою очередь возможно, если будет найдена функция $f(p_1)$ – функция работы регулярных выражений.

Данный модуль очень посредственно иллюстрирует технологию защиты от исследования, т.к. не содержит концепции уникальности (точнее она всегда постоянна и состоит из одного параметра), однако он очень прост в установке и не требует никаких дополнительных настроек. Далее мы рассмотрим расширенный вариант модуля работы с базой данных, позволяющий настраивать концепцию уникальности системы.

Модуль работы с базой данных (PR-DBWeb)

Поскольку подключаемые модули не могут влиять на структуру запроса к базе данных, то все, что мы можем сделать – это увеличить многообразие того, на чем непосредственно строится запрос, т.е. структуру и содержание базы данных. Технология защиты от исследования требует введения множества дискретных параметров $p_1 \ldots p_n$, относительно которых можно ввести функцию отклонения системы $f(p_1, \ldots p_n)$. Поскольку результатом должен быть запрос

$$query(p, f(p_1, \ldots, p_n)) = query(p, DB_i),$$

то функция f есть отображение на множество баз данных:

$$f(p_1,\ldots,p_n) \in \left\{DB_1, DB_2, DB_2^{\,1}, DB_2^{\,2}, \ldots, DB_2^{\,m}\right\}.$$

Принцип формирования запроса для такой функции показан на рис.4.

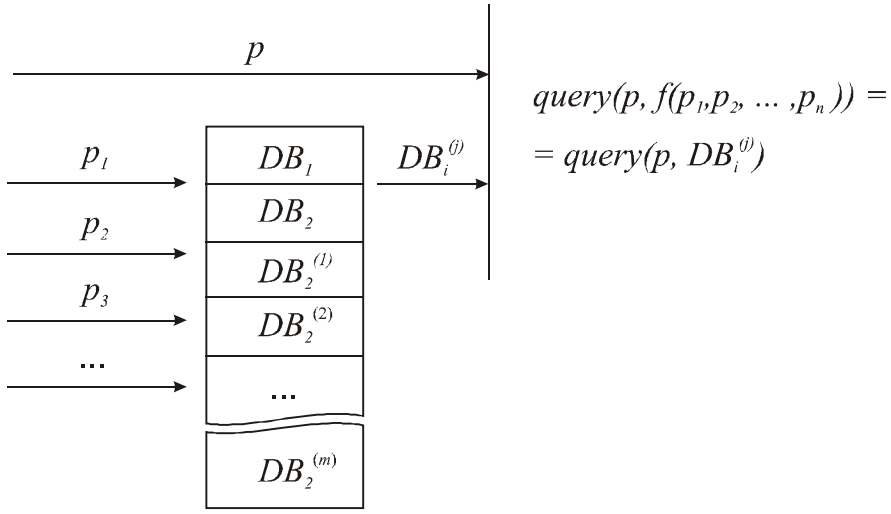


Рис.4. Формирование запроса к базе данных для модуля PR-DBWeb

Запись баз данных с двумя индексами отражает принцип их формирования. DB_1 – исходная (оригинальная) база данных сайта. DB_2 – как и в предыдущем примере – копия ее структуры с пустыми таблицами. Если в концепции уникальности прописаны правила модификации структуры в зависимости от найденных параметров, то структура DB_2 меняется и формируется новое состояние $DB_2^{(j)}$.

Концепция уникальности позволяет администратору настраивать индивидуальную функциональную структуру системы. Она выполнена в виде xml-файла. Структура концепции показана на рис. 5.

Тип параметра	Параметр	Тип функции	Функция
1	DELETE	1	DB_2
2	UNION + LOAD_FILE	3	+1
3	USERS	2	pass = md5(pass)
...	...	...	...

Рис. 5. Концепция уникальности системы

Тип параметра
1 Оператор языка SQL
2 Пара операторов SQL
3 Имена таблиц

Тип функции
1 Выбор базы данных
2 Количество столбцов
3 Значение столбцов

Для примера на рис. 5 рассмотрим принцип работы модуля. Первая строка: если в SQL-запросе встречается оператор DELETE, то происходит переадресация к базе данных DB_2. Вторая строка: если одновременно встречаются операторы UNION и LOAD_FILE, то в таблицу вставляется дополнительный столбец. Это может быть необходимо для запрета загрузки файлов. Если в исходной и в объединяемой таблицах не совпадает количество столбцов, то MySQL выдает ошибку. И последняя строчка: если в тексте SQL-инъекции запрашивается таблица USERS, то над каждой ее строкой в базе данных DB_2 выполняется оператор UPDATE с указанной функцией. В данном случае для каждого пароля еще раз высчитывается хэш-свертка.

Такой подход позволяет администратору добавлять в работу сайта (запрос к базе данных) любые дополнительные параметры и строить, таким образом, уникальную с точки зрения защиты от исследования систему.

Работа системы

Работу модулей можно проиллюстрировать следующим образом. В поисках уязвимостей первое, что сделает злоумышленник, – попытается определить есть ли на сайте проверка параметров передаваемых через массивы $GET и $POST. Для этого он может ввести в запросе одинарную кавычку или конструкции “=1 and 1=1”, “=1 and 1=0” и т.п. Любые простые запросы система переадресует к исходной базе данных, и нарушитель может сделать вывод о возможности успешной атаки. Однако дальнейшие его исследования будут осуществляться на множестве $\{DB_1, DB_2, DB_2^{\,1}, DB_2^{\,2}, ..., DB_2^{\,m}\}$ и вряд ли дадут ему сколько-нибудь значительную информативную обратную связь. Кроме того, модуль сразу запротоколирует источник несанкционированной активности (IP-адрес, версию браузера, тип операционной системы и т.д.).

Механизмы защиты от исследования не подразумевают блокирование уязвимостей (хотя и не исключают их применение). Здесь используется принципиально иной ресурс защиты от преднамеренных атак – информационное управление нарушителем, Следовательно, технология защиты от исследования позволяет дополнительно снижать риск систем информационной безопасности. Рассмотренные механизмы являются примером технической реализации данной технологии.

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-СЕРВЕРА МЕТОДОМ ЗАЩИТЫ ОТ ИССЛЕДОВАНИЯ

Е.С. Семенкин, д.т.н.; М.А. Стюгин (Сибирский государственный аэркосмический университет имени академика М.Ф. Решетнева, styugin@rambler.ru)

Рассматривается подход к обеспечению информационной безопасности на основе информационного управления нарушителем. Приводится алгоритм технологии защиты от исследования систем. Подход иллюстрируется на примере двух технических реализаций технологии для защиты веб-сервера от преднамеренных атак.

Ключевые слова: информационная безопасность, информационное управление, защита от исследования, сдерживание несанкционированной активности.

WEB-SERVER INFORMATION SECURITY IMPROVEMENT WITH TECHNIQUES OF PROTECTION FROM INVESTIGATION

Eugene S. Semenkin, Mikhail A. Styugin (Siberian State Aerospace University, styugin@rambler.ru)

The approach to information security improvement based on informational control of the violator is considered. The algorithm of the technology of systems protection from investigation is presented. The approach is illustrated with two examples of technology implementation for web-server protection from aforethought attacks.

Key words: information security, informational control, protection from investigation, deterrence of unauthorized activity

Сведения об авторах

Семенкин Евгений Станиславович
Сибирский государственный аэрокосмический университет им. ак. М.Ф. Решетнева
профессор кафедры системного анализа и исследования операций,
доктор технических наук, профессор,
т.р. 391-291-91-41
адрес: 660014, г. Красноярск, пр. им. газет "Красноярский рабочий", 34

Стюгин Михаил Андреевич
Сибирский государственный аэрокосмический университет им. ак. М.Ф. Решетнева
аспирант кафедры системного анализа и исследования операций,
т.р. 391-291-91-41
адрес: 660014, г. Красноярск, пр. им. газет "Красноярский рабочий", 34

Сведения об авторах на английском языке

1. Semenkin Eugene, Siberian state aerospace university named after academician M. F. Reshetnev (SibSAU), professor of system analysis and operation research department, doctor of technical sciences, professor.

Phone: ++7- 391-291-91-41
Postal address: "Krasnoyarskiy rabochiy" avenue, 34, Krasnoyarsk, 660014, Russia

2. Styugin Mikhail, Siberian state aerospace university named after academician M. F. Reshetnev (SibSAU), postgraduate student of system analysis and operation research department.

Phone: ++7- 391-291-91-41
Postal address: "Krasnoyarskiy rabochiy" avenue, 34, Krasnoyarsk, 660014, Russia