Спивак Антон Игоревич, Осовецкий Леонид Георгиевич

РЕЗИСТЕНТНОСТЬ КАК ОЦЕНКА БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Адрес статьи: www.gramota.net/materials/1/2010/3-1/15.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2010. № 3 (34): в 2-х ч. Ч. I. С. 62-64. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2010/3-1/

УДК 004.056

Антон Игоревич Спивак, Леонид Георгиевич Осовецкий
Санкт-Петербургский государственный университет информационных технологий механики и оптики

РЕЗИСТЕНТНОСТЬ КАК ОЦЕНКА БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ©

Введение

Процесс совершенствования системы обеспечения безопасности сопровождается измерениями параметров безопасности системы в процессе внедрения изменений. Усиление безопасности свидетельствует о положительном эффекте улучшений, в то время как снижение символизирует о необходимости отказа от сделанных изменений. Выполнение действий по контролю над состоянием систем безопасности, так же включает в себя оценку их безопасности. Важность наличия возможностей для сравнения предоставляемых уровней обеспечения безопасности различных систем обусловливает необходимость проведения исследований в этой области теории защиты информации.

Измерение показателей безопасности упростит разработку систем защиты и прогнозирование изменений уровня безопасности на всем протяжении жизненного цикла работы системы защиты информации.

Сложность оценки безопасности вызвана несколькими особенностями:

- различия в понимании смысла понятия безопасность;
- применение понятия безопасность в разном контексте;
- неопределенность величины.

Понимание определения безопасности может быть различным. Сложность заключается в фиксировании состояния, в котором систему можно считать безопасной. То есть определения границ безопасного и небезопасного состояний.

Безопасность нельзя воспринимать отдельно от окружающего контекста - внешние факторы влияют на интерпретацию значения безопасности. Одна и та же система защита в одной организации может считаться безопасной, в то время как в другой не будет удовлетворять предъявляемым требованиям.

Неопределенность вызвана отсутствием критерия оценки нарушений безопасности, с точки зрение влияния на защищенность. Является нарушение значительным или несущественным в конкретных условиях функционирования системы.

Все эти особенности накладывают на процесс оценки безопасности определенные ограничения, которые должны быть учтены в методах ее измерения. Не исключено применение адаптированных под конкретные задачи способов измерения показателей безопасности. В таких случаях выделяются наиболее важные аспекты и их значения доминируют над остальными, не существенными в конкретном контексте. Разработка частных методов оценки безопасности объектов информатизации является частью проектирования общего подхода определения показателей безопасности.

Существующие разработки методов оценки безопасности

Актуальность разработки методов оценки безопасности обусловило проведение ряда исследований в этом направлении.

В [8] различается два уровня абстракции (высокий и низкий), которые используются для проведения оценки безопасности. На высоком уровне абстракции безопасность представляет собой поддающиеся количественному определению показатели системы. При этом объекты, под ними подразумеваются программные продукты, информационные системы и др. обладают атрибутами, которые объединяют характеристики, отражающие безопасность оцениваемого объекта. Таким образом, безопасность - это количественное измерение того каким количеством таких атрибутов обладает объект. Эти атрибуты могут быть определены на основе физических характеристик низкого уровня абстракции.

Согласно [3] метрики являются инструментами, которые предназначены для содействия в принятии решений по улучшению функционирования работы системы. При этом производится сбор и анализ значимых данных. Основываясь на наблюдениях за параметрами, производятся корректирующие изменения процессов работы системы. Аналогичное значение имеет оценка параметров безопасности для систем защиты информации.

Измерение параметров, отражающих безопасность, предоставляет единую точку зрения во времени специфичных для безопасности дискретных данных. Они могут сравниваться с предопределенными базовыми требованиями безопасности и тем самым производить мониторинг изменений уровня безопасности [7].

Проведение аналогии между безопасностью и надежностью представляется одним из способов оценки безопасности системы [2, p. 211-230]. Данный подход основан на прогнозировании промежутка времени до следующего нарушения безопасности, используя данные об атаках со стороны злоумышленников. При этом проводится сопоставление понятий отказ системы и нарушение ее безопасности.

Измерение безопасности одной системы в сравнении с другой имеет место в [5; 6]. Для этого предлагается использование величины «атакуемости» системы, формируемой на основе анализа способов, которыми можно воспользоваться для осуществления взлома. Основными существенными характеристиками для проведения атаки на систему являются каналы сетевой передачи, методы передачи, а также потоки данных (вводимые данные, файлы). Чем больше ресурсов системы доступно атакующему, тем более она уязвима. Производится деление ресурсов системы на классы в соответствии с эффективностью их использования в ходе атаки.

Оценка безопасности системы может производиться на основе измерения величины воздействий нарушителей [1]. Для этого применим способ оценки изменения вероятности реализации угроз безопасности до воздействия на объект защиты и после него. Для вероятности реализации угрозы предлагается соотношение, которое зависит от количества уровней защиты объекта. Их изменение дает возможность оценить вероятность реализации угрозы безопасности.

В [4] приводится попытка определения оценки безопасности для систем выполняющих телекоммуникационные функции. Утверждается, что возможно производить оценку систем одинаковых по функционалу и имеющих различия только в уровне безопасности. При этом предлагается два подхода к оценке безопасности. Первый основан на оценке возможностей нарушителя безопасности, а именно его знаниях и физических ресурсах. Вторым методом является способ определения безопасности системы на базе информации о слабости ее защиты против угроз безопасности. Уязвимости системы определяются на основе тщательного анализа, осуществляемого силами обслуживающего персонала системы.

Резистентность объекта

Исследования проблемы оценки безопасности в большинстве случаев сводятся к разработке методов оценки безопасности для определенных условий и разработки универсального метода измерения безопасности.

Предлагаемый в данной статье подход относится к числу специализированных методов, предназначенных для оценки безопасности в условиях передачи информации в сети связи.

Предполагается, что существует сложная сетевая инфраструктура, в которой присутствует множество маршрутов передачи информации между всеми узлами сети. Безопасность узла оценивается с точки зрения ее влияния на безопасность информации, передаваемой через данный узел. Такое условие обуславливает необходимость анализа параметров узла, способных воздействовать на безопасность передачи информации.

Для измерения безопасности объекта информатизации введем новое понятие резистентности. Такое название связано со специальным контекстом, в рамках которого применяется оценка безопасности. Подвергается измерению безопасность, которую предоставляет узел сети связи проходимой через него информации. Снижение безопасности узла вследствие угроз безопасности может влиять на передаваемую информацию. Если предположить что безопасность информации базируется на предоставлении ей при передаче целостности, конфиденциальности и доступности, то любое изменение безопасности узла сети вызовет закономерное изменение безопасности передаваемой информации. Взлом узла сети может позволить злоумышленникам получить доступ к передаваемой информации и тем самым потенциально реализовать угрозу целостности и конфиденциальности, так как в этом случае нарушители безопасности получают контроль над потоком передаваемых данных. Атаки злоумышленника, сопровождающиеся высокой загрузкой канала связи, а также возможными мерами, вызывающими повышенное использование ресурсов узла связи, могут привести к значительному снижению его производительности и как следствие низкой скорости передачи, а возможно ее полному прекращению. Данное поведение приводит к реализации атаки на доступность передаваемой информации. Описанные атакующие действия позволяют говорить об интерпретации безопасности как о свойстве уязвимости узлов сети атакам, направленным на передаваемую информацию. Другими словами подверженности узлов влиянию угроз на безопасность информации.

Влияние безопасности сетевого узла на безопасность, следуемой через него информации, можно охарактеризовать как возможное снижение безопасности информации путем реализации угроз безопасности, направленных на узел сети. Если предположить что сетевой узел будет сопротивляться такого рода действиям со стороны нарушителей безопасности, то можно поставить в соответствие свойство сопротивляемости таким угрозам - резистентности. Данное понятие означает устойчивость объекта к воздействиям внешних сил.

Для оценки безопасности пути следования целесообразно применять понятие резистентности узлов связи. Сложение резистентностей всех узлов, через которые проходит информация, позволяет оценивать безопасность маршрута следования информации.

Заключение

Исследования в области создания количественных и качественных измерений величины безопасности ведутся постоянно. Применяются различные методы оценки безопасности, цель которых получить качественно новые способы управления и контроля над безопасностью объектов информатизации.

В данной статье описано применение нового понятия резистентность узла сети, призванного решить проблему оценки изменения безопасности информации в процессе следования по сети передачи данных. Применение данного метода основано на свойствах подверженности узлов сети атакам злоумышленников. Дальнейшие исследования в данной области необходимо посвятить разработке методов оценки уязвимости узлов сети, а также их способностям противодействовать внешним воздействиям злоумышленников.

Список литературы

1. **Спивак А. И.** Оценка эффективности атак злоумышленника в процессе построения его модели // Научно-технический вестник. СПб.: СПбГУ ИТМО, 2010. Вып. 66.
2. **Bev Littlewood et al.** Towards operational measures of computer security // Journal of computer security. 1993. V. 2. № 2-3.
3. **Marianne Swanson et al.** Security metrics guide for information technology systems // NIST special publication. 2003. July. № 800-55.
4. **Mark Torgerson.** Security metrics for communication systems // 12th International command and control research and technology symposium. Rhode Island, 2007.
5. **Pratyusa Manadhata, Jeannette M. Wing.** An attack surface metric. CMU-CS-05-155. Carnegie Mellon University, 2005.
6. **Pratyusa Manadhata, Kymie M. C. Tan, Roy A. Maxion, Jeannette M. Wing.** An approach to measuring a system's attack surface. CMU-CS-07-146. Carnegie Mellon University, 2007.
7. **Shirley C. Payne.** A guide to security metrics // SANS security essentials: GSEC practical assignment. 2006. Version 1.2e.
8. **SSE-CMM: Systems security engineering capability maturity model** // International systems security engineering association (ISSEA). 2008.

УДК 004.413.2

Игорь Александрович Янков
Пензенский государственный университет

ОБЩАЯ СХЕМА ПОСТРОЕНИЯ РАСПИСАНИЙ С ИЕРАРХИЧЕСКОЙ ДРЕВОВИДНОЙ СТРУКТУРОЙ СВЯЗЕЙ©

Качество работы отраслей современной экономики во многом зависит от качества решений, принимаемых на этапах планирования и оперативного управления. В ряде областей человеческой деятельности (управлении, производстве, транспорте, образовании, сельском хозяйстве и т.д.) использование средств автоматизированного планирования позволяет вывести эффективность работы на принципиально новый уровень. Именно поэтому в последнее время большое распространение получили системы автоматического построения и динамического управления расписаниями. Задачей таких систем является генерация оптимальных расписаний и поддержка сводного плана в актуальном состоянии, т.е. динамическое перестроение расписания согласно изменяющимся внешним условиям и данным о выполнении плана. Наиболее выгодным является использование таких систем в областях, где в сводном расписании участвуют множество разнотипных ресурсов, выполняя различные действия, направленные на достижение заданной цели. Хорошим примером может служить расписание машин и водителей, работающих в компании по сдаче автомобилей в аренду. Так как, выполняя доставку (забор) автомобилей, водители подвозят другу друга на различных участках пути [4]. Для таких предметных областей характерна большая связанность всех ресурсов, когда расписание одного участника тесно переплетается с другими и почти не может быть изменено без серьезного перестроения всего плана.

В ходе анализа практических задач подобного рода было выявлено, что структура таких расписаний несколько сложнее, чем абстрактные модели расписаний для одностадийных и многостадийных систем обслуживания, которые хорошо исследованы в рамках теории расписаний [1]. Особенностью является то, что каждое требование обрабатывается на нескольких ресурсах, а порядок выполнения операций имеет древовидную структуру [3]. Для решения этой задачи были предложены модель расписания с иерархической древовидной структурой связей, которая позволяет описать процесс обслуживания каждого требования. В данной статье мы рассмотрим общую схему построения таких расписаний.

Согласно ранее предложенной модели процесс обслуживания каждого требования это последовательное выполнение ресурсами множества задач, связанных друг с другом причинно-следственными связями, позволяющими определять необходимость существования тех или иных элементов расписания. Правила задания таких связей характеризуются конкретной предметной областью, и в общем случае, задаются в виде схемы ветвления задач [2], которая определяет, при каких условиях требуется создавать подчиненные задачи, а при каких - нет. Будем считать расписание допустимым, если оно соответствует схеме ветвления задач в данной области, т.е. дерево задач обслуживания каждого требования строго следует условиям ветвления. Именно по этой причине процесс поиска допустимых решений целесообразно вести на основе схемы ветвления, поэтапно создавая подчиненные задачи и находя наиболее подходящие ресурсы для размещения каждой из них.

Таким образом, построение расписания обслуживания множества требований осуществляется поэлементно, как совокупность построения расписаний для каждого требования отдельно. Для этого сначала все требования очереди сортируются в порядке, который бы максимально сильно соответствовал порядку естественного обслуживания требований.
