2009 Математические основы компьютерной безопасности №1(3)
DOI 10.17223/20710410/3/7
УДК 681.322

ОБ ИСПОЛЬЗОВАНИИ ФОРМАЛЬНЫХ МОДЕЛЕЙ ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ

Д. Н. Колегов

Томский государственный университет, г. Томск

E-mail: d.n.kolegov@gmail.com

В статье рассматривается возможный подход к анализу уязвимостей с использованием математических моделей безопасности компьютерных систем. В рамках ДП-моделей строится модель нарушителя, описанная в «Критериях оценки безопасности информационных технологий», и дается математическое определение стойкости к проникновению.

Ключевые слова: *анализ уязвимостей, модель нарушителя, тестирование проникновения, модели безопасности, функциональные требования, обоснование безопасности, доверие.*

Введение

Использование математических моделей является обязательным при разработке и анализе безопасности компьютерных систем (КС) с высоким уровнем доверия. Так, в соответствии с «Критериями оценки безопасности информационных технологий» [1–4] для КС с оценочным уровнем доверия (ОУД) более 5 требуется, чтобы при их разработке была использована формальная (математическая) модель политики безопасности (ADV_SPM.3) [4]. Для КС, начиная с ОУД 2, требуется обязательное проведение анализа уязвимостей и тестирования проникновения. При этом указано, что разработчик должен предоставить документацию, содержащую строгое обоснование того, что объект оценки (ОО) с идентифицированными уязвимостями является стойким к явным нападениям проникновения. Под термином «строгое обоснование» (justification) следует понимать анализ (менее строгий, чем формальный), ведущий к необходимому заключению. Начиная с ОУД 4, для КС требуется независимый анализ того, что ОО с идентифицированными уязвимостями является стойким к проникновению со стороны нарушителя, обладающего низким, умеренным или высоким потенциалом нападения (AVA_VLA). Однако требования по использованию формальных моделей для проведения анализа уязвимостей КС в [1–4] отсутствуют. В данной работе показывается возможность применения математических моделей для анализа уязвимостей КС. Для этого в рамках ДП-моделей [5, 6] описывается модель нарушителя и дается математическое определение стойкости КС к проникновению в соответствии с требованиями семейства доверия 14.4 «Анализ уязвимостей» (AVA_VLA) в [4].

1. Общие предположения и определения

Дальнейшее изложение будет вестись на основе работ [5, 6] с учетом всех определений, обозначений и теорем в них. В соответствии с [7, 8] под уязвимостью понимается некоторый недостаток КС, который может использоваться для реализации угроз. Анализ уязвимостей КС [4] включает идентификацию недостатков, внесенных на различных этапах жизненного цикла КС, и подтверждение выявленных уязвимостей посредством тестирования проникновения, позволяющим сделать заключение о возможности использования уязвимостей для нарушения безопасности. Дадим определение.

Определение 1. *Уязвимостями* будем называть сущности, функционально или параметрически ассоциированные с другими субъектами КС, если при реализации информационных потоков к ним или от них соответственно происходит нарушение безопасности. Субъекты, имеющие такие сущности, назовем *уязвимыми*.

Замечание 1. По определению 1 уязвимость является сущность-субъектом или сущность-объектом.

Определение 2. Пусть $G = (S, E, R \cup A \cup F, H)$ — состояние КС $\Sigma(G^*, OP)$. Определим элементы состояния G: E — множество сущностей; EC — множество узлов; V — множество уязвимостей; CC — множество коммуникационных каналов; IC — множество интерфейсов взаимодействия; S — множество субъектов; R — множество ребер графа-состояния G, соответствующих правам доступа пользователей к сущностям; A — множество ребер графа-состояния G, соответствующих доступам пользователей к сущностям; F — множество ребер графа-состояния G, соответствующих информационным потокам между сущностями; $H : E \to 2^E$ — функция иерархии сущностей, ее значения на множестве узлов EC соответствуют заданной в КС иерархии подчиненности компьютеров. При этом выполняются следующие условия:

1) $V \subset E,\ CC \subset E,\ IC \subset E,\ EC \subset E$;
2) множества V, CC, EC, IC попарно не пересекаются;
3) каждая сущность $e \in E$:
   - либо является узлом КС ($e \in EC$), либо размещена на некотором единственном для каждой сущности узле (для сущности $e \in E$ существует единственный узел $c \in EC$ такой, что $e < c$),
   - либо является коммуникационным каналом ($e \in EC$),
   - либо является интерфейсом взаимодействия с КС($e \in IC$),
   - либо является уязвимостью ($e \in V$),
   - либо является пользователем или процессом пользователя ($e \in S$).

КС будем рассматривать с учетом сетевого уровня, поэтому с учетом положений БК ДП-модели [5] будем считать, что выполняется следующее предположение.

Предположение 1. Для каждого узла (компьютера) $c \in EC$ определены доверенные пользователи, обладающие правом доступа владения к каждой сущности, размещенной на данном узле, и коммуникационные каналы (сущности-объекты), через которые осуществляется передача данных между субъектами узлов КС. Если пользователь $os_c \in S$ является доверенным пользователем компьютера c или пользователь $s \in S$ обладает правом доступа владения own_r к компьютеру c в состоянии G, то он обладает правом доступа владения к каждой сущности, размещенной на данном узле. Для каждого узла определены коммуникационные каналы и интерфейсы взаимодействия (сущности-объекты), через которые осуществляется передача данных между субъектами узлов КС.

В зависимости от архитектуры системы безопасности современных КС возможно несколько способов передачи прав доступа при активизации и функционировании пользовательского процесса. Для реализаций нарушений безопасности субъектами-нарушителями используются следующие уязвимости современных КС, приводящие к получению субъектом-нарушителем прав пользователей КС:

— ошибки в ПО, реализующем прикладные и системные процессы ОС;

— ошибки в реализации, конфигурировании и использовании КС, приводящие к реализации информационных потоков по памяти и по времени между нарушителем и субъектами КС;
— возможность получения или изменения некоторых параметров КС.

Таким образом, будем использовать следующее предположение.

Предположение 2. В КС выполняются следующие условия:

— при активации субъектом-пользователем $u \in S$ некоторого процесса $p \in S$ последний наследует все права пользователя u;
— уязвимости процесса функционально-ассоциированы с субъектом-пользователем, от имени которого данный процесс запущен;
— уязвимости, связанные с раскрытием параметров функционирования КС, параметрически-ассоциированы с субъектом-пользователем, преобразования данных которого определяются этими параметрами.

2. Модель нарушителя и определение стойкости к проникновению

В семействе доверия «Анализ уязвимостей» (AVA_VLA) класса «Оценка уязвимостей» (AVA) «Критериев оценки безопасности информационных технологий» [4] определены три компоненты, включающие независимый анализ уязвимостей, проводимый оценщиком. Основная цель данного анализа — сделать заключение, что ОО является стойким к нападениям проникновения со стороны нарушителя, обладающего низким (для AVA_VLA.2), умеренным (для AVA_VLA.3) или высоким (для AVA_VLA.4) потенциалом нападения. Для достижения этой цели оценщик сначала проверяет возможности использования всех идентифицированных уязвимостей. Это осуществляется посредством тестирования проникновения. Оценщику следует принять на себя роль нарушителя с одним из указанным выше потенциалов нападения при попытке проникновения в ОО. Любое использование уязвимостей таким нарушителем оценщику следует рассматривать как «явное нападение проникновения» (в отношении элементов AVA_VLA.*.2C) в контексте компонентов AVA_VLA.2 – 4. Кроме того, при анализе уязвимостей рассматривают угрозы в предположении, что нарушитель будет в состоянии обнаружить недостатки, позволяющие получить несанкционированный доступ к ресурсам (например, данным), препятствовать выполнению функций безопасности и искажать их или же ограничивать санкционированные возможности других пользователей. Так, идентификация известных уязвимостей может быть проведена путем анализа исходного кода ПО, применения сканеров безопасности уровня узла или сети. Будем использовать следующее предположение.

Определение 3. Модель нарушителя содержит такие условия:

— существует три класса нарушителей;
— нарушитель любого класса имеет все данные о КС (например, исходные коды программного обеспечения, документация);
— нарушитель с низким потенциалом нападения инициирует выполнение всех правил преобразования в КС;
— нарушитель с умеренным потенциалом нападения может кооперироваться с некоторыми субъектами КС, кроме субъектов тестируемого узла КС;
— нарушитель с высоким потенциалом нападения может кооперироваться с любыми субъектами КС;
— нарушитель любого класса знает все уязвимости КС;

— нарушитель может осуществлять удаленный или локальный доступ к субъектам КС через коммуникационные каналы или интерфейсы взаимодействия.

С учетом «Критериев оценки безопасности информационных технологий» [4] и введенной модели нарушителя дадим следующее определение.

Определение 4. Пусть имеются $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — начальное состояние КС (G^*, OP), недоверенный субъект-нарушитель $x \in N_S \cap S_0$ и контейнер-узел $c \in EC$. Будем говорить, что узел $c \in EC$ является *стойким к проникновению нарушителя с низким потенциалом нападения* (*НПН-стойким*) тогда и только тогда, когда для любого недоверенного субъекта $y \in N_S \cap S_0$, размещенного на узле c, предикат $directly\_can\_share\_own(x, y, G_0, L_S)$ является ложным. Будем говорить, что узел $c \in EC$ является *стойким к проникновению нарушителя с умеренным потенциалом нападения* (*УПН-стойким*) тогда и только тогда, когда для любого доверенного субъекта $y \in L_S \cap S_0$, размещенного на узле c, предикат $can\_steal\_own(x, y, G_0, L_S)$ является ложным. Наконец, будем говорить, что узел $c \in EC$ является *стойким к проникновению нарушителя с высоким потенциалом нападения* (*ВПН-стойким*) тогда и только тогда, когда для любого доверенного субъекта $y \in L_S \cap S_0$, размещенного на узле c, предикат $can\_share\_own(x, y, G_0, L_S)$ является ложным.

В [5, 6] сформулированы и обоснованы условия истинности предикатов $directly\_can\_share\_own(x, y, G_0, L_S)$, $can\_share\_own(x, y, G_0, L_S)$ и $can\_steal\_own(x, y, G_0, L_S)$. Кроме того, существуют алгоритмы проверки условий истинности данных предикатов за конечное время.

Таким образом, математические модели безопасности возможно использовать не только для разработки формальных политик безопасности, но и для анализа уязвимостей КС: описания модели нарушителя, математического определения стойкости к нарушениям безопасности (проникновению), описания уязвимостей, условий их использования и передачи прав доступов и реализации информационных потоков, возникающих при этом.

ЛИТЕРАТУРА

1. Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. ISO/IEC 15408–1, 1999.
2. Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements. ISO/IEC 15408–2, 1999.
3. Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements. ISO/IEC 15408–3, 1999.
4. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Ч. 1, 2 и 3. М., 2002.
5. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
6. *Колегов Д. Н.* Анализ безопасности информационных потоков по памяти в компьютерных системах с функционально и параметрически ассоциированными сущностями // Прикладная дискретная математика. 2009. № 1. С. 117–125.
7. NIST. Technical guide to information security testing and assessment. Recommendations of the National Institute of Standarts and Technology. September, 2008.
8. ФСТЭК России. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации. М., 2004.