УДК 681.3.06

О.С. Волковский

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ РАСПОЗНАВАНИЯ УДАЛЕННЫХ СЕТЕВЫХ АТАК НА УРОВНЕ ПРИЛОЖЕНИЙ

Постановка проблемы. Объединение компьютеров в локальные и глобальные сети открывает огромные возможности для решения задач, связанных с обменом и обработкой информации. Однако, при этом возникает множество проблем, связанных обеспечением безопасности соединения, защитой сети и конкретного хоста от несанкционированного сетевого доступа. В последнее время развиваются методы построения защиты систем, основанные на категоризации новых объектов по степени их безопасности и установке некоторого низшего уровня безопасности (порога доверия), преодоление которого приводит к тому, что объект считается доверенным[1-4]. Применение такой модели представляется оправданным благодаря возможности реализации гибкой политики безопасности, т.к. порог доверия может изменяться во времени. При этом возникает потребность в разработке соответствующих правил работы системы защиты, минимизирующих количество ошибочных ситуаций (доверенный объект признается не доверенным и наоборот).

Результаты исследований. Целью исследований являлась разработка модели системы, альтернативной к антивирусам и брандмауэрам прикладного уровня, позволяющей осуществлять защиту хоста или сети от несанкционированного доступа путем отслеживания e-mail сообщений, содержащих вирусы или потенциально опасный исполняемый код.

Исходно принималось, что сообщение должно соответствовать определенной структуре и должно быть сформированным по определенным правилам. Иначе это сообщение считается подозрительным, а в случае невозможности корректного разбора – опасным. Схема обработки сообщения состоит из следующих этапов: рекурсивная декомпозиция электронного письма; анализ структуры заголовка сообщения; анализ содержимого письма с последующей его категоризацией; действия над письмом в зависимости от присвоения

категории. Приведенная схема конкретизирована в следующий общий алгоритм обработки:

1. получение сообщения;
2. разбивка сообщения на заголовок, тело и вложения;
3. выделение тел отдельных вложений;
4. декодирование файла вложения по методу его кодирования;
5. определение действительного типа вложения;
6. выделение кода из файла вложения;
7. проверка полученного кода на содержание элементов кода вируса;
8. классификация сообщения и последующие действия над ним.

При выборе параметров для анализа почтового сообщения исходили из следующих предпосылок: сообщение однозначно считается опасным при совпадении структуры кода в теле вложения с известными опасными структурами кодов но, поскольку сигнатурный метод может не выявить все существующие вирусы, требуется ввести правила для оценки корректности структуры самого сообщения. По результатам анализа типового поведения вирусов в сообщениях электронной почты были выделены основные параметры сообщения, подлежащие детальной проверке. Чтобы определить порог доверия для почтового сообщения введем некоторую шкалу, на основе которой будет определяться степень его безопасности. Для этого опишем идеальное с точки зрения безопасности почтовое сообщение и примем его за образец. Введем соответствующие обозначения и определим возможные значения выделенных ранее параметров.

Таблица 1

Параметры почтовых сообщений

Название параметра почтового сообщения	Обозначение	Идеальное значение	Возможные значения
Совпадение поля “От” и обратного адреса	$Р_{адр}$	Да	Да/Нет
Совпадение указанного в заголовке сообщения MIME–типа вложения и его реального типа	$Р_{тип}$	Да	Да/Нет
Совпадение указанной в теле сообщения контрольной суммы вложения и ее реального значения	$Р_{ксум}$	Да	Да/Нет
Совпадение первой и второй подписей boundary, которые ограничивают вложения в теле почтового сообщения	$Р_{подп}$	Да	Да/Нет

 ISSN 1562-9945

Количество фрагментов данных между подписями boundary равно 1	Рфрагм	Да	Да/Нет
Степень вложенности почтовых сообщений <=15	РвлП	Да	Да/Нет
Степень вложенности архивов во вложениях в почтовые сообщения <= 33	РвлА	Да	Да/Нет
Отсутствие исполняемого кода в теле вложений	Ркод	Да	Да/Нет

Наиболее весомыми из параметров являются отсутствие исполняемого кода в теле вложений, степень вложенности архивов во вложениях в почтовые сообщения, совпадение указанного в заголовке сообщения MIME–типа вложения и его реального типа. Далее по степени опасности следуют несовпадения полей “От” и обратного адреса а также несовпадение указанной в теле сообщения контрольной суммы вложения и ее реального значения. На последнем месте, с точки зрения безопасности, находятся параметры несовпадения первой и второй подписей boundary, которые ограничивают вложения в теле сообщения, и количество фрагментов данных между этими подписями.

Более подробно остановимся на принятых значениях степеней вложенности

РвлП и РвлА. Среди известных вирусов, использующих вложения почтовых сообщений одно в другое, вирусом, который использует наименьшую среди других степень вложенности, является Email-Worm.Win32.Swen и его разновидность I- Worm/Swen.A, создающие вложения, которые выглядят как вложение письма в письмо. Количество вложений колеблется от 16 до 666. Поэтому максимальное допустимое число вложений было ограничено 15. Существует также 3ARC-Worm.Win32.Gen – червь, создающий архивы, вложенные один в один, и присоединяющий их к почтовым сообщениям в качестве вложений. Количество таких вложенных архивов может быть в пределах от 34 до 134. Вложения архива в архив происходит для всех известных червю типов архивов, количество которых составляет 34. Поэтому максимальная степень вложения архивов ограничена 33.

Для оценки степени безопасности почтового сообщения использовалась интегральная оценка в виде взвешенной суммы всех параметров:

$$Р_{инт} = \sum P_i V_i \ ,(1)$$

где P_i - значение i-того параметра почтового сообщения, V_i -его весовой коэффициент.

Для определения весовых коэффициентов параметров было проведено шесть серий практических экспериментов на базе разработанного proxy-сервера с почтовыми сообщениями с заранее известной степенью безопасности. Учитывались всевозможные комбинации значений выделенных параметров. Исходно принималось, что наиболее значимые параметры должны иметь весовые коэффициенты не менее чем на 75% большие, чем остальные. Результаты экспериментов приведены в таблице 2.

Таблица 2

Результаты экспериментов

№ п/п	Ртип	РвлП	РвлА	Ркод	Радр	Ркcум	Рподп	Рфрагм	Точность классификации
	0.15	0.15	0.15	0.15	0.12	0.12	0.08	0.08	не точная
2.	0.16	0.16	0.16	0.16	0.11	0.11	0.07	0.07	не точная
3.	0.17	0.17	0.17	0.17	0.10	0.10	0.06	0.06	точная
4.	0.18	0.18	0.18	0.18	0.10	0.10	0.04	0.04	точная
5.	0.19	0.19	0.19	0.19	0.10	0.10	0.02	0.02	точная
6.	0.20	0.20	0.20	0.20	0.08	0.08	0.02	0.02	точная

Наивысшая точность при классификации принимаемых сообщений была достигнута в 6-ой серии экспериментов.

Согласно таблице 1 будем считать, что “да”=1, а “нет”=0 для возможных значений анализируемых параметров сообщения. Тогда для идеального сообщения имеем сигнатуру “11111111” при значении интегральной оценки равном 1. Введем классы почтовых сообщений и установим границы интегральной оценки степени безопасности. В качестве значений границ примем результаты из 6-ой серии экспериментов.

Таблица 3

Значения интегральных оценок для различных классов сообщений

Название класса сообщения	Интервал значения интегральной оценки степени безопасности
Инфицированное	совпадение сигнатуры кода вложения с сигнатурой опасного кода
Возможное заражение	>=0,00 и < 0,70

 ISSN 1562-9945

Небезопасное	>=0,70 и < 0,92
Безопасное	>=0,92

Выводы. Исследована возможность использования в качестве правила определения степени безопасности почтового сообщения косвенных признаков наличия вирусов и потенциально опасного кода. При анализе статистических данных, полученных в результате применения разработанной proxy-серверной программы, установлены параметры почтовых сообщений, значения которых влияют на степень их безопасности, и определены степени влияния каждого из параметров на интегральную оценку. Выделены 4 класса почтовых сообщений, для которых установлены границы значений интегральной оценки степени безопасности. Разработанная система обеспечивает точную классификацию как на тестовых наборах данных, так и в отношении вновь поступающих сообщений. При смене политики безопасности возможна адаптация системы путем смены значений весовых коэффициентов или значений границ интегральной оценки для выделенных классов безопасности.

ЛИТЕРАТУРА

1. Diapankar DasGupta. Artifikal Immune Systems and Their Applikations.Springer-Verlag New York, Incorporated, 1998.
2. S. Hofmeyr, S. Forrest. Architekture for Artifikal Immune System. // Evolutionari Computation 7(1):45-68, the Massachusetts Institute of Technology, 1999.
3. Волковский О.С., Фенога Д.А. О применении иммунных систем для защиты от несанкционированного доступа по компьютерной сети// Системные технологии. Региональный межвузовский сборник научных трудов.-Выпуск 5(16), Днепропетровск, 2001.-с.127-130.
4. Волковский О.С., Комарова М.Г. Синтез адаптивных правил идентификации пакета при построении системы безопасности компьютерной сети //Системные технологии. Региональный межвузовский сборник научных трудов. -Выпуск 2(31), Днепропетровск, 2004.-с.109-114.

Получено 21.12.2007 г.