На правах рукописи

ГАЙДАР
Михаил Борисович

РАЗРАБОТКА И ИССЛЕДОВАНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ УДАЛЕННОЙ АТАКИ ТИПА «ПОДМЕНА ДОВЕРЕННОГО СУБЪЕКТА TCP-СОЕДИНЕНИЯ» С ЦЕЛЬЮ ПОСТРОЕНИЯ ЭФФЕКТИВНОГО МЕХАНИЗМА ЗАЩИТЫ ЭЛЕМЕНТОВ КОМПЬЮТЕРНОЙ СЕТИ

05.13.18 – Математическое моделирование,
численные методы и комплексы программ.

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург
2004

Работа выполнена на кафедре «Прикладная математика»
ГОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:
Доктор технических наук, профессор — Вильчевский Н.О.

Официальные оппоненты:
Доктор физико-математических наук, профессор — Шевляков Г.Л.
Кандидат технических наук — Молдовян А.А.

Ведущая организация: Центральный научно-исследовательский и проектно-конструкторский институт робототехники и технической кибернетики министерства науки и образования РФ

Защита диссертации состоится «29» 12 2004 г. в 16⁰⁰ часов на заседании Диссертационного совета Д 212.229.13 Санкт-Петербургского государственного политехнического университета по адресу: 195251, Санкт-Петербург, Политехническая ул., №29, корпус I, аудитория 41.

Автореферат разослан «29» ноября 2004 г.

Ученый секретарь диссертационного совета
Д 212.229.13 доктор биологических наук, профессор — Зинковский А.В.

Актуальность темы

Экономическая и технологическая безопасность государств в условиях, характеризуемых возрастающей ролью информационной сферы, представляющей собой совокупность телекоммуникационных средств, информационных ресурсов и субъектов осуществляющих их сбор, формирование и использование, в огромной степени зависит от интеграции научных исследований и разработок в области обеспечения безопасности в информационной сфере с промышленно-производственными и военными системами. Реализация такого подхода требует взаимоувязанного решения ряда сложных научно-технических и организационных задач, таких как: создание информационной сети для передачи открытой информации, включая создание средств управления информационными ресурсами, средств, обеспечивающих защищенное межсетевое взаимодействие информационных систем. Таким образом, построение защищенного информационного пространства РФ становится приоритетной целью развития отечественного научно-производственного комплекса, а создание инструментальных средств достижения этой цели – важным направлением прикладных исследований и разработок.

Анализ источников возникающих внештатных ситуаций в работе телекоммуникационных систем дает основания утверждать, что лидирующие позиции, как по количеству попыток, так и по успешности их реализации, занимают удаленные атаки на узлы компьютерных сетей. Этому заключению могут быть даны различные объяснения – масштабность сетей, их открытость, особенности реализаций и подобные. Но ни одно из объяснений не противоречит ни требованию обеспечить безопасность как самой телекоммуникационной структуры, так и информации, в ней содержащейся, ни актуальности усилий для достижения этой цели.

Цель работы

Данная диссертационная работа имела целью создание и исследование математической модели атаки типа «*Подмена доверенного объекта или субъекта распределенной вычислительной системы*» и использование ее для построения возможных вариантов эффективных защит элементов компьютерных сетей.

Основные задачи работы.

Разработать математическую модель атаки на удаленные хосты компьютерной сети.

Используя разработанную математическую модель удаленной атаки найти условия, при достижении которых опасность успешной реализации атаки наиболее вероятна.

Предложить варианты защит от атак выбранного для рассмотрения класса, оценить их эффективность.

Структура работы

Работа состоит из введения, четырех глав, заключения и библиографии, включающей 66 наименований работ отечественных и зарубежных авторов. Объем диссертации 86 страниц. В работе приведено 36 рисунков.

Глава 1 диссертации посвящена введению в предметную область, обоснованию выбора предмета исследований.

Глава 2 заключает в себе неформальную, содержательную постановку задачи. Рассматриваются особенности принятых протоколов передачи данных, обусловивших возможность интервенции. Описаны все шаги интервента при организации атаки. Рассматриваются особенности различных операционных сред, учитываемые при планировании нападения. Приводятся результаты некоторых экспериментов по формированию атрибутов диалога, проведенных с распространенными операционными системами.

Глава 3 работы посвящена формальной постановке задаче. Строится формальная модель атаки. Выясняется зависимость вероятности успеха атаки от поведения интервента на каждом шаге при различных законах распределения параметров сети. Приводятся результаты численных экспериментов. Делаются важные для построения защиты выводы.

Глава 4 носит прагматический характер; здесь обсуждаются возможные варианты защиты от атак рассматриваемого класса.

Научная новизна

Научная новизна работы заключается в: разработке математической модели удаленной сетевой атаки, позволяющей создать на ее основе инструментальные средства обнаружения и защиты узлов компьютерной сети;

алгоритмической реализации средств защиты сети на основе разработанного математического аппарата.

Практическая значимость работы

Разработанные математические модели могут быть без изменений использованы для построения системы обнаружения удаленной сетевой атаки выбранного типа после уточнения параметров используемой операционной системы и статистических характеристик защищаемого фрагмента сети и организации защиты узлов компьютерной сети. Выводы, сделанные после обсуждения разработанного формализма, могут быть без труда использованы для обоснованного предложения других – превентивных – мер защиты сети.

Апробация работы

Результаты работы были представлены на

международной конференции по неразрушающим методам исследований и компьютерному моделированию (Nondestructive Testing and Computer Simulations in Science and Engineering. Vol.7, pp. F21-23. 2003.),

конференции «Математика и безопасность информационных технологий (МаБИТ-03)», МГУ им. М.В.Ломоносова, 23-24 октября 2003г.

конференции «Формирование технической политики инновационных наукоемких технологий». СПбГПУ .14-16.06.03,

VII Всероссийской конференции по проблемам науки и высшей школы. Фундаментальные исследования в технических университетах. СПбГПУ, 2003.

Основные результаты работы изложены в шести публикациях.

Содержание работы

Во ***введении*** обоснован выбор темы, ее актуальность. Проведен обзор литературы по теме диссертационной работы и существующих методов защиты от удаленных атак. Дается общая характеристика инструментария, который может быть построен с использованием результатов проводимых в работе исследований.

Первая глава диссертации посвящена обоснованию выбора класса атак, для которых строится зашита. В этом разделе работы приведен подробный анализ классов удаленных атак на узлы компьютерной сети, причем, классификация проводится с различных точек зрения на проблему безопасности

сети. Из всего множества удаленных атак для более подробного изучения была выбран класс, известный как удаленная атака "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)", схема которой впервые была использована Кевином Митником для атаки на Суперкомпьютерный центр в Сан-Диего 12 декабря 1994 года. Показано, во-первых, что опасность атаки по данной схеме по-прежнему реальна и в настоящее время. Во-вторых, это один из тех классов атак, для которых, в принципе возможно построение системы защиты в реальном времени. Поэтому в работе уделено особое внимание механизму реализации атаки, а также особенностям идентификации пакетов в существующей реализации TCP (Transmission Control Protocol), послужившим причиной возникновения атак подобного рода. В этом же разделе работы определены основные понятия, которыми оперирует теория компьютерной безопасности.

Вторая глава посвящена содержательной постановке задачи работы.

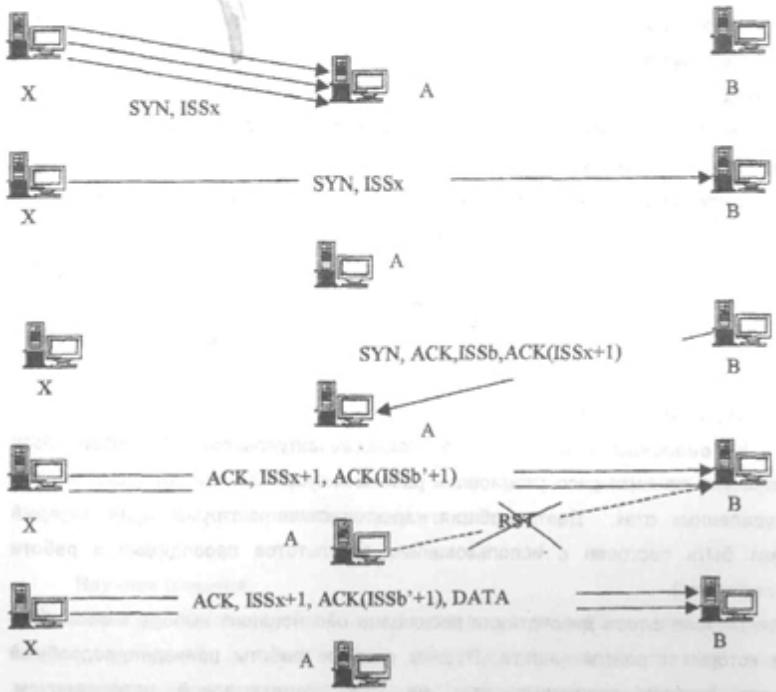

Рис.1. Схема атаки.

Здесь детально рассмотрена схема удаленной атаки "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)", и особенности протокола, позволяющие осуществить атаку. Схема такой атаки показана на рис. 1, где X - интервент, B – атакуемый хост, A – хост, которому доверяет B.

Отметим, что для поддержания диалога интервенту потребуется «угадывать» ACK(ISSb'+1), т.е., формировать на каждом шаге атаки «залп» из некоторого количества пакетов. Но не потребуется подбора ISSx+1, так как этот параметр TCP-соединения был послан с хоста X на B в первом пакете.

В большинстве операционных систем используется времязависимый алгоритм генерации начального значения идентификатора TCP-соединения. Так, изначально в TCP предполагалась генерация ISN увеличением счетчика на единицу каждые 4 миллисекунды, а в ОС Windows NT 4.0 значение ISN увеличивается на 10 примерно каждую миллисекунду.

Современные ядра ОС Linux используют более сложный, алгоритм формирования ISN]. Пример вида этой функции представлен на приведенном ниже рисунке 2.

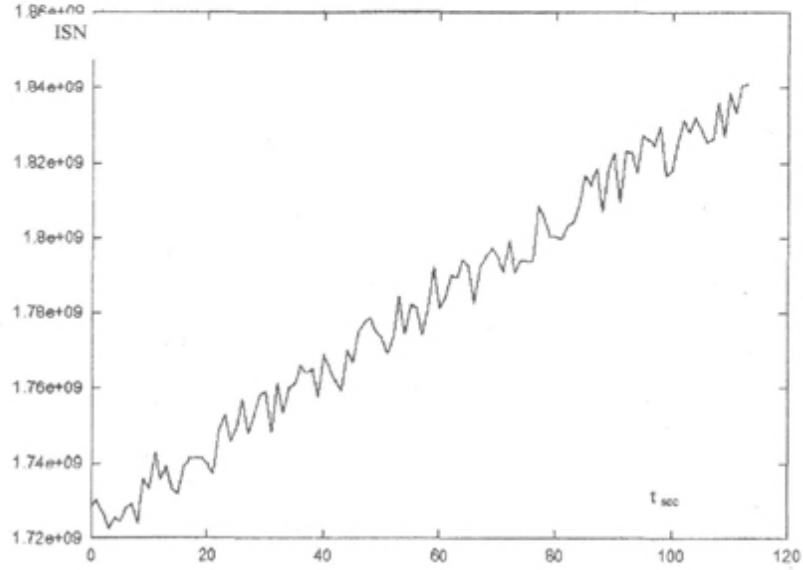

Рис. .2. Зависимость ISN от времени в ОС Linux 2.4.19.

Отметим, вместе с тем, попытку компании Microsoft сделать генерацию ISN «более случайной», реализованную в ОС Windows NT 4.0 ServisPack 4 и постигшую разработчиков неудачу. Генерируемые этим алгоритмом ISN оказывались иногда совпадающими с идентификаторами других соединений, что приводило к сбоям в сети и вынудило компанию вернуться линейному закону формирования ISN уже в ОС Windows NT 4.0 ServisPack 5. Этот же закон без изменений появился и в Windows 2000

При этом, в предположении, о линейном характере зависимости от времени закона формирования ISN, необходимо учесть случайный характер задержки пакетов в сети.

На Рис 3. приведена схема развития событий во время разведки. Очевидно, что истинное значение определяемого идентификатора **N** на момент окончания разведки (начала атаки) **T**, лежит на отрезке значений **ΔN** ограниченном, двумя линиями, соответствующим двум максимально неблагоприятным случаям распределения задержек тестовых пакетов на этапе разведки.

Здесь: N_1 и N_2 – измеренные значения ISN в моменты времени t = 0 и t = t завершения этапа разведки, а колебания задержек τ_1 и τ_2 разведочных пакетов определяют колебания предположительно нужного ISSb относительно истинного на момент начала атаки.

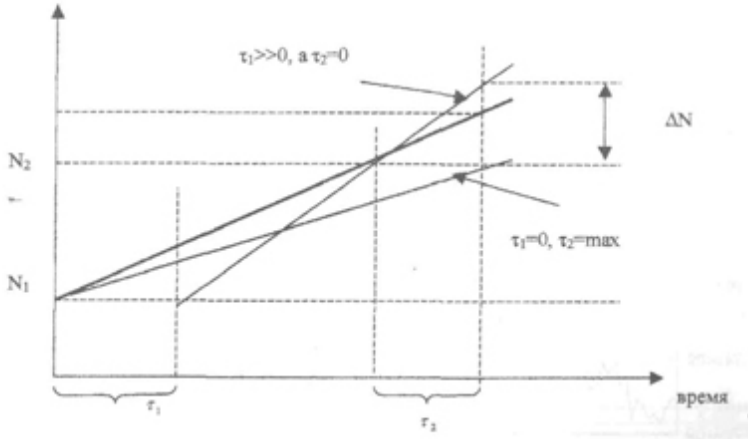

Рис. 3. Схема разведки.

В ***третьей главе*** так же рассмотрены обе фазы атаки – фаза разведки и фаза собственно атаки (Рис. 4.), но уже на основании формальных рассуждений. Построенная математическая модель типовой удаленной атаки, позволила судить о зависимости вероятности успеха всего комплекса атакующих мероприятий от

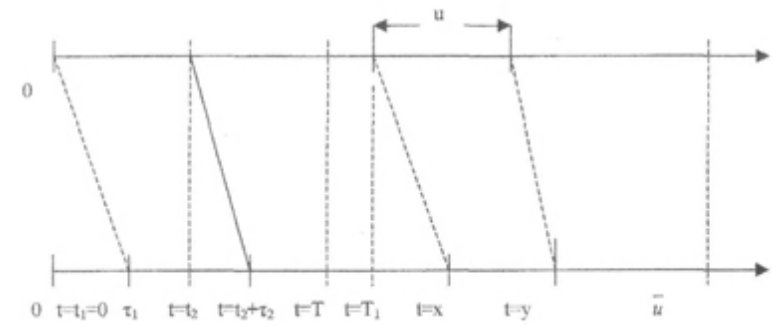

Рис. 4 Временной график развития атаки.

u – время атаки, $\bar{u}$ - некое предельно допустимое время.

параметров, которыми может манипулировать интервент и параметров атакуемой системы. Вводятся понятия:

Определение 1. Будем называть разведкой (подготовкой к атаке) посылку хостом X на хост B последовательности пакетов с целью определения вероятностной характеристики значения идентификационного номера, присваиваемого хостом B сообщению, в момент T - времени начала планируемой атаки.

Определение 2. Будем называть началом атаки посылку в момент времени T хостом X на хост B от имени хоста A запроса на открытие соединения.

Определение 3. Будем называть атакой отправку хостом X на хост B двух последовательных, размером K, серий пакетов в моменты времени T_1 и T_1+u соответственно ($T_1>T$, $u\geq 0$). Причем, номера пакетов в серии соответствуют предполагаемому номеру пакета, начавшего атаку. Будем далее обозначать через $\bar{k}$ - множество номеров пакетов в сериях.

Определение 4. Будем называть атаку успешной при выполнении условий:

1. в каждой серии пакетов, посылаемых во время атаки, содержится пакет с номером, связанным с номером пакета, начавшим атаку;

2. пакет, с номером, связанным с номером пакета, начавшим атаку, во второй серии пришел на хост B после аналогичного пакета в первой серии, но раньше некоторого предельного времени $T_1+\bar{u}$.

Далее строятся условия, при которых «разведка» может дать достоверные результаты:

если истинное значение идентификационного номера пакета, участвующего в разведке, вычислить как

$$N^* = N_1 + K * \frac{T - \tau_1}{t + \tau_2 - \tau_1} \quad (1)$$

а прогнозируемое интервентом значение того же параметра –

$$N = N_1 + K * \frac{T}{t} \quad (2)$$

где $K = N_2 - N_1$ (использованные здесь обозначения соответствуют введенным Рис. 3, а N_1 и N_2 - идентификационные номера пакетов, участвовавших в «разведке»),

атака состоится после получения ответов на оба тестовых запроса –

$$T - \tau_1 > 0; \quad T - t - \tau_2 > 0, \quad (3)$$

$N_2 > N_1$ – требование равносильно тому, что второй пробный пакет пришел на хост B позже первого, т.е.:

$$t + \tau_2 - \tau_1 > 0 \quad (4)$$

Обозначив область значений (τ_1, τ_2), удовлетворяющую условию (3)-(4) и очевидному условию $\tau_1 \geq 0$, $\tau_2 \geq 0$ через S_0. Нетрудно видеть, что

$$S_0 = \begin{cases} 0 \leq \tau_2 \leq T - t \\ 0 \leq \tau_1 \leq t + \tau_2 \end{cases} \quad (5)$$

Для оценки качества проведенной разведки рассматривается неравенство

$$N^* - N \leq \Delta \quad (6)$$

при выполнении условий принадлежности (τ_1, τ_2) множеству S_0. В силу (1)-(2) эта система неравенств имеет вид:

$$\begin{cases} K * \left(\frac{T - \tau_1}{t + \tau_2 - \tau_1} - \frac{T}{t} \right) < \Delta \\ (\tau_1, \tau_2 \in S_0) \end{cases} \quad (7)$$

Решение этой системы неравенств дается формулами:

$$\Delta \geq 0$$

$$S_1 = \begin{cases} 0 \leq \tau_2 \leq T - t \\ 0 \leq \tau_1 \leq \frac{(TK + \Delta t)\tau_2 + \Delta t^2}{TK + \Delta t - tK} \end{cases}$$

$$-K(T - t) < \Delta t < 0 \quad (8)$$

$$S_2 = \begin{cases} -\frac{\Delta t^2}{TK + \Delta t} \leq \tau_2 \leq T - t \\ 0 \leq \tau_1 \leq \frac{(TK + \Delta t)\tau_2 + \Delta t^2}{TK + \Delta t - tK} \end{cases}$$

$\Delta < -K(T - t)$ - решений нет.

Эти результаты позволили утверждать:

Теорема 1. Пусть запаздывания в сети являются независимыми случайными величинами с функцией распределения $F(\tau)$. Тогда функция распределения случайной величины $N^* - N$, при условии, что $(\tau_1, \tau_2) \in S_0$, определяется зависимостью:

$$P(\Delta) = \begin{cases} \int_0^{T-t} \left[\int_0^{\frac{(TK + \Delta t)\tau_2 + \Delta t^2}{TK + \Delta t - tK}} dF(\tau 1) \right] dF(\tau_2) ... при ... \Delta > 0; \\ \int_{-\frac{\Delta t^2}{TK + \Delta t}}^{T-t} \left[\int_0^{\frac{(TK + \Delta t)\tau_2 + \Delta t^2}{TK + \Delta t - tK}} dF(\tau_1) \right] dF(\tau_2) ... при ... -\frac{K}{t}(T - t) < \Delta < 0 \\ 0; ... при ... \Delta < -\frac{K}{t}(T - t) \end{cases} \quad (9)$$

После чего доказывается, что:

Теорему 2. Вероятность успеха атаки определяется формулой:

$$P = P_k * \left[F(\bar{u}) * F(\bar{u} - u) - \int_u^{\bar{u}} F(x - u) dF(x) \right] \quad (10)$$

где $P_k(s)$ – вероятность того, нужный идентификационный номер равен s. Тогда вероятность того, что этот пакет удовлетворит условию 2 определения 4:

$$P = \int_{T_1}^{T_1+\overline{u}} \left[\int_{x}^{T_1+\overline{w}} dF(y - T_1 - u) \right] dF(x - T_1) \qquad (*)$$

где x – момент прихода пакета с s-м идентификационным номером из первой атакующей серии, y – время прихода пакета с нужным номером во второй серии, а $dF(\tau)$ - плотность вероятности того, что время доставки пакетов серии не превысило τ.

Доказывается, что следствиями последнего будут:

Следствие 4.1

$$u = 0 \Rightarrow P = P_n \frac{F^2(\overline{u})}{2}$$

и *Следствие 4.2*

$$u = \overline{u} \Rightarrow P = 0$$

В этом же разделе работы состоятельность разработанного аппарата иллюстрируется возможными реализациями – при экспоненциальном, характерном для абсолютного большинства реальных сетей:

Теорема 3. При экспоненциальном законе распределения вероятности $F(\tau)$,

$$P = P_n \left[1 - e^{-\lambda(\overline{w}-u)} + \frac{1}{2} e^{-\lambda(2\overline{w}-u)} - \frac{1}{2} e^{-\lambda u} \right]$$

и равномерном распределении статистических характеристик сети.

Проведен ряд численных экспериментов при различных значениях параметров, характеризующих процесс, которые демонстрируют, что:

- успех атаки мало зависит от величины среднего времени задержки пакета в сети при любом характере распределения задержек в сети.
- при существенном сокращении времени, отводимом на «разведку», вероятность успешности атаки так же существенно падает, как этого и следовало ожидать.
- уменьшение времени между концом разведки и началом собственно атаки увеличивает вероятность попадания нужного пакета в заданный диапазон.
- при сокращении мощности «залпа» при атаке, вероятность ее успеха уменьшается.
- при уменьшении интервала времени между «залпами» при атаке, вероятность ее успеха уменьшается.

- при равномерном характере распределения времени задержки в сети интервент имеет существенно меньшие шансы на успех, при этом временные рамки при организации атаки более жесткие.

Из всего вышеизложенного делаются очень важные практические выводы:

1. для достижения успеха атаки интервент должен действовать по определенному алгоритму, который однозначно определяется параметрами атакуемой системы (сегмента сети). Это дает возможность определить момент начала атаки и своевременно ее пресечь.
2. для достижения успеха атаки поведение атакуемого сегмента сети должно быть предсказуемо. Таким образом, сделав поведение сегмента слабо предсказуемым, можно снизить вероятность успеха атаки при любых действиях интервента.

В ***четвертой главе*** рассматриваются один из возможных алгоритмов обнаружения рассматриваемого типа атак, построенный на основе проведенных рассуждений и превентивные меры, способные существенно уменьшить вероятность успешной атаки.

Предложенный алгоритм анализирует время прихода каждого TCP-пакета, сравнивая его со временем прихода предыдущего, а затем, используя описанный в главе 3 механизм атаки "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)", в частности, количество пакетов, необходимое для угадывания начального значения идентификатора TCP-соединения и интервал, в который должна входить разность времен между получением первой и второй серий пакетов, выявляет атаку на первых стадиях. Показано, что никакая загрузка – ни нормальная, ни даже самая напряженная работа сервера, обрабатывающего запросы на соединение – не вызовет настороженности системы защиты сервера. Подозрение о готовящейся атаке возникают только в случае, когда подозрительного размера серия пакетов, пришедших с частотой, вызвавшей заполнение буфера, прервалась, и прервалась именно на опасный промежуток времени, после чего возобновилась с прежней интенсивностью. Эта ситуация идентифицируется как атака.

В этой же главе предложен и способ предотвращения атаки, основанный на разработанной в данной работе модели. Поскольку успех атаки обеспечен, помимо всего прочего, точностью прогноза задержки пакета в сети – объективной характеристики сети, влияние на которую не может оказать ни интервент, ни его потенциальная жертва, в силах администратора атакуемого хоста увеличить на

непонятную для хакера величину задержку пакета, введя ее как случайную величину, распределенную по некоторому закону, на собственном роутере.

В наиболее благоприятном для интервента случае, будем считать, что время задержки пакета до роутера распределено показательно, задержку на роутере введем в соответствии с менее удобным, для интервента, равномерным законом распределения.

Тогда распределение вероятности суммарной задержки

$$= \begin{cases} \frac{1}{b}\left[\tau + \frac{e^{-\lambda\tau}}{\lambda} - \frac{1}{\lambda}\right] & для\ \tau < b \\ \frac{1}{\lambda b}\left[b + e^{-\lambda\tau} - e^{-\lambda(\tau - b)}\right] & для\ \tau \geq b \end{cases}$$

Положив $\frac{1}{\lambda} << \frac{b}{2}$, то есть, среднее время задержки на роутере много больше времени задержки в сети до роутера, останемся в пределах $\tau < b$, т.е.,

$$F(\tau) = F_1(\tau) = \frac{1}{b}\left[\tau + \frac{e^{-\lambda\tau}}{\lambda} - \frac{1}{\lambda}\right]$$

Подставив это выражение в выражение (10) получим:

$$= \frac{1}{\lambda b^2}\left[\frac{\lambda^2}{2}\bar{u}^2 + \lambda e^{-\lambda\bar{u}}(2\bar{u} - u) - \lambda\bar{u} + e^{-\lambda(2\bar{u}-u)}\left(1 - \frac{\lambda}{2}\right) + \frac{3\lambda^2}{2}u^2 + \lambda e^{-\lambda\bar{u}} - e^{-\lambda u}\left(1 + \frac{\lambda}{2}\right)\right].$$

Численные эксперименты с полученным выражения показали, что при колебаниях параметра u в пределах предполагаемого управления процессом со стороны интервента, зависимость вероятности успеха атаки от любых маневров хакера не велика, равно как мала и сама вероятность достижения им цели. А с увеличением b, т.е., при выполнении условия $\frac{1}{\lambda} << \frac{b}{2}$ вероятность успеха хакера не превышает 5% и не зависит от его усилий.

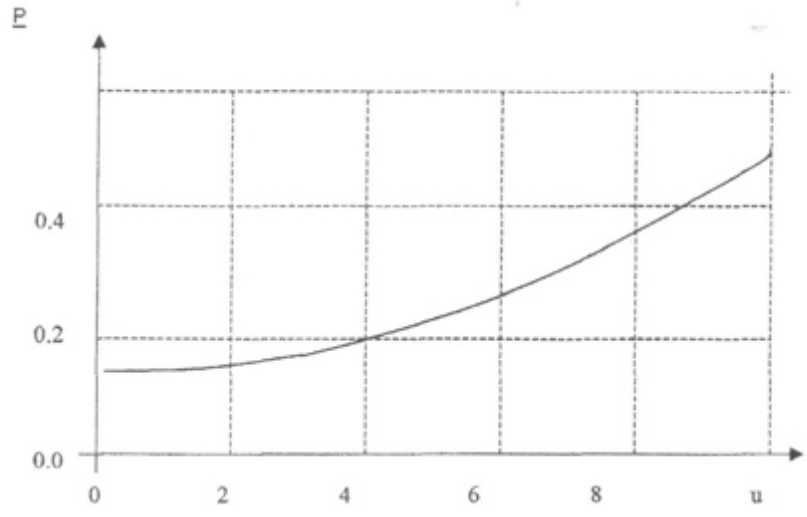

Рис.5. Зависимость P(u) при ū=10, λ=5, b=20

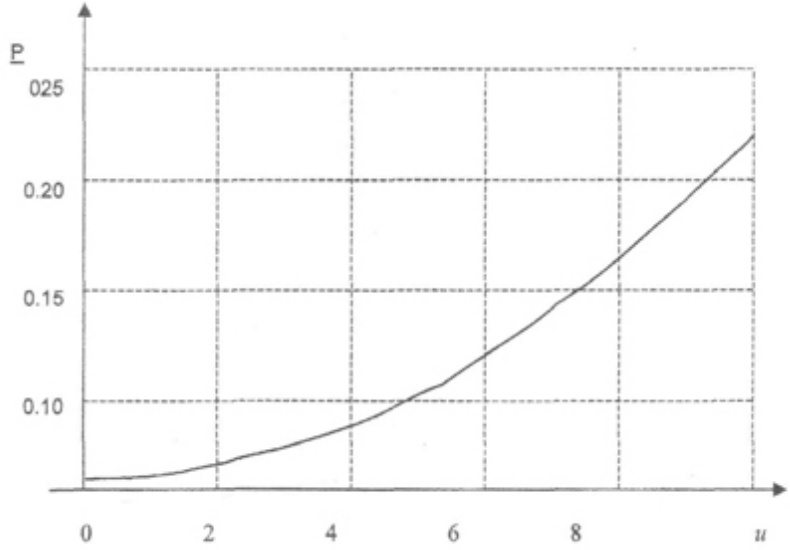

Рис.6. Зависимость P(u) при ū=10, λ=5, b=30

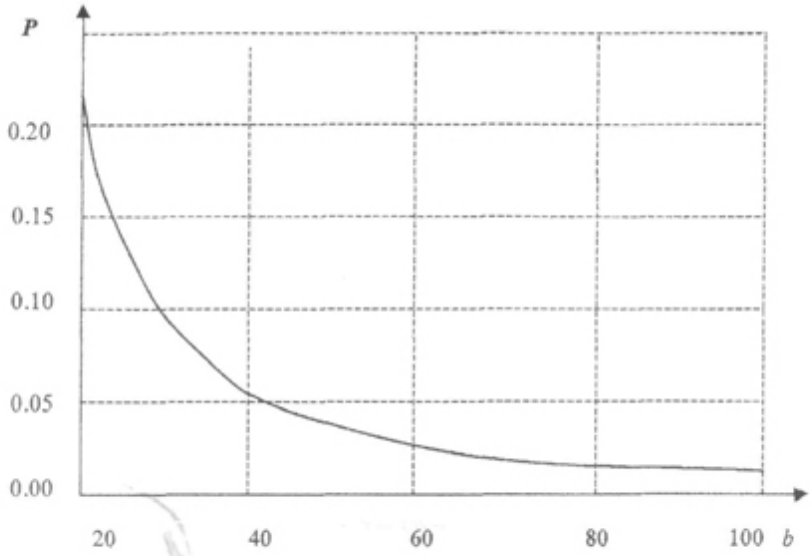

Рис.7. Зависимость P(b) при Ω=10, λ=5, u= Ω/2

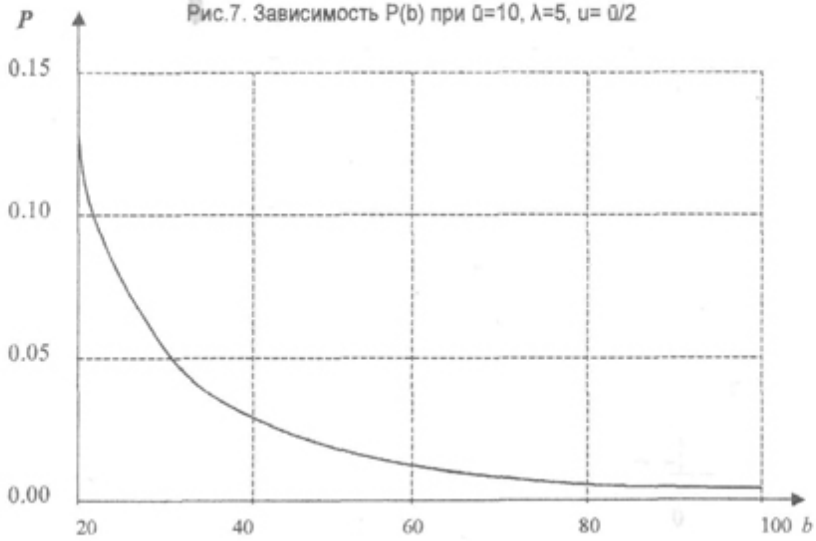

Рис.8. Зависимость P(b) при Ω=10, λ=5, u= Ω/8

Выводы

Разработанная математическая модель типовой удаленной атаки по схеме "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)"

позволила установить зависимость вероятности удачной атаки от параметров — интервала времени между отправкой первой и второй атакующих серий пакетов, общего времени атаки, времени между этапом разведки и началом атаки, т.е., теми параметрами атаки, которыми может манипулировать хакер. Используя численные значения параметров, были построены графики этих зависимостей. Этот иллюстрационный материал позволил наглядно определить численный интервал, в котором должны находиться параметры, чтобы обеспечить максимально возможную вероятность удачной атаки.

Чтобы применить полученные результаты для анализа возможности атаки по схеме "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)" на какой-либо определенный узел компьютерной сети, необходимо определить соответствующие параметры объекта атаки и его окружения, а затем воспользоваться полученными в данной работе формулами.

Результатом изучения механизма атаки и построения ее математической модели стало определение двух слабых сторон этого класса атак. Предложены варианты защиты от атаки.

Необходимая для успешности атаки предсказуемость поведения интервента в сети позволила предложить простой и надежный способ защиты, правда, несколько снижающий скорость работы сети. Проведены расчеты максимальной вероятности успеха атаки в зависимости от значения выбранного параметра.

Заметим, что предложенные средства защиты, их эксплуатация не предполагает никаких особых требований ни к аппаратным средствам вычислительной системы, ни к ее программному обеспечению.

Для повышения защищенности системы, на этапе инсталляции средств защиты следует отказаться от предположения, что защищаемые объекты находятся в среде со «средними» характеристиками, и провести численные эксперименты с целью сбора статистического материала для уточнения характеристик сети и ее окружения. После этого уточняются использованные в модели атаки параметры.

Список работ, опубликованных по теме диссертации.

N.O. Vilchevsky, M.B. Gaidar, V.E. Klavdiev. Development of means of defection of the remote attacs on computer network hosts. Seventh Int. Workshop on New

approches to Hiigh-Tech: Nondestructive Testing and Computer Simulations in Science and Engineering. Vol.7, pp. F21-23. 2003.

Вильчевский Н.О., Гайдар М.Б., Заборовский В.С., Клавдиев В.Е. «Статистическая модель обнаружения одного класса удаленных атак в высокопроизводительных компьютерных сетях», Материалы конференции «Математика и безопасность информационных технологий (МаБИТ-03)», МГУ им. М.В.Ломоносова, 23-24 октября 2003г.

Вильчевский Н.О., Гайдар М.Б., Клавдиев В.Е. Организация защиты от удаленных атак на узлы компьютерной сети. Материалы конференции «Формирование технической политики инновационных наукоемких технологий». 14-16.06.03, СПбГПУ, СПб. Стр. 326-330.

М.Б. Гайдар. Защита узлов компьютерной сети от удаленных атак. Материалы VII Всероссийской конференции по проблемам науки и высшей школы. Фундаментальные исследования в технических университетах. Т.2, Ч.2, стр. 225-227. СПбГПУ, Санкт-Петербург, 2003.

Nikita O. Vilchevsky, Michael B. Gaydar, Vladimir E. Klavdiev. Development of means-of-detection for remote attacks on computer network hosts. Seventh International Workshop on Nondestructive Testing and Computer Simulations in Science and Engineering. Proceedings of SPIE Volume: 5400 pp. 292-300 Publication Date: Apr 2004.

Вильчевский Н.О., Гайдар М.Б., Заборовский В.С., Клавдиев В.Е. Защита от удаленных атак. Математика и безопасность информационных технологий. Материалы конференции в МГУ 23-24 октября 2003 г. М.: МЦНМО 2004. стр.383-393.

Подписано в печать 24.11.04. Формат 60x84/16. Печать офсетная.
Уч. печ. л. 1,0 . Тираж 100 . Заказ 561 .

Отпечатано с готового оригинал-макета, предоставленного автором,
в типографии Издательства Политехнического университета.
195251, Санкт-Петербург, Политехническая, 29.