Корпоративная компьютерная система защиты материальных объектов, контроля и интеллектуального управления торговой сети гипермаркета защищена патентами на изобретения.

АРХИТЕКТУРА СИСТЕМЫ КОНТРОЛЯ ДОСТУПА LPS ЗАЩИЩЕННОЙ ОС BASTION

Д.С. КОЧУРОВ

Unix-подобные ОС с открытым кодом (Linux, FreeBSD и т.д.) с точки зрения безопасности имеют ряд существенных недостатков, которые невозможно преодолеть только грамотным администрированием и настройкой системы.

По этой причине пользователи таких ОС вынуждены применять дополнительные системы защиты, которые в свою очередь либо сложны в настройке и эксплуатации, либо ориентированы на отдельные частные случаи.

Для решения приведенных проблем с организацией защиты и построения защищенной ОС Linux (Bastion) применена система LPS (Linux Protection System), являющаяся разработкой кафедры ЭВМ БГУИР.

LPS имеет модульную структуру, причем каждый модуль реализует свою собственную модель защиты. Окончательное решение о предоставлении доступа или отказе в нем получается как суммарное после обсуждения этого вопроса всеми модулями.

Основа защиты в LPS — мониторинг поведения процессов, в частности, перехода процессов от одного пользователя к другому.

Система LPS разграничивает полномочия администратора системы и администратора безопасности. Администратор системы занимается обеспечением корректности функционирования системы, а администратор безопасности — обеспечением конфиденциальности данных. Такое разделение позволяет разграничивать ответственность и выполнять требование по обязательному присутствию нескольких лиц при принятии ответственных решений.

Такой универсальный подход позволяет защитить не только конфиденциальные данные, но и данные ОС, добавляя дополнительный уровень защиты. Для того чтобы преодолеть механизмы защиты LPS, необходимо получить и права администратора системы и права администратора безопасности, притом, что каждый из них контролирует действие другого.

ОЦЕНКА ПАРАМЕТРОВ СЛОЖНЫХ СИГНАЛОВ С ПОМОЩЬЮ ПРЕОБРАЗОВАНИЯ ГАБОРА В СИСТЕМАХ РАДИОКОНТРОЛЯ

С.Б. САЛОМАТИН, Д.Л. ХОДЫКО

Современные средства радиоконтроля несанкционированных источников передачи информации по радиоканалу внутри здания сталкиваются с необходимостью быстро и точно оценить параметры сложных псевдослучайных сигналов в условиях априорной неопределенности и многолучевого распространения.

Одним из подходов к решению такого рода задач является применение частотно-временных преобразований Габора.

Модель сигнала. Принимаемый сигнал $y(t)$ имеет вид:

$$y(t-\Delta t)=\sum_{i=1}^{M} s_i(t-\tau_i)+n(t),$$

где $s_i(t-\tau_i)$ — i-ый луч радиосигнала $i=1\ldots M$, Δt — задержка суммарного сигнала $y(t)$, $s_i(t-\tau_i)=\xi(t)\,A(t)\,sin[\omega(t-\tau_i)+\psi_i]$, $\xi(t)$ — множитель, определяющий затухание сигнала в среде распространения, $A(t)$ — кодовая огибающая радиосигнала, $\omega=2\pi f$.

Преобразование Габора. Используя преобразование Габора с окном $g(t)$ обрабатываемый сигнал можно представить в следующем виде[1]:

$$y(t)=\sum_{m,n=-\infty}^{\infty} C_{m,n}\,g(t-n)\,exp(j2\pi mt),$$

где $C_{m,n}=D_{m,n}-exp(-\lambda)D_{m,n-1}$ — коэффициенты Габора, m,n — отсчеты по частоте и времени соответственно, $m,n=0..N-1$, λ — параметр, контролирующий эффективную ширину окна.

Алгоритм оценки параметров. Входной сигнал $y(t)$ разбивается на N частей, каждая — длины L. Обработка осуществляется на длине L, с шагом $1/L$, начиная с $1/(2L)$. В процессе

обработки вычисляются коэффициенты $C_{m,n}$. Оценка частоты f производится по параметру m, оценка длительность сигнала $\widehat{T}$ определяется как разность $\Delta n = n_2 - n_1$, где n_1, n_2 начало и конец i-го луча. Оценка задержки $\Delta \widehat{t}$ определяется параметром n. Точность оценки зависит от λ_{opt}, которое является оптимальным для каждого из параметров.

Литература

1. B. Porat, B. Friedlander, Detection of transient signals by the Gabor representation IEEE Trans. Acoust., Speech, signal processing, Vol. 37, No. 2. February 1989.

СТАТИСТИЧЕСКИЙ АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

С.Б. САЛОМАТИН

Стеганографические методы защиты объектов используют в качестве скрывающих спектральные и корреляционные широкополосные преобразования данных. При этом возникает задача оценка стойкости стегосистем к обнаружению факта передачи скрываемых сообщений [1].

Для анализа стойкости стеганографических систем удобно использовать статистические методы распознавания образов.

Модель стеганографического процесса. Стегосообщение y представляется в виде аддитивной суммы стегошума n и скрываемых данных x. Стегошум характеризуется вероятностной функцией:

$$v[n] = p(y - x = n),$$

гистограмма стегосообщения может быть вычислена через свертку гистограммы скрываемых данных и вероятностной функции стегошума.

В качестве характеристических функций используются дискретные преобразования Фурье от соответствующих гистограмм и вероятностных функций.

Схема обнаружения. В условиях априори известного метода стеганографических преобразований анализатор строится на основе многомерного Байесовского классификатора, использующего линейную разделяющую функцию.

Дискриминантная функция задается в виде [2]

$$S_{ll'}(\vec{k}) = -\frac{1}{2}\vec{k}^T \Sigma^{-1}\vec{k} - \frac{1}{2}\vec{\mu}^T \Sigma^{-1}\vec{\mu} + (\Sigma^{-1}\vec{\mu})^T \vec{k} - \frac{1}{2} ln|\Sigma|,$$

где Σ^{-1}-общая ковариационная матрица классов l и l', $\vec{\mu}$ — вектор средних значений.

В условиях априорной неопределенности типа стегопреобразования, но в рамках анализа классов с многомерным нормальным распределением, которые отличаются лишь средними значениями, критерий оценки адекватности набора признаков использует понятие расстояния Махаланобиса:

$$\varphi = (\vec{\mu}_l - \vec{\mu}_{l'})^T \Sigma^{-1} (\vec{\mu}_l - \vec{\mu}_{l'}).$$

Для снижения вычислительной сложности алгоритма используется метод выбора "лучшего признака" [3].

Литература

1. Грибунин, Оков И.Н., Туринцев И.В. Цифровая стеганография. М., 2002.
2. Harmsen J.J, Pearlman W.A. Stegaanalysis of additive noise modelable information hiding. Center for ImageProcessing Research, Troy, NY.
3. Верхаген К.,Дейн Р., Грун Ф., Йостен Й., Вербек П. Распознование образов: состояние и перспективы. М., 1985.

О ФОРМИРОВАНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

О.А. КАЧАН, И.В. МИТЯНОВ, В.К. ФИСЕНКО

В общем случае модель нарушителя определяется совокупностью признаков, характеризующих квалификацию C, мотивацию M и ресурсы R нарушителя, представленные в виде множеств (подмножеств).

Элементы множеств C, M и R также могут задаваться в виде подмножеств. Это позволяет сформировать вложенную систему подмножеств признаков и элементов. Достаточность глубины детализации и полноты охвата оценивается экспертным путем.

Множества C, M и R характеризуют различные аспекты процесса НСД. При этом:

C={c_1, c_2, c_3}, где c_1 — способности нарушителя, определяемые уровнем его подготовки; c_2 — степень информированности нарушителя о характеристиках объекта информатизации (ОИ); c_3 — статус нарушителя;

M={m_1, m_2, m_3, m_4}, где m_1 — ошибочные действия; m_2 — любознательность; m_3 — попытка взлома; m_4 — корыстные цели;