Модуль process.sys реализует работу с опкодом процессора, внутренними таблицами, PE_loader.sys реализует загрузку зашифрованного модуля библитек перехвата (с введением имитовставки) и определяет точку вхождения в imagine_path модуля ntoskernel.exe, позволяет контролировать выполнение всех процессов. Нельзя контролировать загрузку всех кодов в системе, так как есть недокументированные интерфейсы, но выполнение можно контролировать на уровне тегов данных ядра, поскольку все вызовы модуля ntoskernel.exe транслируются в семантический запрос.

Мой оригинальный алгоритм основан на низкоуровневой спецификации. В ходе исследования были обнаружены новые 4 класса уязвимостей модулей ядра Windows NT 5.1. Сочетание системно-методологического подхода и имитационного моделирования позволило раскрыть базовые закономерности функционирования ядра ОС и скрытые каналы доступа.

Более того, автор рассмотрел операционную систему как организационно-технологическую, представил правовые, организационные, технические и технологические аспекты разрешения коллизий (трудностей).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Искусственный интеллект: Справочник в 3-х книгах. – М.: Радио и связь, 1990. Книга 2. Модели и методы / Под ред. Д.А. Поспелова. – 304 с.

2. Горелик А.Л., Гуревич И.Б., Скрипкин В.А. Современное состояние проблемы распознавания: Некоторые аспекты. - М.: Радио и связь, 1985. – 160 с., ил. – (Кибернетика).

3. Горелик А.Л., Скрипкин В.А. Методы распознавания: Учебное пособие для вузов. – 3-е изд., перераб. и доп. - М.: Высш. шк., 1989. – 232 с..

4. Теория вероятностей: Учеб. для вузов / А.В. Печинкин, О.И. Тескин, Г.М. Цветкова и др. Под ред. В.С. Зарубина, А.П. Крищенко. – М.: Изд-во МГТУ им. Н.Э. Баумана, 1999. – 456 с. (Сер. Математика в техническом университете; Вып. XVI).

5. Heckerman D. A tutorial on learning Bayesian Networks: Technical Report MSR-TR-95-06. – Microsoft Research: Advanced Technology Division, 1996. – 58 p.

6. Androutsopoulos et al. An evaluation of naive Bayesian anti-spam filtering. // Proceedings of the 11th European Conference on Machine Learning. – 2000. – pp. 9–17.

7. Elkan C. Boosting and naive Bayesian learning: Technical Report No. CS97-557.– Department of Computer Science and Engineering, University of California, San Diego.– 1997.– 11p.

8. Умрюхин Е.А. Механизмы мозга: информационная модель и оптимизация обучения. – М., 1999. – 96 с.

9. Ганецкий М.А. Методы программирования // Труды №1 молодых учёных, аспирантов и студентов «Информатика и системы управления». – М: МГТУ, 2002. – 460 с.

А.Г. Лысенко
Россия, г. Санкт - Петербург, ГОУ ВПО Санкт-Петербургский
Государственный политехнический университет

СИСТЕМАТИЗАЦИЯ УГРОЗ ГИБРИДНЫХ СЕТЕЙ

1. Введение

Быстрое развитие беспроводной технологии привлекло внимание множество компаний, которые стали использовать мобильные технологии наряду с фиксированными. Введем определение гибридной сети. Гибридная компьютерная сеть – сеть, в которой используются фиксированные и мобильные технологии.

Для корпоративных клиентов наиболее частый вариант использования мобильных устройства – это их подключение к корпоративной сети.

Мобильные пользователи, подключаясь к фиксированному сегменту, образуют мобильный сегмент корпоративной сети, что в целом составляет гибридную

сеть компании. Организация мобильного офиса позволяет мобильным устройствам получать доступ к корпоративным ресурсам. При этом пользователи отделены от ресурсов и от процессов их обработки.

В настоящее время гибридные получают все большее распространение. Однако интеграция фиксированных и мобильных технологий порождает ряд проблем, связанных с новыми возможностями нарушения информационной безопасности и слабой защищенностью мобильных технологий и стыка этих технологий.

Вопросы обеспечения безопасности корпоративной сети становятся актуальными при добавлении в сеть мобильного сегмента, что порождает множество новых угроз. Помимо угроз утечки информации из сети, возникают угрозы подмены точки доступа, угроза ложного клиента и т.д.

Пользователи все чаще хранят конфиденциальные данные на мобильных устройствах: финансовая документация, переписка.

Существующие политики безопасности организаций не готовы для поддержания безопасности в состоянии обеспечить должный уровень защиты. Целью данной работы является рассмотрение вопросов безопасности гибридных сетей и систематизация угроз гибридных сетей.

2. Особенности гибридных сетей

Для рассмотрения возможных механизмов реализации угроз рассмотрим особенности гибридных сетей.

Проблема безопасности сети на базе фиксированной технологии рассматривается достаточно давно. Безопасность в таких сетях обеспечивается с использованием программно-аппаратных устройств, реализующих политику контроля доступа к ресурсам сети.

анные средства также осуществляют обнаружение вторжений как изнутри, так и извне и поддерживают должный уровень защищенности сети.

Стоит отметить некоторые специфические особенности гибридных сетей:

- пользователи отделены от ресурсов и обработки данных;
- недостаточная аутентификация;
- затрудненное администрирование (разные устройства, разные ОС);
- пользователь не получает результат обработки;
- процесс управления сетью затруднен ввиду наличия различных протоколов, ОС и т.д.

Выше перечисленные особенности беспроводных сетей предопределяют основные классы атак на гибридные сети, что позволяет произвести систематизацию угроз.

3. Систематизация угроз

В мобильных сетях, особенно без точек доступа, существует сложность в определении периметра сети, и, как следствие, разделение угроз на внешние и внутренние. Поэтому предлагается не рассматривать данный признак при классификации угроз.

Угрозы для гибридной сети можно разделить на имеющие моментальный либо отложенный эффект.

К угрозам, оказывающим моментальное влияние, относятся угрозы целостности и доступности отдельных узлов, угрозы конфиденциальности, целостности и доступности сервисных сообщений, истощение ресурсов либо энергии мобильных узлов сети. К угрозам, оказывающим отложенное влияние, относятся угрозы корректности структуры сети, компрометация узлов сети. Учитываются угрозы, направленные на устройство пользователя, на беспроводный канал передачи информации, на протоколы маршрутизации и сетевое оборудование.

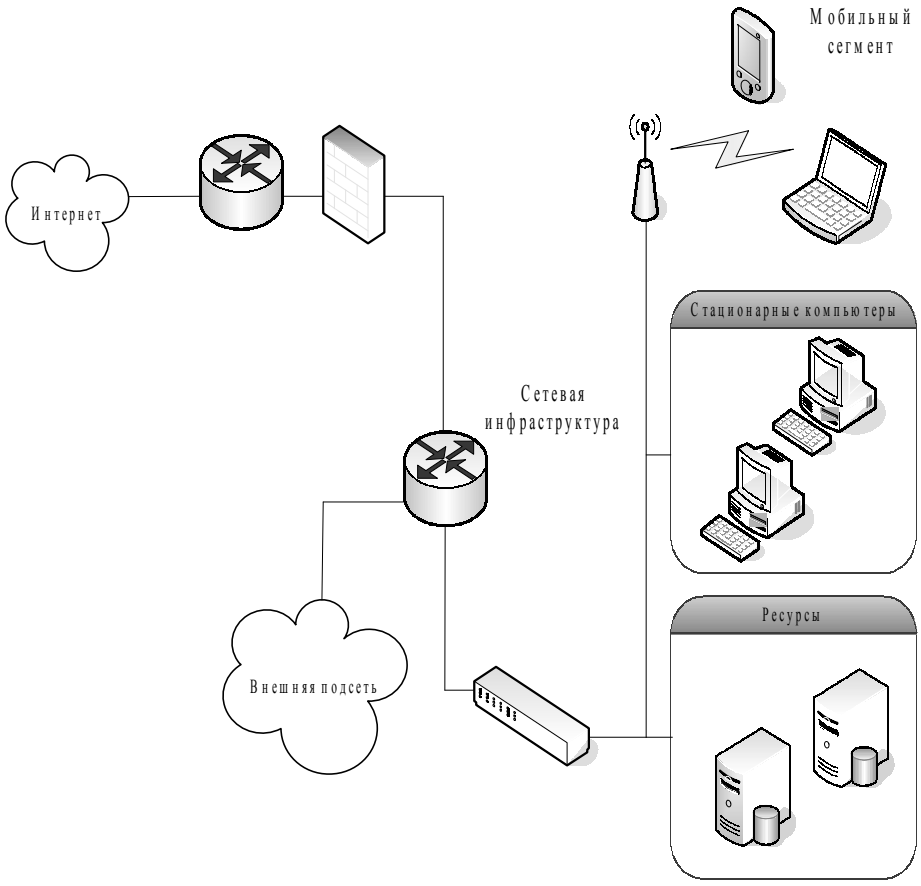

Рис. 1. Гибридная сеть

На рис. 2 представлена систематизация угроз. Угрозы относятся к угрозам конфиденциальности, целостности, доступности. Угрозы также разделяются на активные и пассивные угрозы. Наличие некоторых угроз может привести к появлению других угроз.

Итак, все рассмотренные угрозы классифицируются на угрозы конфиденциальности, целостности, доступности, а также на активные и пассивные угрозы. В некоторых случаях существует взаимосвязь между угрозами.

К примеру, существование угрозы истощения запасов энергии может привести к угрозе отказа в обслуживании. В данном случае угроза отказа в обслуживании является более общей, а угроза истощения запасов энергии более частной.

Также рассматривается отношение «причина – следствие». К примеру, спуфинг сетевого трафика может привести как к расширению привилегий, так и к разглашению информации.

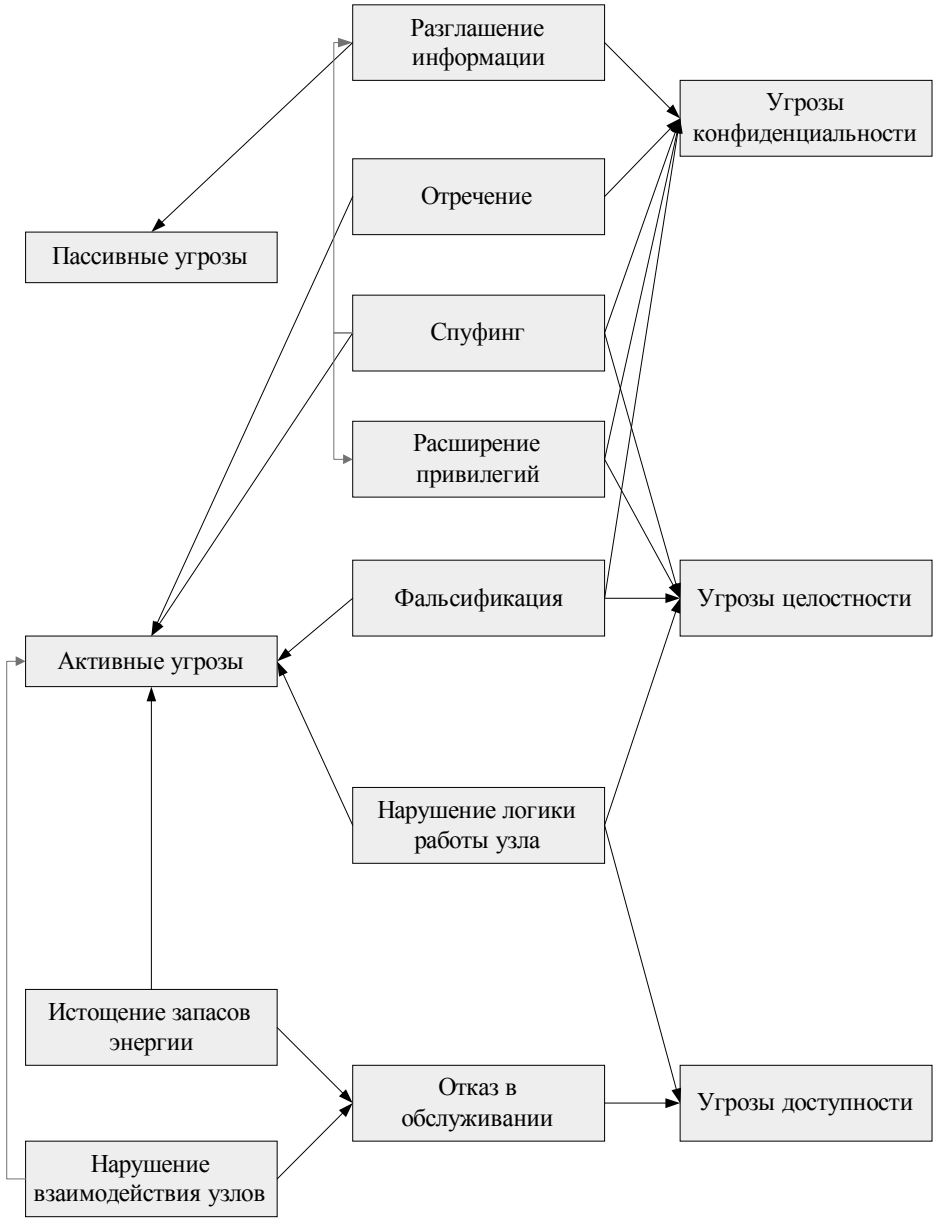

Рис. 2. Систематизация угроз мобильного сегмента

4. Заключение

В данной статье рассмотрены угрозы гибридной сети, состоящей из фиксированного и мобильного сегментов. Предложена систематизация угроз мобильного сегмента. Систематизация угроз позволяет, во-первых, выделить наиболее опасные угрозы, во-вторых, определить дополнительные угрозы, возникающие из-за особенностей гибридных сетей, а, в-третьих, является отправной точкой для дальнейших исследований безопасности гибридных сетей.