Подход к оценке вероятностно-временных характеристик процесса, описывающего действия организованного злоумышленника на завершающем этапе реализации атаки на систему управления сетью синхронизации

А. К. Канаев[1], Е. В. Опарина[2]
ФГБОУ ВО ПГУПС
[1]kanaevak@mail.ru, [2]sirayaekaterina@mail.ru

Е. В. Опарин
«Гипротранссигналсвязь» – филиал АО «Росжелдорпроект»
onapuh@mail.ru

***Аннотация*. This article presents an approach for assessing the probability-time characteristics of security of a synchronization network management system at the stage of completion of an attack by an organized attacker.**

Ключевые слова: telecommunication system; synchronization network; control system; attack; vulnerability; security; attacker

I. Введение

Современные информационные системы с учетом применяемых информационных технологий в своей работе опираются на телекоммуникационные системы (ТКС). Одной из ключевых подсистем ТКС, обеспечивающих ее функционирование, является сеть синхронизации [1].

Основной задачей сети синхронизации является поддержание согласованного взаимодействия цифровой аппаратуры связи ТКС. Данное согласованное взаимодействие обеспечивается путём формирования, передачи и доставки синхросигналов, необходимых для обеспечения и поддержания синхронной работы оборудования ТКС [1].

Современные сети синхронизации являются сложными гетерогенными структурами, для организации функционирования которых необходимы системы управления (СУ).

Реализовав целенаправленную атаку на СУ сетью синхронизации злоумышленник способен значительно снизить качество передаваемых синхросигналов, что также будет способствовать снижению качества предоставляемых услуг связи. Отметим, что рассматриваемая СУ сетью синхронизации выполняет функции как по управлению тактовой сетевой синхронизацией, так и системой единого времени.

II. Основные этапы реализации атаки на систему управления сетью синхронизации

В общем случае можно выделить 3 этапа реализации атаки организованным злоумышленником на СУ сетью синхронизации (рис. 1) [2]:

- предварительный сбор информации об объекте атаки;
- реализация атаки;
- завершение атаки.

Рис. 1. Этапы реализации атаки

После этапа реализации атаки, когда злоумышленник получил доступ к СУ сетью синхронизации, злоумышленник в большинстве случаев будет иметь намерение поддерживать доступ, а также оставаться незамеченным, чтобы иметь возможность удерживать СУ под своим контролем в течение долгого времени, добывая необходимую информацию или используя ресурсы СУ сетью синхронизации в своих целях.

Проведенный анализ процесса проведения атак позволил сформировать следующую модель действий злоумышленника на завершающем этапе реализации атаки на СУ сетью синхронизации (рис. 2). Данная модель отражает все основные действия организованного злоумышленника. Несмотря на большое многообразие видов атак и инструментов по их реализации, модель действий злоумышленника на завершающем этапе реализации атаки на СУ сетью синхронизации обязательно включает в себя следующие состояния [3]:

a_1 – злоумышленник завершил второй этап реализации атаки (рис. 1) и получил доступ к СУ сетью синхронизации;

a_2 – Злоумышленник в соответствии со своими возможностями устраняет существующие уязвимости в СУ сетью синхронизации и настраивает её под себя с целью организации единой точки управления;

a_3 – Злоумышленник устанавливает в СУ «черный ход» уровня приложения;

a_4 – Злоумышленник устанавливает в СУ сетью синхронизации традиционный *RootKit*;

a_5 – Злоумышленник устанавливает в СУ сетью синхронизации *RootKit* уровня ядра;

a_6 – Злоумышленник изменяет в СУ сетью синхронизации файлы регистрации событий.

a_7 – Злоумышленник добавляет в память СУ сетью синхронизации дополнительные «труднообнаруживаемые» файлы.

a_8 – Злоумышленник организует тайные сетевые каналы между скомпрометированной СУ сетью синхронизации и своим узлом для обмена информацией.

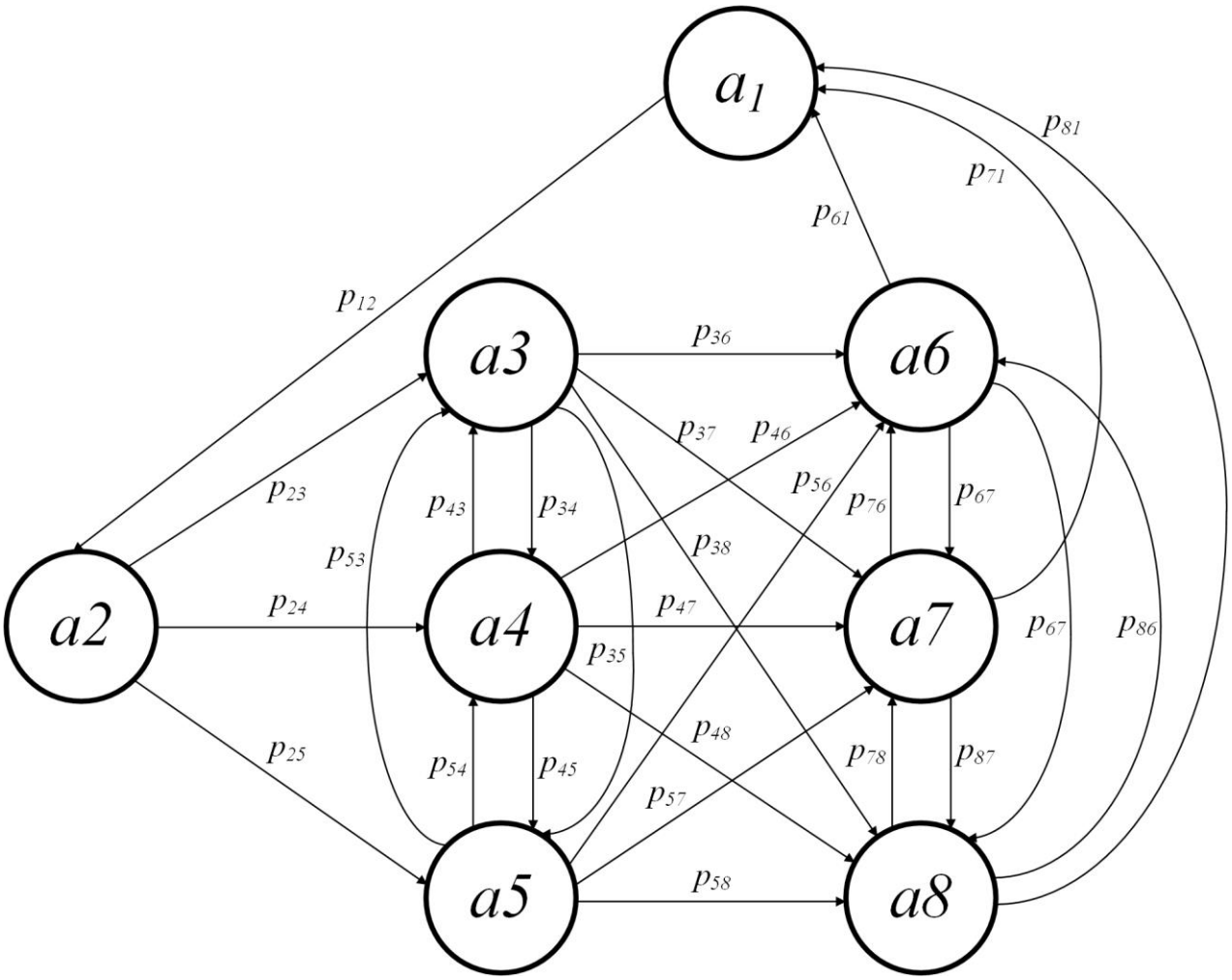

Рис. 2. Модель процесса этапа завершения атаки при ее реализации

Процесс действий злоумышленника на завершающем этапе реализации атаки на СУ сетью синхронизации выглядит следующим образом. Исходным состоянием является состояние a_1, когда злоумышленник в соответствие со своими целями и используемым инструментарием реализовал атаку и получил доступ к СУ сетью синхронизации.

На следующем этапе в состоянии a_2 злоумышленник приложит все свои усилия, чтобы устранить возможные и найденные им уязвимости в СУ сетью синхронизации, в том числе и ту, через которую он сам получил доступ. Данные действия необходимы злоумышленнику для того, чтобы, во-первых, ограничить доступ других злоумышленников к скомпрометированной СУ, а во-вторых, по возможности, сокрыть следы своего

нелигитимного присутствия в ней. Таким образом, на данном этапе злоумышленник полностью обосновывается в СУ сетью синхронизации.

На следующих этапах злоумышленник установит в СУ сетью синхронизации вредоносное программное обеспечение, обеспечивающее «черный ход». «Черный ход» обеспечит доступ злоумышленника к СУ, даже если первоначальная точка входа злоумышленника, которая способна его выдать, будет удалена или изменена администраторами безопасности.

Вредоносное программное обеспечение может обладать в СУ сетью синхронизации правами стандартной программы (состояние a_3), традиционного *RootKit* (состояние a_4) или *RootKit* уровня ядра (состояние a_5).

Чтобы избежать обнаружения администраторами безопасности, злоумышленник будет изменять файлы регистрации в СУ сетью синхронизации, откорректировав в них определенные события, связанные с получением доступа, повышением привилегий, установкой *RootKit* и «черных ходов» (состояние a_6).

Для сокрытия своих следов в СУ сетью синхронизации злоумышленник будет создавать файлы и каталоги с соответствующими атрибутами (состояние a_7).

Для организации взаимодействия с вредоносным ПО в СУ сетью синхронизации злоумышленник будет использовать механизмы тайных сетевых каналов, которые могут быть реализованы поверх различных протоколов, например, *ICMP* и *HTTP*. Злоумышленник в состоянии задействовать дополнительное пространство в заголовках передаваемых пакетов и кадров, чтобы обмениваться информацией (состояние a_8).

Отметим, что в состояниях a_6, a_7 и a_8 злоумышленник реализует свою программу действий, а системы обеспечения информационной безопасности обеспечивают мониторинг вредоносной активности и восстановление процесса функционирования СУ сетью синхронизации.

После реализации данных этапов в СУ сетью синхронизации, злоумышленник может начать процесс заново, проводя атаки на другие подсистемы ТКС, используют подконтрольные узлы и системы как дополнительный ресурс.

На основе разработанной модели возможно произвести расчет вероятностно-временных характеристик процесса, описывающего действия организованного злоумышленника [4]. В качестве примера ниже приведен результат расчета по оценке зависимости коэффициента исправного действия $К_и$ СУ сети синхронизации от интенсивности попыток организованного злоумышленника по установке традиционного *RootKit* (рис. 3).

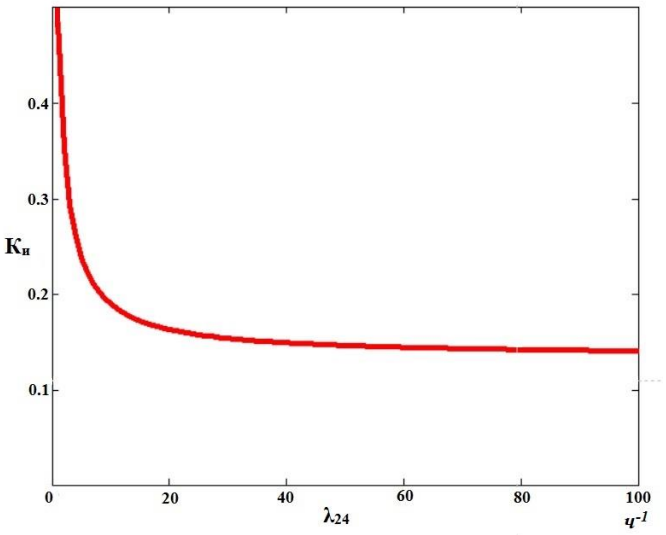

Рис. 3. Зависимость коэффициента исправного действия $К_и$ СУ сети синхронизации от интенсивности попыток организованного злоумышленника по установке традиционного *RootKit*

Коэффициент исправного действия $К_и$ СУ сети синхронизации является показателем, характеризующим устойчивость СУ сети синхронизации в процессе её функционирования, в том числе в условиях воздействия атак организованных злоумышленников [4].

По результатам моделирования можно сделать следующие выводы:

- Коэффициент исправного действия $К_и$ СУ сети синхронизации имеет достаточно низкие значения (в интервале 0,15–0,4) в независимости от интенсивности попыток организованного злоумышленника по установке традиционного *RootKit*. Данные значения являются вполне логичными, так как в статье рассматривается завершающий этап атаки на СУ сетью синхронизации, когда, по сути, злоумышленник уже получил доступ к СУ, ему остается только совершить завершающие действия, установить зловредное программное обеспечение и настроить СУ под свои цели.
- Интервал интенсивности попыток организованного злоумышленника по установке традиционного *RootKit* можно разделить на 2 диапазона. В первом диапазоне незначительное изменение интенсивности попыток по установке традиционного *RootKit* приводит к значительному изменению коэффициента исправного действия $К_и$. Во втором диапазоне изменение интенсивности попыток по установке традиционного *RootKit* не приводит к значительному изменению коэффициента исправного действия $К_и$. Оценив данные диапазоны, злоумышленник может оптимально управлять своими усилиями по организации атаки на СУ сетью синхронизации, а администраторы безопасности соответственно средствами защиты.

III. Заключение

Сеть синхронизации является важной подсистемой ТКС, непосредственно влияющей на качество предоставления услуг связи. Для своевременного предотвращения атак на СУ сетью синхронизации требуется обоснованная оценка их защищенности от воздействия атак организованных злоумышленников. В связи с чем в данной статье представлен подход по оценке вероятностно-временных характеристик процесса, описывающего действия организованного злоумышленника на завершающем этапе реализации атаки на СУ сетью синхронизации. Получена модель (рис. 2), позволяющая на основе требований к вероятностно-временным характеристикам защищенности СУ сетью синхронизации сформировать обоснованные требования к качественному и количественному составу средств защиты СУ сетью синхронизации, учитывая при этом характер потенциального злоумышленника. Существует возможность достижения заданных значений вероятностно-временных характеристик защищенности СУ сетью синхронизации путём управления параметрами средств защиты. Данная модель универсальна и отличается полнотой учёта состояний, отражающих полный комплекс деструктивных воздействий организованного злоумышленника.

Список литературы

[1] Давыдкин П.Н., Колтунов М.Н., Рыжков А.В. Тактовая сетевая синхронизация. М.: Эко-Трендз, 2004. 205 с.

[2] Лукацкий А. Обнаружение атак. СПб.: БХВ-Санкт-Петербург, 2003. 596 с.

[3] Скудис Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите / Пер. с англ. М.: ДМК Пресс, 2003. 512 с.

[4] Коцыняк М.А., Осадчий А.И., Коцыняк М.М., О.С. Лаута., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2014. 126 с.