– Наличие в трафике ARP-пакета для IP, который не входит в инфраструктуру компании.

Инъекция маршрута:

– Большое число несуществующих маршрутов в таблице маршрутизации.

– Быстрорастущее число update пакетов в dump’е трафика.

Данные характеристики помогли написать программу, представляющую собой средство защиты информации, которое использует правила, помогающие корректно детектировать атаки на протокол EIGRP. Ниже представлен пример детектирования DDoS атаки.

Исходя из вышеописанного можно сделать вывод о том, что для любой атаки, кроме атак нулевого дня, возможно создать средство защиты либо написать правило, которое поможет обнаружить злоумышленника, что поспособствует защите различной чувствительной информации. Также можно сказать, что разработанное средство детектирования атак оказалось эффективным для обнаружения атак.

Список использованных источников

1. Okonkwo Comparative study of EIGRP and OSPF protocols based on network convergence / Okonkwo, a. E. IJ, ID. — Текст : непосредственный // International Journal of Advanced Computer Science and Applications. — 2020, № 6. — С. 39-45.

2. Understand and Use the Enhanced Interior Gateway Routing Protocol. — Текст: электронный // Cisco: [сайт]. — URL: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html (дата обращения: 16.12.2023).

3. EIGRP // Cisco Learning URL: https://ciscolearning.ru/cisco-router/eigrp/ (дата обращения: 16.12.2023).

Мозжухин Даниил Ринатович, студент каф. 402 Московского Авиационного Института, danigrok3@gmail.com.

УДК 621.396:629.7

РАЗРАБОТКА ПРОТОКОЛА СВЯЗИ

А.Т. Хакимхан, Е.А. Бобина
КНИТУ-КАИ им. А. Н. Туполева, г. Казань

Ключевые слова: ультрафиолетовая связь, протокол передачи, система.

Лазеры, благодаря своей способности преобразовывать энергию в высоконаправленные лучи электромагнитного излучения, нашли широкое применение в современных оптических системах связи [1]. Основываясь на принципе возбуждения атомов или молекул в активном элементе и последующей генерации когерентного излучения, лазеры обеспечивают

надежный и эффективный метод передачи информации на большие расстояния. Важным компонентом лазерной системы является оптический резонатор, состоящий из двух зеркал и активного элемента, что позволяет управлять параметрами излучения для оптимизации передачи данных [2].

Несмотря на то, что ультрафиолетовые технологии отличаются от традиционных лазерных систем связи, изучение лазеров предоставляет важные основы для понимания принципов оптической связи в целом. Ультрафиолетовая связь предлагает ряд преимуществ, включая возможность работы в условиях прямой видимости и при высоких скоростях передачи данных, что делает ее перспективным направлением для развития беспроводной оптической связи [3]. В данной работе акцент сделан на разработке протокола оптической связи, использующего ультрафиолетовое излучение.

Решение поставленной задачи состоит из нескольких этапов:

1) Определение критериев, структурных и функциональных параметров.

2) Выбор передатчика в соответствии с критериями, анализ характеристик источника излучения.

3) Разработка схемы источника излучения.

На данном этапе осуществляется выбор и анализ характеристик источника излучения на теоретическом уровне, без детализации схематического представления.

Обозначим необходимость соблюдения нескольких условий для функционирования эффективной и надежной системы:

- обеспечение прямой видимости между передатчиком и приемником;
- обеспечение высокой скорости передачи данных;
- гарантирование адаптации приемника к изменениям характеристик источника излучения.

Условие прямой видимости обеспечивает защиту от перехвата сообщений сторонними приемниками. Требование высокой скорости передачи данных соответствует критериям эффективности. Кроме того, адаптация приемника под различные условия гарантирует эффективное функционирование системы.

В структурную схему разрабатываемой системы входят: источник информации, кодер, модулятор, передатчик, канал связи, приемник, демодулятор, декодер, получатель информации.

Каждый элемент системы выполняет функцию:

— источник информации отправляет сообщение;

— кодер шифрует сообщение, шифрование осуществляет защиту передачи данных;

— модулятор преобразовывает электрический сигнал в оптический;

— передатчик осуществляет передачу информации по оптическому каналу связи;

— приемник распознает в принимаемых колебаниях переданный оптический сигнал;

— демодулятор преобразовывает принятый оптический сигнал в электрический;

— декодер расшифровывает сообщение принятого сигнала;

— получатель информации принимает исходное сообщение.

Разрабатываемый протокол должен обладать высокой эффективностью и надежностью. Механизм управления с использованием ультрафиолетового излучения основывается на передаче сообщений, модулированных ультрафиолетовым излучением, к приемнику ультрафиолетового излучения. Передатчик отправляет серию импульсов, каждый импульс имеет определенную, предварительно заданную длительность. Между последовательными импульсами формируется интервал, разделяющий передаваемые данные.

В качестве приемного элемента системы выбран ультрафиолетовый датчик, способный принимать излучение в трех диапазонах: ультрафиолет A (400 – 315 нм), ультрафиолет B (315 – 280 нм) и ультрафиолет C (280 – 100 нм), при этом пороговая длина волны составляет 370 нм. Данный датчик ультрафиолета характеризуется высокой чувствительностью исключительно к ультрафиолетовому излучению, что делает его идеальным для точного определения уровня ультрафиолетового излучения без необходимости использования волновых фильтров.

Учитывая характеристики датчика, в качестве источника излучения был выбран ультрафиолетовый светодиод с рабочей длиной волны 275 нм. Исходя из анализа, можно утверждать, что ультрафиолетовое излучение для передачи данных относится к коротковолновому спектру (ультрафиолет C), что обеспечивает эффективное распространение сигнала в заданном диапазоне.

Следует подчеркнуть, что диапазон ультрафиолета C характеризуется отсутствием влияния солнечного излучения, что делает его устойчивым к солнечным помехам. Это обстоятельство, в сочетании с согласованностью характеристик приемника и передатчика, способствует повышению эффективности передачи данных, упрощая тем самым выполнение остальных требований системы.

Список использованных источников

1. Тарасов Л. В. Лазеры: действительность и надежды. – М. : Наука. Главная редакция физико-математической литературы, 1985. – 176 с.

2. Martin B. Spencer and Willis E. Lamb, Jr. Theory of Two Coupled Lasers. Phys. Rev. A **5**, p.p. 893 – 898. February 1972.

3. Беспроводная оптическая связь в ультрафиолетовом с-диапазоне / Ефимова Ю. И., Прощенок Э. В., Роменский М. В., Унру П. П. // Modern Science. – 2021. – № 4-1. – С. 445-450.

Хакимхан Алина Тахировна, студент каф. электронных и квантовых средств передачи информации (ЭКСПИ), alinahakimhan@mail.ru.

Бобина Елена Андреевна, к.т.н., доцент каф. электронных и квантовых средств передачи информации (ЭКСПИ), eabobina@yandex.ru.

УДК 004.056

СРЕДСТВА ПРОВЕДЕНИЯ MITM-АТАК НА УРОВНЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Э.М.Вахитова, А.Ф.Фатхелисламов
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: анализ трафика, сетевая инфраструктура, MITM, моделирование атак, система защиты, трафик, сетевые аномалии.

Атаки типа "человек посередине" (MITM, Man-in-the-middle attack) на уровне операционной системы представляют серьезную угрозу для безопасности сетей и частной информации. В данной научной статье проводится анализ различных средств, используемых злоумышленниками для осуществления атак типа MITM на уровне операционной системы. Будут рассмотрены основные методы, такие как ARP spoofing, DNS spoofing и SSL stripping, а также уязвимости, связанные с каждым из них. Кроме того, статья представляет различные меры и средства защиты, которые могут быть использованы для предотвращения и обнаружения атак MITM на уровне операционной системы.

Сетевая атака – одна из самых больших проблем при обеспечении безопасности информации предприятий и бесперебойной работы информационных систем. Обеспечение безопасности сетевой инфраструктуры играет важную роль при проектировании систем защиты [1]. Атаки типа "Человек посередине" (MITM), проводимые на уровне операционной системы, представляют значительную угрозу безопасности информационных систем. В этой статье мы приводим обзор основных инструментов, используемых злоумышленниками для проведения MITM-атак [2], уделяя особое внимание Bettercap, Mitmproxy и Hetty в качестве наглядных примеров. MITM-атаки предполагают, что злоумышленник перехватывает сетевой трафик между двумя или более узлами и манипулирует им, выдавая себя за доверенного посредника. Такие атаки могут привести к несанкционированному раскрытию конфиденциальной информации, такой как пароли, банковские данные, а также внедрению вредоносного кода или изменению передаваемых данных. MITM-атаки на уровне операционной системы получили широкое распространение