УДК 004.056

РАЗРАБОТКА МЕТОДА ПЕРЕХВАТА И ПОДМЕНЫ ВИДЕОПОТОКА В СИСТЕМАХ IP-ВИДЕОНАБЛЮДЕНИЯ

Домницкий Е.А. (Федеральное государственное автономное образовательное учреждение высшего образование «Национальный исследовательский университет ИТМО»),
Научный руководитель – кандидат технических наук, доцент Попов И.Ю.
(Федеральное государственное автономное образовательное учреждение высшего образование «Национальный исследовательский университет ИТМО»)

Аннотация

В настоящем докладе предложен разрабатываемый метод перехвата и подмены видеопотока с IP-камеры системы видеонаблюдения. В процессе разработки применены техники пассивного прослушивания и анализа сетевого трафика между камерой и принимающим компьютером. В состав метода входит использование техник отравления ARP-кеша и создания ложных сетевых пакетов, применяются сетевые утилиты и разработанные скрипты. Решение протестировано на локальном виртуальном и на лабораторных стендах с применением реальной IP-камеры иностранного производителя.

Введение

Постепенно IP-камеры вытесняют аналоговые CCTV камеры и записывающие устройства. В 2021 году рынок IP-камер систем видеонаблюдения (в штуках) в России вырос почти на 23%, а сама Россия вышла на второе место по темпу роста видеонаблюдения за гражданами [1]. Использование IP-камер растет и в частном сегменте - в мире объем рынка камер для систем частного видеонаблюдения в 2021 году достиг 72 млн штук [2].

Вместе с этим расширяется и область применения IP-камер. Один из наиболее заметных примеров, важных в контексте темы настоящего доклада – применение системы IP-видеонаблюдения в связке с системой распознавания лиц. Камера системы наблюдения, установленная, например, в проходной некоторого режимного объекта, передает по сети видеопоток, в фокусе которого - лица граждан, проходящих на территорию объекта. Принимающий компьютер или сервер, находящийся в одной сети с камерой, принимает видеопоток и подает кадры на вход нейронной сети распознавания лиц.

Интегрируемость и масштабируемость систем IP-видеонаблюдения позволяют встраивать их в комплексные системы подобного рода, но это же и создает обширную поверхность для реализации угроз безопасности информации. Для нейронной сети распознавания лиц реальную угрозу составляют состязательные атаки на нейронные сети, которые сейчас активно исследуются [3]. Суть атаки состоит в нанесении на изображение (на один или несколько его цветовых каналов) состязательной маски, приводящей к присвоению изображению ложного лейбла. Однако, исследования состязательных атак не затрагивают того, каким образом подобная маска будет внедрена в изображение при работе реальной системы. Возникает вопрос, возможно ли перехватить и модифицировать/подменить видеопоток с IP-камеры.

Цель настоящей работы - разработать метод перехвата и модификации видеопотока камеры IP-видеонаблюдения; нарушить целостность и достоверность визуальной информации, передаваемой в видеопотоке на экспериментальном стенде, при помощи разработанного метода.

Разработка метода перехвата и подмены видеопотока в системах IP-видеонаблюдения

В качестве IP-камеры для выполнения задач была взята модель, распространенная на пользовательском рынке – Dahua DH-IPC-HDW1230SP-0280B. Это купольная камера пользовательского сегмента, передает видеопоток в кодеке AVC (H.264H), управление

потоками осуществляется посредством протокола RTSP, а передача посредством протокола RTP (над UDP) [4].

В качестве принимающего устройства будем использовать компьютер с VLC media player. Libvlc – библиотека и фреймворк, содержащая в себе множества кодеков и плагинов для работы с медиа. Является движком VLC media player и составляющей множества программ агрегации медиа, например, как программа iSpy для сведения множества потоков с камер наблюдения на один дэшборд, записи и анализа архивных записей [5].

Сценарий:

1) Жертва принимает видеопоток с IPC на некоторый локальный UDP порт по протоколу RTP (над UDP), который согласовывает посредством RTSP.
2) Принимающее устройство – VLC media player
3) Атакующий находится в одной подсети с камерой и хостом, может прослушивать и анализировать трафик в подсети а так же отправлять свои пакеты.
4) На данном этапе считаем, что атакующий способен заполучить аутентификационные данные для камеры (соц. инжненерия, перебор по словарю, поиск коллизий хешей дайджест аутентификации и т.д.)

Для подмены видеопотока атакующий может воспользоваться недостатком протокола RTP (над UDP): во время установления сессии при помощи RTSP, после получения SDP пакета от камеры, принимающее устройство будет ожидать входящий UDP трафик на определенном порту (установленном в пакете RSTP SETUP). При этом принимающее устройство будет игнорировать IP адрес отправителя. Нарушитель может воспользоваться этим, перехватив RSTP SETUP пакет во время установления сессии, и подменив в нем порт, на котором принимающее устройство ожидает поток от камеры. Камера начнет отправлять поток принимающему устройству на подмененный нарушителем порт, тогда как принимающее устройство по-прежнему будет ожидать трафик на изначальном порту. В этот момент нарушитель почти без задержки должен начать отправлять принимающему устройству (жертве) свой видеопоток. Это может быть или предзаписаное видео, или видеопоток все с той же камеры. Если нарушитель располагает аутентификационными данными для камеры – он может запросить новый поток все с той же камеры, модифицировать его, и отправлять на необходимый порт жертвы. Возможно улучшение метода – наруштель посредством IP-форвардинга на своём устройстве должен перехватить изначальный видеопоток (и модифицировать), который «уведен» на ложный порт, и тогда новый поток от камеры запрашивать не потребуется.

Для того, чтобы осуществить данную атаку, нарушитель должен стать посредником между камерой и принимающим устройством (Man-In-The-Middle). Для этого перед проведением атаки нарушитель должен отравить ARP-кеш камеры и принимающего устройства (произвести ARP-spoofing). После этого необходимо разорвать существующее соединение между камерой и принимающим устройством посредством имитации ложного RTSP TEARDOWN пакета или посредством RTP-dos техник.

Для того чтобы удерживать соединение между нарушителем и принимающим устройством (жертвой) необходимо всячески блокировать сообщение между камерой и жертвой (посредством фильтрации, например, пакетов ICMP destination unreachable и т.п.).

Выводы

Атака протестирована на лабораторном стенде с использованием камеры Dahua DH-IPC-HDW1230SP-0280. Перехват и модификация/подмена видеопотока в системах IP-видеонаблюдения возможны и реализованы для сценария, описанного в основной части доклада. Это означает, что конфигурации, подобные описанной в докладе, потенциально уязвимы для атак типа «человек посередине», целостность и достоверность видеопотока в них могут быть нарушены указанным в статье способом. Тем более такие конфигурации непригодны для использования в связке с нейронными сетями распознавания лиц или иных

объектов, так как существует вероятность проведения атаки, подобной описанной, с целью наложения состязательных масок.

Список источников

1. Статья: Видеонаблюдение (Рынок России). TAdviser // TAdviser.ru – [Электронный ресурс] – URL: https://www.tadviser.ru
2. Статья: Видеонаблюдение (Мировой рынок). TAdviser // TAdviser.ru – [Электронный ресурс] – URL: https://www.tadviser.ru
3. A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, D. Mukhopadhyay. A survey on adversarial attack and defenses. // CAAI Transactions on Intelligence Technology – 2021 – [Электронный ресурс] – URL: https://ietresearch.onlinelibrary.wiley.com/doi/pdfdirect/10.1049/cit2.12028
4. Dahua Technology. Dahua DH-IPC-HDW1230SP-0280B Specification. // – [Электронный ресурс] – URL: https://www.dahua.market/kamery-videonablyudeniya/ip-videokamera-dh-ipc-hdw1230sp-0280b-dahua
5. LibVLC. VidoLAN. // VideoLAN.org – [Электронный ресурс] – URL: https://www.videolan.org/vlc/libvlc.html