

РАЗРАБОТКА И ВНЕДРЕНИЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА К ВИДЕОПОТОКУ КАМЕРЫ НАБЛЮДЕНИЯ

Клопов М. П.¹

Научный руководитель – Мигулаева Т.А.¹

¹Университет ИТМО

itmo368306@gmail.com

Введение

Системы видеонаблюдения на базе IP-камер активно используются как организациями, так и частными лицами. Их использование помогает обеспечивать физическую безопасность объектов, контролировать промышленные процессы и обеспечивать работу систем Интернета вещей и компьютерного зрения. Однако, такие системы часто имеют уязвимости, которые могут быть использованы злоумышленниками[1]. Зачастую, производители IP-камер используют протоколы связи без шифрования, создающие риск перехвата данных, и проприетарные решения для обеспечения безопасности, противоречащие принципу Керкгоффа и затрудняющие независимый аудит криптостойкости[2]. Если система видеонаблюдения не защищена должным образом, то злоумышленник, используя инструменты, доступные для бесплатного скачивания, может получить доступ к камере с правами администратора, что даст ему возможность перехватывать видеопоток, изображения и оповещения сигнализации с камеры, а также изменять конфигурацию и исполнять вредоносный код, в том числе для использования камеры для дальнейших атак в составе ботнета[3].

Основная часть

Было решено разработать систему, предоставляющую удаленный доступ к камере видеонаблюдения с помощью VPN-туннеля. Был проведен анализ существующих аналогов и показаны их недостатки. Сформулированы функциональные (удаленный доступ к видеопотоку в реальном времени, возможность записи видео) и нефункциональные (защита от известных уязвимостей, совместимость с настольными и мобильными ОС, простота использования, способность передавать видео высокой четкости с минимальной задержкой при условии достаточного качества соединения) требования к системе. Предложена архитектура системы: в локальной сети камеры развернут VPN-клиент, в удалённой сети VPN-сервер, прокси-сервер и центр сертификации.

Выводы

По результатам работы разработана система безопасного удаленного доступа к видеопотоку IP-камеры при помощи VPN-туннеля. Разработанное решение может быть как использовано в личных целях, так и масштабировано для промышленного использования.

Литература

1. Naor Kalbo, Yisroel Mirsky, Asaf Shabtai, Yuval Elovici. 2020. The Security of IP-Based Video Surveillance Systems. Sensors. Vol. 20, №17. 4806. <https://doi.org/10.3390/s20174806>.
2. Johannes Obermaier, Martin Hutle. 2016. Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS '16). Association for Computing Machinery, New York, NY, USA, 22–28. <https://doi.org/10.1145/2899007.2899008>.

3. Brian Cusack, Zhuang Tian. 2017. Evaluating IP surveillance camera vulnerabilities. Proceedings of the 15th Australian Information Security Management Conference. Edith Cowan University, Perth, WA, Australia. 5-32. <https://ro.ecu.edu.au/ism/202>.