УДК 004

Концепция защиты трафика систем видеонаблюдения

А. А. Алтухов
ЗАО «ОКБ САПР», Москва, Россия

Изучена задача обеспечения аутентичности трафика систем видеонаблюдения и рассмотрена содержательная модель нарушителя, учитывающая такие факторы, как сложность и размер системы, а также расположение камер. Предложена архитектура комплексного решения, обеспечивающего аутентичность трафика систем видеонаблюдения.

Ключевые слова: системы видеонаблюдения, аутентичность, архитектура, криптографические преобразования, симметричные криптосистемы, комплексное решение.

Информация, получаемая с устройства видеонаблюдения, представляет ценность в том и только в том случае, если мы можем установить источник информации, убедиться в том, что данная информация была получена именно с установленного источника (никто ее не подменил) и она подвергалась модификации.

На настоящий момент количество инфраструктур видеонаблюдения велико и продолжает расти. Инфраструктуры систем могут быть как небольшие (в рамках одного здания —видеонаблюдение в офисе маленькой компании), так и огромные системы в рамках масштаба города.

Существует много различных видов камер видеонаблюдения. Все камеры можно сгруппировать в два класса:

- аналоговые;
- цифровые.

Камеры, с которых сигнал поступает на монитор или на сохраняющее устройство в аналоговом виде, называются аналоговыми. Недостатки аналоговых камер: сложность в обработке сигнала, хранении и передаче на большие расстояния, а цифровые камеры, занимающие лидирующее положение на рынке, этих недостатков не имеют.

Все множество цифровых камер можно разделить на два больших класса:

- камеры на базе цифровых видеорегистраторов;
- IP-камеры.

Большой интерес представляют IP-камеры как наиболее приоритетное направление развития систем видеонаблюдения.

Алтухов Андрей Андреевич, инженер-программист.
E-mail: altuhov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

IP-камера (или Сетевая камера) — цифровая видеокамера, которая передает видеоданные в цифровой форме по сети, использующей IP-протоколы. IP-камера является полноценным сетевым устройством, обладает своим собственным IP-адресом.

IP-камеры, в отличие от аналоговых камер и камер с видеорегистраторами, могут располагаться на значительном расстоянии от центра наблюдения, передавая информацию по сети. Камеры с видеорегистраторами также могут находиться вдали от места обработки информации, но не на большом расстоянии от видеорегистратора и сервера, передающего информацию в этот центр обработки. Если сеть камер с видеорегистратором или система аналоговых камер в большинстве случаев не выходит за пределы контролируемой зоны или находится в ее непосредственной близости, то сфера применения IP-камер такова, что они скорее всего размещены в неконтролируемой зоне и потенциально к ним может иметь физический доступ «любой желающий», не говоря о том, что трафик идет по сети.

Прежде чем говорить о существующих технологиях безопасности в области систем видеонаблюдения, следует обратить внимание на тот факт, что существуют различные ценовые категории камер. Есть и очень дешевые камеры и, как следствие, мало функциональные. Есть очень дорогие камеры, сравнимые по стоимости с серверами (по сути, сами являющиеся ЭВМ). Большое количество камер из ценовой категории выше среднего предлагают поддержку стандартных протоколов аутентификации IEEE802.1X.

Протоколы аутентификации не решают весь комплекс проблем безопасности. Часто механизмы безопасности предполагают наличие дополнительных серверов или локальных сетей, обладающих специальными свойствами. Также следует отметить, что не одно из предлагаемых решений не является комплексным.

Не следует забывать, что камеры низкой ценовой категории не реализуют никаких функций безопасности, а для создания больших сетей камер логично было бы использовать недорогие камеры, особенно если велика вероятность физического повреждения, но в то же время нельзя отказываться от безопасности. В данной ситуации универсальное решение по обеспечению безопасности, поддерживающее произвольные камеры, позволило бы решить возникающий конфликт, предоставив пользователю право выбирать произвольные камеры для системы видеонаблюдения в зависимости от желаемых качеств (цена, качество видео и т. д.), не беспокоясь о безопасности в момент выбора видеокамеры.

Грамотное введение в эксплуатацию и настройка систем видеонаблюдения — весьма не тривиальная задача, требующая технически квалифицированных работников. Вполне естественно, что заказчик систем видеонаблюдения делегирует обязанности по созданию и настройке системы специалистам в этой области (компания интегратор). Системы видеонаблюдения, состоящие из огромной сети камер, нуждаются в обслуживании. Владельцы достаточно больших по количеству и обширных по занимаемой территории сетей камер в подавляющем большинстве случаев не могут (да это и невыгодно) содержать свой штат сотрудников, которые будут заниматься ремонтом и обслуживанием системы видеонаблюдения. Обычно пользуются услугами специальных фирм, которые разворачивают системы видеонаблюдения и затем обслуживают их.

Обслуживающий персонал наряду с вандалами, физически разрушающими систему, и хакерами также является потенциальным нарушителем, обладающими достаточно широкими возможностями. Комплексная система безопасности обязательно должна учитывать такого нарушителя. Пользователь системы видеонаблюдения не обязан знать «внутреннюю кухню» и устройство системы, он лишь должен получать своевременную и подлинную информацию. Для решения задачи «обеспечения подлинности информации» необходимо простое в настройке и использовании комплексное решение, позволяющее гарантировать пользователю тот факт, что независимо от действий обслуживающего персонала и/или других нарушителей подлинности информации ничто не угрожает.

Для комплексного решения проблемы безопасности трафика систем видеонаблюдения предлагается создать систему, состоящую из встраиваемого в камеру устройства, реализующего функционал безопасности, специальное оборудованное рабочее место для оператора системы и центр обработки данных видеонаблюдения (в дальнейшем — Центр), который представляет собой СВТ с доверенной средой и необходимым ПО.

Что должно быть обеспечено системой?

- Аутентичность данных и аутентификация источника данных.
- Все необходимые механизмы безопасности должны быть реализованы только в конечных точках (камерах) и центре управления.

Проблема идентификации источника уже решена. У каждой IP-камеры есть IP-адрес.

Проблему аутентичности данных и аутентификацию источника можно решать на основе уже существующих стандартов безопасности в области сетевых технологий их правильным внедрением, либо создав свое решение, обрабатывающее данные на прикладном уровне модели ЭМВОС. Остановимся на реализации собственных методов на прикладном уровне.

Обеспечить аутентификацию данных и источника можно с помощью криптографического преобразования [1].

Первый вопрос, на который нужно ответить: какой тип криптографического преобразования использовать (симметричное или асимметричное)?

С одной стороны, методы асимметричного криптографического преобразования, реализующие ЭЦП, как нельзя лучше подходят для решения данной задачи. С другой стороны, реализации алгоритмов симметричного шифрования работают гораздо быстрее. В данной ситуации высокая скорость — огромный плюс. В силу централизации системы количество ключей, как для асимметричных, так и для симметричных систем проверки подлинности, будет одинаковое (возможность связи «каждый с каждым» бессмысленна в данном случае) [1]. Остановимся на системе на базе симметричного шифрования.

Всю систему можно разделить на три части:

- камеры видеонаблюдения и соответствующее устройство ИБ;
- центр управления (он же центр безопасности);
- служба распределения ключей.

Какие функции должно обеспечивать, устройство, встраиваемое в камеру и обеспечивающее функционал безопасности трафика видеонаблюдения?

- Шифрование данных видеонаблюдения и некоторых атрибутов.
- Аппаратное хранения ключа.
- Защита ключа от компрометации.
- Постоянная передача в центр сигнала, сообщающего о том, что ключ в камере не был скомпрометирован (дальше — сигнал «жизни»).

Шифрование данных обеспечивает аутентичность трафика (при условии, что можно установить взаимно-однозначное соответствие между камерой и соответствующим ключом шифрования в центре управления). Аутентичность источника обеспечивается за счет добавления к зашифрованным данным информации о камере и некоторых дополнительных меток. Сигнал «жизни» можно обеспечить, добавляя к данным зашифрованные метки времени, хотя лучше использовать альтернативные каналы для передачи данного сигнала.

Наличие сигнала «жизни» — это условие для признания ключа актуальным в конкретный момент времени. Если данный сигнал перестает поступать, то ключ на данном устройстве следует признать скомпрометированным.

Из-за того, что к устройствам возможен физический доступ, необходимо своевременно определять компрометацию. Для этого необходимо контролировать целостность корпуса камеры или ключевого хранилища в камере. Должна быть возможность фиксировать попытку физического проникновения или вскрытия устройства. В этом случае ключ должен быть удален из памяти и сигнал «жизни» должен перестать передаваться.

Устройство должно обеспечивать шифрование видеоданных (достаточно быстро). Оптимальным вариантом будет, если шифрование будет осуществляться непосредственно перед формированием пакетов для отправки в сеть, так как информация в этом случае находится уже в обработанном (сжатом) виде. Из-за технических сложностей реализации «вклинивания» в уже существующую технологию работы, возможно, следует реализовывать шифрование либо после формирования пакета, непосредственно перед его отправкой в сеть (в этом случае придется переформировать пакет), либо сразу с интерфейса цифровой камеры (здесь придется реализовать сжатие).

Какие функции должен обеспечивать «Центр»?

- Учет соответствия камер и ключей.
- Признание ключей скомпрометированными.
- Инициализация механизма распределения ключей для камер, ключи которых были скомпрометированы.
- Проверка подлинности трафика.
- Регистрация нарушения.

В общем случае «Центр» находится в контролируемой зоне и представляет собой СВТ с доверенной средой и с ПО, способным реализовать все вышеописанные функции.

Необходим также правильно составленный регламент для того, чтобы операторы системы безопасности в Центре правильно реагировали на соответствующие события компрометации и могли инициализировать процесс распределения ключей.

Описанная модель решения проблемы не учитывает множество технических аспектов. Приведены только концепция модели и функции компонентов системы обеспечения подлинности трафика систем видеонаблюдения.

Литература

1. *Menezes A., van Oorschot P., Vanstone S.* Handbook of applied cryptography. — CRC Press, 1996.

The idea of protecting video surveillance systems data

A. A. Altukhov
OKB SAPR JSC, Moscow, Russia

The article is devoted to the problem of ensuring authenticity of video surveillance data. The author has described the model of information security violator which takes into account such specific factors as size of a video surveillance system, its complexity and location of cameras. The author has proposed architecture of complete solution which provides authentication mechanism of video surveillance data.

Keywords: video surveillance system, authenticity, architecture, cryptography, symmetric-key cryptography, complete solution.

Bibliography —1 reference. *Received June 14, 2014*