Hanwha Techwin

«Информационный бюллетень»

Wisenet7
Новый уровень кибербезопасности

29 июня 2020 г.

Содержание

1. Общие сведения и предпосылки

Достаточно давно существуют опасения, что злоумышленники могут получить доступ к видео в реальном времени или к видеозаписям с камер видеонаблюдения, установленных в зонах действия систем безопасности. Многие производители камер профессионального уровня восприняли эту угрозу всерьез и представили протоколы настройки сетевых устройств, которые не допускают использования паролей «по умолчанию», либо предъявляют специальные требования к сложности заданных пользователем паролей. Однако хакеры продолжают искать новые способы несанкционированного доступа к данным, в том числе с помощью так называемых «бэкдоров» - недокументированных возможностей или уязвимостей систем.

Конфиденциальные данные конечного пользователя должны быть надежно защищены как от злоумышленника, планирующего использовать их в криминальных целях, так и от «честного хакера», воспринимающего все меры защиты как личный вызов. Это справедливо как для многих тысяч мелких предприятий, доверяющих видеонаблюдению защиту своих активов, людей и собственности, так и для конечных пользователей с высокими требованиями к безопасности критически важных систем и инфраструктурных объектов, таких как аэропорты, банки, местные органы власти, правительственные и военные учреждения, аварийно-спасательные службы и т.д.

В этих условиях компания Hanwha Techwin постоянно работает над повышением уровня защищенности своей продукции. В 2020 году надежные функции и технологии защиты реализованы в продуктах, построенных на собственной разработке компании Hanwha Techwin - чипсете Wisenet7 (SoC — System on Chip).

Первое: внедрение технологии аппаратной защиты позволило преодолеть ограничения, налагаемые технологиями программной защиты. Безопасное хранилище предоставляет место для хранения защищенных данных и на этой основе обеспечивает работу расширенных аппаратных функций защиты, таких как безопасная загрузка, безопасная ОС и безопасный интерфейс JTAG.

Второе: конечная цель сквозной защиты — предотвращение перехвата или фальсификации конфиденциальной информации неавторизованными пользователями путем вмешательства в процесс обмена данными или доступа к устройству для фальсификации или подделки конфиденциальной информации. Для этого необходима идентификация и аутентификация между устройствами, а также контроль доступа и защиты данных с помощью шифрования.

Третье: крайне важно рассматривать безопасность как наивысший приоритет в технических характеристиках и параметрах изделия. Иногда реализация функций защиты высокого уровня может несколько ухудшить характеристики и обратную совместимость изделия, однако с этим приходится мириться, учитывая важность безопасности и тенденциям в промышленности и в обществе.

Некоторые из этих функций являются новинками и разрабатывались они специально для борьбы с кибератаками, в то время как другие функции изначально предназначались для повышения эффективности чипсетов, но и они также вносят свой вклад в защиту камеры.

Настоящий документ предназначен для того, чтобы помочь пользователю лучше понять технологии Hanwha Techwin, обеспечивающие новый уровень кибербезопасности, реализованный в изделиях, оснащенных системой Wisenet7.

2.1. Аппаратная защита

Использование аппаратной защиты очень важно для повышения уровня защищенности изделия, поскольку аппаратные средства позволяют бороться с уязвимостями эффективнее, чем программные. Киберпреступникам гораздо сложнее вмешиваться в работу доверенного ПО («корень доверия»), которое входит в состав защищенных аппаратных средств. Начиная с изделий с Wisenet7, Hanwha Techwin применяет следующие четыре основные технологии аппаратной защиты:

2.1.1. Безопасная загрузка

Начиная с Wisenet7, Hanwha Techwin реализовала безопасную загрузку.

Безопасная загрузка — это механизм проверки целостности ПО, работающего на камере во время загрузки, который гарантирует, что ПО не пострадало от вмешательства внешнего вредоносного кода или других вредоносных программ.

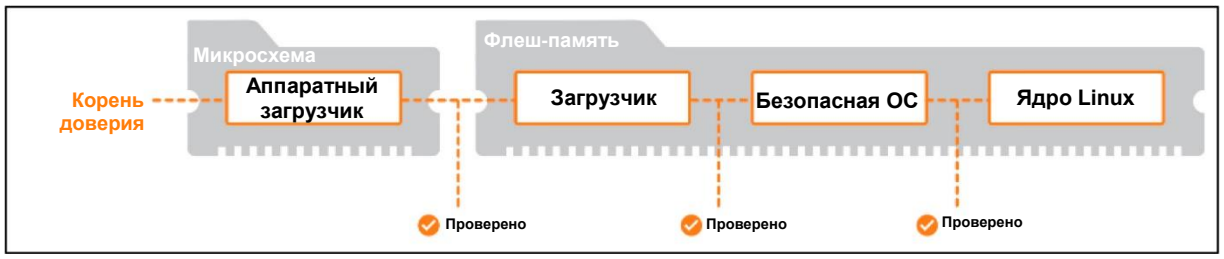

Рисунок 1. Безопасная загрузка в изделиях с Wisenet7

2.1.2. Безопасное хранилище

Wisenet7 также поддерживает независимый модуль аппаратной защиты, который называется HTPM (Hanwha Trusted Platform Module, модуль доверенной платформы Hanwha). HTPM состоит из крипто-процессора (специализированного микроконтроллера, предназначенного для выполнения защищенных операций), генератора случайных чисел, безопасного хранилища, безопасной ОС и пр.

Зона безопасного хранилища HTPM состоит из ОППЗУ (однократно программируемой постоянной памяти) и ЭСППЗУ (электрически стираемой перепрограммируемой постоянной памяти) и служит для хранения важной информации внутри камеры. Важная информация, составляющая корень доверия, записывается в ОППЗУ в ходе производства, а важная рабочая информация хранится в ЭСППЗУ.

2.1.3. Безопасная ОС

Для защищенной обработки важной информации, хранящейся в безопасном хранилище, необходима отдельная безопасная ОС.

Не предусмотрено никаких способов доступа к безопасной ОС извне камеры. Для доступа к безопасной ОС и к безопасному хранилищу необходимо использовать отдельное API из ОС Linux. Безопасная ОС предоставляет независимые функции шифрования и дешифрования, снижая нагрузку на основную ОС, а также обеспечивая дополнительный уровень защиты и разграничения. Приложения, выполняемые в безопасной ОС, проходят проверку для предотвращения подмены и искажения.

2.1.4. Безопасный интерфейс JTAG

Основная часть электроники и устройств «интернета вещей» (IoT) имеет физический интерфейс для отладки и испытаний, называемый JTAG и предназначенный для использования во время производства, проверки качества и технического обслуживания. Самый надежный способ предотвращения несанкционированного доступа через этот интерфейс — его отключение. Однако в этом случае невозможно будет определить причины сбоев, возникающих в кристалле или на плате во время разработки изделия или его производства.

Для предотвращения описанной проблемы в Wisenet7 был реализован механизм аутентификации на основании секретного ключа, который позволяет использовать JTAG, сохраняя при этом высокий уровень безопасности. Только изготовитель владеет соответствующим ключом аутентификации, который при этом разрешает доступ лишь к информации, относящейся к системе, но не к конфиденциальной информации заказчика. В случае неисправности ее анализ можно проводить только при непосредственном локальном доступе к устройству, используя ключ аутентификации, предоставленный изготовителем, но не удаленно, поэтому пользователь может не беспокоиться насчет несанкционированного доступа к его информации.

2.2. Сквозная защита

В дополнение к контролю доступа на основании традиционных паролей, можно повысить уровень защищенности соединения путем использования сертификата устройства, добавленного с целью аутентификации устройства между устройствами. Это предотвращает перехват и искажение информации третьей стороной во время связи. Кроме того, введение цифровой подписи и функций шифрования позволяет распространить сквозную защиту на хранение и резервное копирование данных, а также на обновление аппаратной прошивки и загрузку.

2.2.1. Сертификат устройства (предварительно установленный)

Hanwha использует аппаратные модули безопасности Thales для генерации сертификатов/секретных ключей для каждого устройства Wisenet7 и программирует каждое устройство во время его изготовления. Когда пользователь создает сертификат, он получает цифровую подпись с использованием нашего секретного корневого ЦС, и он может убедиться, что сертификат выпущен компанией Hanwha. С помощью этого сертификата пользователь может устанавливать защищенные соединения без сообщений о нарушении безопасности в его веб-браузере. Веб-браузер позволяет просмотреть этот сертификат, а также проверить его происхождение и подлинность.

2.2.2. Взаимная аутентификация

Проведение взаимной аутентификации для защищенного соединения — это надежный способ повысить конфиденциальность, целостность и достоверность защищаемой информации. Устройства Wisenet7 от Hanwha Techwin используют аутентификацию клиента для взаимной аутентификации между камерами и устройствами пользователя в соединении типа HTTPS (HTTP через TLS, RTSP через HTTPS).

В общем случае взаимная аутентификация может быть произведена как пользователем, так и устройством. Hanwha Techwin реализовала взаимную аутентификацию между своими устройствами.

Аутентификация камеры, выступающей в роли сервера при взаимной аутентификации, называется аутентификацией сервера, а аутентификация клиентских устройств (видеорегистраторов, систем видеонаблюдения, рабочих станций пользователя) называется аутентификацией клиента. Аутентификация сервера происходит на клиенте, а аутентификация клиента происходит на сервере. Аутентификация клиента предоставляется в качестве опции на основе аутентификации сервера, таким образом обеспечивая взаимную аутентификацию путем аутентификации клиентов в более широком смысле слова.

2.2.3 Проверка цепочки сертификатов

Существует сертификат корневого центра сертификации (ЦС), гарантирующий корень доверия в камере, и цепочка сертификатов проверяется с использованием сертификата корневого ЦС. В изделиях Wisenet7 существует два типа сертификатов корневого ЦС. Один предназначен для сертификата самого устройства, а второй для приложений Open Platform.

Сертификат корневого ЦС для сертификата устройства используется при установке сертификата устройства на камеру и для проведения аутентификации клиента с использованием сертификата клиентского устройства (ПК, видеорегистратора). В первом случае он требуется для предотвращения установки любых сертификатов без разрешения изготовителя, для чего при установке сертификата устройства на камеру производится проверка цепочки сертификатов. Во втором случае он служит напоминанием о том, что это доверенное устройство, выпущенное компанией Hanwha, путем проверки цепочки сертификатов клиентских устройств.

Сертификат корневого ЦС для приложений Open Platform не позволяет устанавливать неавторизованные приложения благодаря проверке цепочки

сертификатов, удостоверяющей, что каждый отдельный ключ и сертификат, которыми подписано приложение Wisenet7 Open Platform, сгенерирован и выдан компанией Hanwha. Это гарантирует, что на камере будет работать только безопасное, авторизованное и не видоизмененное программное обеспечение. Вредоносные программы ни при каких условиях не получат доступа ни к камере, ни к сети.

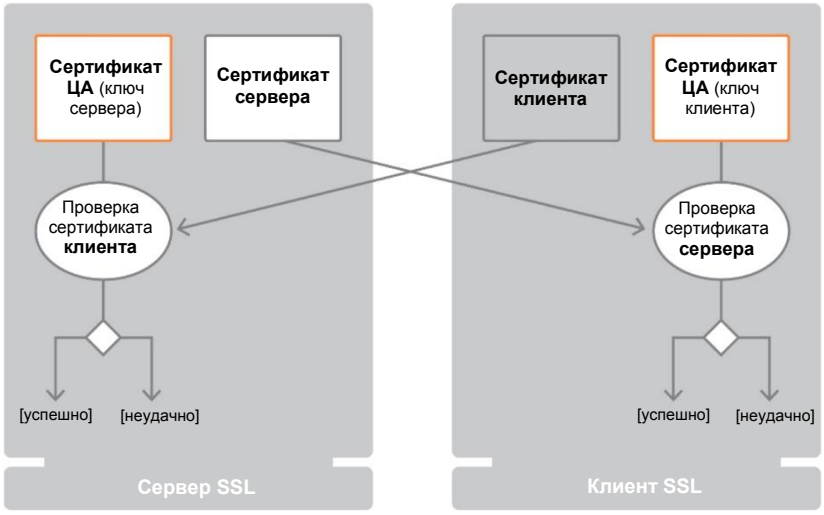

Рисунок 2. Принцип проверки цепочки сертификатов

2.2.4 Проверка вмешательства в аппаратную прошивку

Технология подписанных аппаратных прошивок Hanwha Techwin позволяет безопасно обновлять аппаратные прошивки. В аппаратную прошивку внедряется цифровая подпись, значение которой будет проверено во время обновления, что гарантирует целостность и подлинность загружаемой аппаратной прошивки.

Цифровая подпись аппаратной прошивки генерируется с помощью закрытого ключа через сервер ключей, безопасно управляемый компанией Hanwha Techwin, а открытый ключ, который проверяет цифровую подпись, хранится в области безопасного хранилища Wisenet7 (HTPM).

Цифровые подписи обеспечивают более надежную защиту целостности аппаратной прошивки, чем простое использование хэшей, контрольных сумм и пр. Хэш или контрольную сумму для взломанной аппаратной прошивки очень просто вычислить и подделать.

2.2.5 Шифрование видео (во время простоя и резервного копирования)

Видео, полученное с камеры, представляет собой важные пользовательские данные. Поэтому необходимо не только использовать защищенное соединение для передачи видео, но и применять соответствующие механизмы защиты при хранении изображений на внешних носителях и при резервном копировании видео с камеры на ПК/в систему видеонаблюдения/на видеорегистратор.

Изделия Wisenet7 поддерживают шифрование файловой системы при записи на SD-карту.

Шифрование всей файловой системы, а не индивидуальное шифрование каждого файла устраняет нагрузку, связанную с дешифрованием во время передачи и воспроизведения видео. Кроме того, при AES-шифровании в качестве ключа шифрования используется пароль, заданный пользователем, поэтому злоумышленник не сможет получить доступ к видео, даже если похитит SD-карту.

Изделия Wisenet7 поддерживают шифрование видео при резервном копировании. Для защиты видео они шифруют ZIP-файл при резервном копировании видео, сохраненного на камере, или при ручной записи видео в реальном времени на ПК.

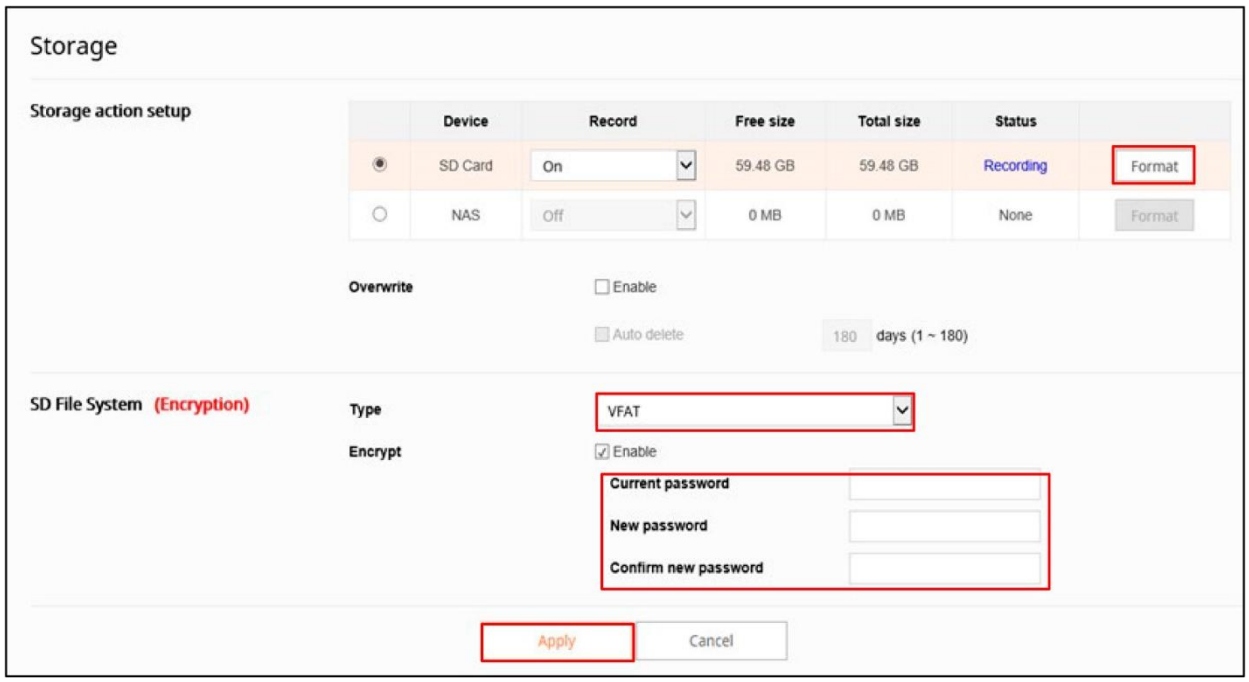

Рисунок 3. Пользовательский интерфейс шифрования SD-карты

2.3. Спроектированная защита данных и конфиденциальность по умолчанию

При разработке новых моделей изготовитель не должен забывать о стандартах защиты, обеспечивающих конфиденциальность, целостность и подлинность системы и конфиденциальных данных пользователя. Необходимо реализовывать эти стандарты защиты, начиная со стадии проектирования; это называется «спроектированная защита данных».

«Конфиденциальность по умолчанию» означает, что принятые по умолчанию настройки — это самая безопасная конфигурация (при этом необязательно самая дружественная к пользователю или лучше всего обеспечивающая обратную совместимость). При этом пользователь должен оценить угрозу безопасности, возникающую при изменении любой из настроек на более подходящую с точки зрения удобства использования или совместимости.

2.3.1. Повышение уровня настроек защиты

Изделия Wisenet7 обеспечивают улучшенную защиту «из коробки», с заводскими настройками по умолчанию. По умолчанию включен режим HTTPS и отключены все ненужные начальные службы, такие как SNMP («простой протокол управления сетью»), локальный адрес канала, обнаружение UPnP и протокол Bonjour. Кроме того, по умолчанию отключены протоколы SUNAPI и ONVIF, пока не будет сконфигурирован пароль пользователя. Все изделия Hanwha Techwin поставляются без пароля по умолчанию. Во время первоначальной установки пользователь должен задать сложный пароль в утилите Диспетчер устройств Wisenet, и лишь после этого он сможет просматривать видео или вносить какие-либо изменения в конфигурацию. Пароль безопасно передается с защитой шифрованием.

2.3.2. Применение последней версии протокола TLS

Изделия Wisenet7 поддерживают последнюю версию протокола TLS, а именно 1.3. По умолчанию для связи можно использовать только безопасные версии TLS (1.2, 1.3). TLS 1.2 до сих пор остается безопасной: несмотря на некоторые ошибки, она широко используется и на сегодня является стандартом для «интернета вещей».

В качестве дополнительных опций доступны и другие версии TLS (1.0, 1.1) и HTTP; их можно использовать, если это необходимо с точки зрения обратной совместимости, однако делать это не рекомендуется.

Самыми существенными отличиями версии TLS 1.3 стали ее более высокая производительность и улучшенная защита:

3. Безопасность в деталях

Для дальнейшего усовершенствования кибербезопасности камеры рекомендуется использовать несколько уровней защиты. Если один из уровней будет нарушен, то ваша сеть и ваши устройства все еще будут защищены на оставшихся уровнях. Рекомендуется создать рабочую группу в составе специалистов по ИТ, видеонаблюдению, системного интегратора и конечного пользователя, чтобы определить системные требования и обязанности каждого подразделения. Ниже приведен перечень рекомендаций, связанных с кибербезопасностью, которые можно реализовать на ваших сетевых устройствах для повышения безопасности вашей сети, в том числе камер, маршрутизаторов и пр.

- Создайте пользовательские аккаунты с минимумом самых необходимых привилегий
- Отключите гостевой/неаутентифицированный доступ RTSP
- Регулярно меняйте пароли; не используйте одинаковые пароли для разных систем
- Обновляйте системные часы/NTP, поддерживайте в актуальном состоянии настройки перехода на летнее время и часовой пояс
- Включите контроль доступа на основе сертификата 802.1x
- Не включайте Multicast, если не уверены, что это вам нужно
- Не включайте DDNS, если не уверены, что это вам нужно
- Не включайте Bonjour, если не уверены, что это вам нужно
- Не включайте UPnP, если не уверены, что это вам нужно
- Не включайте локальный адрес канала, если не уверены, что это вам нужно
- Не включайте FTP, если не уверены, что это вам нужно
- Если вам нужен протокол SNMP, то используйте SNMP версии 3
- Если вам нужна электронная почта, то используйте защищенный протокол SMTP
- Не включайте QoS, если не уверены, что это вам нужно
- Организуйте виртуальные сети VLAN в общей сети

- Устанавливайте камеру там, где она будет недоступна для посторонних, защищайте проложенные кабели
- Вместо «традиционных» портов по умолчанию используйте порты с другими номерами
- Включите фильтрацию по IP
- Камеры должны быть подключены к собственной сети, отделенной от корпоративной/производственной сети и от сети интернет
- Включите запись на SD-карту в качестве резервной меры на случай прерывания связи с системой видеонаблюдения или сбоя сети
- Документируйте все изменения конфигурации, экспортируйте настройки/создавайте резервные копии конфигураций
- Сохраните снимок поля зрения камеры
- Сделайте узнаваемую настройку, по которой вы сможете определить вмешательство в конфигурацию/сброс к настройкам по умолчанию
- Для удаленного доступа используйте только виртуальную сеть VPN или защищенное облако
- Для записи на SD и экспорта видео используйте проприетарный формат видеофайлов
- Защитите все сетевые маршрутизаторы, видеорегистраторы/системы видеонаблюдения, а также PoE-инжекторы с помощью ИБП
- Включите аналитику, обнаруживающую внешнее воздействие и расфокусировку
- Включите обнаружение отключения сети, если используется низковольтное питание
- Регулярно проверяйте журналы устройств

4. Заключение

Wisenet7 предлагает сквозную кибербезопасность с самыми высокими уровнями кибербезопасности с безопасной загрузкой ОС, хранилищем, подписыванием аппаратной прошивки, приложения Open Platform, безопасным интерфейсом JTAG и многим другим. Hanwha Techwin установила свою собственную систему выдачи сертификатов устройств, чтобы внедрять сертификаты в продукт не только в процессе разработки, но и в процессе производства. Благодаря новому уровню кибербезопасности Wisenet7 пользователи могут строить системы видеонаблюдения, не имеющие себе равных с точки зрения защищенности.

WISENET

Hanwha Techwin Co., Ltd

13488 Hanwha Techwin R&D Center,

6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do

ТЕЛ. : 070.7147.8771-8

ФАКС : 031.8018.3715

http://hanwha-security.com

Hanwha Techwin