Семь уровней защиты данных в системе учета энергоресурсов БАЛАНС

Безопасность IoT часто воспринимается как очаг сбоев. Тем не менее, в этой области ведется большой прогресс, и множество компаний работают над решением общих проблем, которые приводят к сбоям безопасности, которые часто бывают в новостях. Вот лишь несколько примеров проблем, с которыми сталкиваются в области безопасности IoT, и методы, разработанные компанией DJV-COM для их решения.

Семь уровней защиты данных:

На уровне доступа по Интернет – база данных. Для администратора, операторов и пользователей – пароль с распределением прав на уровне объектов. Реализация «облачный сервис» с отсутствием прямого доступа к данным. Весь сервис реализуется на базе API интерфейса.

На уровне доступа концентратор – база данных. Два уровня защиты – первый концентратор выходит на заранее заданный IP, независимо откуда инициировано соединение. Второй уровень защиты – закрытый протокол связи SSL на IP соединении.

На уровне радиомодуль – концентратор. Сети разделяются по логическим адресам, не зная который невозможно реализовать обмен данными в радио-сети. Дополнительно используется цифровая подпись. Заказчик имеет возможность самостоятельно изменить логический адрес сети.

На уровне радиомодуль – прибор учета. Использование импульсного выхода для снятия информации с прибора учета **не позволяет принципиально «хакнуть» счетчик** – изменить показания или нарушить функционирование прибора учета. Дополнительно соединение контролируется на целостность – обрыв и замыкание.

На уровне радиомодуля – не существует в принципе команды для изменения накапливаемых данных на радиомодуле. Накопление данных проводится по аналогии с механическим отсчетным устройством – только в сторону накопления. **Команды сброса счетчика или его изменения отсутствуют.**

На уровне базы данных. Дублирование, резервное копирование и контроль достоверности данных.

На уровне Аналитики. Контроль максимального расхода за час и за сутки, контроль равномерности нарастания данных, контроль отсутствия данных. Дополнительно контроль уникальности сетевых адресов радиомодулей и дублирования пакетов данных.

Рассмотрим вариант подмены устройств. Основная атака такова: противник создает устройство, которое имитирует аппаратное обеспечение в сети IoT и использует свое вновь созданное устройство для подачи ложных данных в сеть IoT.

Если такого устройства в сети нет, оно попадает в раздел UNKNOWN и оператор или администратор сети должен определить куда это устройство отнести.

Если это устройство оператору неизвестно, оно так и останется в разделе UNKNOWN.

Если же это устройство известно сети – контролируется уникальности сетевых адресов радиомодулей и дублирования пакетов данных, следовательно система выдаст ошибку – дублирование устройств. Дополнительно каждое устройство имеет привязку к своему концентратору, т.е. нельзя прислать пакет с другого концентратора – система выдаст предупреждение администратору.

Seven levels of data protection in the AMR/AMI system BALANCE

IoT security is often perceived as a hotbed of failures. Nevertheless, great progress is being made in this area, and many companies are working to solve common problems that lead to security failures, which are often in the news. Here are just a few examples of problems encountered in the field of IoT security, and methods developed by DJV-COM to solve them.

Seven levels of data protection:

At the level of access via the Internet - the database. For administrators, operators and users, a password with rights distribution at the object level. Implementation of the "cloud service" with the lack of direct access to data. The whole service is implemented on the basis of the API interface.

At the access level, the concentrator - the database. Two levels of protection - the first concentrator goes to a pre-defined IP, regardless of where the connection is initiated. The second level of protection is a private SSL connection protocol on the IP connection.

At the level of the radio module - the concentrator. Networks are divided into logical addresses, not knowing which it is impossible to realize the data exchange in the radio network. Additionally, a digital signature is used. The customer has the opportunity to change the logical address of the network.

At the level of the radio module - the metering device. Using a pulse output to remove information from the meter **does not allow you to fundamentally "hack" the meter** - to change the readings or disrupt the functioning of the meter. Additionally, the connection is monitored for integrity - open and short.

At the radio module level - there is basically no command for changing the accumulated data on the radio module. Accumulation of data is carried out by analogy with a mechanical reading device - only towards accumulation. There are no instructions for resetting the counter or changing it.

At the database level. Duplication, backup and data validation.

At the level of Analytics. Monitoring of the maximum flow rate for an hour and a day, control of the uniformity of data growth, control of the lack of data. In addition, control of the uniqueness of network addresses of radio modules and duplication of data packets.

Consider the option of spoofing devices. The main attack is as follows: the enemy creates a device that simulates the hardware in the IoT network and uses its newly created device to feed false data into the IoT network.

If there is no such device on the network, it falls into the UNKNOWN section and the operator or network administrator must determine where this device belongs.

If this device is unknown to the operator, it will remain in the UNKNOWN section.

If this device is known to the network, it controls the uniqueness of network addresses of radio modules and duplicates of data packets, hence the system will give an error - duplication of devices. Additionally, each device has a binding to its concentrator, i.e. you can not send a packet from another concentrator - the system will alert the administrator.