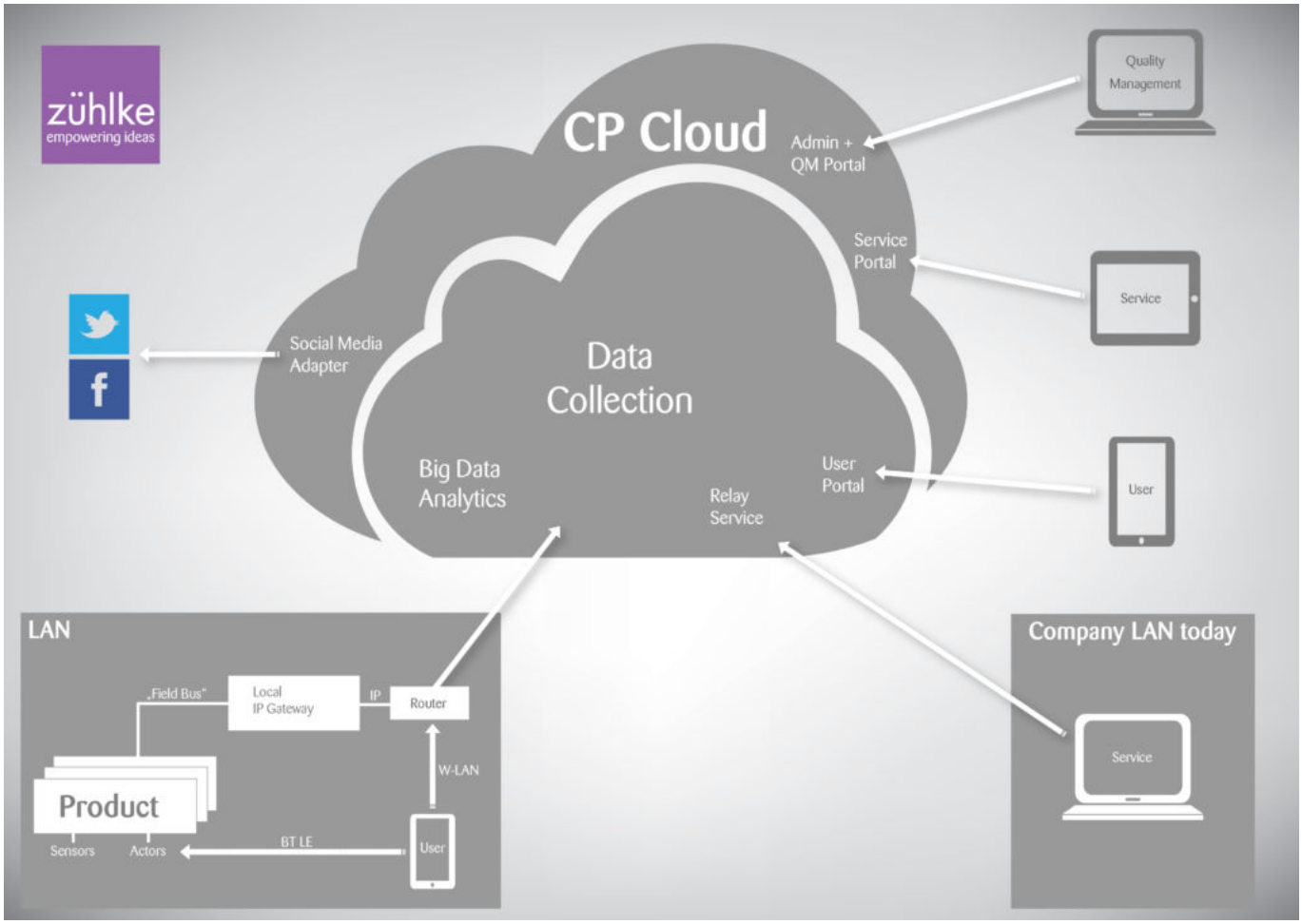
SSL isn’t enough for Internet of Things

25 June 2014 | **Internet of Things, Internet of Things Articles** | **Christian Heger**
Reading time: 4 minutes

For most applications of the Internet, Transport Layer Security is considered the gold standard for security. For a majority of users, a web site that runs over HTTPS is safe – and in the World Wide Web, it most likely is: there is direct interaction between a user (via a browser) and a server system. The user needs to implicitly trust the server, as it processes all data and operations displayed in the browser anyway.

Even for basic Internet of Things applications, this assumption is no longer sufficient. Looking at two very different simple scenarios, the need to consider the system from end to end becomes visible.

Basic architecture



Typical IoT-Architecture, Zühlke

The system we’re looking at consists of a simple temperature sensor. It sends a

measurement every five seconds via Bluetooth. A gateway device is connected to the Internet via LAN. It captures the measurement from this and a set of other wireless sensors to a cloud service. A user connects to the cloud service with a tablet.

For more details why this architecture makes a lot of sense, this blog post provides some solid background.

Scenario: Prevent Tampering

Prevent Tampering

In this scenario, the temperature sensor is part of a wearable medical device that sends vital data to a hospital. The data does not contain any information that might identify the patient, so the confidentiality of the data is not critical. The system does not need to provide security against unauthorized parties trying to read messages.

However, the hospital needs to have a reliable history of the patient's vital data. They need to be absolutely sure that the incoming messages have been sent from the correct sensors so that a physicist can make decisions based on the data.

In order to fulfill these requirements, the sensor signs each message it sends to the gateway with a key that has been assigned to it during productions. The gateway device can read the message in order to create local alarm messages. Before it sends the sensor message to the cloud service, it signs the message with its own key so the message's way can be traced.

The cloud service stores the sensor messages until they are downloaded into an archiving system. It also processes them in order to provide the physicist with reports about the patient's health, and raises alarms when critical situations occur. In order to do this, the cloud service needs to access the message content. The digital signatures on the messages allow verification that the data is authentic.

If the connection between the gateway and the cloud service uses transport layer security, it does not hurt – but there is no benefit either. It does not solve the problem of proving the authenticity of the data.

Scenario: Ensure Privacy

Ensure Privacy

In this scenario, the temperature sensor is part of a home automation solution. It records the room temperature in the living room. It sends data to a gateway device that controls the heating system. The tenants can view the temperature on a smart phone app.

While this is convenient, they are concerned that burglars could gain access to the home automation data and glean at which times there's no one at home. They do not trust the cloud solution: the cloud provider company is known to use data to build up precise profiles on user's behavior, which would be useful for planning housebreaking.

For the connection between sensor and gateway, there are no specific requirements. However, there needs to be end-to-end encryption between the gateway and the client application. The cloud service can queue messages, but it does not know their content. The client application decrypts the messages, aggregates and visualizes the data.

Transport layer security between the gateway and the cloud, or between the cloud and the mobile device, would not solve the security requirements of the solution.

Don't rely on SSL

To be clear: if it is possible to use transport layer security, it should be used. An additional layer of protection does not harm, and mechanisms like PFS are helpful in case that parts of the system get compromised.

However, the communication patterns in Internet of Things applications are different from the standard pattern of a World Wide Web application. The transport layer may or may not provide a solution for the individual security requirements. In any case, the end-to-end scenario needs to be considered.