The secrets of Schneider Electric's UMAS protocol

Authors

- Expert Kaspersky ICS CERT

UMAS (Unified Messaging Application Services) is a proprietary Schneider Electric (SE) protocol used to configure and monitor Schneider Electric PLCs. Schneider Electric controllers that use UMAS include Modicon M580 CPU (part numbers BMEP* and BMEH*) and Modicon M340 CPU (part numbers BMXP34*). Controllers are configured and programmed using engineering software – EcoStruxure™ Control Expert (Unity Pro), EcoStruxure™ Process Expert, etc.

In 2020, CVE-2020-28212, a vulnerability affecting this software, was reported, which could be exploited by a remote unauthorized attacker to gain control of a PLC with the privileges of an operator already authenticated on the controller. To address the vulnerability, Schneider Electric developed a new mechanism, Application Password, which should provide protection against unauthorized access to PLCs and unwanted modifications.

An analysis conducted by Kaspersky ICS CERT experts has shown that the implementation of the new security mechanism also has flaws. The CVE-2021-22779 vulnerability, identified in the course of the research, could allow a remote attacker to make changes to the PLC, bypassing authentication.

It was established that the UMAS protocol, in its implementation prior to the version in which the CVE-2021-22779 vulnerability was fixed, had significant shortcomings that had a critical effect on the security of control systems based on SE controllers.

By mid-August 2022, Schneider Electric had released an update for the EcoStruxure™ Control Expert software, as well as for Modicon M340 and Modicon M580 PLC firmware, that fixes the vulnerability.

This report describes:

- the implementation of the UMAS protocol that does not use the Application Password security mechanism;
- authentication bypass if Application Password is not enabled;
- the principles on which the Application Password security mechanism is based;
- mechanisms that can be used to exploit the CVE-2021-22779 vulnerability (authentication bypass where Application Password is configured);
- operating principles of the updated device reservation mechanism.

A detailed report on the research, Schneider Electric measures designed to fix the authentication bypass vulnerability, and Kaspersky ICS CERT recommendations can be found in the full version of the article published on the Kaspersky ICS CERT website.

Object of research

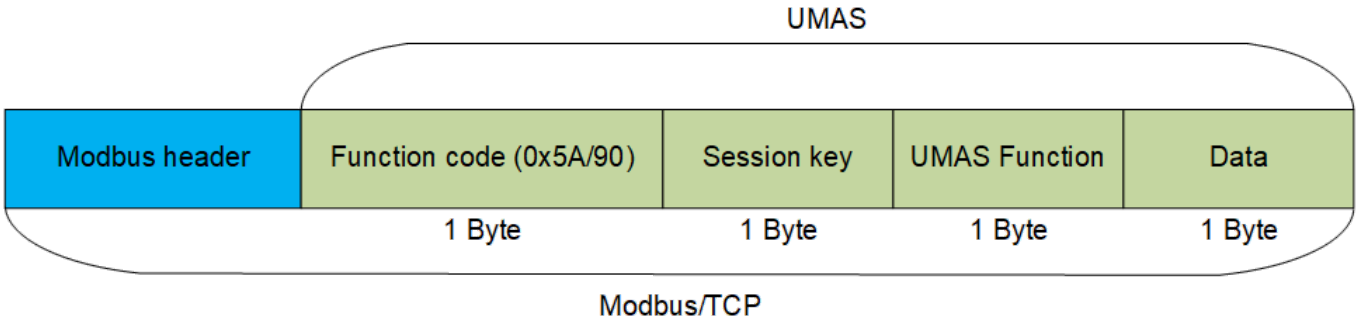
UMAS (Unified Messaging Application Services) is Schneider Electric's proprietary protocol used to configure, monitor, collect data and control Schneider Electric industrial controllers.

UMAS is based on a client-server architecture. During the research process, we used the EcoStruxure™ Control Expert PLC configuration software as the client part and a Modicon M340 CPU controller as the server part.

UMAS protocol

Network packet structure

UMAS is based on the Modbus/TCP protocol.



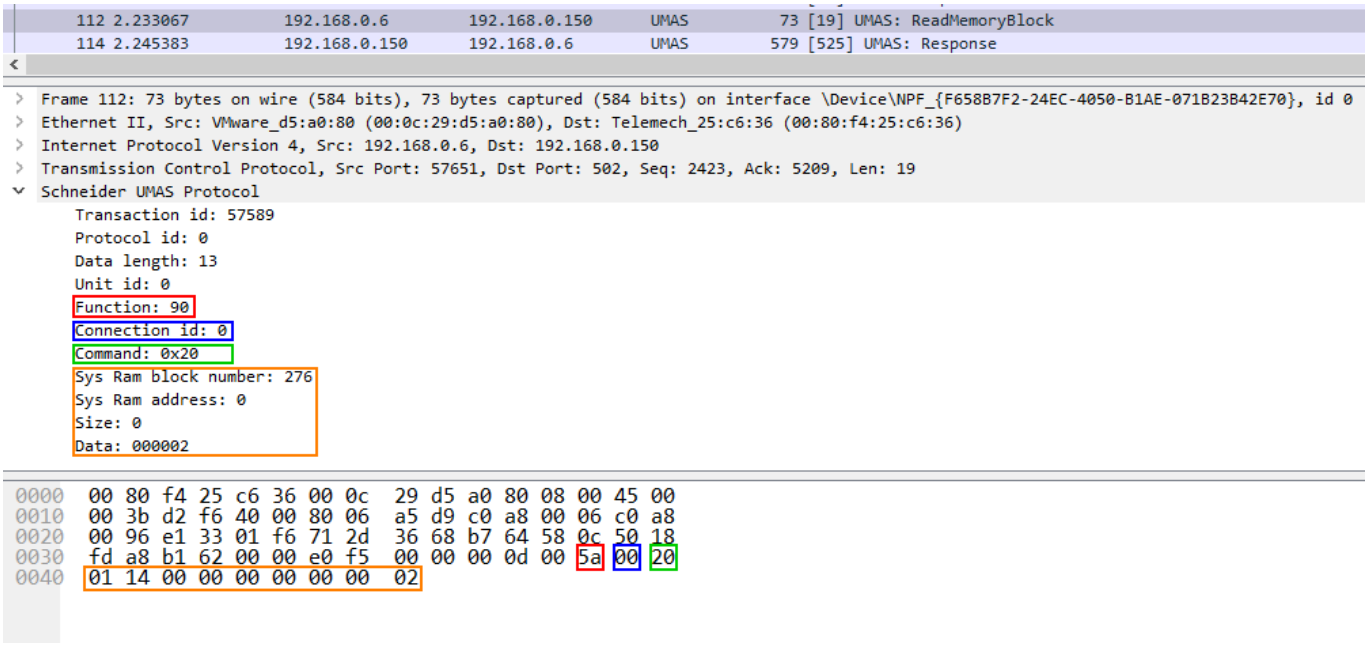
Structure of the UMAS protocol

Specifications of the Modbus/TCP protocol include reserved Function Code values that developers can use according to their needs. A complete list of reserved values can be found in the official documentation.

Schneider Electric uses Function Code 90 (0x5A) to define that the value in the Data field is UMAS compliant.

The network packet structure is shown below, using a request to read a memory block (pu_ReadMemoryBlock) on the PLC as an example:

- Red: Function Code 90 (0x5A)
- Blue: Session Key 0 (0x00)
- Green: UMAS Function 20 (0x20)
- Orange: Data

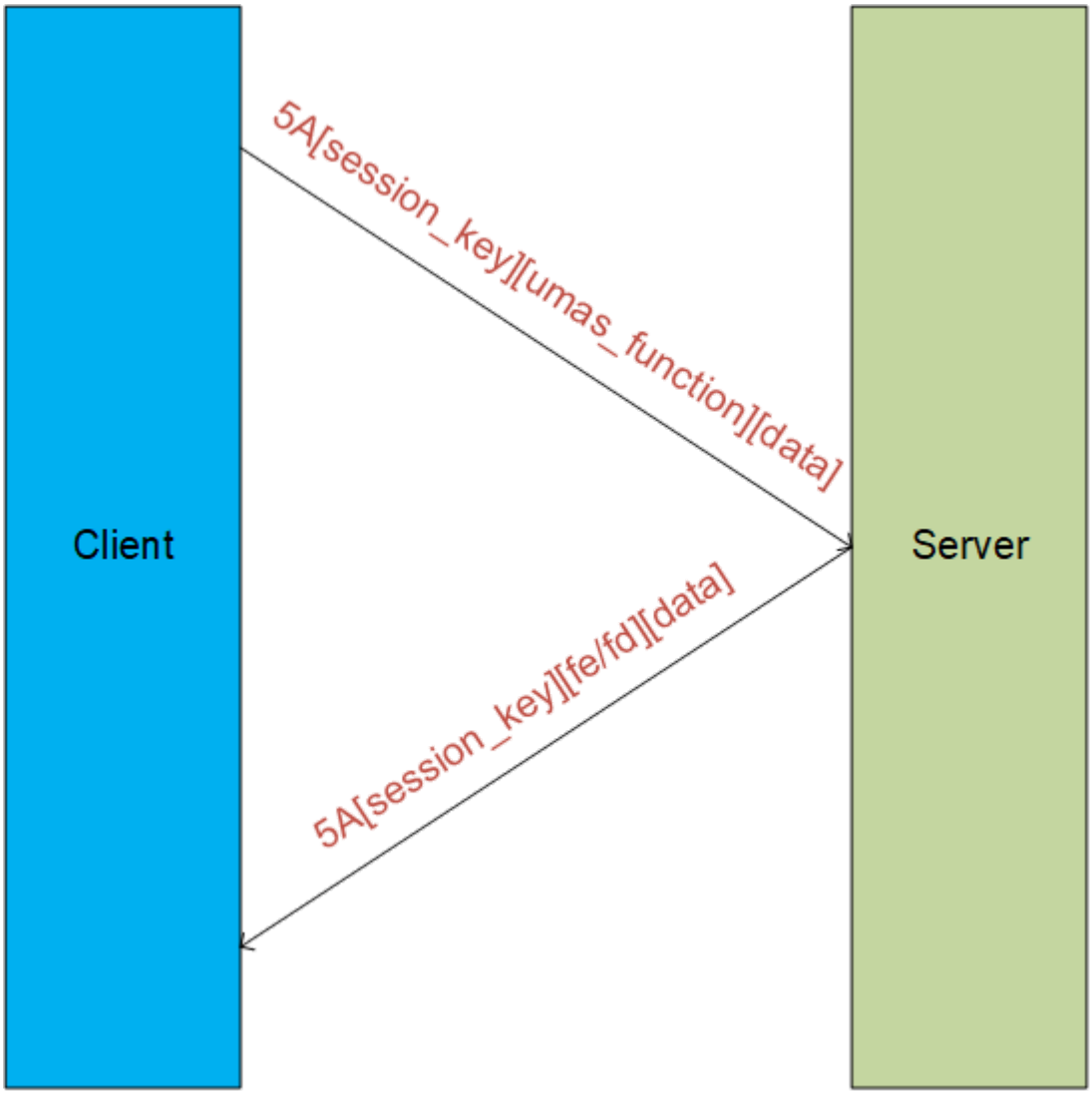


Network packet structure

Each function includes a certain set of information in the Data field, such as offset from the base memory address, size of the data sent, memory block number, etc. For more details on the functions and session key, see the full version of the article.

Network communication

UMAS also inherits the Modbus client-server architecture. A structural diagram of the communication between the client and the server is provided below.



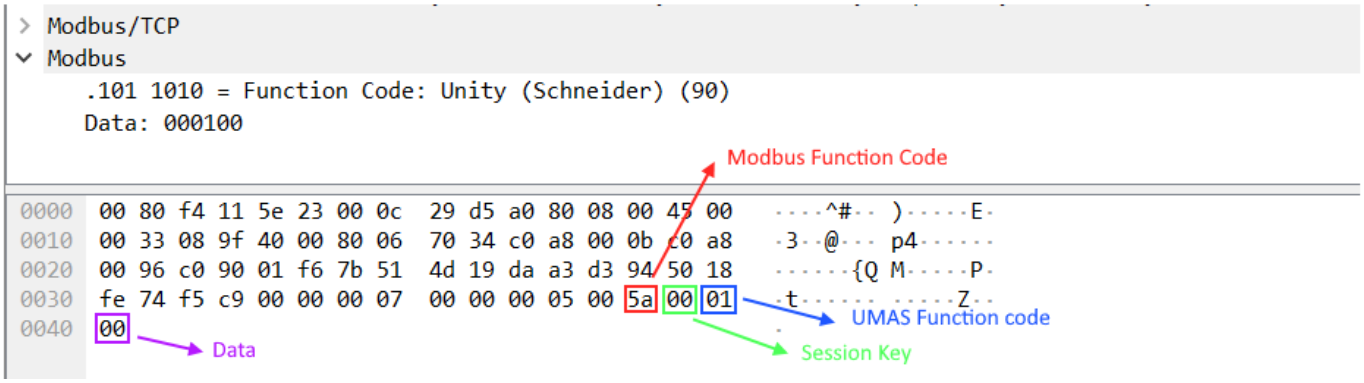
Communication between the client (EcoStruxure™ Control Expert) and server (PLC)

In a UMAS network packet, Function Code 0x5A is immediately followed by the Session Key.

UMAS network packet structure

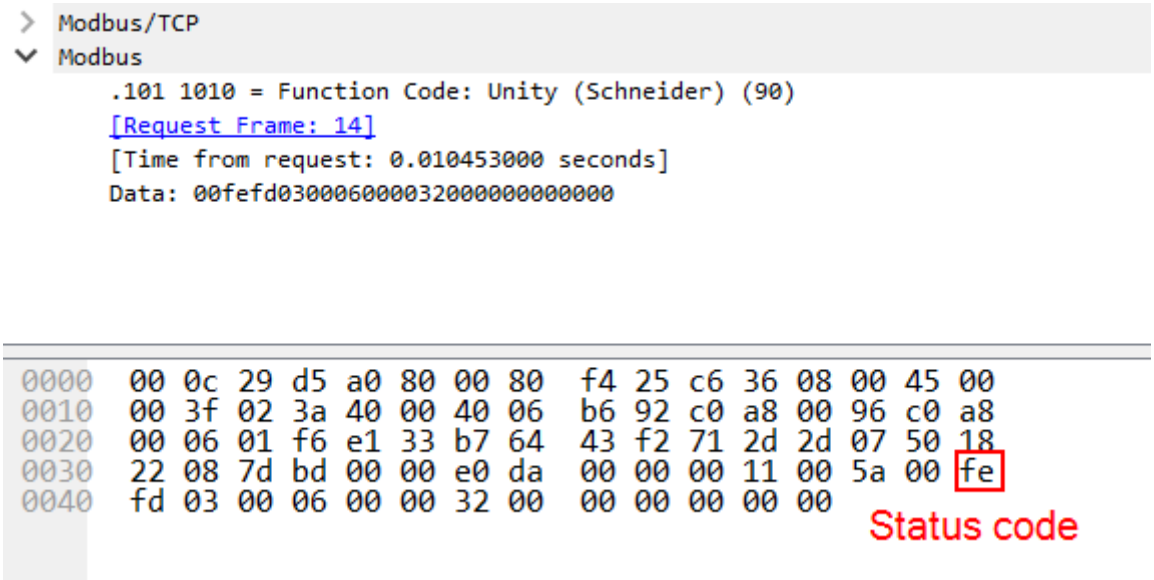
Let's examine the communication between a client and a server (a PLC, also referred to as "device" below) by analyzing a real-world traffic fragment. The screenshot below shows a packet containing the function **umas_QueryGetComInfo(0x01)** sent from the client (EcoStruxure™ Control Expert) to the server (the PLC).

Structure of the function:
TCP DATA – Modbus Header – 0x5A – session – 01(UMAS function code) – 00(data).



Network packet containing the function umas_QueryGetComInfo(0x01)

The device should send a response to each request received. The screenshot below shows the device's response to the client's request:



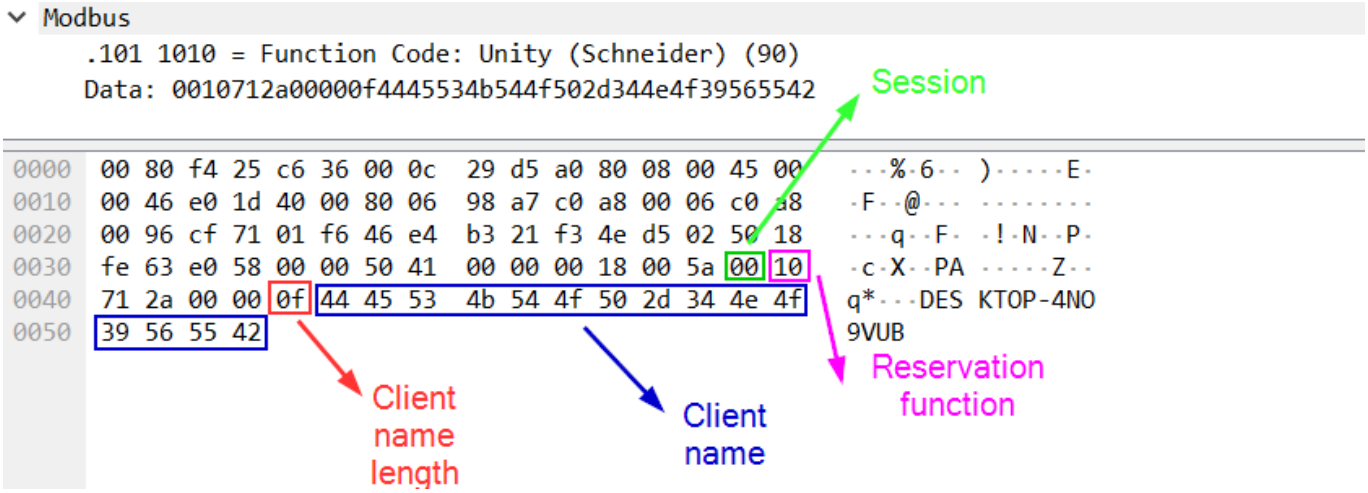
Server response

The status code is the status of the device's execution of the function sent to it by the client in the previous request. The value "fe" corresponds to successful execution of the function; "fd" indicates an error. The status code is present in each response sent by the device to thecontaining a function. It is always located immediately after the session key.

Reservation procedure

A "reservation" procedure is required to make changes to a PLC. The procedure acts as authentication. Only one client (e.g., an engineering workstation) can reserve a device at any specific time for configuration or status monitoring. This is required to prevent changes from being made to a device in parallel without coordination.

The screenshot below shows a request from the engineering software to the PLC to perform the device reservation procedure in its basic variant that does not use the Application Password security mechanism.



Device reservation

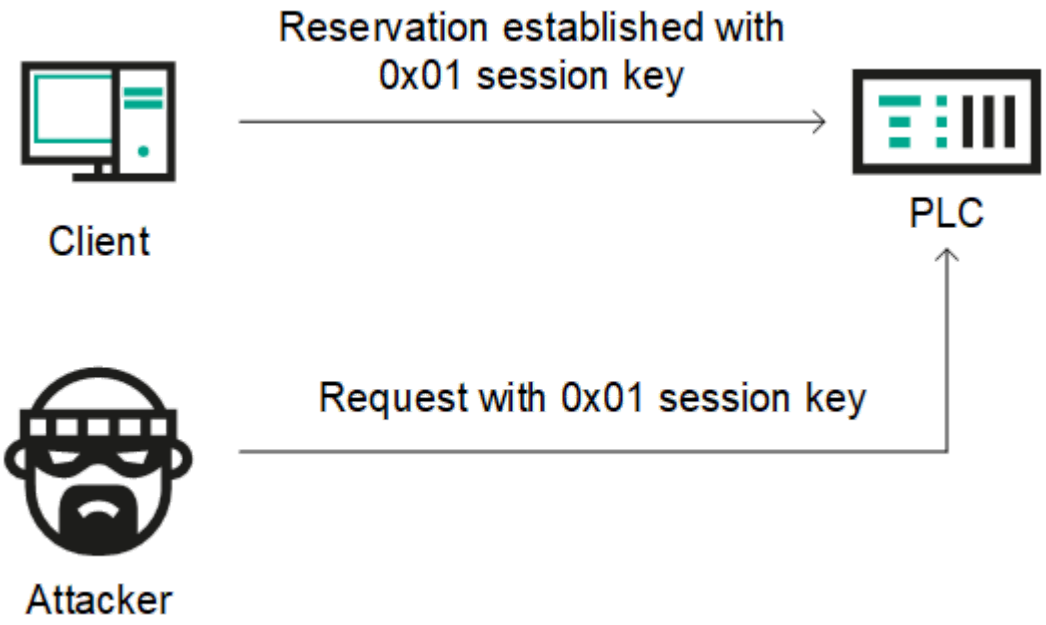
The **umas_QueryTakePLCReservation(0x10)** function is used to reserve a device. The request containing this function includes the name of the client reserving the device and a value equal to the length of that name.

CVE-2020-28212: authentication bypass without Application Password

The main issue with the basic reservation mechanism that does not use Application Password is that an attacker can use the session key to send requests and change the device's configuration.

In firmware versions prior to 2.7 for Modicon M340 devices, the session key has the same value each time the device is reserved, and is equal to "0x01". This means that attackers can make changes on the device by calling the relevant functions after the device has been reserved by a legitimate user.

The attack workflow is shown in the diagram below:



Remote threat actor attack workflow. Modicon M340 firmware prior to version 2.7, device reserved by an engineer

If the device has not been reserved at the time of an attack, the attacker can use the **umas_QueryTakePLCReservation(0x10)** function to reserve the device in order to make changes to it.

With Modicon M340 firmware version 2.7 or later, the session key takes a random value after device reservation. However, the session key is one byte in length, which means there are only 256 possible session ID values. This enables a remote unauthorized attacker to brute-force an existing ID of a session between a legitimate user and the PLC.

To carry out this type of attack, a remote attacker needs to send a series of network requests on port 502/TCP of the PLC with different session ID values and look at responses returned by the PLC. If the correct session ID was sent, the attacker will get the status code 0xfe, which means the request was fulfilled successfully. Otherwise, the attacker will get the status code 0xfd.

The operations described above can be implemented using any programming language – an attacker does not have to use EcoStruxure™ Control Expert or any other dedicated software to communicate with the device.

Application Password

To mitigate the CVE-2020-28212 vulnerability, exploitation of which could allow a remote unauthorized attacker to gain control of the PLC with the privileges of an operator already authenticated on the PLC, Schneider Electric developed a new security mechanism that used cryptographic algorithms to compute the session ID and increased the session ID length. Schneider Electric believed implementing this security mechanism would prevent brute-force attacks that could be used to crack single-byte session IDs.

The new mechanism was introduced starting with firmware version 3.01 for Modicon M340 devices. To implement authentication between the client and the device, Application Password needs to be enabled in project settings (“Project & Controller Protection”). The mechanism is designed to provide protection against unauthorized access, unwanted changes, as well as unauthorized downloading or uploading of PLC strategies.

After activating the mechanism using EcoStruxure™ Control Expert, the client needs to enter the password when connecting to a device as part of the reservation procedure. Application Password also makes changes to the reservation mechanism itself.

An analysis conducted by Kaspersky ICS CERT experts has shown that the implementation of the new security mechanism was, unfortunately, also flawed. Its main shortcoming is that during the authentication process, all computations are performed on the client side, i.e., on the side of EcoStruxure™ Control Expert engineering software. The vulnerability identified during research, CVE-2021-22779, could allow a remote attacker to bypass authentication and use functions that require reservation to make changes to the PLC.

For more details on the implementation of Application Password and on the security flaws identified by Kaspersky ICS CERT researchers, read the full version of the article published on the Kaspersky ICS CERT website. For more information, you can also contact us at ics-cert@kaspersky.com.