

MODBUS/TCP

MODBUS Over Transmission Control Protocol

- Very Common Protocol for Connecting Industrial Electronic Devices Over IP Networks
- Encapsulates Fieldbus Packets Inside TCP/IP Data Packets
- Mu-4000 Identifies Vulnerabilities in MODBUS/TCP Implementations

Where is MODBUS/TCP Used?

MODBUS/TCP is an open protocol used by most I/O makers for communicating with industrial devices such as remote terminal units (RTUs) in supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs). MODBUS protocol packets are transmitted inside TCP/IP data packets. MODBUS protocol is a derivative of the MODBUS serial communications protocol published by Modicon in 1979 – now a *de facto* standard and a very common way to connect industrial intelligent electronic devices (IEDs).

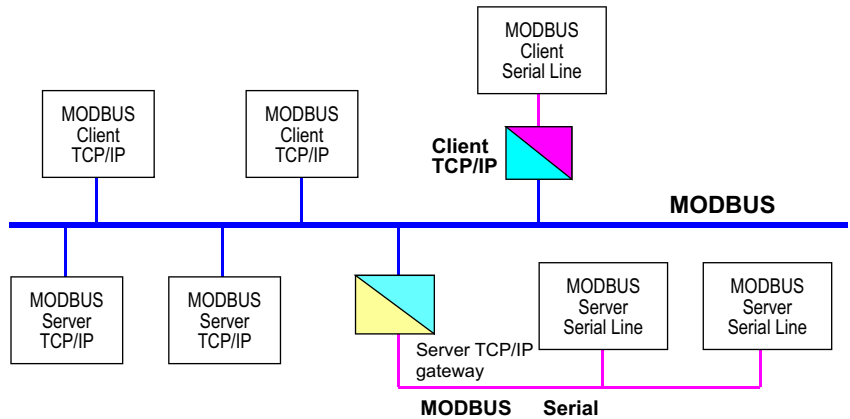


Figure-1: MODBUS/TCP COMMUNICATION ARCHITECTURE
 Source: http://www.modbus.org/docs/MODBUS_Messaging_Implementation_Guide_V1_0b.pdf

MODBUS/TCP supports the increasingly prevalent use of Ethernet in Manufacturing Execution Systems (MES), Digital Control Systems (DCS) and SCADA systems because it allows implementers to replace or augment data limits, node limitations, and distance limitations of older serial bus-type architectures. Use of MODBUS/TCP also eliminates the need to use a gateway to get to the internal network (see Fig. 1), and makes it easier to integrate other devices such as security appliances, smart cards and bar code scanners. Connectivity to the IP-based business

network also allows remote control of devices without having to issue commands from the control room. Despite the convenience, the extension of the control perimeter outside the control room should not be undertaken without extremely careful consideration.

Mu-4000 Identifies MODBUS/TCP Vulnerabilities

The prevalence of devices supporting MODBUS presents an exponentially dangerous volume of potential attack vectors and failure modes. Even if devices use serial-based MODBUS, gateways to implementations using MODBUS/TCP create exposure for MODBUS hardware: modems; sensors; RTUs; PLCs; I/O interfaces; AC/DC drive controllers; software such as device drivers, HMI and SCADA applications; and many other devices. By utilizing MODBUS/TCP attack suites, the Mu-4000 analyzer enables organizations to test for and expose dormant vulnerabilities in MODBUS implementations used by any directly attached or gateway-attached device. Mutation libraries in the attack suites are designed according to the MODBUS/TCP specification and include techniques such as truncated messages, overflow injections, out-of-range register addresses, and string-based mutations. By using the Mu-4000 to attack likely (or unlikely!) points of vulnerability in MODBUS/TCP implementations, developers and operators of critical infrastructure can reliably assess the security and safety of command-and-control systems for industrial electronic devices.

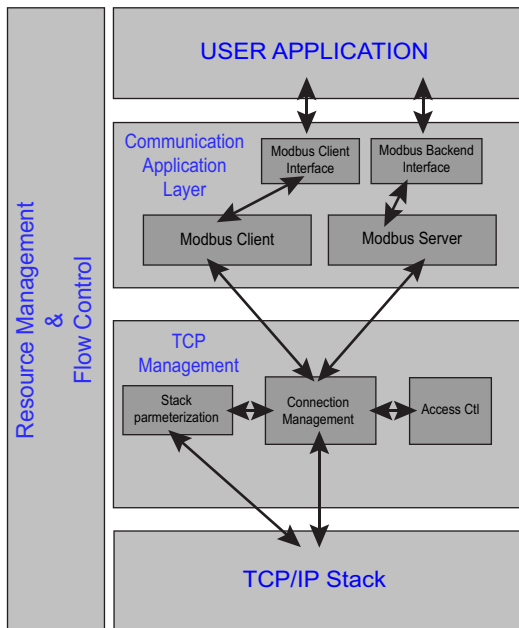


Figure-2: MODBUS/TCP MESSAGING SERVICE CONCEPTUAL ARCHITECTURE
 Source: http://www.modbus.org/docs/MODBUS_Messaging_Implementation_Guide_V1_0b.pdf

MODBUS/TCP Primer

MODBUS is an application layer protocol for client/server communication between devices on different types of buses or networks. The protocol's messaging services provide real-time information exchange between two device applications, device application to another device, HMI/SCADA applications and devices, or a PC and a device program providing on-line services. MODBUS is a variant of the MODBUS RTU protocol and is accessed on port 502 on the TCP/IP stack. It is a request/reply protocol providing services specified by function codes.

The protocol defines a simple Protocol Data Unit (PDU) that is independent of underlying communication layers. Clients initiating a

transaction build a MODBUS Application Data Unit (ADU); a function code tells the server what kind of application to perform. The protocol uses binary encoding of data and the TCP/IP error detection mechanism for finding transmission errors. (The TCP checksum is a very weak checksum and it is easy for errors to be undetected.) Because it is a connection-oriented protocol, a TCP/IP time-out or protocol failure will cause the master to close and re-open the connection, and then repeat the message. MODBUS registers start their numbering sequence from 1, which is different from common C programming logic that addresses the first array reference or index as 0. MODBUS presents another programming variation by starting at 1 to address the most significant bit in a 16-bit word. Conventional logic addresses the first reference as 0 and the least significant bit is 0. For more information about MODBUS/TCP, see the "MODBUS Application Protocol Specification V1.1a" at www.modbus.org/docs/MODBUS_Application_Protocol_V1_1a.pdf and the "MODBUS Messaging on TCP/IP Implementation Guide V1.0b" at www.modbus.org/docs/MODBUS_Messaging_Implementation_Guide_V1_0b.pdf.

About the Mu-4000 Analyzer

The Mu-4000 analyzer is a security analysis platform that delivers the industry's first systematic and repeatable process to identify unknown and published vulnerabilities in any IP-based system, application or network device without requiring access to source code. The process, known as "mutate, monitor and manage," easily integrates with existing security controls. The Mu-4000 subjects the target under analysis to a virtually unlimited number of attack vectors (the "mutations"). It monitors the target and captures results in a database while managing the process in a reproducible and actionable manner. Results include detailed reports and utilities to speed fault remediation. This lifecycle approach enables the creation of security-enabled processes in all phases of product development and deployment. The extensible security analysis platform also enables organizations to integrate their own suites of attacks. The Mu-4000 analyzer is a self-contained, 2U rack-mountable appliance that is easily configured, operated and managed.

POTENTIAL MODBUS/TCP WEAK SPOTS

Requires a unique numbering sequence for addressing that is different from conventional programming logic.
Connection-oriented stateful protocol is vulnerable to out-of-order or unexpected packets.
Implementations using TLS for security are exposed to additional weaknesses such as fragmentation and illegal nesting of TLVs.

BENEFITS OF MU-4000

A suite of attacks targets the ability of MODBUS/TCP implementations to resist out-of-range read or write requests.
Extensive mutation library sends valid protocol packets out-of-order and in the wrong state to look for implementation side effects including crashes or increased latency.
Rich set of TLS mutations ensure that MODBUS/TCP is carried safely over either IPv4 or IPv6 transport.

Table-1.

OTHER PROTOCOLS SUPPORTED BY THE MU-4000 (partial list)

ARP	IPv6	SNMP
BGP4	ISAKMP	SNMP Traps
CDP	LDAP	SSL-TLS
DHCP	MGCP	SSDP
DNP	MODBUS	SSH
FTP	PIM-DM	Sun RPC
HTTP	PIM-SM	TCP
ICMP	POP3	TFTP
IGMP	RADIUS	TLSv1
IMAP	RTSP	UDP
IPv4	SIP	

Table-2.



web: www.mudynamics.com | email: info@mudynamics.com
 address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317