Integrating the Modbus SCADA Communication Protocol with Elliptic Curve Cryptography

Authors : Despoina Chochtoula, Aristidis Ilias, Yannis Stamatiou

Abstract : Modbus is a protocol that enables the communication among devices which are connected to the same network. This protocol is, often, deployed in connecting sensor and monitoring units to central supervisory servers in Supervisory Control and Data Acquisition, or SCADA, systems. These systems monitor critical infrastructures, such as factories, power generation stations, nuclear power reactors etc. in order to detect malfunctions and ignite alerts and corrective actions. However, due to their criticality, SCADA systems are vulnerable to attacks that range from simple eavesdropping on operation parameters, exchanged messages, and valuable infrastructure information to malicious modification of vital infrastructure data towards infliction of damage. Thus, the SCADA research community has been active over strengthening SCADA systems with suitable data protection mechanisms based, to a large extend, on cryptographic methods for data encryption, device authentication, and message integrity protection. However, due to the limited computation power of many SCADA sensor and embedded devices, the usual public key cryptographic methods are not appropriate due to their high computational requirements. As an alternative, Elliptic Curve Cryptography has been proposed, which requires smaller key sizes and, thus, less demanding cryptographic operations. Until now, however, no such implementation has been proposed in the SCADA literature, to the best of our knowledge. In order to fill this gap, our methodology was focused on integrating Modbus, a frequently used SCADA communication protocol, with Elliptic Curve based cryptography and develop a server/client application to demonstrate the proof of concept. For the implementation we deployed two C language libraries, which were suitably modify in order to be successfully integrated: libmodbus (https://github.com/stephane/libmodbus) and ecc-lib https://www.ceid.upatras.gr/webpages/faculty/zaro/software/ecc-lib/). The first library provides a C implementation of the Modbus/TCP protocol while the second one offers the functionality to develop cryptographic protocols based on Elliptic Curve Cryptography. These two libraries were combined, after suitable modifications and enhancements, in order to give a modified version of the Modbus/TCP protocol focusing on the security of the data exchanged among the devices and the supervisory servers. The mechanisms we implemented include key generation, key exchange/sharing, message authentication, data integrity check, and encryption/decryption of data. The key generation and key exchange protocols were implemented with the use of Elliptic Curve Cryptography primitives. The keys established by each device are saved in their local memory and are retained during the whole communication session and are used in encrypting and decrypting exchanged messages as well as certifying entities and the integrity of the messages. Finally, the modified library was compiled for the Android environment in order to run the server application as an Android app. The client program runs on a regular computer. The communication between these two entities is an example of the successful establishment of an Elliptic Curve Cryptography based, secure Modbus wireless communication session between a portable device acting as a supervisor station and a monitoring computer. Our first performance measurements are, also, very promising and demonstrate the feasibility of embedding Elliptic Curve Cryptography into SCADA systems, filling in a gap in the relevant scientific literature.

Keywords : elliptic curve cryptography, ICT security, modbus protocol, SCADA, TCP/IP protocol
Conference Title : ICSEDS 2017 : International Conference on Software Encryption and Data Security
Conference Location : Amsterdam, Netherlands
Conference Dates : August 07-08, 2017