A SECURED FIRMWARE UPDATE PROCEDURE TO PREVENT CROSS CHANNEL SCRIPTING ATTACK IN EMBEDDED DEVICES

M. KAMESWARAO[1] & P. BHAVYA SREE[2]

[1]Associate Professor, Department of Electronics & Computer Engineering, K. L. University, Vaddeswaram, Guntur, Andhra Pradesh, India

[2]Department of Electronics & Computer Engineering, K. L. University, Vaddeswaram, Guntur, Andhra Pradesh, India

ABSTRACT

Many embedded systems are complex, and it is often required that the firmware updates in these systems will become necessary due to bug fixes, improved functions, extensions, and parameter changes. For confidentiality it is important that these systems only accept firmware approved by the firmware producer. In this work we propose a framework that only accepts approved firmware and protects against unauthorized or vulnerable firmware updates in embedded systems. In this work the secured framework for web interface of embedded devices defines a protocol for data exchange between web interface and the firmware repository and verifies the authentication of firmware update using data authentication code.

KEYWORDS: Data Authentication Code, Cross Channel Scripting Attack, Firmware Update, Embedded Devices