Vulnerability analysis of Z-wave products used in Korea

WYP[1*]

[1*] *Best of the Best 7th (Ki-Yun Cho, Ji-Hwan Lim, Min-Seok Sung, Young-Ho Jung, Seong-Beom Kim)*

Abstract

This presentation focuses on vulnerabilities of products that use the Z-Wave wireless communication protocol which has the advantage of good usability, scalbility, and low power protocol. The presentation will mainly be divided into two parts: the first part introduces the related research and trends of Z-Wave and presents the results of the directly analyzed Z-Wave products from the viewpoint of security. The second part demonstrates the process of controlling commercial products through arbitrarily created packets using the Z-Wave spoofing tool that we created. First, the necessary information is sniffed through sniffing, and then the malicious control packet created based on the information that the attacker took is used to control the product.

We will demonstrate attacks on several major products, including K company's and L company's smart door locks which are equipped with K company's Z-Wave communication modules on S company's products, which are gas lockers and IoT door openers. It also introduces and demonstrates various attack vectors, which include DoS attacks and Replay attacks.

Althoguh this demonstration is based on the specific products from these companies, the vulnerability and attack can generally be applied to all the products that use z-Wave protocol.

Keywords: Z-Wave, Protocol, Spoofing, Sniffing, Attack Vector

*Corresponding author
Email address: whatisyourprotocol@gmail.com (WYP[1])