USB as an Attack Platform

Aaron S. DeVera

November 18th, 2014

CISC 3580 Cyber Security and Applications

Professor Kevin Kelly, Fordham University

Abstract

A team of engineers from Germany-based Security Research Labs (SRLabs) submitted a presentation dubbed BadUSB at Blackhat 2014 Security Conference, along with an abstract which supposedly demonstrated the fatal flaws in the USB architecture that exposes many USB devices a means of an attack platform. In this paper, I will evaluate the legitimate and practical concerns in the usage of USB devices under the consideration of BadUSB-modeled attacks. I will specifically report on the viability of BadUSB as a means of probable attack, and compare it with other documented and popular USB attacks.

Executive Summary

The "BadUSB" vulnerability in USB devices is not an exploit that is patchable by means of software. It is rather a framework or guideline in which an actor may follow in order to alter the very nature of a USB device's design. BadUSB-modeled attacks target the USB microcontroller, which is a powerful enough processor to mount attacks that can steal data or cripple machine systems. A BadUSB-modeled attacks can only be currently implemented on a limited amount of microcontroller chips. BadUSB-modeled attacks are not convenient to a malicious actor in many attack scenarios. BadUSB-modeled attacks will do the most damage in environments where physical security considerations are not as strict as remote attack vectors over digital networks. This makes workplaces and

shared spaces the most susceptible environments for a BadUSB-modeled attacks, due to the popular usage of local data transport by means of USB peripherals.

References

1. Greenberg, Andy. "Why the Security of USB Is Fundamentally Broken | WIRED." Wired. July 29, 14. Accessed November 7, 2014. http://www.wired.com/2014/07/usb-security/.
2. Nohl, Karsten. "BadUSB - On Accessories that Turn Evil by Karsten Nohl + Jakob Lell." Lecture, Blackhat 2014 Security Conference from SRLabs, Las Vegas, Nevada, August 7, 2014.
3. Caudill, Adam, and Brandon Wilson. "Phison 2251-03 (2303) Custom Firmware & Existing Firmware Patches (BadUSB)." GitHub. September 26, 2014. Accessed November 7, 2014. https://github.com/adamcaudill/Psychson.
4. Caudill, Adam and Brandon Wilson. "Making BadUSB Work for You" Lecture, DerbyCon 4.0 Security Conference, Louisville, Kentucky, September 26th, 2014.
5. "Endpoint Protector 4." Device Control, Data Loss Prevention, MDM. Enterprise Solutions. Accessed November 15, 2014. http://www.endpointprotector.com/products/endpoint_protector.

