Keynote Talk: BadUSB-C: Revisiting BadUSB with Type-C

Fengwei Zhang
zhangfw@sustech.edu.cn
Department of Computer Science and Engineering
Research Institute of Trustworthy Autonomous Systems
Southern University of Science and Technology
Shenzhen, China 518055

ABSTRACT

The security of the USB protocol has been paid extensive attention to because of its wide usage. Due to the *trust-by-default* characteristics, USB security has caused severe problems. In this work, we extended BadUSB to support the new USB Type-C features and proposed a multi-mode attack model, BadUSB-C. This obtains UI status to make attacks more precise and effective. To the best of our knowledge, BadUSB-C is the first attack model utilizing USB Type-C. To validate the usability and effectiveness, we conducted extensive experiments to simulate daily usage and summarized the private information collected. We also discussed the recommended countermeasures for our attack model, including isolated UI rendering, which may be inspiring for future research on defense methods. This paper describes the journey of discovering BadUSB-C in my CS315 Computer Security course taught in the Fall 2020 semester.

ACM Reference Format:
Fengwei Zhang. 2021. Keynote Talk: BadUSB-C: Revisiting BadUSB with Type-C. In *Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems (ASSS '21), June 7, 2021, Virtual Event, Hong Kong*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3457340.3458299

1 INTRODUCTION

The USB protocol has become popular worldwide since its appearance in 1996, as it provides a unified and easy-to-use approach for an extensive range of devices to communicate with each other. From version 1.0 till now, USB specification has evolved rapidly and offered more and more functionalities. Nowadays, devices with USB support are ubiquitous.

Conversely, the security of USB has caused severe problems. Recent research of all USB specifications indicates that security has not been taken into consideration [11]. There are more than 400 vulnerabilities related to USB on CVE list [1]. As a result, many attackers exploit these vulnerabilities and the *trust-by-default* characteristics of USB to conduct attacks, which puts the privacy and financial security of USB users in danger [11].

We implemented a multi-mode attack model of USB, named BadUSB-C. BadUSB-C extends BadUSB [10] to support the features of USB Type-C. Although smartphones equipped with USB-C connectors do not support USB 3.x protocol, such as products of Xiaomi, however, vendors like HUAWEI and Samsung tend to support USB 3.x protocol in their high-end smartphones [3]. Since USB Type-C can transfer video stream data, BadUSB-C could obtain the information of the victim's GUI during attacks. Combining it with the emulation of traditional HID, e.g., keyboards and mice, attackers are capable of performing precise attacks.

This paper is an extension of our previous paper entitled "BadUSB-C: Revisiting BadUSB with Type-C" at WOOT 2021 [9], which was accomplished by five undergraduate students (Hongyi Lu, Yechang Wu, Shuqing Li, You Lin, and Chaozu Zhang) as their course project in my CS315 Computer Security course in the Fall 2020 semester. The purpose of this paper is to share my teaching experience while working with these undergraduate students on this BadUSB-C attack. Furthermore, I would like to point out that good teaching and research may be achieved together.

The rest of this paper is structured as follows. Section 2 provides a brief introduction of my CS315 Computer Security Course at Southern University of Science and Technology. Section 3 introduces BadUSB-C. Section 4 states the final thoughts of my mentoring experience.

2 PROJECT MOTIVATION

CS315 Computer Security course [12, 13] is a selective course for junior undergraduate students (third-year) at Department of Computer Science at Southern University of Science and Technology. This course aims help students to learn the principles of computer security and understand how various security attacks and countermeasures work. It provides hands-on experience in playing with security software and network systems in a live laboratory environment, with the purpose of understating real-world threats. The course will take both offensive and defense methods to help student explore security tools and attacks in practice. It will focus on attacks (e.g., buffer overflow, dirty COW, format-string, XSS, and return oriented programming), hacking fundamentals (e.g., scanning and reconnaissance), defenses (e.g., intrusion detection systems and firewalls). Students are expected to finish intensive lab assignments that use real-world malware, exploits, and defenses. This course offers an in depth experience of real-world threats and defenses. Upon successful completion of this class, the student will gain experience in: (1) Understanding on real-world security vulnerabilities, exploits and defenses; (2) Having hands-on labs in network and system security experiments; (3) Learning knowledge of practical security problems and their solutions.

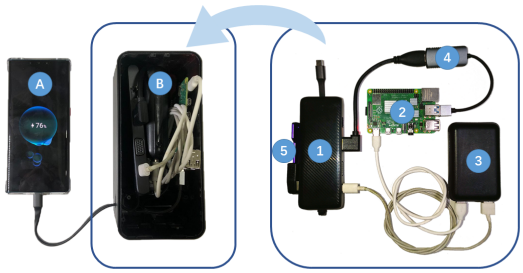
Course Project: The grades for the course are based upon the Table 1. Note that this course requires a term project as part of the grade. The term project aims to be a mini research project with 2-5

ASSS '21, June 7, 2021, Virtual Event, Hong Kong.

ACM ISBN 978-1-4503-8403-2/21/06.
https://doi.org/10.1145/3457340.3458299

Table 1: CS315 Computer Security Course Grades

Topics	Grade
Class Participation	80
Lab 1: Packet Sniffing and Wireshark	60
Lab 2: Secure Coding and Buffer Overflows	60
Lab 3: Secure Coding and Format-String Vulnerability	60
Lab 4: Scanning, Reconnaissance, and Penetration Testing	60
Lab 5: Reverse Engineering and Obfuscation	60
Lab 7: Firewalls and Intrusion Detection Systems (IDS)	60
Lab 8: Heartbleed Attack Lab	60
Lab 9: Dirty COW Attack	60
Lab 10: RSA Public-Key Encryption and Signature	60
Lab 11: Web Security	60
Lab 12: Return-to-libc & Return Oriented Programming	60
Term Project Proposal	50
Term Project Presentation	50
Term Project Report	50
Total	1000



A Victim's Device
1 USB 3.x Hub
3 Auxiliary Power Bank
5 ATMEGAA32U4 Board
B BadUSB-C
2 Raspberry Pi 4B
4 Video Capture

Figure 1: BadUSB-C Prototype.

individuals. The project types include (1) building a new system, (2) improving/re-showing an existing technique/attack, and (3) performing a large case study. The term project has three stages during the semester: proposal, presentation, and report. The BadUSB-C work [9] is a term project in my CS315 Computer Security course in Fall 2020 [13], which was led by five undergraduate students.

3 BADUSB-C

In BadUSB-C, we utilize the new features of USB 3.x [2, 6] to launch attacks. Benefiting from the latest protocol, we simulate an external display and thus obtain the video stream to perform accurate attacks. As there were various BadUSB implementations available, this work focuses on new extensions. Next, we briefly introduce the components we used in BadUSB-C.

our BadUSB-C only requires common components that are easy to access online or in any electronic store. Here we chose the following parts to build a prototype. To begin with, we chose the Raspberry Pi 4B [4] as the embedded Single Board Computer inside BadUSB-C, which is powerful enough to process video data and has an onboard WiFi chip. As for the HID Emulator, we used an Atmel ATMEGA32U4 board [7] with USB protocol support, which is able to emulate multiple HID with our modified firmware. About the USB 3.x Hub, we used one from UGREEN [8], which supports HDMI, USB 2.0, and many other exported peripherals. Apart from these essential parts, we also used an auxiliary power bank to provide power for the Raspberry Pi and the mobile devices used by the victim. The image of our BadUSB-C prototype can be found in Figure 1.

A is a HUAWEI mobile phone, the victim's device; B is a compact look of BadUSB-C prototype; 1 is the USB 3.x Hub; 2 is a Raspberry Pi 4B as the Single Board Computer; 3 is an auxiliary power bank; 4 is the Video Capture Card; 5 is an Atmel ATMEGA32U4 board as the HID Emulator.

Leveraging the new features of USB 3.x [2, 5, 6], we explore a new attack scheme named BadUSB-C and three attack modes. To our best knowledge, this is the first work to utilize new features of USB Type-C. The combination of new support with conventional BadUSB makes attacks more precise and effective, such as interacting with the user interface and controlling the consequences of their attacks. In summary, BADUSB-C can be applied in various application scenarios and brings rather huge impact. See our full paper [9] for more details.

4 FINAL THOUGHTS

This paper presents an experience report of mentoring a course project entitled "BadUSB-C: Revisiting BadUSB with Type-C" in my CS315 Computer Security course at Southern University of Science and Technology, which was published at WOOT 2021 [9]. Teaching, Research, and Services are the three components of our academia job. In particular, as a junior faculty, Teaching and Research would cost most of our time. In the mentoring experience of this BadUSB-C course project, I am very humbled and glad to obtain credits from both Teaching and Research. Additionally, I would like to draw attention to the academia community that Teaching and Research are not parallel but rendezvous at some points.

REFERENCES

[1] Common vulnerabilities and exposures, 2020.
[2] I. M. R. S. Apple, Hewlett-Packard and T. Instruments. Universal serial bus 3.2 specification, 2017.
[3] EverybodyWiki. List of devices with video output over usb-c, 2021.
[4] R. P. Foundation. Raspberry pi 4B, 2019.
[5] I. HP et al. Universal serial bus 3.0 specification, 2008.
[6] I. HP et al. Universal serial bus 3.1 specification, 2013.
[7] M. T. Incorporated. ATmega32u4 chip, 2016.
[8] U. G. Limited. UGREEN company introduction, 2012.
[9] H. Lu, Y. Wu, S. Li, Y. Lin, C. Zhang, and F. Zhang. BadUSB-C: Revisiting BadUSB with Type-C. In *15th IEEE Workshop on Offensive Technologies, WOOT*, 2021.
[10] K. Nohl and J. Lell. Badusb-on accessories that turn evil. *Black Hat USA*, 1(9):1–22, 2014.
[11] J. D. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates, and K. R. B. Butler. Sok: "plug & pray" today - understanding USB insecurity in versions 1 through C. In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*, pages 1032–1047. IEEE Computer Society, 2018.
[12] F. Zhang. Fall 2019 Semester: CS315 Computer Security. https://fengweiz.github.io/19fa-cs315/index.html, 2019.
[13] F. Zhang. Fall 2020 Semester: CS315 Computer Security. https://fengweiz.github.io/20fa-cs315/index.html, 2020.

BIOGRAPHY

Dr. Fengwei Zhang is the Director of the COMPASS (COMPuter And Systems Security) Lab and Associate Professor at the Department of Computer Science and Engineering at Southern University of Science and Technology (SUSTech), China. He came to SUSTech from Wayne State University, USA, where he was an Assistant Professor at Department of Computer Science from 2015 to 2019. He received his Ph.D. degree in computer science from George Mason University in 2015.

His research interests are in the areas of systems security, with a focus on trustworthy execution, hardware-assisted security, transparent malware debugging, transportation security, and plausible deniability encryption. He published over 50 conferences/journal papers, including IEEE S&P, USENIX Security, NDSS, IEEE TIFS, and IEEE TDSC. He has served as Program Committee at top conferences including IEEE S&P, ACM CCS, and USENIX Security. He is a recipient of the Distinguished Paper Award in ACSAC 2017 and Runner-up Best Paper Award in IEEE/IFIP DSN 2020. His high-quality work received several NSF Awards in the USA. More information can be found at his homepage: https://fengweiz.github.io/.